Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2025-03-25

Generated by Acunetix

Scan of securityscans.qa.granicus.com

Scan details

Scan information	
Start time	2025-03-18T04:26:01.080349-05:00
Start url	https://securityscans.qa.granicus.com/apps/peakagenda/
Host	securityscans.qa.granicus.com
Scan time	2880 minutes, 18 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Application build	25.3.250305133

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	63
Critical	0
High	2
Medium	29
Low	15
Informational	17

Alerts summary

Cross-site Scripting

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-79

Affected items	Variation
/boards/superadmin/people/	1

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H Base Score: 7.2 Attack Vector: Network Attack Complexity: Low Privileges Required: High User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: High
CWE	CWE-94
CVE	CVE-2021-23358

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification

CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2018-14040

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2018-20677

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2024-6484

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707

CVE	CVE-2018-14042

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2018-20676

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2019-8331

Affected items	Variation
Web Server	1

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2016-10735

Affected items	Variation
Web Server	1

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2015-9251

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2020-11023

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2020-23064

Affected items	Variation
Web Server	1

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2020-11022

Affected items	Variation
Web Server	1

jQuery Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-1321

CVE	CVE-2019-11358

Affected items	Variation
Web Server	1

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2022-31160

Affected items	Variation
Web Server	1

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2021-41183

Affected items	Variation
Web Server	1

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2021-41182

Affected items	Variation
Web Server	1

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2021-41184

Affected items	Variation
Web Server	1

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2022-31160

Affected items	Variation
Web Server	1

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2021-41184

Affected items	Variation
Web Server	1

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707

CVE	CVE-2021-41183

Affected items	Variation
Web Server	1

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N Base Score: 6.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-707
CVE	CVE-2021-41182

Affected items	Variation
Web Server	1

Open Redirection

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-601

Affected items	Variation
/DeleteFolder.php	1
/DeleteView.php	1

TLS/SSL Weak Cipher Suites

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 3.3 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310

Affected items	Variation
Web Server	1

Vulnerable JavaScript libraries

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None

CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-937

Affected items	Variation
Web Server	5

[Possible] Internal IP Address Disclosure

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

Clickjacking: CSP frame-ancestors missing

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 5.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Cookies Not Marked as HttpOnly

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1004

Affected items	Variation
Web Server	1

Cookies Not Marked as Secure

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 2.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score: 3.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 2.6 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-614

Affected items	Variation
Web Server	1

Cookies with missing, inconsistent or contradictory properties

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Insecure Frame (External)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L Base Score: 1.8 Attack Vector: Network Attack Complexity: High Privileges Required: High User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: Low Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: Low
CVSS3	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:L Base Score: 5.1 Attack Vector: Network Attack Complexity: High Privileges Required: High User Interaction: Required Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: Low

CVSS2	Base Score: 4.6 Access Vector: Network_accessible Access Complexity: High Authentication: Single Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-829

Affected items	Variation
/Reports.php	1

Programming Error Messages

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-209

Affected items	Variation
Web Server	1

Ruby on Rails CookieStore session cookie persistence

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Proof_of_concept Remediation Level: Workaround Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Sensitive pages could be cached

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

Session cookies scoped to parent domain

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-284

Affected items	Variation
Web Server	1

Session ID in URL

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	2

Symfony debug mode enabled

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: Low Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
/api/metrics/cspreport	1
/profile/process	1
/services/permissions/	1

[Possible] Internal Path Disclosure (*nix)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

[Possible] Internal Path Disclosure (Windows)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

An Unsafe Content Security Policy (CSP) Directive in Use

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

data: Used in a Content Security Policy (CSP) Directive

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

default-src Used in Content Security Policy (CSP)

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

Generic Email Address Disclosure

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

Outdated JavaScript libraries

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: High Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-937

Affected items	Variation
Web Server	7

Permissions-Policy header not implemented

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation
Web Server	1

Scheme URI Detected in Content Security Policy (CSP) Directive

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

Subresource Integrity (SRI) Not Implemented

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: Low Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-830

Affected items	Variation
Web Server	1

TLS/SSL (EC)DHE Key Reuse

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 2.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None

CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score: 3.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 1.9 Access Vector: Local_access Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-310

Affected items	Variation
Web Server	1

Alerts details

Cross-site Scripting

Severity	**High**
Reported by module	/Scripts/PerScheme/XSS.script

Description

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

References

Cross-site Scripting (XSS) Attack - Acunetix (https://www.acunetix.com/websitesecurity/cross-site-scripting/)
Types of XSS - Acunetix (https://www.acunetix.com/websitesecurity/xss/)
XSS Filter Evasion Cheat Sheet (https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
Excess XSS, a comprehensive tutorial on cross-site scripting (https://excess-xss.com/)
Cross site scripting (https://en.wikipedia.org/wiki/Cross-site_scripting)

Affected items

/boards/superadmin/people/
Details
URL encoded GET input **search[search_text]** was set to **the</script><script>XQ3N(9389)</script>** The input is reflected inside a <script> tag between double quotes.
Request headers

```
GET /boards/superadmin/people/?
search[search_text]=%74%68%65%3C%2F%73%63%72%69%70%74%3E%3C%73%63%72%69%70%74%3E%58%51%33%4E%28%39%33%38%39%29%3C%2F%
73%63%72%69%70%74%3E HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Cookie:
PHPSESSID=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
jAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=c55b033e98bd93b583ce3653696ed20f;
_gat=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMD
c6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TlRSbVlUTTROV0ppT0RSaE5ETm1aamxoWWpWaU5UaGtNMkUzWVdNd1l6VXViRHdkVzd0ZDlhZHFJOXhUVHhDUmlQbmthbWt6UTdjUlY0Q1I3V2pW
bFpWUDdFWVNUelRkMWVWbHd2clM;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%
2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0

x-csrf-token: MCErtFoG3a3h3UrA1wIdzmCpcs3FyjBqH0xxQQrL+2D/HLjQUTmBsMLxIPJOCacXHnGe9kNCYO+hc25SBS0QtQ==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

Severity	**High**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

Impact

Recommendation

References

CVE-2021-23358 (https://nvd.nist.gov/vuln/detail/CVE-2021-23358)
CVE-2021-23358 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23358)

Affected items

Web Server
Details
underscore.js v1.5.2-1.5.2
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

Impact

Recommendation

References

CVE-2018-14040 (https://nvd.nist.gov/vuln/detail/CVE-2018-14040)
CVE-2018-14040 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14040)

Affected items

Web Server
Details
bootstrap.js v3.2.0-3.2.0
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.

Impact

Recommendation

References

CVE-2018-20677 (https://nvd.nist.gov/vuln/detail/CVE-2018-20677)
CVE-2018-20677 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20677)

Affected items

Web Server
Details
bootstrap.js v3.2.0-3.2.0
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

A vulnerability has been identified in Bootstrap that exposes users to Cross-Site Scripting (XSS) attacks. The issue is present in the carousel component, where the data-slide and data-slide-to attributes can be exploited through the href attribute of an <a> tag due to inadequate sanitization. This vulnerability could potentially enable attackers to execute arbitrary JavaScript within the victim's browser.

Impact

Recommendation

References

CVE-2024-6484 (https://nvd.nist.gov/vuln/detail/CVE-2024-6484)
CVE-2024-6484 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6484)

Affected items

Web Server
Details
bootstrap.js v3.2.0-3.2.0
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Impact

Recommendation

References

CVE-2018-14042 (https://nvd.nist.gov/vuln/detail/CVE-2018-14042)
CVE-2018-14042 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14042)

Affected items

Web Server
Details
bootstrap.js v3.2.0-3.2.0
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.

Impact

Recommendation

References

CVE-2018-20676 (https://nvd.nist.gov/vuln/detail/CVE-2018-20676)
CVE-2018-20676 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20676)

Affected items

Web Server
Details

bootstrap.js v3.2.0-3.2.0
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.

Impact

Recommendation

References

CVE-2019-8331 (https://nvd.nist.gov/vuln/detail/CVE-2019-8331)
CVE-2019-8331 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8331)

Affected items

Web Server
Details
bootstrap.js v3.2.0-3.2.0
Request headers

Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Impact

Recommendation

References

CVE-2016-10735 (https://nvd.nist.gov/vuln/detail/CVE-2016-10735)
CVE-2016-10735 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10735)

Affected items

Web Server
Details
bootstrap.js v3.2.0-3.2.0
Request headers

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Severity	**Medium**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org (https://hstspreload.org/)
Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server

Details

URLs where HSTS is not enabled:

- https://securityscans.qa.granicus.com/account/login
- https://securityscans.qa.granicus.com/
- https://securityscans.qa.granicus.com/api/metrics/cspreport
- https://securityscans.qa.granicus.com/legistar/dashboard.json
- https://securityscans.qa.granicus.com/legistar
- https://securityscans.qa.granicus.com/boards/admin
- https://securityscans.qa.granicus.com/SearchResults.php
- https://securityscans.qa.granicus.com/check_expired
- https://securityscans.qa.granicus.com/JSON.php
- https://securityscans.qa.granicus.com/images/
- https://securityscans.qa.granicus.com/index
- https://securityscans.qa.granicus.com/index.php
- https://securityscans.qa.granicus.com/EditCameraBasic.php
- https://securityscans.qa.granicus.com/log
- https://securityscans.qa.granicus.com/Cameras.php
- https://securityscans.qa.granicus.com/log.php
- https://securityscans.qa.granicus.com/Archives.php
- https://securityscans.qa.granicus.com/Events.php
- https://securityscans.qa.granicus.com/Reports.php
- https://securityscans.qa.granicus.com/myaccount.php
- https://securityscans.qa.granicus.com/EditCameraDistribution.php

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Impact

Recommendation

References

CVE-2015-9251 (https://nvd.nist.gov/vuln/detail/CVE-2015-9251)
CVE-2015-9251 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9251)

Affected items

Web Server
Details
jquery v2.1.4-2.1.4
Request headers

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Impact

Recommendation

References

CVE-2020-11023 (https://nvd.nist.gov/vuln/detail/CVE-2020-11023)
CVE-2020-11023 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023)

Affected items

Web Server
Details
jquery v3.4.1-3.4.1
Request headers

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

Cross Site Scripting vulnerability in jQuery 2.2.0 through 3.x before 3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.

Impact

Recommendation

References

CVE-2020-23064 (https://nvd.nist.gov/vuln/detail/CVE-2020-23064)
CVE-2020-23064 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-23064)

Affected items

Web Server
Details
jquery v3.4.1-3.4.1
Request headers

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Impact

Recommendation

References

CVE-2020-11022 (https://nvd.nist.gov/vuln/detail/CVE-2020-11022)
CVE-2020-11022 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022)

Affected items

Web Server
Details
jquery v3.4.1-3.4.1
Request headers

jQuery Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') Vulnerability

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.

Impact

Recommendation

References

CVE-2019-11358 (https://nvd.nist.gov/vuln/detail/CVE-2019-11358)
CVE-2019-11358 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11358)

Affected items

Web Server
Details
jquery v2.1.4-2.1.4
Request headers

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio( "refresh" )` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.

Impact

Recommendation

References

CVE-2022-31160 (https://nvd.nist.gov/vuln/detail/CVE-2022-31160)
CVE-2022-31160 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160)

Affected items

Web Server
Details
jquery-ui-dialog v1.12.1-1.12.1
Request headers

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

Impact

Recommendation

References

CVE-2021-41183 (https://nvd.nist.gov/vuln/detail/CVE-2021-41183)
CVE-2021-41183 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183)

Affected items

Web Server
Details
jquery-ui-dialog v1.12.1-1.12.1
Request headers

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

Impact

Recommendation

References

CVE-2021-41182 (https://nvd.nist.gov/vuln/detail/CVE-2021-41182)
CVE-2021-41182 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41182)

Affected items

Web Server
Details
jquery-ui-dialog v1.12.1-1.12.1
Request headers

jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

Impact

Recommendation

References

CVE-2021-41184 (https://nvd.nist.gov/vuln/detail/CVE-2021-41184)
CVE-2021-41184 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184)

Affected items

Web Server
Details
jquery-ui-dialog v1.12.1-1.12.1
Request headers

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery UI is a curated set of user interface interactions, effects, widgets, and themes built on top of jQuery. Versions prior to 1.13.2 are potentially vulnerable to cross-site scripting. Initializing a checkboxradio widget on an input enclosed within a label makes that parent label contents considered as the input label. Calling `.checkboxradio( "refresh" )` on such a widget and the initial HTML contained encoded HTML entities will make them erroneously get decoded. This can lead to potentially executing JavaScript code. The bug has been patched in jQuery UI 1.13.2. To remediate the issue, someone who can change the initial HTML can wrap all the non-input contents of the `label` in a `span`.

Impact

Recommendation

References

CVE-2022-31160 (https://nvd.nist.gov/vuln/detail/CVE-2022-31160)
CVE-2022-31160 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160)

Affected items

Web Server
Details
jquery-ui-tooltip v1.12.1-1.12.1
Request headers

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

Impact

Recommendation

References

CVE-2021-41184 (https://nvd.nist.gov/vuln/detail/CVE-2021-41184)
CVE-2021-41184 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184)

Affected items

Web Server
Details
jquery-ui-tooltip v1.12.1-1.12.1
Request headers

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.

Impact

Recommendation

References

CVE-2021-41183 (https://nvd.nist.gov/vuln/detail/CVE-2021-41183)
CVE-2021-41183 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183)

Affected items

Web Server
Details
jquery-ui-tooltip v1.12.1-1.12.1
Request headers

jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

Impact

Recommendation

References

CVE-2021-41182 (https://nvd.nist.gov/vuln/detail/CVE-2021-41182)
CVE-2021-41182 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41182)

Affected items

Web Server
Details
jquery-ui-tooltip v1.12.1-1.12.1
Request headers

Open Redirection

Severity	**Medium**
Reported by module	/Scripts/PerScheme/Open_Redir.script

Description

This endpoint is possibly vulnerable to URL redirection attacks.

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact

A remote attacker can redirect users from your website to a specified URL. This problem may assist an attacker to conduct phishing attacks, trojan distribution, spammers.

Recommendation

Your script should properly sanitize user input.

References

Unvalidated Redirects and Forwards Cheat Sheet
(https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html)
Unvalidated redirects and forwards (https://www.invicti.com/learn/unvalidated-redirects-and-forwards/)

Affected items

/DeleteFolder.php

Details

URL encoded GET input **return-to** was set to **https://bxss.me/**

Request headers

```
GET /DeleteFolder.php?folder_id=1&return-to=https://bxss.me/ HTTP/1.1

Cookie: PHPSESSID=y8nWWFisH13cnod_7kXW7-
TadobXBULskGBgW5nSlwo.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDY6MjY6NDUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUNPQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMiLCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D; _boule_session=b3141a70f8e10b93f3d8f30e283b3855; _gat=y8nWWFisH13cnod_7kXW7-
TadobXBULskGBgW5nSlwo.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDY6MjY6NDUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TXpSa1kyRTJPV0pqTVdVMFpHWmpPREUwWmpVNFlUVmhOMlptWmprMk56RXVjZDhsUG1yL1IxTWNpUWhvaEdTbEpJRi94VGhHQmRxR0FCOUFCSmpMQ2x2ZVlobDFxcm5Zc0luc1dROEU;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0; request_method=POST

x-csrf-token: PRLAzg/6KC0SXjLZ+ORr2JXCg1Ec+fgr4Qvi/+CqZzsZm9HlqQqx2HmwEqJDdhUT8w46UQPEkQc5WUqstP02Ug==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

