Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2026-01-15

Generated by Acunetix

Scan of web.hs.edu.tw

Scan details

Scan information	
Start time	2026-01-15T00:10:14.873176+08:00
Start url	https://web.hs.edu.tw
Host	web.hs.edu.tw
Scan time	37 minutes, 32 seconds
Profile	Full Scan
Responsive	True
Server OS	Unknown
Application build	25.5.250613157

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	25
Critical	0
High	0
Medium	3
Low	11
Informational	11

Alerts summary

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

SSL Certificate Is About To Expire

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:3.0/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: 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-298

Affected items	Variation
Web Server	1

URL rewrite vulnerability

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/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: None Availability Impact to the Vulnerable System: Low 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:L Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None 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-436
CVE	CVE-2018-14773

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 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

Documentation files

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-538

Affected items	Variation
Web Server	1

Passive Mixed Content over HTTPS

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:L/SI:L/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: 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: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-284

Affected items	Variation
Web Server	1
/%E9%A6%96%E9%A0%81/	1
/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/	1
/blog/2020/10/%E7%B3%BB%E7%B5%B1%E4%BD%BF%E7%94%A8%E8%AA%AA%E6%98%8E/	1
/blog/2020/10/%E7%B3%BB%E7%B5%B1%E9%81%8B%E4%BD%9C%E5%8E%9F%E7%90%86/	1
/blog/2020/10/dns%E5%B8%B8%E8%A6%8B%E8%A8%98%E9%8C%84/	1
/blog/2021/02/web%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/	1

WordPress admin accessible without HTTP authentication

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:3.1/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-16

Affected items	Variation
/wp-admin/	1

An Unsafe Content Security Policy (CSP) Directive in Use

Classification	
CWE	CWE-16

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-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

Insecure Referrer Policy

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/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: None 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: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-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

Reverse Proxy Detected

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-16

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

Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive

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

Alerts details

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://web.hs.edu.tw/wp-content/themes/oceanwp/
Request headers

```
GET /wp-content/themes/oceanwp/ HTTP/1.1
Referer: https://web.hs.edu.tw/wp-content/themes/oceanwp/
Cookie:
TS018c8ebf=01d5a5990ef735c1d7aa691780dad0697ae9dcd0b60fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea9292f03bf7a56374fa063dff032b58b8cdd57dea0ce8eb22e4d0d15bfd8a714577775bb412b8409b12ac921d789e8182ed
51b8152091e49abf3146a25ca29be1da91da98d7779f991aa17e570185dc2c383d8e39136db0ba1e97db99f4c1bd2fd24eac8190e9
c3cffde2a458b161bb07329f529d4e838419d222d3dd7ee4a2523b0aff385fc2ce86b8930533edb8bdeea172a0e9d0a907b50d0696
8dc026e566320fed38c94990dcedf3752c2628a6d0ad5d70f0b16842a521a70084428080f72c0406ca6856cd4dc0dd89224fa83b64
c39df496ce0e64c34a65cde48ae90d773b09cdbf5f97d247f886b0a468f3b321f6d42e9ef94f4fe8a34c9d37f8c18c41c9751e9c1d
a5925db726b9c98d601c7917118af33667df0adf5e2643988ae9af7fd; pvc_visits_1[0]=1768493482b138;
wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

SSL Certificate Is About To Expire

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

Description

One of the TLS/SSL certificates used by your server is about to expire.

Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server.

This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.

Impact

If an application server detects an expired certificate with a system it is communicating with, the application server may continue processing data as if nothing happened, or the connection may be abruptly terminated.

Recommendation

Contact your Certificate Authority to renew the SSL certificate.

References

SSL Certificate Is About To Expire (https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/ssl-certificate-is-about-to-expire/)

Affected items

Web Server
Details

The TLS/SSL certificate (serial: 47e900000007a8b16a602ba1aa410d17) will expire in less than **60** days. The certificate validity period is from **Thu Jan 09 2025 11:02:47 GMT+0800 (CST)** to **Thu Feb 05 2026 23:59:59 GMT+0800 (CST)** (21 days left)

Request headers

URL rewrite vulnerability

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

Description

It was identified that this application supports the legacy headers **X-Original-URL** and/or **X-Rewrite-URL**.

Support for these headers lets users override the path in the request URL via the X-Original-URL or X-Rewrite-URL HTTP request header and allows a user to access one URL but have web application return a different one which can bypass restrictions on higher level caches and web servers.

Many web frameworks such as Symfony 2.7.0 to 2.7.48, 2.8.0 to 2.8.43, 3.3.0 to 3.3.17, 3.4.0 to 3.4.13, 4.0.0 to 4.0.13 and 4.1.0 to 4.1.2 , zend-diactoros up to 1.8.4, zend-http up to 2.8.1, zend-feed up to 2.10.3 are affected by this security issue.

Impact

The impact of this vulnerability depends on the affected web application/framework.

Recommendation

Upgrade the affected web frameworks to their latest versions.

References

CVE-2018-14773: Remove support for legacy and risky HTTP headers (https://symfony.com/blog/cve-2018-14773-remove-support-for-legacy-and-risky-http-headers)
ZF2018-01: URL Rewrite vulnerability (https://framework.zend.com/security/advisory/ZF2018-01)
CVE-2018-14773 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14773)

Affected items

Web Server
Details
Request headers

