

Developer Report

Acunetix Security Audit

2025-08-06

Scan of ap.tnnua.edu.tw

Scan details

Scan information	
Start time	2025-08-06T00:08:52.128541+08:00
Start url	https://ap.tnnua.edu.tw/Teacher/
Host	ap.tnnua.edu.tw
Scan time	15 minutes, 48 seconds
Profile	Full Scan
Responsive	True
Server OS	Windows
Server technologies	ASP.NET,ASP.NET
Application build	25.4.250417124

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	22
 Critical	0
 High	1
 Medium	15
 Low	2
 Informational	4

Alerts summary

 Insecure Transportation Security Protocol Supported (TLS 1.0)

Classification		
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/SA:N Base Score: 6.3 Attack Vector: Network Attack Complexity: High 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: Low Integrity Impact to the Subsequent System: Low Availability Impact to the Subsequent System: None	
CVSS3	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None	
CVSS2	Base Score: 5.8 Access Vector: Network_accessible 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-326	
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 UI Cross-site Scripting (XSS) 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
CVE	CVE-2016-7103

Affected items	Variation
Web Server	1

 JQuery UI Cross-site Scripting (XSS) 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
CVE	CVE-2016-7103
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

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	3

▼ **ASP.NET debugging enabled**

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-11
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

 Content Security Policy (CSP) 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

 Insecure Transportation Security Protocol Supported (TLS 1.1)

Classification	
CVSS4	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:N/SA:N Base Score: 6.3 Attack Vector: Network Attack Complexity: High 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: Low 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:N/S:C/C:L/I:L/A:N Base Score: 5.4 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None

CVSS2	Base Score: 5.8 Access Vector: Network_accessible 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-326
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	1

 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	

Alerts details

Insecure Transportation Security Protocol Supported (TLS 1.0)

Severity	High
Reported by module	/Scripts/PerServer/SSL_Audit.script

Description

The web server supports encryption through TLS 1.0, which was formally deprecated in March 2021 as a result of inherent security issues. In addition, TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

References

[RFC 8996: Deprecating TLS 1.0 and TLS 1.1](https://tools.ietf.org/html/rfc8996) (<https://tools.ietf.org/html/rfc8996>)

[Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls) (<https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls>)

[PCI 3.1 and TLS 1.2 \(Cloudflare Support\)](https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2) (<https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2>)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.0.
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 accessible 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) (<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://ap.tnnua.edu.tw/Teacher/ - https://ap.tnnua.edu.tw/teacher/ErrorPage.aspx - https://ap.tnnua.edu.tw/Teacher/login.aspx
Request headers
GET /Teacher/ HTTP/1.1
Referer: https://ap.tnnua.edu.tw/Teacher/
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/135.0.0.0 Safari/537.36
Host: ap.tnnua.edu.tw
Connection: Keep-alive

 JQuery UI Cross-site Scripting (XSS) Vulnerability

Severity	Medium
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

Impact

Recommendation

References

[CVE-2016-7103](https://nvd.nist.gov/vuln/detail/CVE-2016-7103) (<https://nvd.nist.gov/vuln/detail/CVE-2016-7103>)
[CVE-2016-7103](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>)

Affected items

Web Server
Details
jquery-ui-dialog v1.11.4-1.11.4
Request headers

⬆️ JQuery UI Cross-site Scripting (XSS) Vulnerability

Severity	Medium
Reported by module	/deepscan/javascript_library_audit_deepscan.js

Description

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

Impact

Recommendation

References

[CVE-2016-7103](https://nvd.nist.gov/vuln/detail/CVE-2016-7103) (<https://nvd.nist.gov/vuln/detail/CVE-2016-7103>)
[CVE-2016-7103](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>)

Affected items

Web Server
Details
jquery-ui-tooltip v1.11.4-1.11.4
Request headers

⬆️ jQuery UI Dialog 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 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) (<https://nvd.nist.gov/vuln/detail/CVE-2022-31160>)
[CVE-2022-31160](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160>)

Affected items

Web Server
Details
jquery-ui-dialog v1.11.4-1.11.4
Request headers

jQuery UI Dialog 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-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) (<https://nvd.nist.gov/vuln/detail/CVE-2021-41183>)
[CVE-2021-41183](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183>)

Affected items

Web Server
Details
jquery-ui-dialog v1.11.4-1.11.4
Request headers

jQuery UI Dialog 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-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) (<https://nvd.nist.gov/vuln/detail/CVE-2021-41182>)
[CVE-2021-41182](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41182) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41182>)