/DeleteView.php

Details

URL encoded GET input **return-to** was set to **//bxss.me/**

Request headers

```
GET /DeleteView.php?commit=1&return-to=//bxss.me/&view_id= HTTP/1.1

Cookie:
PHPSESSID=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUNPQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMiLCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=c55b033e98bd93b583ce3653696ed20f;
_gat=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TlRSbVlUTTROV0ppT0RSaE5ETm1aamxoWWpWaU5UaGtNMkUzWVdNd1l6VXViRHdkVzd0ZDlhZHFJOXhUVHhDUmlQbmthbWt6UTdjUlY0Q1I3V2pWbFpWUDdFWVNUelRkMWVWbHd2clM;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0

x-csrf-token: MCErtFoG3a3h3UrA1wIdzmCpcs3FyjBqH0xxQQrL+2D/HLjQUTmBsMLxIPJOCacXHnGe9kNCYO+hc25SBS0QtQ==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

TLS/SSL Weak Cipher Suites

Severity	**Medium**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The remote host supports TLS/SSL cipher suites with weak or insecure properties.

Impact

Recommendation

Reconfigure the affected application to avoid use of weak cipher suites.

References

OWASP: TLS Cipher String Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html)
OWASP: Transport Layer Protection Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)
Mozilla: TLS Cipher Suite Recommendations (https://wiki.mozilla.org/Security/Server_Side_TLS)
SSLlabs: SSL and TLS Deployment Best Practices (https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices)
RFC 9155: Deprecating MD5 and SHA-1 Signature Hashes in TLS 1.2 and DTLS 1.2 (https://datatracker.ietf.org/doc/html/rfc9155)

Affected items

Web Server
Details

Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 443):

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Request headers

Vulnerable JavaScript libraries

Severity	**Medium**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

References

How Invicti identifies Out-of-date technologies (https://www.invicti.com/support/how-invicti-identifies-outofdate/)

Affected items

Web Server

Details

- **jQuery 3.4.1**
  - URL: https://securityscans.qa.granicus.com/account/login
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request headers

```
GET /account/login?ReturnUrl=/apps/peakagenda/ HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Web Server

Details

- **jQuery 2.1.4**
  - URL: https://securityscans.qa.granicus.com/legistar
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET /legistar?
signed_request=tn_d8m2ytKp79GXbY6FiyZGrTNPjYTZJDRGX9U21atg.eyJpZCI6MjE1OTEsImVtYWlsIjoiZ292ZGFjdW5ldGl4QGdyYW5pY3VzLm
NvbSIsImNyZWF0ZWRfYXQiOiIyMDIyLTA4LTI2VDE1OjI2OjM2LjAwMFoiLCJ1cGRhdGVkX2F0IjoiMjAyNS0wMy0wNFQwOToxMDo0MC4wMDBaIiwidXV
pZCI6ImZlZmNlNjBlLWIwNmYtNDI2OC1hYjZhLTQ4NmM0ZDliMmYwYyIsInVzZXJuYW1lIjoic2VjdXJpdHlzY2FucyIsImZpcnN0X25hbWUiOiJlIiwi
bGFzdF9uYW1lIjoiZSIsIm1pZGRsZV9uYW1lIjoiZSIsImRlZmF1bHRfYXBwIjoiY2l2aWNpZGVhcyIsImJ1aWx0X2luIjpmYWxzZSwicGhvbmUiOiIiL
CJkZWxldGVkX2F0IjpudWxsLCJkb21haW5faWQiOjIwLCJhZG1pbiI6ZmFsc2UsImdyb3VwcyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZG
IyYjA1NDgiXSwidWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwibmFtZSI6ImUgZSIsImZpcnN0bmFtZSI6ImUiLCJsYXN
0bmFtZSI6ImUiLCJkb21haW4iOiJzZWN1cml0eXNjYW5zLnFhLmdyYW5pY3VzLmNvbSJ9 HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: iframe

cookie:
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6
TXFiSUN0UXFyajNXdnNKanlTcGo;
_gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMD
I6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
TkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Web Server

Details

- **jQuery 1.12.4**
  - URL: https://securityscans.qa.granicus.com/boards/admin
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023
  - Description: Possible Cross Site Scripting via third-party text/javascript responses (1.12.0-1.12.2 mitigation reverted) / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
  - References:
    - https://github.com/jquery/jquery/issues/2432
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

Request headers

```
GET /boards/admin?signed_request=5TdR8kLMWEmOQYPIbqujv-iWSNSw12wSFPHpFH3-
AQY.eyJpZCI6MjE1OTEsImVtYWlsIjoiZ292ZGFjdW5ldGl4QGdyYW5pY3VzLmNvbSIsImNyZWF0ZWRfYXQiOiIyMDIyLTA4LTI2VDE1OjI2OjM2LjAwM
FoiLCJ1cGRhdGVkX2F0IjoiMjAyNS0wMy0wNFQwOToxMDo0MC4wMDBaIiwidXVpZCI6ImZlZmNlNjBlLWIwNmYtNDI2OC1hYjZhLTQ4NmM0ZDliMmYwYy
IsInVzZXJuYW1lIjoic2VjdXJpdHlzY2FucyIsImZpcnN0X25hbWUiOiJlIiwibGFzdF9uYW1lIjoiZSIsIm1pZGRsZV9uYW1lIjoiZSIsImRlZmF1bHR
fYXBwIjoiY2l2aWNpZGVhcyIsImJ1aWx0X2luIjpmYWxzZSwicGhvbmUiOiIiLCJkZWxldGVkX2F0IjpudWxsLCJkb21haW5faWQiOjIwLCJhZG1pbiI6
ZmFsc2UsImdyb3VwcyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwidWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtN
Dg2YzRkOWIyZjBjIiwibmFtZSI6ImUgZSIsImZpcnN0bmFtZSI6ImUiLCJsYXN0bmFtZSI6ImUiLCJkb21haW4iOiJzZWN1cml0eXNjYW5zLnFhLmdyYW
5pY3VzLmNvbSJ9 HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: iframe

cookie:
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6
TXFiSUN0UXFyajNXdnNKanlTcGo;
_gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMD
I6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
TkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=6b8d5ad38657a7ef9c99010ab375f7a5

Referer: https://securityscans.qa.granicus.com/apps/boards

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Web Server

Details

- **jQuery UI 1.12.1**
  - URL: https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
  - CVE-ID: CVE-2021-41184
  - Description: XSS in the 'of' option of the '.position()' util
  - References:
    - https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/
    - https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327

Request headers

```
GET /core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197 HTTP/1.1

Cookie: _boule_session=c55b033e98bd93b583ce3653696ed20f; login_failed=0; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%
2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D;
_gus=TlRSbVlUTTROV0ppT0RSaE5ETm1aamxoWWpWaU5UaGtNMkUzWVdNd1l6VXViRHdkVzd0ZDlhZHFJOXhUVHhDUmlQbmthbWt6UTdjUlY0Q1I3V2pW
bFpWUDdFWVNUelRkMWVWbHd2clM;
_gat=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMD
c6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
jAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: MCErtFoG3a3h3UrA1wIdzmCpcs3FyjBqH0xxQQrL+2D/HLjQUTmBsMLxIPJOCacXHnGe9kNCYO+hc25SBS0QtQ==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Web Server

Details

- **jQuery 3.3.1**
  - URL: https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jquery_6dcf74cd635ac06a8b9efc7c0c711d7cf7a38110
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
  - CVE-ID: CVE-2020-11022, CVE-2020-11023, CVE-2019-11358
  - Description: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / jQuery mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/
    - https://www.cvedetails.com/cve/CVE-2020-11022/
    - https://github.com/advisories/GHSA-gxr4-xjj5-5px2
    - https://www.cvedetails.com/cve/CVE-2020-11023/
    - https://github.com/advisories/GHSA-jpcq-cgw6-v4j6
    - https://github.com/jquery/jquery/pull/4333
    - https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    - https://nvd.nist.gov/vuln/detail/CVE-2019-5428
    - https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/

Request headers

```
GET /core/_cassette/scriptbundle/Lib/jquery_6dcf74cd635ac06a8b9efc7c0c711d7cf7a38110 HTTP/1.1

Cookie: _boule_session=9fddb7190f29c1d0c7bcf0c15e24ac2d; login_failed=0; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC;
_hypatia_session=8Wl8BvLiwAYXVmdgCl8TpcrToGQCG3jJZ8E%2FvF3b7iOODSP7vk4r26qshNSruZlIMO7szRLdrbavL%2FyzBO8QwzZyObeyZGE%
2BiVZMdQIZjf4U%2BLi7VffZ%2FDsl6qQX8UUe%2BwF9VWK8j%2FJh%2FK9hg58%3D--QopIFx95ozN7%2BkTs--RdMuVsO3dmKcdehRYPjMoQ%3D%3D;
_gus=TXprME9XWTVNekJqWWpSbE16VTFNR1F6WldNek1HUTBOVEkzWkdJeU9UQXViMlpENFJ5dWh3ZE10MGNYOW1wZUxEdnNLWDQ5UnVWOHpvWkw4Q0pN
NFRQMWtHZWpzaWt2VWw1akk3cFk; _gat=Js5U2jedneGaY7YgPX4RoPhie-
P8Ly8jwsVm4niulb0.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9
tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRt
aW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMjI6MDQ6MTgiLCJncyI6WyIyOGM5NTM4Y
y1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; PHPSESSID=Js5U2jedneGaY7YgPX4RoPhie-
P8Ly8jwsVm4niulb0.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9
tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRt
aW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMjI6MDQ6MTgiLCJncyI6WyIyOGM5NTM4Y
y1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: t/H7KF2lWNwp9JukTnOLRrBK4GGS63cByxJ1XkXRHO8/xpZ+kB0QjrT6LCRBm5lThsCRzOizS53565Z63Y0iZg==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

[Possible] Internal IP Address Disclosure

Severity	**Low**
Reported by module	/target/404_text_search.js

Description

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Internal IP Address Disclosure | Invicti (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/internal-ip-address-disclosure/)

Affected items

Web Server

Details

Pages with internal IPs:

- https://securityscans.qa.granicus.com/
  10.3.53.25
- https://securityscans.qa.granicus.com/account/login
  10.3.53.26
- https://securityscans.qa.granicus.com/appstorev2/launch/boards/
  10.3.53.25
- https://securityscans.qa.granicus.com/appstorev2/launch/peakagenda/
  10.3.53.26
- https://securityscans.qa.granicus.com/api/installed_applications
  10.3.53.25
- https://securityscans.qa.granicus.com/account/login
  10.3.53.25
- https://securityscans.qa.granicus.com/
  10.3.53.26
- https://securityscans.qa.granicus.com/legistar/dashboard.json
  10.3.53.25
- https://securityscans.qa.granicus.com/legistar/dashboard.json
  10.3.53.26
- https://securityscans.qa.granicus.com/api/installed_applications
  10.3.53.26
- https://securityscans.qa.granicus.com/legistar
  10.3.53.25
- https://securityscans.qa.granicus.com/api/metrics/cspreport
  10.3.53.25
- https://securityscans.qa.granicus.com/SearchResults.php
  10.3.53.25
- https://securityscans.qa.granicus.com/SearchResults.php
  10.3.53.26
- https://securityscans.qa.granicus.com/check_expired
  10.3.53.26
- https://securityscans.qa.granicus.com/JSON.php
  10.3.53.25
- https://securityscans.qa.granicus.com/images/
  10.3.53.25
- https://securityscans.qa.granicus.com/index
  10.3.53.26
- https://securityscans.qa.granicus.com/index.php
  10.3.53.26
- https://securityscans.qa.granicus.com/EditCameraBasic.php
  10.3.53.26
- https://securityscans.qa.granicus.com/log
  10.3.53.25

Request headers

```
GET /apps/peakagenda/ HTTP/1.1

Cookie:
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6
TXFiSUN0UXFyajNXdnNKanlTcGo;
_gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMD
I6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
TkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: x8POei845lCDapb/OE9gE80DIxN7NHAPteWSIEuiYgbgVE1bK5iimFBZmUEIzu1m98sSMF3ZrFztaD+Vgn+0Zw==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Clickjacking: CSP frame-ancestors missing

Severity	**Low**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return a **frame-ancestors** directive in the Content-Security-Policy header which means that this website could be at risk of a clickjacking attack. The frame-ancestors directives can be used to indicate whether or not a browser should be allowed to render a page inside a frame. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include a CSP header with frame-ancestors directive and an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
CSP: frame-ancestors (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors)
The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

Affected items

Web Server
Details

Paths without CSP frame-ancestors:

- https://securityscans.qa.granicus.com/boards/admin
- https://securityscans.qa.granicus.com/boards/superadmin/people/
- https://securityscans.qa.granicus.com/boards/
- https://securityscans.qa.granicus.com/boards/admin/documents
- https://securityscans.qa.granicus.com/boards/admin/members

Request headers

```
GET /boards/admin HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Cookie: PHPSESSID=Oalux-
J2uVIWv2QAYB4Ja0Am697lgAqKPe5ZuF98HtA.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg
2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFt
ZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDI6Mjc6MTIiL
CJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=116f37e6db5ba32b8c9bc9a849d78ba9; _gat=Oalux-
J2uVIWv2QAYB4Ja0Am697lgAqKPe5ZuF98HtA.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg
2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFt
ZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDI6Mjc6MTIiL
CJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TVdWaE1XVm1NV1ZsTldJd1lqRXlZMlEwWVRVMVlUQmhPVEkzWVdRMU9UQXVQTFFQNC9KYWNSbS9ZRUdqem9PdHkra0JvYitKU05uS3pHbURDYjFK
dnRoS2t3dEpKUEdyZEYzOTZTMHI; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; login_failed=1

x-csrf-token: wqn2i+gQSpr2ugynj2cggzpCnlOJI3cFz0/4u4a2n+871FcjEns1KRjfOMcacwrak1xZd7/2169/vgu5IBh8JA==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Cookies Not Marked as HttpOnly

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

References

Cookie Not Marked as HttpOnly | Invicti (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/cookie-not-marked-as-httponly/)

Affected items

Web Server
Verified vulnerability
Details

Cookies without HttpOnly flag set:

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.qa.granicus.com
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=.qa.granicus.com
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.securityscans.qa.granicus.com
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=.securityscans.qa.gran
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: PHPSESSID=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: login_failed=1; path=/; expires=Tue, 18-Mar-2025 09:47:05 UTC
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmV
```

- https://securityscans.qa.granicus.com/boards/admin

```
Set-Cookie: granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c3863
```