```
GET /?cb785021=1 HTTP/1.1
Referer: https://web.hs.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: web.hs.edu.tw
Connection: Keep-alive
X-Original-URL: /ygtlnjwzoq
X-Rewrite-URL: /ygtlnjwzoq
```

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://web.hs.edu.tw/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/

```
Set-Cookie: TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71
```

- https://web.hs.edu.tw/

```
Set-Cookie: TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS018c8ebf=01d5a5990ee9ea0589aaa72c9ef7cf7f366e6eff5692d5e4b03e3726e7ca91b13ad12d206c17b71
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS01521c32=01d5a5990e7aca3db1de486bdcee0570198763944b92d5e4b03e3726e7ca91b13ad12d206c17b71
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS018c8ebf=01d5a5990e9fbb7746bcbf1e3862ef598acda933b792d5e4b03e3726e7ca91b13ad12d206c17b71
```

- https://web.hs.edu.tw/wp-json/

```
Set-Cookie: TS018c8ebf=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS018c8ebf=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS01521c32=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS018c8ebf=01d5a5990ed9e39cd403f568ea6e5daeb1399c2ead0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS018c8ebf=01d5a5990ef735c1d7aa691780dad0697ae9dcd0b60fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/wp-login.php

```
Set-Cookie: TS01521c32=01d5a5990ed9e39cd403f568ea6e5daeb1399c2ead0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2020/10/dns-faq/

```
Set-Cookie: TS018c8ebf=01d5a5990e77f98a3d5c229c055af132f235fac0600fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2021/03/web-faq/

```
Set-Cookie: TS018c8ebf=01d5a5990e170fc259fc4c2fd1c3b055f9e87789020fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2022/02/email-faq/

```
Set-Cookie: TS018c8ebf=01d5a5990e9d6738612be58c35e52a41fc6dc553ab0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2023/04/test/

```
Set-Cookie: TS018c8ebf=01d5a5990ecb7f96bed8edfe23baadc3c4c040b2f00fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2024/03/dnsupdate/

```
Set-Cookie: TS018c8ebf=01d5a5990ed6724973122a77e9ce9d9d090e5302270fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2020/10/%E7%B3%BB%E7%B5%B1%E4%BD%BF%E7%94%A8%E8%AA%AA%E6%98%8E/

```
Set-Cookie: TS018c8ebf=01d5a5990e0083b5ab3961cc3644804b9d0ac3eb1d0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2020/10/%E7%B3%BB%E7%B5%B1%E9%81%8B%E4%BD%9C%E5%8E%9F%E7%90%86/

```
Set-Cookie: TS018c8ebf=01d5a5990e8135a40afbc3b2ab6d337f21eebe9f740fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2020/10/dns%E5%B8%B8%E8%A6%8B%E8%A8%98%E9%8C%84/

```
Set-Cookie: TS018c8ebf=01d5a5990ef88848301e74a63e78cf2c9a422828bd0fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2020/10/dns%E9%80%B2%E9%9A%8E%E8%A8%98%E9%8C%84%E8%A8%AD%E5%AE%9A/

```
Set-Cookie: TS018c8ebf=01d5a5990ed84202002b60552b64d2eb0a64733a870fab0f309530a1d5abb79e1fa4323b5249a6b
```

- https://web.hs.edu.tw/blog/2021/02/web%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/

```
Set-Cookie: TS018c8ebf=01d5a5990ee2ab077e2291f940e318c6c48e17a75c0fab0f309530a1d5abb79e1fa4323b5249a6b
```

Request headers

```
GET
/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/
HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71fbed0db3bbee0f31
9510e464fbdf56283c5049d8e0554b5d18b87fa406f; pvc_visits_1[0]=1768493482b138
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: web.hs.edu.tw
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://web.hs.edu.tw/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ee9ea0589aaa72c9ef7cf7f366e6eff5692d5e4b03e3726e7ca91b13ad12d206c17b71
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS01521c32=01d5a5990e7aca3db1de486bdcee0570198763944b92d5e4b03e3726e7ca91b13ad12d206c17b71
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e9fbb7746bcbf1e3862ef598acda933b792d5e4b03e3726e7ca91b13ad12d206c17b71
  ```

This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-json/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS01521c32=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ed9e39cd403f568ea6e5daeb1399c2ead0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ef735c1d7aa691780dad0697ae9dcd0b60fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/wp-login.php

  Cookie was set with:

  ```
  Set-Cookie: TS01521c32=01d5a5990ed9e39cd403f568ea6e5daeb1399c2ead0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2020/10/dns-faq/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e77f98a3d5c229c055af132f235fac0600fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2021/03/web-faq/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e170fc259fc4c2fd1c3b055f9e87789020fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2022/02/email-faq/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e9d6738612be58c35e52a41fc6dc553ab0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2023/04/test/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ecb7f96bed8edfe23baadc3c4c040b2f00fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2024/03/dnsupdate/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ed6724973122a77e9ce9d9d090e5302270fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2020/10/%E7%B3%BB%E7%B5%B1%E4%BD%BF%E7%94%A8%E8%AA%AA%E6%98%8E/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e0083b5ab3961cc3644804b9d0ac3eb1d0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2020/10/%E7%B3%BB%E7%B5%B1%E9%81%8B%E4%BD%9C%E5%8E%9F%E7%90%86/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990e8135a40afbc3b2ab6d337f21eebe9f740fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2020/10/dns%E5%B8%B8%E8%A6%8B%E8%A8%98%E9%8C%84/

Cookie was set with:

```
Set-Cookie: TS018c8ebf=01d5a5990ef88848301e74a63e78cf2c9a422828bd0fab0f309530a1d5abb79e1fa4323b5249a6b
```

This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2020/10/dns%E9%80%B2%E9%9A%8E%E8%A8%98%E9%8C%84%E8%A8%AD%E5%AE%9A/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ed84202002b60552b64d2eb0a64733a870fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

- https://web.hs.edu.tw/blog/2021/02/web%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/

  Cookie was set with:

  ```
  Set-Cookie: TS018c8ebf=01d5a5990ee2ab077e2291f940e318c6c48e17a75c0fab0f309530a1d5abb79e1fa4323b5249a6b
  ```

  This cookie has the following issues:

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

Request headers

```
GET
/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/
HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71fbed0db3bbee0f31
9510e464fbdf56283c5049d8e0554b5d18b87fa406f; pvc_visits_1[0]=1768493482b138
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: web.hs.edu.tw
Connection: Keep-alive
```

Documentation files

Severity	**Low**
Reported by module	/Scripts/PerFolder/Readme_Files.script

Description

One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

References

INT08:2023 – Information Leakage (https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT08_2023-Information_Leakage)

Affected items

Web Server

Details

Documentation files:

- https://web.hs.edu.tw/**license.txt**
  File contents (first 100 characters):

```
WordPress - Web publishing software

Copyright 2011-2022 by the contributors

This program is fr ...
```

Request headers

```
GET /license.txt HTTP/1.1
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: web.hs.edu.tw
Connection: Keep-alive
```

Passive Mixed Content over HTTPS

Severity	**Low**

Reported by module	/httpdata/mixed_content_over_https.js

Description

Acunetix detected a mixed content loaded over HTTP within an HTTPS page. If the HTTPS page includes content retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

Impact

A man-in-the-middle attacker can intercept the request and also rewrite the response to include malicious or deceptive content. This content can be used to steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

Recommendation

There are two technologies to defense against the mixed content issues: - HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page) - Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites - Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example: A protocol relative URL to load an style would look like >link rel="stylesheet" href="//example.com/style.css"/<. Same for scripts >script type="text/javascript" src="//example.com/code.js"<>/script< The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

References

MDN: Mixed Content (https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content)
What is mixed content? (https://web.dev/what-is-mixed-content/)
Fixing mixed content (https://web.dev/fixing-mixed-content/)

Affected items

Web Server

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/hslogo.png**

Request headers

```
GET / HTTP/1.1
Referer: https://web.hs.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: web.hs.edu.tw
Connection: Keep-alive
```

/%E9%A6%96%E9%A0%81/

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/LOGO-news.png**

Request headers

```
GET /%E9%A6%96%E9%A0%81/ HTTP/1.1
Referer: https://web.hs.edu.tw/page/3/
Cookie:
TS018c8ebf=01d5a5990e701c2410d2e770de786bca4835d2a49a0fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea9292f03bf7a56374fa063dff032b58b8cdd57dea0ce8eb22e4d0d15bfd8a714577775bb412b8409b12ac921d789e8182ed
51b8152091e49abf3146a25ca29be1da91da98d7779f991aa17e570185dc2c383d8e39136db0ba1e97db99f4c1bd2fd24eac8190e9
c3cffde2a458b161bb07329f529d4e838419d222d3dd7ee4a2523b0aff385fc2ce86b8930533edb8bdeea172a0e9d0a907b50d0696
8dc026e566320fed38c94990dcedf3752c2628a6d0ad5d70f0b16842a521a70084428080f72c0406ca6856cd4dc0dd89224fa83b64
c39df496ce0e64c34a65cde48ae90d773b09cdbf5f97d247f886b0a468f3b321f6d42e9ef94f4fe8a34c9d37f8c18c41c97b5fec35
e0198dcb832e64b2d15f10b71; pvc_visits_1[0]=1768493482b138; wordpress_test_cookie=WP%20Cookie%20check;
wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/02-DNSå□□ä¸□é□□ä¸-SOP-V20201007B.png**

Request headers