Affected items

Web Server
Details
jquery-ui-dialog v1.11.4-1.11.4
Request headers

 jQuery UI Dialog 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-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) (<https://nvd.nist.gov/vuln/detail/CVE-2021-41184>)
[CVE-2021-41184](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184>)

Affected items

Web Server
Details
jquery-ui-dialog v1.11.4-1.11.4
Request headers

jQuery UI Tooltip 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 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) (<https://nvd.nist.gov/vuln/detail/CVE-2022-31160>)
[CVE-2022-31160](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160>)

Affected items

Web Server
Details
jquery-ui-tooltip v1.11.4-1.11.4
Request headers

jQuery UI Tooltip 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-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) (<https://nvd.nist.gov/vuln/detail/CVE-2021-41184>)
[CVE-2021-41184](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184>)

Affected items

Web Server
Details
jquery-ui-tooltip v1.11.4-1.11.4
Request headers

jQuery UI Tooltip 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-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) (<https://nvd.nist.gov/vuln/detail/CVE-2021-41183>)
- [CVE-2021-41183](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183) (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183>)

Affected items

Web Server
Details
jquery-ui-tooltip v1.11.4-1.11.4
Request headers

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

Affected items

Web Server
Details
jquery-ui-tooltip v1.11.4-1.11.4
Request headers

 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)
(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)
(https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)
[Mozilla: TLS Cipher Suite Recommendations](https://wiki.mozilla.org/Security/Server_Side_TLS) (https://wiki.mozilla.org/Security/Server_Side_TLS)
[SSLabs: SSL and TLS Deployment Best Practices](https://github.com/ssllabs/research/wiki/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)
(https://datatracker.ietf.org/doc/html/rfc9155)

Affected items

Web Server
Details

Weak TLS/SSL Cipher Suites: (offered via TLS1.0 on port 443):

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

Weak TLS/SSL Cipher Suites: (offered via TLS1.1 on port 443):

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

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_256_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_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/) (https://www.invicti.com/support/how-invicti-identifies-outofdate/)

Affected items

Web Server

Details

- **jQuery UI Dialog 1.11.4**

- URL: <https://ap.tnnua.edu.tw/Teacher/>
- Detection method: The library's name and version were determined based on its dynamic behavior.
- CVE-ID: CVE-2016-7103
- Description: XSS in dialog closeText
- References:
 - <https://nodesecurity.io/advisories/127>
 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7103>
 - <https://www.cvedetails.com/cve/CVE-2016-7103/>

Request headers

GET /Teacher/ HTTP/1.1

Referer: <https://ap.tnnua.edu.tw/Teacher/>

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/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive

Web Server

Details

- **jQuery UI Datepicker 1.11.4**

- URL: <https://ap.tnnua.edu.tw/Teacher/>
- Detection method: The library's name and version were determined based on its dynamic behavior.
- CVE-ID: CVE-2021-41182, CVE-2021-41183
- Description: XSS in the 'altField' option of the Datepicker widget / XSS in '*Text' options of the Datepicker widget
- References:
 - <https://blog.jqueryui.com/2021/10/jquery-ui-1-13-0-released/>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc>
 - <https://github.com/jquery/jquery-ui/security/advisories/GHSA-j7qv-pgfh-hvh4>

Request headers

GET /Teacher/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/Teacher/

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/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive

Web Server

Verified vulnerability

Details

- **jQuery UI 1.11.4**

- URL: https://ap.tnnua.edu.tw/Teacher/Script/jquery-ui.js
- Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version and the associated vulnerabilities with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix.
- 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 /Teacher/Script/jquery-ui.js HTTP/1.1

Cookie: ASP.NET_SessionId=w0ro31sxlx3wx3kbsss1oznn

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/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive

✎ ASP.NET debugging enabled

Severity	Low
Reported by module	/Scripts/PerFolder/ASP-NET_Debugging_Enabled.script

Description

ASP.NET debugging is enabled on this application. It is recommended to disable debug mode before deploying a production application. By default, debugging is disabled, and although debugging is frequently enabled to troubleshoot a problem, it is also frequently not disabled again after the problem is resolved.

Impact

It may be possible that sensitive information about the web sever is disclosed through the ASP.NET application.

Recommendation

Check References for details on how to fix this problem.