- https://securityscans.qa.granicus.com/profile

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6InozazRjVXc2ZXF2VWJuWkIraTdxc3c9PSIsInZhbHVlIjoiUm9qNU9qbVQ4S2FpMU5JUGNTVEVjNkoyaD
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlZVVmtYUG1LRGVQMmMzQ2MvclVXY1E9PSIsInZhbHVlIjoiR3N0Nm9yRWZLbkk5ZFcvaUNId3hYZXdGVz
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkVhM2Q4elpqc3gzemxxVUVUa0JuaXc9PSIsInZhbHVlIjoiMkdlY1kwTjcxNUdid1JQRzB1UjVONnExcT
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6Ik1seGYzclJSclhzbVpVdnZ4WHZSbVE9PSIsInZhbHVlIjoiRXFIbUhrcWpJelBiSkFaSUwxVWpZNTU5VD
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6InljOTlqZjNabEZ4bjBrblpWS2hybHc9PSIsInZhbHVlIjoiWW5UOG11RStGME9yMVo1Z1VCYjk0R3Y1Qm
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: login_failed=1; path=/; expires=Tue, 18-Mar-2025 09:47:01 UTC
```

- https://securityscans.qa.granicus.com/appstorev2/storefront

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlU1QXJxU0IwZW55bFlqa1RVZFVsUmc9PSIsInZhbHVlIjoidkc1Qk9CdEZ0N3NObE9yS29oMGpZaWZFYU
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: login_failed=0; path=/; expires=Tue, 18-Mar-2025 11:19:37 UTC
```

- https://securityscans.qa.granicus.com/profile/

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUj
```

- https://securityscans.qa.granicus.com/account/forgotpassword

```
Set-Cookie: login_failed=0; path=/; expires=Tue, 18-Mar-2025 11:25:01 UTC
```

- https://securityscans.qa.granicus.com/boards/admin/members/reapply

```
Set-Cookie: request_method=POST; path=/
```

- https://securityscans.qa.granicus.com/boards/admin/boards/9883

```
Set-Cookie: request_method=PATCH; path=/
```

- https://securityscans.qa.granicus.com/boards/admin/boards/9883

```
Set-Cookie: request_method=; path=/; max-age=0; expires=Thu, 01 Jan 1970 00:00:00 GMT
```

- https://securityscans.qa.granicus.com/boards/admin/documents

```
Set-Cookie: request_method=POST; path=/
```

- https://securityscans.qa.granicus.com/boards/admin/members

```
Set-Cookie: request_method=; path=/; max-age=0; expires=Thu, 01 Jan 1970 00:00:00 GMT
```

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Cookies Not Marked as Secure

Severity	**Low**
Reported by module	/RPA/Cookie_Without_Secure.js

Description

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Recommendation

If possible, you should set the Secure flag for these cookies.

References

SameSite None Cookie Not Marked as Secure - Invicti (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/samesite-none-cookie-not-marked-as-secure/)

Affected items

Web Server
Verified vulnerability
Details

Cookies without Secure flag set:

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.qa.granicus.com
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=.qa.granicus.com
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.securityscans.qa.granicus.com
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=.securityscans.qa.gran
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: PHPSESSID=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gus=WldZd09ETTFObVV4TVRVeE1EVXpNekEzTjJaak1tTTJaamN6WkRZeU5ERXVLcHpiQzhqRGs2WDE4d1d1SUt6VVFkc05TNVdv
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNh
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: login_failed=1; path=/; expires=Tue, 18-Mar-2025 09:47:05 UTC
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmV
```

- https://securityscans.qa.granicus.com/boards/admin

```
Set-Cookie: granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c3863
```

- https://securityscans.qa.granicus.com/profile

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6InozazRjVXc2ZXF2VWJuWkIraTdxc3c9PSIsInZhbHVlIjoiUm9qNU9qbVQ4S2FpMU5JUGNTVEVjNkoyaD
```

- https://securityscans.qa.granicus.com/profile

```
Set-Cookie: laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; expires=Tue, 18-Mar-2025 12:53:20 GMT; Max-
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlZVVmtYUG1LRGVQMmMzQ2MvclVXY1E9PSIsInZhbHVlIjoiR3N0Nm9yRWZLbkk5ZFcvaUNId3hYZXdGVz
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; expires=Tue, 18-Mar-2025 12:55:06 GMT; Max-
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IkVhM2Q4elpqc3gzemxxVUVUa0JuaXc9PSIsInZhbHVlIjoiMkdlY1kwTjcxNUdid1JQRzB1UjVONnExcT
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; expires=Tue, 18-Mar-2025 12:55:10 GMT; Max-
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6Ik1seGYzclJSclhzbVpVdnZ4WHZSbVE9PSIsInZhbHVlIjoiRXFIbUhrcWpJelBiSkFaSUwxVWpZNTU5VD
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; expires=Tue, 18-Mar-2025 12:55:14 GMT; Max-
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6InljOTlqZjNabEZ4bjBrblpWS2hybHc9PSIsInZhbHVlIjoiWW5UOG11RStGME9yMVo1Z1VCYjk0R3Y1Qm
```

- https://securityscans.qa.granicus.com/profile/process

```
Set-Cookie: laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; expires=Tue, 18-Mar-2025 12:55:08 GMT; Max-
```

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: login_failed=1; path=/; expires=Tue, 18-Mar-2025 09:47:01 UTC
```

- https://securityscans.qa.granicus.com/appstorev2/storefront

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlU1QXJxU0IwZW55bFlqa1RVZFVsUmc9PSIsInZhbHVlIjoidkc1Qk9CdEZ0N3NObE9yS29oMGpZaWZFYU
```

- https://securityscans.qa.granicus.com/appstorev2/storefront

```
Set-Cookie: laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; expires=Tue, 18-Mar-2025 14:08:31 GMT; Max-
```

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Cookies with missing, inconsistent or contradictory properties

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
Securing cookies with cookie prefixes (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
Cookies: HTTP State Management Mechanism (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
SameSite Updates - The Chromium Projects (https://www.chromium.org/updates/same-site)
draft-west-first-party-cookies-07: Same-site Cookies (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server
Verified vulnerability
Details

List of cookies with missing, inconsistent or contradictory properties:

- https://securityscans.qa.granicus.com/boards/v1/securityscans.qa/stats

  Cookie was set with:

  ```
  Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:37 GMT; secur
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/boards/v1/16/stats

  Cookie was set with:

  ```
  Set-Cookie: _boule_session=116f37e6db5ba32b8c9bc9a849d78ba9; path=/; expires=Tue, 18 Mar 2025 21:27:36 GMT; secur
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

  ```
  Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.qa.granicus.com
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

  ```
  Set-Cookie: PHPSESSID=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

  ```
  Set-Cookie: _gus=WldZd09ETTFObVV4TVRVeE1EVXpNekEzTjJaak1tTTJaamN6WkRZeU5ERXVLcHpiQzhqRGs2WDE4d1d1SUt6VVFkc05TNVdv
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/boards/v1/securityscans.qa/stats

  Cookie was set with:

  ```
  Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:55 GMT; secur
  ```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

```
Set-Cookie: _gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNh
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/services/boards/users/fefce60e-b06f-4268-ab6a-486c4d9b2f0c/person

  Cookie was set with:

```
Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:55 GMT; secur
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/boards/v1/securityscans.qa/stats

  Cookie was set with:

```
Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:38 GMT; secur
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/boards/v1/16/stats

  Cookie was set with:

```
Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:38 GMT; secur
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/services/boards/users/fefce60e-b06f-4268-ab6a-486c4d9b2f0c/person

  Cookie was set with:

```
Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:27 GMT; secur
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

```
Set-Cookie: login_failed=1; path=/; expires=Tue, 18-Mar-2025 09:47:05 UTC
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

```
Set-Cookie: _gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

```
Set-Cookie: PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmV
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/boards/admin

  Cookie was set with:

```
Set-Cookie: _boule_session=116f37e6db5ba32b8c9bc9a849d78ba9; path=/; expires=Tue, 18 Mar 2025 21:27:36 GMT; secur
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/boards/admin

  Cookie was set with:

```
Set-Cookie: granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c3863
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/boards/admin

  Cookie was set with:

```
Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:26:36 GMT; secur
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

```
Set-Cookie: login_failed=1; path=/; expires=Tue, 18-Mar-2025 09:47:01 UTC
```

  This cookie has the following issues:

```
 - Cookie without SameSite attribute.
When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
```

- https://securityscans.qa.granicus.com/account/login

  Cookie was set with:

  ```
  Set-Cookie: login_failed=0; path=/; expires=Tue, 18-Mar-2025 11:19:37 UTC
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/account/forgotpassword

  Cookie was set with:

  ```
  Set-Cookie: login_failed=0; path=/; expires=Tue, 18-Mar-2025 11:25:01 UTC
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

- https://securityscans.qa.granicus.com/boards/admin/members

  Cookie was set with:

  ```
  Set-Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; path=/; expires=Tue, 18 Mar 2025 21:27:26 GMT; secur
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It
  ```

Request headers

```
GET /boards/v1/securityscans.qa/stats?appointments=ending_schedule HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept: */*

accept-language: en-US

cookie:
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6TXFiSUN0UXFyajNXdnNKanlTcGo;
_gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=6b8d5ad38657a7ef9c99010ab375f7a5; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: x8POei845lCDapb/OE9gE80DIxN7NHAPteWSIEuiYgbgVE1bK5iimFBZmUEIzu1m98sSMF3ZrFztaD+Vgn+0Zw==

x-requested-with: XMLHttpRequest

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

Referer: https://securityscans.qa.granicus.com/boards/admin?signed_request=5TdR8kLMWEmOQYPIbqujv-iWSNSw12wSFPHpFH3-
AQY.eyJpZCI6MjE1OTEsImVtYWlsIjoiZ292ZGFjdW5ldGl4QGdyYW5pY3VzLmNvbSIsImNyZWF0ZWRfYXQiOiIyMDIyLTA4LTI2VDE1OjI2OjM2LjAwMFoiLCJ1cGRhdGVkX2F0IjoiMjAyNS0wMy0wNFQwOToxMDo0MC4wMDBaIiwidXVpZCI6ImZlZmNlNjBlLWIwNmYtNDI2OC1hYjZhLTQ4NmM0ZDliMmYwYyIsInVzZXJuYW1lIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJmdWxsbmFtZSI6ImUgZSBlIiwibGFzdF9uYW1lIjoiZSIsIm1pZGRsZV9uYW1lIjoiZSIsImRlZmF1bHRfYXBwIjoiY2l2aWNpZGVhcyIsImJ1aWx0X2luIjpmYWxzZSwicGhvbmUiOiIiLCJkZWxldGVkX2F0IjpudWxsLCJkb21haW5faWQiOjIwLCJhZG1pbiI6ZmFsc2UsImdyb3VwcyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwidWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwibmFtZSI6ImUgZSIsImZpcnN0bmFtZSI6ImUiLCJsYXN0bmFtZSI6ImUiLCJkb21haW4iOiJzZWN1cml0eXNjYW5zLnFhLmdyYW5pY3VzLmNvbSJ9

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Insecure Frame (External)

Severity	**Low**
Reported by module	/httpdata/iframe_sandbox.js

Description

The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

Recommendation

Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.

References

MDN | iframe: The Inline Frame Element (https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe)
HTML Standard: iframe (https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element)
HTML 5.2: 4.7. Embedded content (https://www.w3.org/TR/html52/semantics-embedded-content.html#element-attrdef-iframe-sandbox)

Affected items

/Reports.php
Verified vulnerability
Details
An iframe tag references an external resource, and no sandbox attribute is set.
Request headers

```
GET /Reports.php HTTP/1.1

Referer: https://securityscans.qa.granicus.com/

Cookie: PHPSESSID=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; _boule_session=c13aa4ae96c58bbd2eca5c9afcea23a8;
_gat=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=WmpreE9USmhPVEEwWldNelpXRmtaVEprTldaalkySXhPR0ppTlRCa016WXVicUVGOXVneVJWRnpRWlRKVnBTbjlEaW5Nank1VnFpcDA0NUkzMmEw
WTBaa3BvZEY4d25FQkdhTlB6REE; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; login_failed=0

x-csrf-token: kHF3HYwcTwqU0qqefjy2DjRvMr5K6/ucVbLcGPBZ+ttyyqbaaihaNvOy1Qf+Z6DTwYoWxhziOtE9ybctbpOb0Q==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Programming Error Messages

Severity	**Low**
Reported by module	/Scripts/PerScheme/Error_Message.script

Description

This alert requires manual confirmation

Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.
These messages may also contain the location of the file that produced an unhandled exception.
Consult the 'Attack details' section for more information about the affected page(s).

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that these page(s) are disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server

Details

Application error messages:

- https://securityscans.qa.granicus.com/player/camera/1
  <abbr title="ErrorException">ErrorException</abbr>

Request headers

```
GET /player/camera/1?redirect[]=true HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Cookie: PHPSESSID=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=c13aa4ae96c58bbd2eca5c9afcea23a8; _gat=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=WmpreE9USmhPVEEwWldNelpXRmtaVEprTldaalkySXhPR0ppTlRCa016WXVicUVGOXVneVJWRnpRWlRKVnBTbjlEaW5Nank1VnFpcDA0NUkzMmEw
WTBaa3BvZEY4d25FQkdhTlB6REE; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0

x-csrf-token: kHF3HYwcTwqU0qqefjy2DjRvMr5K6/ucVbLcGPBZ+ttyyqbaaihaNvOy1Qf+Z6DTwYoWxhziOtE9ybctbpOb0Q==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Ruby on Rails CookieStore session cookie persistence

Severity	**Low**
Reported by module	/Scripts/PostCrawl/Rails_Weak_secret_token.script

Description

Ruby on Rails contains a flaw in its design that may allow attackers to more easily access applications. The issue is due to the CookieStore mechanism storing cookies on the client side, while not maintaining a corresponding entry on the server side. When an application terminates a session, Ruby on Rails has no method to track this and truly invalidate the cookie with the default configuration. This means that cookies persist "for life" and can be used to access an application even after it is thought to be terminated in many cases.

Impact

A malicious user could use the stolen cookie from any authenticated request by the user to log in as them at any point in the future.

Recommendation

Currently, there are no known upgrades or patches to correct this vulnerability. It is possible to temporarily mitigate the flaw by implementing the following workaround: switch to a more secure authentication management systems (e.g. ActiveRecordStore).

References

Logout is broken by default in ruby on rails web applications (http://maverickblogging.com/logout-is-broken-by-default-ruby-on-rails-web-applications/)
Ruby on Rails CookieStore Session Cookie Persistence Security Vulnerability (https://www.securityfocus.com/bid/62657)

Affected items

Web Server
Details
Affected cookie: **granicus_domain**
Request headers

Sensitive pages could be cached

Severity	**Low**
Reported by module	/RPA/Cacheable_Sensitive_Page.js

Description

One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.

