

Developer Report

Acunetix Security Audit

2025-02-13

Generated by Acunetix

Scan of mail.tnnua.edu.tw

Scan details

Scan information	
Start time	2025-02-13T00:03:33.693932+08:00
Start url	https://mail.tnnua.edu.tw/
Host	mail.tnnua.edu.tw
Scan time	3 minutes, 23 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Application build	24.12.241212129

Threat level

Acunetix Threat Level 0

No vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	3
 Critical	0
 High	0
 Medium	0
 Low	0
 Informational	3

Alerts summary

 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

 HTTP Strict Transport Security (HSTS) Errors and Warnings

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

 **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

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://mail.tnnua.edu.tw/>
- <https://mail.tnnua.edu.tw/index.html>
- <https://mail.tnnua.edu.tw/images/>
- <https://mail.tnnua.edu.tw/en/>
- <https://mail.tnnua.edu.tw/group/>
- <https://mail.tnnua.edu.tw/img/>
- <https://mail.tnnua.edu.tw/images/icon/>
- <https://mail.tnnua.edu.tw/blank.html>
- <https://mail.tnnua.edu.tw/cht/img/>
- <https://mail.tnnua.edu.tw/lib/>
- <https://mail.tnnua.edu.tw/en/img/>
- https://mail.tnnua.edu.tw/cgi-bin/gen_capt
- <https://mail.tnnua.edu.tw/layer.html>
- <https://mail.tnnua.edu.tw/cht/>
- <https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js>
- <https://mail.tnnua.edu.tw/c70/>
- <https://mail.tnnua.edu.tw/j70/>
- <https://mail.tnnua.edu.tw/lib/jquery/>
- <https://mail.tnnua.edu.tw/cht/j70/>
- <https://mail.tnnua.edu.tw/cgi-bin/admin/m2kadm>
- <https://mail.tnnua.edu.tw/cgi-bin/login.otp>

Request headers

GET / HTTP/1.1

Referer: https://mail.tnnua.edu.tw/

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: mail.tnnua.edu.tw

Connection: Keep-alive

HTTP Strict Transport Security (HSTS) Errors and Warnings

Severity	Informational
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Impact

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

Recommendation

It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.

References

hstspreload.org (https://hstspreload.org/)

[MDN: 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 configuration is not according to best practices:

- <https://mail.tnnua.edu.tw/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/index.html> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/cgi-bin/login> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/images/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/en/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/group/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/img/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/images/icon/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/blank.html> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/cht/img/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/lib/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/en/img/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/cgi-bin/gen_capt - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/layer.html> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/cht/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/c70/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/j70/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/cht/j70/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/lib/jquery/> - max-age is less than 1 year (31536000); No includeSubDomains directive
- <https://mail.tnnua.edu.tw/cgi-bin/admin/m2kadm> - max-age is less than 1 year (31536000); No includeSubDomains directive

Request headers

GET / HTTP/1.1

Referer: <https://mail.tnnua.edu.tw/>

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: mail.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://mail.tnnua.edu.tw/ - https://mail.tnnua.edu.tw/index.html - https://mail.tnnua.edu.tw/cgi-bin/login - https://mail.tnnua.edu.tw/images/ - https://mail.tnnua.edu.tw/en/ - https://mail.tnnua.edu.tw/img/ - https://mail.tnnua.edu.tw/group/ - https://mail.tnnua.edu.tw/images/icon/ - https://mail.tnnua.edu.tw/blank.html - https://mail.tnnua.edu.tw/cht/img/ - https://mail.tnnua.edu.tw/lib/ - https://mail.tnnua.edu.tw/en/img/ - https://mail.tnnua.edu.tw/cgi-bin/gen_capt - https://mail.tnnua.edu.tw/layer.html - https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js - https://mail.tnnua.edu.tw/cht/ - https://mail.tnnua.edu.tw/c70/ - https://mail.tnnua.edu.tw/j70/ - https://mail.tnnua.edu.tw/cht/j70/ - https://mail.tnnua.edu.tw/lib/jquery/ - https://mail.tnnua.edu.tw/cgi-bin/admin/m2kadm
Request headers
GET / HTTP/1.1
Referer: https://mail.tnnua.edu.tw/
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: mail.tnnua.edu.tw
Connection: Keep-alive

Scanned items (coverage report)

<https://mail.tnnua.edu.tw/>
<https://mail.tnnua.edu.tw/blank.html>
<https://mail.tnnua.edu.tw/c70/>
<https://mail.tnnua.edu.tw/c70/login.css>
<https://mail.tnnua.edu.tw/c70/m2kv4.css>
<https://mail.tnnua.edu.tw/cgi-bin/>
<https://mail.tnnua.edu.tw/cgi-bin/admin/>
<https://mail.tnnua.edu.tw/cgi-bin/admin/m2kadm>
https://mail.tnnua.edu.tw/cgi-bin/check_session
https://mail.tnnua.edu.tw/cgi-bin/gen_capt
<https://mail.tnnua.edu.tw/cgi-bin/login>
<https://mail.tnnua.edu.tw/cgi-bin/login.otp>
<https://mail.tnnua.edu.tw/cht/>
<https://mail.tnnua.edu.tw/cht/img/>
<https://mail.tnnua.edu.tw/cht/j70/>
<https://mail.tnnua.edu.tw/cht/j70/msgtw.js>
<https://mail.tnnua.edu.tw/en/>
<https://mail.tnnua.edu.tw/en/img/>
<https://mail.tnnua.edu.tw/group/>
<https://mail.tnnua.edu.tw/images/>
<https://mail.tnnua.edu.tw/images/icon/>
<https://mail.tnnua.edu.tw/img/>
<https://mail.tnnua.edu.tw/index.html>
<https://mail.tnnua.edu.tw/j70/>
<https://mail.tnnua.edu.tw/j70/libm2k.js>
https://mail.tnnua.edu.tw/j70/m2k_adm.js
https://mail.tnnua.edu.tw/j70/m2k_ui_dialog.js
<https://mail.tnnua.edu.tw/j70/msgtw.js>
<https://mail.tnnua.edu.tw/j70/OnScreenKeyboard.js>
<https://mail.tnnua.edu.tw/j70/session.js>
<https://mail.tnnua.edu.tw/j70/TagShowDlg.js>
<https://mail.tnnua.edu.tw/layer.html>
<https://mail.tnnua.edu.tw/lib/>
<https://mail.tnnua.edu.tw/lib/jquery/>
<https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js>
<https://mail.tnnua.edu.tw/lib/jquery/jquery-latest-standard.js>