Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2025-08-06

Generated by Acunetix

Scan of mail.tnnua.edu.tw

Scan details

Scan information	
Start time	2025-08-06T00:08:52.031737+08:00
Start url	https://mail.tnnua.edu.tw/
Host	mail.tnnua.edu.tw
Scan time	6 minutes, 10 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
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	6
Critical	0
High	1
Medium	1
Low	0
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

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

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

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

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)
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)
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)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.0.
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)
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 TLS1.0 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

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)
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/cht/img/
- https://mail.tnnua.edu.tw/images/icon/
- https://mail.tnnua.edu.tw/lib/
- https://mail.tnnua.edu.tw/cht/
- https://mail.tnnua.edu.tw/c70/
- https://mail.tnnua.edu.tw/en/img/
- https://mail.tnnua.edu.tw/lib/jquery/
- https://mail.tnnua.edu.tw/j70/
- https://mail.tnnua.edu.tw/cht/j70/
- https://mail.tnnua.edu.tw/cgi-bin/login
- https://mail.tnnua.edu.tw/blank.html
- https://mail.tnnua.edu.tw/layer.html
- https://mail.tnnua.edu.tw/cgi-bin/gen_capt
- https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js
- https://mail.tnnua.edu.tw/j70/msgtw.js

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/135.0.0.0 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)

Affected items

Web Server
Details

URLs where HSTS configuration is not according to best practices:

- https://mail.tnnua.edu.tw/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/cgi-bin/login - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/index.html - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/images/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/en/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/group/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/img/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/cht/img/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/images/icon/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/lib/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/cht/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/c70/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/en/img/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/lib/jquery/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/j70/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/cht/j70/ - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/blank.html - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/layer.html - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/cgi-bin/gen_capt - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js - max-age is less that 1 year (31536000); No includeSubDomains directive
- https://mail.tnnua.edu.tw/j70/msgtw.js - max-age is less that 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/135.0.0.0 Safari/537.36

Host: mail.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)
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)
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)

Affected items

Web Server
Details
The SSL server (port: 443) encrypts traffic using TLSv1.1.
Request headers

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://mail.tnnua.edu.tw/
- https://mail.tnnua.edu.tw/cgi-bin/login
- 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/cht/img/
- https://mail.tnnua.edu.tw/images/icon/
- https://mail.tnnua.edu.tw/lib/
- https://mail.tnnua.edu.tw/cht/
- https://mail.tnnua.edu.tw/c70/
- https://mail.tnnua.edu.tw/en/img/
- https://mail.tnnua.edu.tw/lib/jquery/
- https://mail.tnnua.edu.tw/j70/
- https://mail.tnnua.edu.tw/cht/j70/
- https://mail.tnnua.edu.tw/cgi-bin/
- https://mail.tnnua.edu.tw/blank.html
- https://mail.tnnua.edu.tw/layer.html
- https://mail.tnnua.edu.tw/cgi-bin/gen_capt
- https://mail.tnnua.edu.tw/lib/jquery/jquery-1.12.4.js

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/135.0.0.0 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