References

OWASP - Caching of Sensitive Information (https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses)
MDN Web Docs - Cache-Control (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control)
CWE-524: Use of Cache Containing Sensitive Information (https://cwe.mitre.org/data/definitions/524.html)

Affected items

Web Server
Details

List of pages that could be cached:

- https://securityscans.qa.granicus.com/legislate/login?password-sign-in=u]H[ww6KrA9F.x-F&username=WkYxnTGh
- https://securityscans.qa.granicus.com/legislate/forgot_password?username=WkYxnTGh

Request headers

```
GET /legislate/login?password-sign-in=u]H[ww6KrA9F.x-F&username=WkYxnTGh HTTP/1.1

Referer:
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/

Cookie:
PHPSESSID=bVqCcLhy7l7NuddovxhyxtcwlytcuW1KBEhUMNU9o5Q.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMTg6MTE6MDAiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUNPQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMiLCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=8c9cb056293ec3110a941471751f48b4;
_gat=bVqCcLhy7l7NuddovxhyxtcwlytcuW1KBEhUMNU9o5Q.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMTg6MTE6MDAiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TXpjMlpETmhPREEyTldJeE5XUXdaalkyTnpRNVltSTVOMlkxTURZMVltVXUzYkJPd0hJV3phc24xbzREMkxvWUk2S0pIUUgvSXJUK3djMFl3QjVZVFJvcHBJMmZ0OHFtYmc5WFQ1SUU;
_hypatia_session=uuuXNbbw6y%2FETyV%2BHTZ5zt%2F%2Bc83%2FTZz7%2F5Yq55YbbpOhSM1wfkhgYD6SO41sKxWFTpuJNS7yaIOTwzRrRHOMXbNstmU8tfBBen7%2Bpzqcj4r4PcN%2FbIzNftlff9l86Cvis7O4vbH1W8wQ8kqSJx8%3D--vkwhARLU1nIAuj67--XR4QxTgJ5B2%2Bhhm137t7gA%3D%3D;
granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0

x-csrf-token: nQQLXOYXslpcdkEjdtpWN2TN62kzsvK3T8KpAZgQSL5PbTXfdcec0ALCgP6kuBlNdh5AH2qU5U5yw86U4a/K5g==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Session cookies scoped to parent domain

Severity	**Low**
Reported by module	/RPA/Cookie_On_Parent_Domain.js

Description

One ore more session cookies are scoped to the parent domain instead of a sub-domain. If a cookie is scoped to a parent domain, then this cookie will be accessible by the parent domain and also by any other sub-domains of the parent domain. This could lead to security problems.

Impact

None

Recommendation

If possible, the session cookies should be scoped strictly to a sub-domain.

References

OWASP - Session Management Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html)

Affected items

Web Server
Verified vulnerability
Details

Session cookies scoped to parent domain:

- https://securityscans.qa.granicus.com/account/login

```
Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.qa.granicus.com

Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=.qa.granicus.com

Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0

Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; domain=.securityscans.qa.granicus.com

Set-Cookie: _gat=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/; domain=.securityscans.qa.gran
```

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Session ID in URL

Severity	**Low**
Reported by module	/RPA/Session_Token_In_Url.js

Description

This application contains one or more pages with what appears to be a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The session should be maintained using cookies (or hidden input fields).

References

Session Management - OWASP Cheat Sheet Series (https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html)
Session fixation | OWASP Foundation (https://owasp.org/www-community/attacks/Session_fixation)

Affected items

Web Server

Details

Pages with session token in URL:

- https://securityscans.qa.granicus.com/SearchResults.php?keywords=the&token=f22f2e3288a61c907f30dc60fe7db899 (token)
- https://securityscans.qa.granicus.com/SearchResults.php?keywords=&token=f22f2e3288a61c907f30dc60fe7db899 (token)

Request headers

```
GET /SearchResults.php?keywords=the&token=f22f2e3288a61c907f30dc60fe7db899 HTTP/1.1

Referer: https://securityscans.qa.granicus.com/

Cookie: PHPSESSID=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; _boule_session=c13aa4ae96c58bbd2eca5c9afcea23a8;
_gat=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=WmpreE9USmhPVEEwWldNelpXRmtaVEprTldaalkySXhPR0ppTlRCa016WXVicUVGOXVneVJWRnpRWlRKVnBTbjlEaW5Nank1VnFpcDA0NUkzMmEw
WTBaa3BvZEY4d25FQkdhTlB6REE; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; login_failed=0

x-csrf-token: kHF3HYwcTwqU0qqefjy2DjRvMr5K6/ucVbLcGPBZ+ttyyqbaaihaNvOy1Qf+Z6DTwYoWxhziOtE9ybctbpOb0Q==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Web Server

Details

Pages with session token in URL:

- https://securityscans.qa.granicus.com/SearchResults.php?keywords=the&token=81fb096a40f2520d4a44edbf623a0bdc (token)
- https://securityscans.qa.granicus.com/SearchResults.php?keywords=the&token=2a876059364551aee0264216e1406622 (token)

Request headers

```
GET /SearchResults.php?keywords=the&token=81fb096a40f2520d4a44edbf623a0bdc HTTP/1.1

Referer: https://securityscans.qa.granicus.com/index

Cookie: PHPSESSID=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6Ik1seGYzclJSclhzbVpVdnZ4WHZSbVE9PSIsInZhbHVlIjoiRXFIbUhrcWpJelBiSkFaSUwxVWpZNTU5VDA4WmY3MWtlYkk2Sm9nNW5
QaHMxbE1xYlBiK2p3OFNva3BVc2hmZ2cvbnArMTY0c2dReXdwZnZ2MUZ6VzFhSjY2Q1JQQkpWekFXQ3JvSVZWV1YxWUdTMmIwWGhtK1c5LzFMUk5aSDIi
LCJtYWMiOiIzMjRkNmFjYzA5ZjNkYjE1MTUyYzFlZWJmMDhjNThhYjA1YzIzNTNjNmE2MzM1NWM2YmVmNjY2MmMwODAyMGM3IiwidGFnIjoiIn0%3D;
_boule_session=c13aa4ae96c58bbd2eca5c9afcea23a8; _gat=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=WmpreE9USmhPVEEwWldNelpXRmtaVEprTldaalkySXhPR0ppTlRCa016WXVicUVGOXVneVJWRnpRWlRKVnBTbjlEaW5Nank1VnFpcDA0NUkzMmEw
WTBaa3BvZEY4d25FQkdhTlB6REE; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0

x-csrf-token: kHF3HYwcTwqU0qqefjy2DjRvMr5K6/ucVbLcGPBZ+ttyyqbaaihaNvOy1Qf+Z6DTwYoWxhziOtE9ybctbpOb0Q==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Symfony debug mode enabled

Severity	**Low**
Reported by module	/httpdata/symfony_audit.js

Description

The web application uses Symfony framework. Symfony Debug mode is enabled. Debug mode should be turned off in production environment, as it leads to disclosure of sensitive information about the web application.

Impact

The web application in debug mode discloses sensitive information. This information can be used to launch further attacks.

Recommendation

Disable the debug mode by setting APP_DEBUG to false

References

Debug Mode (https://symfony.com/doc/4.4/configuration/front_controllers_and_kernel.html#debug-mode)

Affected items

/api/metrics/cspreport
Details
Request headers

```
GET /api/metrics/cspreport HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5;
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6
TXFiSUN0UXFyajNXdnNKanlTcGo; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: x8POei845lCDapb/OE9gE80DIxN7NHAPteWSIEuiYgbgVE1bK5iimFBZmUEIzu1m98sSMF3ZrFztaD+Vgn+0Zw==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

/profile/process

Details

Request headers

```
GET /profile/process HTTP/1.1

Referer: https://securityscans.qa.granicus.com/profile

Cookie: PHPSESSID=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=c13aa4ae96c58bbd2eca5c9afcea23a8; _gat=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=WmpreE9USmhPVEEwWldNelpXRmtaVEprTldaalkySXhPR0ppTlRCa016WXVicUVGOXVneVJWRnpRWlRKVnBTbjlEaW5Nank1VnFpcDA0NUkzMmEw
WTBaa3BvZEY4d25FQkdhTlB6REE; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0

x-csrf-token: kHF3HYwcTwqU0qqefjy2DjRvMr5K6/ucVbLcGPBZ+ttyyqbaaihaNvOy1Qf+Z6DTwYoWxhziOtE9ybctbpOb0Q==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

/services/permissions/

Details

Request headers

```
GET /services/permissions/ HTTP/1.1

Referer: https://securityscans.qa.granicus.com/services/permissions/

Cookie:
PHPSESSID=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUNPQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMiLCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=c55b033e98bd93b583ce3653696ed20f;
_gat=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TlRSbVlUTTROV0ppT0RSaE5ETm1aamxoWWpWaU5UaGtNMkUzWVdNd1l6VXViRHdkVzd0ZDlhZHFJOXhUVHhDUmlQbmthbWt6UTdjUlY0Q1I3V2pWbFpWUDdFWVNUelRkMWVWbHd2clM;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--U9bk%2FbhY6T2LNshQzfcksw%3D%3D; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0; request_method=PATCH

x-csrf-token: MCErtFoG3a3h3UrA1wIdzmCpcs3FyjBqH0xxQQrL+2D/HLjQUTmBsMLxIPJOCacXHnGe9kNCYO+hc25SBS0QtQ==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

[Possible] Internal Path Disclosure (*nix)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server
Details

Pages with paths being disclosed:

- https://securityscans.qa.granicus.com/api/metrics/cspreport
  /var/www/mediamanager_php/releases/4682597cc36694fdb8cdfdcbd08458c47057c4d4/vendor/laravel/framework/src/Illuminate/Routing/
- https://securityscans.qa.granicus.com/panes/EditCameraBasic.php
  /var/www/mediamanager_php/releases/4682597cc36694fdb8cdfdcbd08458c47057c4d4/app/lib/DataObject.php:115
- https://securityscans.qa.granicus.com/profile/process
  /var/www/mediamanager_php/releases/4682597cc36694fdb8cdfdcbd08458c47057c4d4/vendor/laravel/framework/src/Illuminate/Routing/
- https://securityscans.qa.granicus.com/panes/EditCameraPermission.php
  /var/www/mediamanager_php/releases/4682597cc36694fdb8cdfdcbd08458c47057c4d4/app/lib/DataObject.php:115
- https://securityscans.qa.granicus.com/panes/EditCameraPublishList.php
  /var/www/mediamanager_php/releases/4682597cc36694fdb8cdfdcbd08458c47057c4d4/app/lib/DataObject.php:115
- https://securityscans.qa.granicus.com/services/permissions/
  /var/www/mediamanager_php/releases/6b0968518d8ab7d59f3ed4b94872dc3c8a9a3f6e/vendor/laravel/framework/src/Illuminate/Routing/
- https://securityscans.qa.granicus.com/services/template_settings/upload_url
  /var/www/mediamanager_php/releases/4682597cc36694fdb8cdfdcbd08458c47057c4d4/vendor/aws/aws-sdk-php/src/ClientResolver.php

Request headers

```
GET /api/metrics/cspreport HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Cookie: _boule_session=6b8d5ad38657a7ef9c99010ab375f7a5;
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6TXFiSUN0UXFyajNXdnNKanlTcGo; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3Jhbmljdc XMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: x8POei845lCDapb/OE9gE80DIxN7NHAPteWSIEuiYgbgVE1bK5iimFBZmUEIzu1m98sSMF3ZrFztaD+Vgn+0Zw==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

[Possible] Internal Path Disclosure (Windows)

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more fully qualified path names were been found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure (https://www.owasp.org/index.php/Full_Path_Disclosure)

Affected items

Web Server
Details
Pages with paths being disclosed: • https://securityscans.qa.granicus.com/panes/NewFolder.php **c:/windows/win.ini** • https://securityscans.qa.granicus.com/panes/NewView.php **c:/windows/win.ini**
Request headers

```
GET /panes/NewFolder.php?type= HTTP/1.1

Referer: https://securityscans.qa.granicus.com/NewFolder.php

Cookie: PHPSESSID=y8nWWFisH13cnod_7kXW7-
TadobXBULskGBgW5nSlwo.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiw
iZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwi
YWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDY6MjY6NDUiLCJncyI6WyIyOGM5N
TM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
_boule_session=b3141a70f8e10b93f3d8f30e283b3855; _gat=y8nWWFisH13cnod_7kXW7-
TadobXBULskGBgW5nSlwo.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiw
iZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwi
YWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDY6MjY6NDUiLCJncyI6WyIyOGM5N
TM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TXpSa1kyRTJPV0pqTVdVMFpHWmpPREUwWmpVNFlUVmhOMlptWmprMk56RXVjZDhsUG1yL1IxTWNpUWhvaEdTbEpJRi94VGhHQmRxR0FCOUFCSmpM
Q2x2ZVlobDFxcm5Zc0luc1dROEU;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%
2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC; login_failed=0;
request_method=POST

x-csrf-token: PRLAzg/6KC0SXjLZ+ORr2JXCg1Ec+fgr4Qvi/+CqZzsZm9HlqQqx2HmwEqJDdhUT8w46UQPEkQc5WUqstP02Ug==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

An Unsafe Content Security Policy (CSP) Directive in Use

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **An Unsafe Content Security Policy (CSP) Directive in Use**
  - **First observed on:** https://securityscans.qa.granicus.com/account/login
  - **CSP Value:** default-src https: 'unsafe-inline' 'unsafe-eval'; media-src https: blob:; img-src https: blob: data:; worker-src https: blob:; connect-src https: wss:; report-uri /api/metrics/cspreport
  - **CSP Source:** header
  - **Summary:** Acunetix detected that one of following CSP directives is used: unsafe-eval, unsafe-inline. By using unsafe-eval, you allow the use of string evaluation functions like eval. By using unsafe-inline, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.
  - **Remediation:** If possible remove unsafe-eval and unsafe-inline from your CSP directives.
  - **References:**
    - N/A

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

data: Used in a Content Security Policy (CSP) Directive

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **data: Used in a Content Security Policy (CSP) Directive**
  - **First observed on:** https://securityscans.qa.granicus.com/account/login
  - **CSP Value:** default-src https: 'unsafe-inline' 'unsafe-eval'; media-src https: blob:; img-src https: blob: data:; worker-src https: blob:; connect-src https: wss:; report-uri /api/metrics/cspreport
  - **CSP Source:** header
  - **Summary:** Acunetix detected data: use in a CSP directive.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using data: protocol.
  - **Remediation:** Remove data: sources from your CSP directives.
  - **References:**
    - N/A

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

default-src Used in Content Security Policy (CSP)

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **default-src Used in Content Security Policy (CSP)**
  - **First observed on:** https://securityscans.qa.granicus.com/account/login
  - **CSP Value:** default-src https: 'unsafe-inline' 'unsafe-eval'; media-src https: blob:; img-src https: blob: data:; worker-src https: blob:; connect-src https: wss:; report-uri /api/metrics/cspreport
  - **CSP Source:** header
  - **Summary:** Acunetix detected that you used default-src in CSP directive. It is important to know that default-src cannot be used as a fallback for the functions below: base-uri, form-action, frame-ancestors, plugin-types, report-uri, sandbox
  - **Impact:** N/A
  - **Remediation:** N/A
  - **References:**
    - N/A

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Generic Email Address Disclosure

Severity	**Informational**
Reported by module	/httpdata/text_search.js

Description

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server
Details

Emails found:

- https://securityscans.qa.granicus.com/profile
  govdacunetix@granicus.com
- https://securityscans.qa.granicus.com/panes/Calendar.html
  feedback@softcomplex.com
- https://securityscans.qa.granicus.com/profile/
  govdacunetix@granicus.com
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12717.3651.de98f.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12718.3651.de98f.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10684.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10688.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12800.3651.48d83.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12801.3651.48d83.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10774.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10775.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12870.3651.48d83.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12871.3651.48d83.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10880.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10883.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12981.3651.48d83.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-12984.3651.48d83.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10945.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3654-10950.3654.2e0b2.20147.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-13109.3651.48d83.20148.2@bxss.me
- https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
  305105.3651-13110.3651.48d83.20148.2@bxss.me