References

[HOW TO: Disable Debugging for ASP.NET Applications](https://support.microsoft.com/en-us/How-TO:Disable-Debugging-for-ASP.NET-Applications) (https://support.microsoft.com/en-us/

Affected items

Web Server
Details
Pages where ASP.NET debugging is enabled: - https://ap.tnnua.edu.tw/Teacher/ - https://ap.tnnua.edu.tw/Teacher/Script/ - https://ap.tnnua.edu.tw/Teacher/content/
Request headers
DEBUG /Teacher/testing_invalid_filename.aspx HTTP/1.1
Command: stop-debug
Cookie: ASP.NET_SessionId=w0ro31sxlx3wx3kbsss1oznn
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/135.0.0.0 Safari/537.36
Host: ap.tnnua.edu.tw
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/) (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://ap.tnnua.edu.tw/Teacher/ Set-Cookie: ASP.NET_SessionId=w0ro31sxlx3wx3kbsss1oznn; path=/; HttpOnly; SameSite=Lax
Request headers
GET /Teacher/ HTTP/1.1
Referer: https://ap.tnnua.edu.tw/Teacher/
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/135.0.0.0 Safari/537.36
Host: ap.tnnua.edu.tw
Connection: Keep-alive

 Content Security Policy (CSP) Not Implemented

Severity	Informational
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
  default-src 'self';
  script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy \(CSP\)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/) (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Paths without CSP header: - https://ap.tnnua.edu.tw/Teacher/ - https://ap.tnnua.edu.tw/teacher/ErrorPage.aspx - https://ap.tnnua.edu.tw/Teacher/login.aspx
Request headers

GET /Teacher/ HTTP/1.1

Referer: https://ap.tnnua.edu.tw/Teacher/

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/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

Connection: Keep-alive

Insecure Transportation Security Protocol Supported (TLS 1.1)

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

Description

The web server supports encryption through TLS 1.1, which was formally deprecated in March 2021 as a result of inherent security issues. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Recommendation

It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.

References

[RFC 8996: Deprecating TLS 1.0 and TLS 1.1](https://tools.ietf.org/html/rfc8996) (https://tools.ietf.org/html/rfc8996)

[Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls) (https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls)

[PCI 3.1 and TLS 1.2 \(Cloudflare Support\)](https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2) (https://support.cloudflare.com/hc/en-us/articles/205043158-PCI-3-1-and-TLS-1-2)

Affected items

Web Server

Details

The SSL server (port: 443) encrypts traffic using TLSv1.1.

Request headers

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/) (<https://www.invicti.com/support/how-invicti-identifies-outofdate/>)

Affected items

Web Server

Details

- **jQuery UI Tooltip 1.11.4**
 - URL: <https://ap.tnnua.edu.tw/Teacher/>
 - Detection method: The library's name and version were determined based on its dynamic behavior.
 - References:
 - <https://jqueryui.com/download/>

Request headers

GET /Teacher/ HTTP/1.1

Referer: <https://ap.tnnua.edu.tw/Teacher/>

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/135.0.0.0 Safari/537.36

Host: ap.tnnua.edu.tw

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

Affected items

Web Server
Details
Locations without Permissions-Policy header: - https://ap.tnnua.edu.tw/Teacher/ - https://ap.tnnua.edu.tw/teacher/ErrorPage.aspx - https://ap.tnnua.edu.tw/Teacher/image/ - https://ap.tnnua.edu.tw/Teacher/content/ - https://ap.tnnua.edu.tw/Teacher/report/ - https://ap.tnnua.edu.tw/Teacher/login.aspx - https://ap.tnnua.edu.tw/Teacher/Script/ - https://ap.tnnua.edu.tw/Teacher/Style/
Request headers
GET /Teacher/ HTTP/1.1
Referer: https://ap.tnnua.edu.tw/Teacher/
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/135.0.0.0 Safari/537.36
Host: ap.tnnua.edu.tw
Connection: Keep-alive

Scanned items (coverage report)

<https://ap.tnnua.edu.tw/>
<https://ap.tnnua.edu.tw/Teacher/>
<https://ap.tnnua.edu.tw/Teacher/content/>
<https://ap.tnnua.edu.tw/teacher/ErrorPage.aspx>
<https://ap.tnnua.edu.tw/Teacher/image/>
<https://ap.tnnua.edu.tw/Teacher/login.aspx>
<https://ap.tnnua.edu.tw/Teacher/report/>
<https://ap.tnnua.edu.tw/Teacher/Script/>
<https://ap.tnnua.edu.tw/Teacher/Script/Default.js>
<https://ap.tnnua.edu.tw/Teacher/Script/jquery-3.7.1.js>
<https://ap.tnnua.edu.tw/Teacher/Script/jquery-ui.js>
<https://ap.tnnua.edu.tw/Teacher/Style/>
<https://ap.tnnua.edu.tw/Teacher/Style/Default.css>
<https://ap.tnnua.edu.tw/Teacher/Style/Site.css>
<https://ap.tnnua.edu.tw/Teacher/Style/Styles.css>
<https://ap.tnnua.edu.tw/Teacher/WebResource.axd>