Request headers

```
GET /profile HTTP/1.1

Referer: https://securityscans.qa.granicus.com/myaccount.php

Cookie: PHPSESSID=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; _boule_session=c13aa4ae96c58bbd2eca5c9afcea23a8;
_gat=HpqvXYiFFtgDQGVKX79nnedaPNYz6iyLU-
47NYiX8as.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjo
ic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZh
bHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDM6MTQ6MjUiLCJncyI6WyIyOGM5NTM4Yy1mNzc2L
TQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=WmpreE9USmhPVEEwWldNelpXRmtaVEprTldaalkySXhPR0ppTlRCa016WXVicUVGOXVneVJWRnpRWlRKVnBTbjlEaW5Nank1VnFpcDA0NUkzMmEw
WTBaa3BvZEY4d25FQkdhTlB6REE; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; login_failed=0

x-csrf-token: kHF3HYwcTwqU0qqefjy2DjRvMr5K6/ucVbLcGPBZ+ttyyqbaaihaNvOy1Qf+Z6DTwYoWxhziOtE9ybctbpOb0Q==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Outdated JavaScript libraries

Severity	**Informational**
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

References

How Invicti identifies Out-of-date technologies (https://www.invicti.com/support/how-invicti-identifies-outofdate/)

Affected items

Web Server

Details

- **bootstrap.js 3.2.0**
  - URL: https://securityscans.qa.granicus.com/account/login
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request headers

```
GET /account/login?ReturnUrl=/apps/peakagenda/ HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: none

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: document

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Web Server

Details

- **Underscore.js 1.5.2**
  - URL: https://securityscans.qa.granicus.com/boards/admin
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/jashkenas/underscore/tags

Request headers

```
GET /boards/admin?signed_request=5TdR8kLMWEmOQYPIbqujv-iWSNSw12wSFPHpFH3-
AQY.eyJpZCI6MjE1OTEsImVtYWlsIjoiZ292ZGFjdW5ldGl4QGdyYW5pY3VzLmNvbSIsImNyZWF0ZWRfYXQiOiIyMDIyLTA4LTI2VDE1OjI2OjM2LjAwM
FoiLCJ1cGRhdGVkX2F0IjoiMjAyNS0wMy0wNFQwOToxMDo0MC4wMDBaIiwidXVpZCI6ImZlZmNlNjBlLWIwNmYtNDI2OC1hYjZhLTQ4NmM0ZDliMmYwYy
IsInVzZXJuYW1lIjoic2VjdXJpdHlzY2FucyIsImZpcnN0X25hbWUiOiJlIiwibGFzdF9uYW1lIjoiZSIsIm1pZGRsZV9uYW1lIjoiZSIsImRlZmF1bHR
fYXBwIjoiY2l2aWNpZGVhcyIsImJ1aWx0X2luIjpmYWxzZSwicGhvbmUiOiIiLCJkZWxldGVkX2F0IjpudWxsLCJkb21haW5faWQiOjIwLCJhZG1pbiI6
ZmFsc2UsImdyb3VwcyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwidWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtN
Dg2YzRkOWIyZjBjIiwibmFtZSI6ImUgZSIsImZpcnN0bmFtZSI6ImUiLCJsYXN0bmFtZSI6ImUiLCJkb21haW4iOiJzZWN1cml0eXNjYW5zLnFhLmdyYW
5pY3VzLmNvbSJ9 HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: iframe

cookie:
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6
TXFiSUN0UXFyajNXdnNKanlTcGo;
_gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMD
I6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
TkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=6b8d5ad38657a7ef9c99010ab375f7a5

Referer: https://securityscans.qa.granicus.com/apps/boards

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Web Server

Details

- **D3.js 3.0.8**
  - URL: https://securityscans.qa.granicus.com/boards/admin
  - Detection method: The library's name and version were determined based on its dynamic behavior.
  - References:
    - https://github.com/d3/d3/releases

Request headers

```
GET /boards/admin?signed_request=5TdR8kLMWEmOQYPIbqujv-iWSNSw12wSFPHpFH3-
AQY.eyJpZCI6MjE1OTEsImVtYWlsIjoiZ292ZGFjdW5ldGl4QGdyYW5pY3VzLmNvbSIsImNyZWF0ZWRfYXQiOiIyMDIyLTA4LTI2VDE1OjI2OjM2LjAwM
FoiLCJ1cGRhdGVkX2F0IjoiMjAyNS0wMy0wNFQwOToxMDo0MC4wMDBaIiwidXVpZCI6ImZlZmNlNjBlLWIwNmYtNDI2OC1hYjZhLTQ4NmM0ZDliMmYwYy
IsInVzZXJuYW1lIjoic2VjdXJpdHlzY2FucyIsImZpcnN0X25hbWUiOiJlIiwibGFzdF9uYW1lIjoiZSIsIm1pZGRsZV9uYW1lIjoiZSIsImRlZmF1bHR
fYXBwIjoiY2l2aWNpZGVhcyIsImJ1aWx0X2luIjpmYWxzZSwicGhvbmUiOiIiLCJkZWxldGVkX2F0IjpudWxsLCJkb21haW5faWQiOjIwLCJhZG1pbiI6
ZmFsc2UsImdyb3VwcyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwidWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtN
Dg2YzRkOWIyZjBjIiwibmFtZSI6ImUgZSIsImZpcnN0bmFtZSI6ImUiLCJsYXN0bmFtZSI6ImUiLCJkb21haW4iOiJzZWN1cml0eXNjYW5zLnFhLmdyYW
5pY3VzLmNvbSJ9 HTTP/1.1

Host: securityscans.qa.granicus.com

Pragma: no-cache

Cache-Control: no-cache

accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7

accept-language: en-US

upgrade-insecure-requests: 1

sec-ch-ua: "HeadlessChrome";v="131", "Chromium";v="131", "Not_A Brand";v="24"

sec-ch-ua-mobile: ?0

sec-ch-ua-platform: "Windows"

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

Sec-Fetch-User: ?1

Sec-Fetch-Dest: iframe

cookie:
_gus=WmpnNU5XWmtOVEJtTWpFd05URTJNamN3TjJVeVltSTVaVFE1TVRFeU1XUXVhQUxWU0RneG05d2tpbjVyYU5zc3FDbVNyOHNhMzBRVWZjQTR5aVJ6
TXFiSUN0UXFyajNXdnNKanlTcGo;
_gat=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMD
I6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=pbEjSSR1AKZ6QTerCGWqA1_po95ufynRWWYT7IM6cIY.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
TkgMDI6MjY6MTciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=6b8d5ad38657a7ef9c99010ab375f7a5

Referer: https://securityscans.qa.granicus.com/apps/boards

Accept-Encoding: gzip,deflate,br

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
```

Web Server

Details

- **jQuery UI Dialog 1.12.1**
  - URL: https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the alert has been lowered.
  - References:
    - https://jqueryui.com/download/

Request headers

```
GET /core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197 HTTP/1.1

Cookie: _boule_session=c55b033e98bd93b583ce3653696ed20f; login_failed=0; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%
2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D;
_gus=TlRSbVlUTTROV0ppT0RSaE5ETm1aamxoWWpWaU5UaGtNMkUzWVdNd1l6VXViRHdkVzd0ZDlhZHFJOXhUVHhDUmlQbmthbWt6UTdjUlY0Q1I3V2pW
bFpWUDdFWVNUelRkMWVWbHd2clM;
_gat=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMD
c6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
jAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: MCErtFoG3a3h3UrA1wIdzmCpcs3FyjBqH0xxQQrL+2D/HLjQUTmBsMLxIPJOCacXHnGe9kNCYO+hc25SBS0QtQ==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Web Server

Details

- **jQuery UI Tooltip 1.12.1**
  - URL: https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the alert has been lowered.
  - References:
    - https://jqueryui.com/download/

Request headers

```
GET /core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197 HTTP/1.1

Cookie: _boule_session=c55b033e98bd93b583ce3653696ed20f; login_failed=0; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC;
_hypatia_session=k%2BlJyi2JVdUTlEL6sHCGwUAzYV97vNF1LYZMNd%2B4ceSrS4ogc3DRRY1D%2Bi9%2BM3DjsXi54oL%2FF24TSESjICcFdHE5T%
2B5VmW2SwE0KMH%2B6%2BAswovvayk0EKNl03xlb5bsIYdZDPcIsM8USmV1TkG0%3D--Uveuum%2BFdtrc4Gad--
U9bk%2FbhY6T2LNshQzfcksw%3D%3D;
_gus=TlRSbVlUTTROV0ppT0RSaE5ETm1aamxoWWpWaU5UaGtNMkUzWVdNd1l6VXViRHdkVzd0ZDlhZHFJOXhUVHhDUmlQbmthbWt6UTdjUlY0Q1I3V2pW
bFpWUDdFWVNUelRkMWVWbHd2clM;
_gat=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4
LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiL
CJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMD
c6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
PHPSESSID=9MIfdJ09HqZ1pWT0Jh3VcnRXywbIUnOvcfhUz3GVkzk.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi0
0MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2Nh
bnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtM
jAgMDc6MDQ6MDIiLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D--69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: MCErtFoG3a3h3UrA1wIdzmCpcs3FyjBqH0xxQQrL+2D/HLjQUTmBsMLxIPJOCacXHnGe9kNCYO+hc25SBS0QtQ==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Web Server

Details

- **React 16.11**
  - URL: https://securityscans.qa.granicus.com/services/minutes/assets/ui/js/application-73c4ff04cedd4051aaac.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/facebook/react/tags

Request headers

```
GET /services/minutes/assets/ui/js/application-73c4ff04cedd4051aaac.js HTTP/1.1

Cookie: _boule_session=7d4e8b084d4ad0032a1d3aae483799c3; login_failed=0; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC;
_hypatia_session=JQcFpMMzDf%2Bk7LTWEDqd6rRUyLFcbEwJk58lsp3pVVzdPQcmbL9YfhwiMlJYiyf4lE8fpbTk1wFL%2FVOUPpzpw%2BDFxhHWS1
4376PwIjSyRKTxJyJqxxAlBPacBkbaottr9ihnJEOI97mWDkumUoU%3D--cVcsliWegITjc0M1--6dryuEb4XQPG%2Beb73M%2FTxg%3D%3D;
request_method=POST;
_gus=WkdRMU9UUXlNRFJtWmpCaU1tRXhaR1l5TUdSa04yRTFNelk1TXpGaU1qUXV0dkRwZnJSNkFhV2kvY2t4NzJ4S2xLY0UwUW1zK0xUY3J6OVdOWGVY
NGc1a3Jieis1THNMUjVmMTBXOW0; _gat=8cFODVKO4I3QG56qYFDkCcviGmPNomb3rmav-
mhPovM.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2
VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHN
lLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMTQ6NDk6MjciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4
ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; PHPSESSID=8cFODVKO4I3QG56qYFDkCcviGmPNomb3rmav-
mhPovM.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2
VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHN
lLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMTQ6NDk6MjciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4
ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: /pawtVrg1mVjSQtQ0hgRfvQQjAO4nm0/lVtUK03ylgNuMoH0eg1nXM6K0Db4sfN6a8aOgw7rmZszLqoDiloamw==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Web Server

Details

- **JavaScript Cookie 2.2.1**
  - URL: https://securityscans.qa.granicus.com/services/minutes/assets/ui/js/legislate-bbc5c6e3b5f20c44f4f2.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/js-cookie/js-cookie/releases

Request headers

```
GET /services/minutes/assets/ui/js/legislate-bbc5c6e3b5f20c44f4f2.js HTTP/1.1

Cookie: _boule_session=7d4e8b084d4ad0032a1d3aae483799c3; login_failed=0; XSRF-
TOKEN=eyJpdiI6IkVWd1lkc2llUHJkQUFyVUtWaEVFVHc9PSIsInZhbHVlIjoidHQvRGp4MURMVFJRT2x5Q0ZzbWpNeE1YUjFDUXRqRFlTaDZVbTJzMUN
PQkdRUmxJcUpRS3QvbkxZcUgvYUZVWHVwbkdnbjdjVzVVcUF6TCtISDNsdW9LUGgzTmdESkFUaDI5NlgwVk9yRGJQN2ZDSnpHVzVXaG5HNTUwVnliYkMi
LCJtYWMiOiJkMDZkZWMzNDA4NWFmMDFiZTg3NjMzYTlhZDdkNzY5Y2U2YzQ1NTg2MDM1YzU2YjdiM2M0NDhjZTg4MTE3NTZmIiwidGFnIjoiIn0%3D;
laravel_session=N72qHiBATcAVwW4VX7kR6V77L6K2cpYELZ1VlQPC;
_hypatia_session=qHRsxNtdRikubqMyvf6w48vI4s3bQpQoae9qGsIvH4rjNUu%2FDWTVeqlzZVSh3U0IWjLj2Hf%2Beuz6y4yHctMBA3O3UpCVXHzV
cbc%2FOTNZAy0kMC73CqvvsQF0guuu%2FDMvM7%2FD8iEeY37UqcNIdQ8%3D--x5F1o3mYE50Og5NP--vqWp0Bi2RkspW3Fvx7Mhow%3D%3D;
_gus=WkdRMU9UUXlNRFJtWmpCaU1tRXhaR1l5TUdSa04yRTFNelk1TXpGaU1qUXV0dkRwZnJSNkFhV2kvY2t4NzJ4S2xLY0UwUW1zK0xUY3J6OVdOWGVY
NGc1a3Jieis1THNMUjVmMTBXOW0; _gat=8cFODVKO4I3QG56qYFDkCcviGmPNomb3rmav-
mhPovM.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2
VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHN
lLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMTQ6NDk6MjciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4
ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; PHPSESSID=8cFODVKO4I3QG56qYFDkCcviGmPNomb3rmav-
mhPovM.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg2YzRkOWIyZjBjIiwiZG9tYWluIjoic2
VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFtZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHN
lLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMjAgMTQ6NDk6MjciLCJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4
ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a

x-csrf-token: /pawtVrg1mVjSQtQ0hgRfvQQjAO4nm0/lVtUK03ylgNuMoH0eg1nXM6K0Db4sfN6a8aOgw7rmZszLqoDiloamw==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Permissions-Policy header not implemented

Severity	**Informational**
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

Permissions-Policy / Feature-Policy (MDN) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server
Details

Locations without Permissions-Policy header:

- https://securityscans.qa.granicus.com/account/login
- https://securityscans.qa.granicus.com/
- https://securityscans.qa.granicus.com/api/metrics/cspreport
- https://securityscans.qa.granicus.com/legistar/dashboard.json
- https://securityscans.qa.granicus.com/legistar
- https://securityscans.qa.granicus.com/boards/admin
- https://securityscans.qa.granicus.com/SearchResults.php
- https://securityscans.qa.granicus.com/check_expired
- https://securityscans.qa.granicus.com/JSON.php
- https://securityscans.qa.granicus.com/images/
- https://securityscans.qa.granicus.com/index
- https://securityscans.qa.granicus.com/index.php
- https://securityscans.qa.granicus.com/EditCameraBasic.php
- https://securityscans.qa.granicus.com/log
- https://securityscans.qa.granicus.com/panes/logs.php
- https://securityscans.qa.granicus.com/Cameras.php
- https://securityscans.qa.granicus.com/log.php
- https://securityscans.qa.granicus.com/Archives.php
- https://securityscans.qa.granicus.com/Events.php
- https://securityscans.qa.granicus.com/Reports.php
- https://securityscans.qa.granicus.com/myaccount.php

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Scheme URI Detected in Content Security Policy (CSP) Directive

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **Scheme URI Detected in Content Security Policy (CSP) Directive**
  - **First observed on:** https://securityscans.qa.granicus.com/account/login
  - **CSP Value:** default-src https: 'unsafe-inline' 'unsafe-eval'; media-src https: blob:; img-src https: blob: data:; worker-src https: blob:; connect-src https: wss:; report-uri /api/metrics/cspreport
  - **CSP Source:** header
  - **Summary:** Acunetix detected that scheme URI was used in CSP directive.
  - **Impact:** This means that scheme URI in script-src (http: or https:) allows the execution of unsafe scripts.
  - **Remediation:** Replace the scheme URI with the domain that you trust.
  - **References:**
    - N/A

Request headers

```
GET /account/login HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

Subresource Integrity (SRI) Not Implemented

Severity	**Informational**
Reported by module	/RPA/SRI_Not_Implemented.js

Description

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
        integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
        crossorigin="anonymous"></script>
```

References

Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)
SRI Hash Generator (https://www.srihash.org/)

Affected items

Web Server
Details

Pages where SRI is not implemented:

- https://securityscans.qa.granicus.com/boards/admin
  Script SRC: **https://d90rfox8mcja7.cloudfront.net/assets/application-801ae729d3de48a5d3c86cd94839aff7912323ae0b9ed2a28276dea2ee2e5693.js**
- https://securityscans.qa.granicus.com/index
  Script SRC: **https://www.googletagmanager.com/gtag/js?id=G-VXTHT9KDGN**
- https://securityscans.qa.granicus.com/legislate
  Script SRC: **https://cdn.flowplayer.com/releases/native/3/stable/flowplayer.min.js**
- https://securityscans.qa.granicus.com/legislate
  Script SRC: **https://pro.fontawesome.com/releases/v5.15.3/js/all.js**

Request headers

```
GET /boards/admin HTTP/1.1

Referer: https://securityscans.qa.granicus.com/apps/peakagenda/

Cookie: PHPSESSID=Oalux-
J2uVIWv2QAYB4Ja0Am697lgAqKPe5ZuF98HtA.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg
2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFt
ZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDI6Mjc6MTIiL
CJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_boule_session=116f37e6db5ba32b8c9bc9a849d78ba9; _gat=Oalux-
J2uVIWv2QAYB4Ja0Am697lgAqKPe5ZuF98HtA.eyJuYW1lIjoiU2VjdXJpdHkgU2NhbnMiLCJ1dWlkIjoiZmVmY2U2MGUtYjA2Zi00MjY4LWFiNmEtNDg
2YzRkOWIyZjBjIiwiZG9tYWluIjoic2VjdXJpdHlzY2Fucy5xYS5ncmFuaWN1cy5jb20iLCJ1c2VybmFtZSI6InNlY3VyaXR5c2NhbnMiLCJmdWxsbmFt
ZSI6ImUgZSBlIiwiYWRtaW4iOmZhbHNlLCJncmFuaWN1cyI6ZmFsc2UsImRhIjoiY2l2aWNpZGVhcyIsImV4cCI6IjIwMjUtMDMtMTkgMDI6Mjc6MTIiL
CJncyI6WyIyOGM5NTM4Yy1mNzc2LTQ4ZGUtYWFjYy1lMDQ5ZGIyYjA1NDgiXSwic2ciOm51bGx9;
_gus=TVdWaE1XVm1NV1ZsTldJd1lqRXlZMlEwWVRVMVlUQmhPVEkzWVdRMU9UQXVQTFFQNC9KYWNSbS9ZRUdqem9PdHkra0JvYitKU05uS3pHbURDYjFK
dnRoS2t3dEpKUEdyZEYzOTZTMHI; granicus_domain=InNlY3VyaXR5c2NhbnMucWEuZ3JhbmljdXMuY29tIg%3D%3D-
-69da4800213081d03801e5f53ff888c38638820a; login_failed=1

x-csrf-token: wqn2i+gQSpr2ugynj2cggzpCnlOJI3cFz0/4u4a2n+871FcjEns1KRjfOMcacwrak1xZd7/2169/vgu5IBh8JA==

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36

Host: securityscans.qa.granicus.com

Connection: Keep-alive
```

TLS/SSL (EC)DHE Key Reuse

Severity	**Informational**
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The remote host reuses Diffie-Hellman Ephemeral public server keys with (EC)DHE cipher suites.

Impact

Recommendation

Reconfigure the affected application to always generate new keys when using tmp_dh/tmp_ecdh parameters.

References

Raccoon Attack (https://raccoon-attack.com/)
Raccoon Attack (Technical Paper, PDF) (https://raccoon-attack.com/RacoonAttack.pdf)
Logjam Attack (https://weakdh.org/)
Logjam Attack (Technical Paper, PDF) (https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf)
List of SSL OP Flags (see: SSL_OP_SINGLE_DH_USE, SSL_OP_SINGLE_ECDH_USE) (https://wiki.openssl.org/index.php/List_of_SSL_OP_Flags)

Affected items

Web Server
Details
Diffie-Hellman Public Key Reuse: • ECDHE public server key reuse: 04 56 6b 75 53 a5 81 09 41 75 e7 ee f3 66 5a 8a bf cd 75 ff 73 e5 6b 23 f0 21 d6 67 67 90 45 2e 68 a2 2c cc 03 c5 d9 f2 f1 66 72 0b c4 f5 79 1b bd 19 dc 40 55 e6 91 86 1e 0c 65 fc 41 58 49 86 84 (with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256)
Request headers

Scanned items (coverage report)

https://securityscans.qa.granicus.com/
https://securityscans.qa.granicus.com/1&callback=
https://securityscans.qa.granicus.com/account/
https://securityscans.qa.granicus.com/account/forgotpassword
https://securityscans.qa.granicus.com/account/login
https://securityscans.qa.granicus.com/agenda_template_documents/
https://securityscans.qa.granicus.com/agenda_template_documents/preview.xml
https://securityscans.qa.granicus.com/AgendaViewer.php
https://securityscans.qa.granicus.com/api/
https://securityscans.qa.granicus.com/api/installed_applications
https://securityscans.qa.granicus.com/api/legislate/
https://securityscans.qa.granicus.com/api/legislate/agendas
https://securityscans.qa.granicus.com/api/legislate/agendas/
https://securityscans.qa.granicus.com/api/legislate/agendas/from-uids
https://securityscans.qa.granicus.com/api/legislate/videos
https://securityscans.qa.granicus.com/api/legislate/videos/
https://securityscans.qa.granicus.com/api/localtime
https://securityscans.qa.granicus.com/api/metrics/
https://securityscans.qa.granicus.com/api/metrics/cspreport
https://securityscans.qa.granicus.com/api/setting/
https://securityscans.qa.granicus.com/api/setting/cloudvoting_enable
https://securityscans.qa.granicus.com/api/setting/name
https://securityscans.qa.granicus.com/apps/
https://securityscans.qa.granicus.com/apps/peakagenda
https://securityscans.qa.granicus.com/apps/peakagenda/
https://securityscans.qa.granicus.com/appstorev2/
https://securityscans.qa.granicus.com/appstorev2/launch/
https://securityscans.qa.granicus.com/appstorev2/launch/boards/
https://securityscans.qa.granicus.com/appstorev2/launch/peakagenda/
https://securityscans.qa.granicus.com/appstorev2/storefront
https://securityscans.qa.granicus.com/Archives.php
https://securityscans.qa.granicus.com/auth/
https://securityscans.qa.granicus.com/auth/sessions
https://securityscans.qa.granicus.com/boards/
https://securityscans.qa.granicus.com/boards/.js
https://securityscans.qa.granicus.com/boards/.json
https://securityscans.qa.granicus.com/boards/admin
https://securityscans.qa.granicus.com/boards/admin/
https://securityscans.qa.granicus.com/boards/admin/answers/
https://securityscans.qa.granicus.com/boards/admin/answers/68373/
https://securityscans.qa.granicus.com/boards/admin/answers/68373/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68378/
https://securityscans.qa.granicus.com/boards/admin/answers/68378/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68379/
https://securityscans.qa.granicus.com/boards/admin/answers/68379/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68380/
https://securityscans.qa.granicus.com/boards/admin/answers/68380/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68381/
https://securityscans.qa.granicus.com/boards/admin/answers/68381/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68382/
https://securityscans.qa.granicus.com/boards/admin/answers/68382/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68383/
https://securityscans.qa.granicus.com/boards/admin/answers/68383/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68386/
https://securityscans.qa.granicus.com/boards/admin/answers/68386/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68387/
https://securityscans.qa.granicus.com/boards/admin/answers/68387/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68404/
https://securityscans.qa.granicus.com/boards/admin/answers/68404/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68405/
https://securityscans.qa.granicus.com/boards/admin/answers/68405/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68406/
https://securityscans.qa.granicus.com/boards/admin/answers/68406/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68407/
https://securityscans.qa.granicus.com/boards/admin/answers/68407/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68408/
https://securityscans.qa.granicus.com/boards/admin/answers/68408/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68409/
https://securityscans.qa.granicus.com/boards/admin/answers/68409/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68410/
https://securityscans.qa.granicus.com/boards/admin/answers/68410/attachment

https://securityscans.qa.granicus.com/boards/admin/answers/68411/
https://securityscans.qa.granicus.com/boards/admin/answers/68411/attachment
https://securityscans.qa.granicus.com/boards/admin/answers/68412/
https://securityscans.qa.granicus.com/boards/admin/answers/68412/attachment
https://securityscans.qa.granicus.com/boards/admin/applicants
https://securityscans.qa.granicus.com/boards/admin/applicants.js
https://securityscans.qa.granicus.com/boards/admin/applicants/
https://securityscans.qa.granicus.com/boards/admin/applicants/1/
https://securityscans.qa.granicus.com/boards/admin/applicants/1/reapply
https://securityscans.qa.granicus.com/boards/admin/applicants/20541/
https://securityscans.qa.granicus.com/boards/admin/applicants/20541/comments
https://securityscans.qa.granicus.com/boards/admin/applicants/20541/comments/
https://securityscans.qa.granicus.com/boards/admin/applicants/20541/comments/217
https://securityscans.qa.granicus.com/boards/admin/applicants/20541/comments/218
https://securityscans.qa.granicus.com/boards/admin/applicants/20541/reapply
https://securityscans.qa.granicus.com/boards/admin/applicants/20542/
https://securityscans.qa.granicus.com/boards/admin/applicants/20542/reapply
https://securityscans.qa.granicus.com/boards/admin/applicants/20966/
https://securityscans.qa.granicus.com/boards/admin/applicants/20966/reapply
https://securityscans.qa.granicus.com/boards/admin/applications/
https://securityscans.qa.granicus.com/boards/admin/applications/20
https://securityscans.qa.granicus.com/boards/admin/applications/20.js
https://securityscans.qa.granicus.com/boards/admin/appointments/
https://securityscans.qa.granicus.com/boards/admin/appointments/search
https://securityscans.qa.granicus.com/boards/admin/appointments/search.js
https://securityscans.qa.granicus.com/boards/admin/board_application_snapshots
https://securityscans.qa.granicus.com/boards/admin/board_roster_columns
https://securityscans.qa.granicus.com/boards/admin/board_roster_columns/
https://securityscans.qa.granicus.com/boards/admin/board_roster_columns/preview
https://securityscans.qa.granicus.com/boards/admin/boards
https://securityscans.qa.granicus.com/boards/admin/boards.csv
https://securityscans.qa.granicus.com/boards/admin/boards/
https://securityscans.qa.granicus.com/boards/admin/boards/9883
https://securityscans.qa.granicus.com/boards/admin/boards/9883.csv
https://securityscans.qa.granicus.com/boards/admin/boards/9883.js
https://securityscans.qa.granicus.com/boards/admin/boards/9883/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/attendance
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11944
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11944/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11944/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11945
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11945/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11945/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11948
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11949
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11949/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11949/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11950
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11950/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11950/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11951
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11951/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11951/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11952
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11952/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11952/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11953
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11953/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11953/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11954
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11954/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11954/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11955
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11955/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11955/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11957
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11957/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/11957/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12667
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12667/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12667/reappoint

https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12668
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12668/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12668/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12669
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12669/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12669/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12670
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12670/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12670/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12671
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12671/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12671/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12672
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12672/
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/12672/reappoint
https://securityscans.qa.granicus.com/boards/admin/boards/9883/members/new
https://securityscans.qa.granicus.com/boards/admin/boards/settings
https://securityscans.qa.granicus.com/boards/admin/custom_reports/
https://securityscans.qa.granicus.com/boards/admin/custom_reports/1136.json
https://securityscans.qa.granicus.com/boards/admin/dashboard
https://securityscans.qa.granicus.com/boards/admin/deleted_items
https://securityscans.qa.granicus.com/boards/admin/documents
https://securityscans.qa.granicus.com/boards/admin/documents/
https://securityscans.qa.granicus.com/boards/admin/documents/16859
https://securityscans.qa.granicus.com/boards/admin/documents/16859/
https://securityscans.qa.granicus.com/boards/admin/documents/16859/attachment
https://securityscans.qa.granicus.com/boards/admin/documents/51476
https://securityscans.qa.granicus.com/boards/admin/documents/51477
https://securityscans.qa.granicus.com/boards/admin/documents/51478
https://securityscans.qa.granicus.com/boards/admin/documents/51479
https://securityscans.qa.granicus.com/boards/admin/documents/52649
https://securityscans.qa.granicus.com/boards/admin/documents/52650
https://securityscans.qa.granicus.com/boards/admin/documents/52651
https://securityscans.qa.granicus.com/boards/admin/documents/52652
https://securityscans.qa.granicus.com/boards/admin/documents/52653
https://securityscans.qa.granicus.com/boards/admin/documents/52654
https://securityscans.qa.granicus.com/boards/admin/documents/52655
https://securityscans.qa.granicus.com/boards/admin/documents/52656
https://securityscans.qa.granicus.com/boards/admin/documents/52657
https://securityscans.qa.granicus.com/boards/admin/documents/52658
https://securityscans.qa.granicus.com/boards/admin/documents/52659
https://securityscans.qa.granicus.com/boards/admin/documents/52660
https://securityscans.qa.granicus.com/boards/admin/documents/52661
https://securityscans.qa.granicus.com/boards/admin/documents/52662
https://securityscans.qa.granicus.com/boards/admin/documents/52663
https://securityscans.qa.granicus.com/boards/admin/documents/52664
https://securityscans.qa.granicus.com/boards/admin/documents/52665
https://securityscans.qa.granicus.com/boards/admin/documents/52666
https://securityscans.qa.granicus.com/boards/admin/documents/52667
https://securityscans.qa.granicus.com/boards/admin/documents/52668
https://securityscans.qa.granicus.com/boards/admin/documents/52669
https://securityscans.qa.granicus.com/boards/admin/documents/52670
https://securityscans.qa.granicus.com/boards/admin/documents/52671
https://securityscans.qa.granicus.com/boards/admin/documents/52672
https://securityscans.qa.granicus.com/boards/admin/documents/52673
https://securityscans.qa.granicus.com/boards/admin/documents/52674
https://securityscans.qa.granicus.com/boards/admin/documents/52675
https://securityscans.qa.granicus.com/boards/admin/documents/52676
https://securityscans.qa.granicus.com/boards/admin/documents/52677
https://securityscans.qa.granicus.com/boards/admin/documents/52678
https://securityscans.qa.granicus.com/boards/admin/documents/new
https://securityscans.qa.granicus.com/boards/admin/email_templates
https://securityscans.qa.granicus.com/boards/admin/emails
https://securityscans.qa.granicus.com/boards/admin/jurisdictions/
https://securityscans.qa.granicus.com/boards/admin/jurisdictions/1.js
https://securityscans.qa.granicus.com/boards/admin/meetings
https://securityscans.qa.granicus.com/boards/admin/meetings.js
https://securityscans.qa.granicus.com/boards/admin/meetings/
https://securityscans.qa.granicus.com/boards/admin/meetings/11907/
https://securityscans.qa.granicus.com/boards/admin/meetings/11907/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11907/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11908/
https://securityscans.qa.granicus.com/boards/admin/meetings/11908/attendance

https://securityscans.qa.granicus.com/boards/admin/meetings/11963/
https://securityscans.qa.granicus.com/boards/admin/meetings/11963/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11964/
https://securityscans.qa.granicus.com/boards/admin/meetings/11964/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11965/
https://securityscans.qa.granicus.com/boards/admin/meetings/11965/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11966/
https://securityscans.qa.granicus.com/boards/admin/meetings/11966/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11967/
https://securityscans.qa.granicus.com/boards/admin/meetings/11967/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11968/
https://securityscans.qa.granicus.com/boards/admin/meetings/11968/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11969/
https://securityscans.qa.granicus.com/boards/admin/meetings/11969/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11970/
https://securityscans.qa.granicus.com/boards/admin/meetings/11970/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11970/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11971/
https://securityscans.qa.granicus.com/boards/admin/meetings/11971/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11971/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11972/
https://securityscans.qa.granicus.com/boards/admin/meetings/11972/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11972/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11973/
https://securityscans.qa.granicus.com/boards/admin/meetings/11973/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11973/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11974/
https://securityscans.qa.granicus.com/boards/admin/meetings/11974/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11974/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11975/
https://securityscans.qa.granicus.com/boards/admin/meetings/11975/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11975/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11976/
https://securityscans.qa.granicus.com/boards/admin/meetings/11976/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11976/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11979/
https://securityscans.qa.granicus.com/boards/admin/meetings/11979/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11979/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11980/
https://securityscans.qa.granicus.com/boards/admin/meetings/11980/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11980/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11981/
https://securityscans.qa.granicus.com/boards/admin/meetings/11981/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11981/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11982/
https://securityscans.qa.granicus.com/boards/admin/meetings/11982/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11982/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11983/
https://securityscans.qa.granicus.com/boards/admin/meetings/11983/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11983/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11984/
https://securityscans.qa.granicus.com/boards/admin/meetings/11984/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11984/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11985/
https://securityscans.qa.granicus.com/boards/admin/meetings/11985/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11985/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11986/
https://securityscans.qa.granicus.com/boards/admin/meetings/11986/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11986/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11987/
https://securityscans.qa.granicus.com/boards/admin/meetings/11987/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11987/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11988/
https://securityscans.qa.granicus.com/boards/admin/meetings/11988/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11988/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11989/
https://securityscans.qa.granicus.com/boards/admin/meetings/11989/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11989/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11990/
https://securityscans.qa.granicus.com/boards/admin/meetings/11990/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11990/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11991/
https://securityscans.qa.granicus.com/boards/admin/meetings/11991/attendance

https://securityscans.qa.granicus.com/boards/admin/meetings/11991/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11992/
https://securityscans.qa.granicus.com/boards/admin/meetings/11992/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11992/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11993/
https://securityscans.qa.granicus.com/boards/admin/meetings/11993/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11993/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11994/
https://securityscans.qa.granicus.com/boards/admin/meetings/11994/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11994/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11995/
https://securityscans.qa.granicus.com/boards/admin/meetings/11995/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11995/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11996/
https://securityscans.qa.granicus.com/boards/admin/meetings/11996/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11996/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11997/
https://securityscans.qa.granicus.com/boards/admin/meetings/11997/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11997/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11998/
https://securityscans.qa.granicus.com/boards/admin/meetings/11998/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11998/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/11999/
https://securityscans.qa.granicus.com/boards/admin/meetings/11999/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/11999/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12000/
https://securityscans.qa.granicus.com/boards/admin/meetings/12000/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12000/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12001/
https://securityscans.qa.granicus.com/boards/admin/meetings/12001/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12001/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12002/
https://securityscans.qa.granicus.com/boards/admin/meetings/12002/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12002/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12003/
https://securityscans.qa.granicus.com/boards/admin/meetings/12003/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12003/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12004/
https://securityscans.qa.granicus.com/boards/admin/meetings/12004/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12004/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12005/
https://securityscans.qa.granicus.com/boards/admin/meetings/12005/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12006/
https://securityscans.qa.granicus.com/boards/admin/meetings/12006/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12007/
https://securityscans.qa.granicus.com/boards/admin/meetings/12007/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12008/
https://securityscans.qa.granicus.com/boards/admin/meetings/12008/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12009/
https://securityscans.qa.granicus.com/boards/admin/meetings/12009/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12010/
https://securityscans.qa.granicus.com/boards/admin/meetings/12010/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12010/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12011/
https://securityscans.qa.granicus.com/boards/admin/meetings/12011/attendance
https://securityscans.qa.granicus.com/boards/admin/meetings/12011/edit
https://securityscans.qa.granicus.com/boards/admin/meetings/12012/
https://securityscans.qa.granicus.com/boards/admin/meetings/12012/attendance
https://securityscans.qa.granicus.com/boards/admin/members
https://securityscans.qa.granicus.com/boards/admin/members.js
https://securityscans.qa.granicus.com/boards/admin/members/
https://securityscans.qa.granicus.com/boards/admin/members/11944.js
https://securityscans.qa.granicus.com/boards/admin/members/11944/
https://securityscans.qa.granicus.com/boards/admin/members/11944/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11945/
https://securityscans.qa.granicus.com/boards/admin/members/11945/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11949/
https://securityscans.qa.granicus.com/boards/admin/members/11949/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11950/
https://securityscans.qa.granicus.com/boards/admin/members/11950/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11951/
https://securityscans.qa.granicus.com/boards/admin/members/11951/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11952/

https://securityscans.qa.granicus.com/boards/admin/members/11952/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11953/
https://securityscans.qa.granicus.com/boards/admin/members/11953/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11954.js
https://securityscans.qa.granicus.com/boards/admin/members/11954/
https://securityscans.qa.granicus.com/boards/admin/members/11954/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11955/
https://securityscans.qa.granicus.com/boards/admin/members/11955/vacate
https://securityscans.qa.granicus.com/boards/admin/members/11957/
https://securityscans.qa.granicus.com/boards/admin/members/11957/vacate
https://securityscans.qa.granicus.com/boards/admin/members/12667/
https://securityscans.qa.granicus.com/boards/admin/members/12667/vacate
https://securityscans.qa.granicus.com/boards/admin/members/12668/
https://securityscans.qa.granicus.com/boards/admin/members/12668/vacate
https://securityscans.qa.granicus.com/boards/admin/members/12669/
https://securityscans.qa.granicus.com/boards/admin/members/12669/vacate
https://securityscans.qa.granicus.com/boards/admin/members/12670/
https://securityscans.qa.granicus.com/boards/admin/members/12670/vacate
https://securityscans.qa.granicus.com/boards/admin/members/12671.js
https://securityscans.qa.granicus.com/boards/admin/members/12671/
https://securityscans.qa.granicus.com/boards/admin/members/12671/vacate
https://securityscans.qa.granicus.com/boards/admin/members/12672/
https://securityscans.qa.granicus.com/boards/admin/members/12672/vacate
https://securityscans.qa.granicus.com/boards/admin/members/all/
https://securityscans.qa.granicus.com/boards/admin/members/all/csv
https://securityscans.qa.granicus.com/boards/admin/members/csv.csv
https://securityscans.qa.granicus.com/boards/admin/members/reapply
https://securityscans.qa.granicus.com/boards/admin/packets
https://securityscans.qa.granicus.com/boards/admin/packets/
https://securityscans.qa.granicus.com/boards/admin/packets/29766/
https://securityscans.qa.granicus.com/boards/admin/packets/29766/edit
https://securityscans.qa.granicus.com/boards/admin/people
https://securityscans.qa.granicus.com/boards/admin/settings
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68373
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68378
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68379
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68380
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68381
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68382
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68383
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68386
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68387
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68404
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68405
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68406
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68407
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68408
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68409
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68410
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68411
https://securityscans.qa.granicus.com/boards/admin/tracking_forms/20/applications/20541/jurisdiction_questions/68412
https://securityscans.qa.granicus.com/boards/admin/user_applications/
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/5245/
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/5245/answer
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/5246/
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/5246/answer
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/5383/
https://securityscans.qa.granicus.com/boards/admin/user_applications/20541/jurisdiction_questions/5383/answer
https://securityscans.qa.granicus.com/boards/admin/user_permissions
https://securityscans.qa.granicus.com/boards/admin/user_permissions/
https://securityscans.qa.granicus.com/boards/admin/view_customizers/
https://securityscans.qa.granicus.com/boards/admin/widgets/
https://securityscans.qa.granicus.com/boards/admin/widgets/new
https://securityscans.qa.granicus.com/boards/apply/

https://securityscans.qa.granicus.com/boards/assets/
https://securityscans.qa.granicus.com/boards/forms/
https://securityscans.qa.granicus.com/boards/forms/20/
https://securityscans.qa.granicus.com/boards/forms/20/apply/
https://securityscans.qa.granicus.com/boards/forms/20/apply/20541
https://securityscans.qa.granicus.com/boards/forms/20/apply/20542
https://securityscans.qa.granicus.com/boards/forms/20/apply/20966
https://securityscans.qa.granicus.com/boards/forms/20/apply/30635
https://securityscans.qa.granicus.com/boards/forms/20/apply/30667
https://securityscans.qa.granicus.com/boards/forms/8/
https://securityscans.qa.granicus.com/boards/forms/8/apply/
https://securityscans.qa.granicus.com/boards/forms/8/apply/1
https://securityscans.qa.granicus.com/boards/superadmin/
https://securityscans.qa.granicus.com/boards/superadmin/people/
https://securityscans.qa.granicus.com/boards/superadmin/people/merge
https://securityscans.qa.granicus.com/boards/v1/
https://securityscans.qa.granicus.com/boards/v1/16/
https://securityscans.qa.granicus.com/boards/v1/16/stats
https://securityscans.qa.granicus.com/boards/v1/securityscans.qa/
https://securityscans.qa.granicus.com/boards/v1/securityscans.qa/stats
https://securityscans.qa.granicus.com/Cameras.php
https://securityscans.qa.granicus.com/check_expired
https://securityscans.qa.granicus.com/citizen/
https://securityscans.qa.granicus.com/citizen/info
https://securityscans.qa.granicus.com/core/
https://securityscans.qa.granicus.com/core/_cassette/
https://securityscans.qa.granicus.com/core/_cassette/file/
https://securityscans.qa.granicus.com/core/_cassette/file/images/
https://securityscans.qa.granicus.com/core/_cassette/htmltemplatebundle/
https://securityscans.qa.granicus.com/core/_cassette/htmltemplatebundle/Templates_dcfa11957c59c6f85148a4c66ce8a89f13338989
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Backbone_72d26839b5b5558f06424a7dc001cbe59ffaf516
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/backbone_4e59838d3d609c9df1658a2ee8bcd03432390896
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/cookies_2913dd63b0ee72a0e46fbef03ce4af2af378e58a
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/fancybox_98171c838dea7c7d51eec2837979da4eafe6401e
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jquery-ui_e045cf3abc14f3d1489828d51a47dd8fb10db197
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jquery_6dcf74cd635ac06a8b9efc7c0c711d7cf7a38110
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/jt-jquery-timepicker_10ff10c949a1e36e4ca06eddc88b49dbed10fbe8
https://securityscans.qa.granicus.com/core/_cassette/scriptbundle/Lib/moment_e6830a8752ff3dab3e0cb822adcd74eddb5caba4
https://securityscans.qa.granicus.com/core/_cassette/stylesheetbundle/
https://securityscans.qa.granicus.com/core/_cassette/stylesheetbundle/Stylesheets/
https://securityscans.qa.granicus.com/core/_cassette/stylesheetbundle/Stylesheets/Events_8918e04e4aeb6bd72d9646d58550e3215906f9c2
https://securityscans.qa.granicus.com/core/_cassette/stylesheetbundle/Stylesheets/images/
https://securityscans.qa.granicus.com/core/admin/
https://securityscans.qa.granicus.com/core/admin/camera/
https://securityscans.qa.granicus.com/core/admin/camera/EditH264Distribution.aspx
https://securityscans.qa.granicus.com/core/admin/camera/js/
https://securityscans.qa.granicus.com/core/admin/templates/
https://securityscans.qa.granicus.com/core/App_Themes/
https://securityscans.qa.granicus.com/core/App_Themes/404/
https://securityscans.qa.granicus.com/core/App_Themes/404/404.css
https://securityscans.qa.granicus.com/core/App_Themes/Default/
https://securityscans.qa.granicus.com/core/App_Themes/default/authentication.css
https://securityscans.qa.granicus.com/core/App_Themes/Default/images/
https://securityscans.qa.granicus.com/core/App_Themes/default/images/PIE.htc
https://securityscans.qa.granicus.com/core/App_Themes/MediaManager/
https://securityscans.qa.granicus.com/core/App_Themes/MediaManager/images/
https://securityscans.qa.granicus.com/core/error/
https://securityscans.qa.granicus.com/core/error/Error.aspx
https://securityscans.qa.granicus.com/core/error/NotFound.aspx
https://securityscans.qa.granicus.com/core/EventsPage.aspx
https://securityscans.qa.granicus.com/core/Fonts/
https://securityscans.qa.granicus.com/core/Home.aspx
https://securityscans.qa.granicus.com/core/Images/
https://securityscans.qa.granicus.com/core/Images/help/
https://securityscans.qa.granicus.com/core/Lib/
https://securityscans.qa.granicus.com/core/Lib/css/
https://securityscans.qa.granicus.com/core/Lib/css/ie7.css
https://securityscans.qa.granicus.com/core/Lib/css/ie8.css
https://securityscans.qa.granicus.com/core/Lib/custom/
https://securityscans.qa.granicus.com/core/Lib/custom/StartStopUtilities.js
https://securityscans.qa.granicus.com/core/ScriptResource.axd

https://securityscans.qa.granicus.com/core/services/
https://securityscans.qa.granicus.com/core/services/authenticated/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/cameraservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/cameraservice.svc/lightweightList
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/eventseriesservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/eventseriesservice.svc/eventseries
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/eventservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/eventservice.svc/event
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/folderservice.svc/LightweightList/meeting
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/sitesettingsservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/sitesettingsservice.svc/motionactions
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/templateservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/templateservice.svc/LightweightList/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/templateservice.svc/LightweightList/document
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/templateservice.svc/LightweightList/player
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/viewservice.svc/
https://securityscans.qa.granicus.com/core/services/authenticated/infrastructure/viewservice.svc/view
https://securityscans.qa.granicus.com/core/WebResource.axd
https://securityscans.qa.granicus.com/crossdomain.xml
https://securityscans.qa.granicus.com/css/
https://securityscans.qa.granicus.com/css/app_switcher.css
https://securityscans.qa.granicus.com/css/authentication.css
https://securityscans.qa.granicus.com/css/img/
https://securityscans.qa.granicus.com/css/non-responsive.css
https://securityscans.qa.granicus.com/css/Widget.css
https://securityscans.qa.granicus.com/Date(1621553523000-0500)/
https://securityscans.qa.granicus.com/DeleteFolder.php
https://securityscans.qa.granicus.com/DeleteView.php
https://securityscans.qa.granicus.com/EditCameraBasic.php
https://securityscans.qa.granicus.com/EditCameraDistribution.php
https://securityscans.qa.granicus.com/EditCameraPermission.php
https://securityscans.qa.granicus.com/EditCameraPublish.php
https://securityscans.qa.granicus.com/EditFile.php
https://securityscans.qa.granicus.com/EditFolderBasic.php
https://securityscans.qa.granicus.com/EditFolderDistribution.php
https://securityscans.qa.granicus.com/EditFolderPermission.php
https://securityscans.qa.granicus.com/EditTemplateBasic.php
https://securityscans.qa.granicus.com/EditTemplateDesigner.php
https://securityscans.qa.granicus.com/EditTemplateEditor.php
https://securityscans.qa.granicus.com/EditTemplatePermission.php
https://securityscans.qa.granicus.com/EditTemplateRevisions.php
https://securityscans.qa.granicus.com/EditViewAccess.php
https://securityscans.qa.granicus.com/EditViewBasic.php
https://securityscans.qa.granicus.com/EditViewContents.php
https://securityscans.qa.granicus.com/EditViewPermission.php
https://securityscans.qa.granicus.com/Events.php
https://securityscans.qa.granicus.com/images/
https://securityscans.qa.granicus.com/images/help/
https://securityscans.qa.granicus.com/images/icons/
https://securityscans.qa.granicus.com/images/navbar/
https://securityscans.qa.granicus.com/index
https://securityscans.qa.granicus.com/index.php
https://securityscans.qa.granicus.com/js/
https://securityscans.qa.granicus.com/js/gat.js
https://securityscans.qa.granicus.com/js/jquery-cookie.js
https://securityscans.qa.granicus.com/js/jquery-pm.min.js
https://securityscans.qa.granicus.com/js/widgetscript.js
https://securityscans.qa.granicus.com/JSON.php
https://securityscans.qa.granicus.com/legislate
https://securityscans.qa.granicus.com/legislate/
https://securityscans.qa.granicus.com/legislate/agendas
https://securityscans.qa.granicus.com/legislate/agendas/
https://securityscans.qa.granicus.com/legislate/agendas/47c8f935-7333-4e3a-8327-9930ebea3dd3
https://securityscans.qa.granicus.com/legislate/agendas/864de390-eabb-4516-8016-12b2b9c22858
https://securityscans.qa.granicus.com/legislate/api/
https://securityscans.qa.granicus.com/legislate/api/agendas/
https://securityscans.qa.granicus.com/legislate/api/agendas/47c8f935-7333-4e3a-8327-9930ebea3dd3
https://securityscans.qa.granicus.com/legislate/api/agendas/864de390-eabb-4516-8016-12b2b9c22858
https://securityscans.qa.granicus.com/legislate/api/agendas/node_modules/
https://securityscans.qa.granicus.com/legislate/api/agendas/node_modules/pspdfkit/

https://securityscans.qa.granicus.com/legislate/api/agendas/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/api/agendas/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/api/bookmarks
https://securityscans.qa.granicus.com/legislate/api/bookmarks/
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/47c8f935-7333-4e3a-8327-9930ebea3dd3
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/864de390-eabb-4516-8016-12b2b9c22858
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/node_modules/
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/api/bookmarks/agenda/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/api/council_notes
https://securityscans.qa.granicus.com/legislate/api/council_notes/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/47c8f935-7333-4e3a-8327-9930ebea3dd3
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/864de390-eabb-4516-8016-12b2b9c22858
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/psp
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/api/council_notes/agenda/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/api/node_modules/
https://securityscans.qa.granicus.com/legislate/api/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/api/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/api/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/api/user
https://securityscans.qa.granicus.com/legislate/bookmarks
https://securityscans.qa.granicus.com/legislate/forgot_password
https://securityscans.qa.granicus.com/legislate/icons/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modu
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modu
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modu
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modu
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/icons/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/login
https://securityscans.qa.granicus.com/legislate/logout
https://securityscans.qa.granicus.com/legislate/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/node_modules/pspdfkit/dist/pspdfkit.js

https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/n
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/n
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/n
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/p
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/d
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/node_modules/pspdfkit/node_modules/pspdfkit/d
https://securityscans.qa.granicus.com/legislate/node_modules/pspdfkit/node_modules/pspdfkit/dist/pspdfkit.js
https://securityscans.qa.granicus.com/legislate/notes
https://securityscans.qa.granicus.com/legislate/pwa.js
https://securityscans.qa.granicus.com/legislate/sw.js
https://securityscans.qa.granicus.com/legislate/videos
https://securityscans.qa.granicus.com/legislate/webmanifest.json
https://securityscans.qa.granicus.com/legistar
https://securityscans.qa.granicus.com/legistar/
https://securityscans.qa.granicus.com/legistar/dashboard.json
https://securityscans.qa.granicus.com/log
https://securityscans.qa.granicus.com/log.php
https://securityscans.qa.granicus.com/Log2.php
https://securityscans.qa.granicus.com/logout
https://securityscans.qa.granicus.com/MediaPlayer.php
https://securityscans.qa.granicus.com/myaccount.php
https://securityscans.qa.granicus.com/NewCamera.php
https://securityscans.qa.granicus.com/NewFolder.php
https://securityscans.qa.granicus.com/NewView.php
https://securityscans.qa.granicus.com/panes/
https://securityscans.qa.granicus.com/panes/ArchiveFiles.php
https://securityscans.qa.granicus.com/panes/ArchiveFilesRecycled.php
https://securityscans.qa.granicus.com/panes/ArchiveFolders.php
https://securityscans.qa.granicus.com/panes/Archives.php
https://securityscans.qa.granicus.com/panes/Calendar.html
https://securityscans.qa.granicus.com/panes/Cameras.php
https://securityscans.qa.granicus.com/panes/EditCameraBasic.php
https://securityscans.qa.granicus.com/panes/EditCameraPermission.php
https://securityscans.qa.granicus.com/panes/EditCameraPublishList.php
https://securityscans.qa.granicus.com/panes/EditFolderBasic.php
https://securityscans.qa.granicus.com/panes/EditFolderDistribution.php
https://securityscans.qa.granicus.com/panes/EditFolderPermission.php
https://securityscans.qa.granicus.com/panes/EditTemplateBasic.php
https://securityscans.qa.granicus.com/panes/EditTemplateEditor.php
https://securityscans.qa.granicus.com/panes/EditTemplatePermission.php

https://securityscans.qa.granicus.com/panes/EditTemplateRevisions.php
https://securityscans.qa.granicus.com/panes/EditViewAccess.php
https://securityscans.qa.granicus.com/panes/EditViewBasic.php
https://securityscans.qa.granicus.com/panes/EditViewContents.php
https://securityscans.qa.granicus.com/panes/EditViewPermission.php
https://securityscans.qa.granicus.com/panes/groups.php
https://securityscans.qa.granicus.com/panes/Logout.php
https://securityscans.qa.granicus.com/panes/logs.php
https://securityscans.qa.granicus.com/panes/NewCamera.php
https://securityscans.qa.granicus.com/panes/NewFolder.php
https://securityscans.qa.granicus.com/panes/NewView.php
https://securityscans.qa.granicus.com/panes/PermissionDenied.php
https://securityscans.qa.granicus.com/panes/SearchResults.php
https://securityscans.qa.granicus.com/panes/Servers.php
https://securityscans.qa.granicus.com/panes/SiteSettings.php
https://securityscans.qa.granicus.com/panes/sso.php
https://securityscans.qa.granicus.com/panes/Templates.php
https://securityscans.qa.granicus.com/panes/Views.php
https://securityscans.qa.granicus.com/player/
https://securityscans.qa.granicus.com/player/camera/
https://securityscans.qa.granicus.com/player/camera/1
https://securityscans.qa.granicus.com/profile
https://securityscans.qa.granicus.com/profile/
https://securityscans.qa.granicus.com/profile/process
https://securityscans.qa.granicus.com/Reports.php
https://securityscans.qa.granicus.com/robots.txt
https://securityscans.qa.granicus.com/SearchResults.php
https://securityscans.qa.granicus.com/servers
https://securityscans.qa.granicus.com/Servers.php
https://securityscans.qa.granicus.com/services/
https://securityscans.qa.granicus.com/services/agendas/
https://securityscans.qa.granicus.com/services/agendas/schema.json
https://securityscans.qa.granicus.com/services/boards/
https://securityscans.qa.granicus.com/services/boards/appointments/
https://securityscans.qa.granicus.com/services/boards/appointments/show_with_offices
https://securityscans.qa.granicus.com/services/boards/boards/
https://securityscans.qa.granicus.com/services/boards/people/
https://securityscans.qa.granicus.com/services/boards/users/
https://securityscans.qa.granicus.com/services/boards/users/fefce60e-b06f-4268-ab6a-486c4d9b2f0c/
https://securityscans.qa.granicus.com/services/boards/users/fefce60e-b06f-4268-ab6a-486c4d9b2f0c/person
https://securityscans.qa.granicus.com/services/events
https://securityscans.qa.granicus.com/services/events/
https://securityscans.qa.granicus.com/services/events/templates
https://securityscans.qa.granicus.com/services/folders
https://securityscans.qa.granicus.com/services/items/
https://securityscans.qa.granicus.com/services/items/coverpage/
https://securityscans.qa.granicus.com/services/items/coverpage/schema.json
https://securityscans.qa.granicus.com/services/items/coverpages_for_future_meetings
https://securityscans.qa.granicus.com/services/items/update_html_coverpages_for_future_meetings
https://securityscans.qa.granicus.com/services/legistar/
https://securityscans.qa.granicus.com/services/legistar/agenda_template_documents
https://securityscans.qa.granicus.com/services/legistar/approvals/
https://securityscans.qa.granicus.com/services/legistar/attachments/
https://securityscans.qa.granicus.com/services/legistar/attachments/attachmentIDs
https://securityscans.qa.granicus.com/services/legistar/custom_item_fields/
https://securityscans.qa.granicus.com/services/legistar/departments/
https://securityscans.qa.granicus.com/services/legistar/html_agenda_templates/
https://securityscans.qa.granicus.com/services/legistar/html_coverpage_templates/
https://securityscans.qa.granicus.com/services/legistar/id_formatters/
https://securityscans.qa.granicus.com/services/legistar/item_packets/
https://securityscans.qa.granicus.com/services/legistar/item_type_custom_item_fields/
https://securityscans.qa.granicus.com/services/legistar/item_type_settings/
https://securityscans.qa.granicus.com/services/legistar/item_type_settings/default_settings
https://securityscans.qa.granicus.com/services/legistar/item_types/
https://securityscans.qa.granicus.com/services/legistar/items/
https://securityscans.qa.granicus.com/services/legistar/items/1/
https://securityscans.qa.granicus.com/services/legistar/items/1/attachments
https://securityscans.qa.granicus.com/services/legistar/meeting_types
https://securityscans.qa.granicus.com/services/legistar/meetings/
https://securityscans.qa.granicus.com/services/legistar/meetings/used_meeting_statuses
https://securityscans.qa.granicus.com/services/legistar/setting/
https://securityscans.qa.granicus.com/services/legistar/site
https://securityscans.qa.granicus.com/services/legistar/site/

https://securityscans.qa.granicus.com/services/legistar/v2/
https://securityscans.qa.granicus.com/services/legistar/v2/active_item_templates
https://securityscans.qa.granicus.com/services/legistar/v2/default_item_template
https://securityscans.qa.granicus.com/services/legistar/v2/item_coverpage_templates
https://securityscans.qa.granicus.com/services/legistar/v2/item_coverpage_templates/
https://securityscans.qa.granicus.com/services/legistar/v2/item_templates/
https://securityscans.qa.granicus.com/services/legistar/v2/items/
https://securityscans.qa.granicus.com/services/legistar/v2/items/expire_access
https://securityscans.qa.granicus.com/services/meeting_statuses
https://securityscans.qa.granicus.com/services/meeting_types
https://securityscans.qa.granicus.com/services/minutes/
https://securityscans.qa.granicus.com/services/minutes/agendas
https://securityscans.qa.granicus.com/services/minutes/agendas/
https://securityscans.qa.granicus.com/services/minutes/agendas/by_meeting_guid.json
https://securityscans.qa.granicus.com/services/minutes/agendas/schema.json
https://securityscans.qa.granicus.com/services/minutes/assets/
https://securityscans.qa.granicus.com/services/minutes/assets/application-859f7402b5a18e898f824b6b69bf8e43521e11f27cba65f1d699855dbcc6ad37.css
https://securityscans.qa.granicus.com/services/minutes/assets/ui/
https://securityscans.qa.granicus.com/services/minutes/assets/ui/css/
https://securityscans.qa.granicus.com/services/minutes/assets/ui/css/legislate-fb5a229d.css
https://securityscans.qa.granicus.com/services/minutes/assets/ui/js/
https://securityscans.qa.granicus.com/services/minutes/assets/ui/js/application-73c4ff04cedd4051aaac.js
https://securityscans.qa.granicus.com/services/minutes/assets/ui/js/legislate-bbc5c6e3b5f20c44f4f2.js
https://securityscans.qa.granicus.com/services/minutes/assets/ui/media/
https://securityscans.qa.granicus.com/services/minutes/assets/ui/media/lib/
https://securityscans.qa.granicus.com/services/minutes/meeting_statuses.json
https://securityscans.qa.granicus.com/services/minutes/meeting_statuses/
https://securityscans.qa.granicus.com/services/minutes/motion_results.json
https://securityscans.qa.granicus.com/services/minutes/motion_results/
https://securityscans.qa.granicus.com/services/minutes/motion_types
https://securityscans.qa.granicus.com/services/minutes/motion_types.json
https://securityscans.qa.granicus.com/services/minutes/report_templates
https://securityscans.qa.granicus.com/services/minutes/report_templates/
https://securityscans.qa.granicus.com/services/minutes/voting_configurations.json
https://securityscans.qa.granicus.com/services/permissions/
https://securityscans.qa.granicus.com/services/permissions/groups
https://securityscans.qa.granicus.com/services/permissions/users
https://securityscans.qa.granicus.com/services/template_builder/
https://securityscans.qa.granicus.com/services/template_builder/templates
https://securityscans.qa.granicus.com/services/template_settings/
https://securityscans.qa.granicus.com/services/template_settings/upload_url
https://securityscans.qa.granicus.com/services/views
https://securityscans.qa.granicus.com/SiteSettings.php
https://securityscans.qa.granicus.com/SSO.php
https://securityscans.qa.granicus.com/Templates.php
https://securityscans.qa.granicus.com/templates/
https://securityscans.qa.granicus.com/templates/1386/
https://securityscans.qa.granicus.com/templates/1386/designer
https://securityscans.qa.granicus.com/templates/1386/settings
https://securityscans.qa.granicus.com/UndeleteFile.php
https://securityscans.qa.granicus.com/users/
https://securityscans.qa.granicus.com/users/groups.php
https://securityscans.qa.granicus.com/Users2.php
https://securityscans.qa.granicus.com/Views.php