```
GET
/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/
HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990e5081b99e20ece3371c12e2c1dafbfd8692d5e4b03e3726e7ca91b13ad12d206c17b71fbed0db3bbee0f31
9510e464fbdf56283c5049d8e0554b5d18b87fa406f; pvc_visits_1[0]=1768493482b138
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: web.hs.edu.tw
Connection: Keep-alive
```

/blog/2020/10/%E7%B3%BB%E7%B5%B1%E4%BD%BF%E7%94%A8%E8%AA%AA%E6%98%8E/

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/ç®¡ç□□ç□»å□¥2-1024x955.png**
- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/ç®¡ç□□ç□»å□¥3-1024x96.png**

Request headers

```
GET /blog/2020/10/%E7%B3%BB%E7%B5%B1%E4%BD%BF%E7%94%A8%E8%AA%AA%E6%98%8E/ HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990e0083b5ab3961cc3644804b9d0ac3eb1d0fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea929fa77dfd1a5a338d07d057548d84518a25ad3e3d9ee7fbd81b4cf9bad1c2929221242a487b0dbb3f695ad5bd40461e91
93f33ed794a381c6d2b35d5d79e629b3f1c16e55cbd01a5f2c9f71c1a29fa42e235d8d0373b779b15e1778b502d541673606288a5d
7d497468724215964a13247aff73798f33aa7b8db562c2980b543ddcc2cf12893a23cc36121a0f26b72ee63efae7857e6bf41093e7
32d6643f173756a3f5849b9195ea92d362e2062d883317dd9f231ac5b71963e9bdbba9f613c4c88e2f97e23634ba4f68bdf9fc152a
313252dd08d608d0fa8e20230bb4fe8a42b0eb5ffd41ef2f9a5da9498e5b8963298cab88276ed3f30d218482112d764b6887ddd917
f4bae3cb0aad5e72aca7362cf663615f5c634adfc0e9732ad23f9be49;
pvc_visits_1[0]=1768493482b138a1768494034b238a1768494037b520a1768494042b788a1768494045b1378a1768494048b183
4a1768494065b140; wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

/blog/2020/10/%E7%B3%BB%E7%B5%B1%E9%81%8B%E4%BD%9C%E5%8E%9F%E7%90%86/

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/åŽ□ç□□1.png**

Request headers

```
GET /blog/2020/10/%E7%B3%BB%E7%B5%B1%E9%81%8B%E4%BD%9C%E5%8E%9F%E7%90%86/ HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990e8135a40afbc3b2ab6d337f21eebe9f740fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea929c53e3371e91e2f615911c80e7bdbeb25d909d40a7cfb811a67bd4e72267945481fe40c7e7ed842f8b7865351ebce6d6
53caaa87b8064128319aa537441250cc384000cd919411b591585bd4e843466cfc32d622c8302474a7a0da4d7c502b993c75732906
c49c6e3448d4f63a7f2da89f6cbdd8633c0c8267420a521b76be7ccdfd15c63a041458e30b4e71e9922bebe4874a9a06c0aaebdb9f
b37f591a860bd43fa819c4c856d6410eaf588a7690fd7004b450849ced0d6d79af2cf4461c15e17d9d5832e62875fad5a2e4fafdfe
5745bfd7e59a978a71616a6ddb52035e371daf0bdf821c93714f227e43992b706a59075f9928cb663246290f5f6c21d6d13a412a8c
da4d4ba2608a0126ad1853fe8a63663becaffe6f11c3de5c2ab7364d8;
pvc_visits_1[0]=1768493482b138a1768494034b238a1768494037b520a1768494042b788a1768494045b1378a1768494048b183
4a1768494065b140a1768494065b142; wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

/blog/2020/10/dns%E5%B8%B8%E8%A6%8B%E8%A8%98%E9%8C%84/

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/08-1.png**
- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/09-1.png**

Request headers

```
GET /blog/2020/10/dns%E5%B8%B8%E8%A6%8B%E8%A8%98%E9%8C%84/ HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990ef88848301e74a63e78cf2c9a422828bd0fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea929e4107c3d6ca7330c296c97270e5a5b12896bbf01318f4a027aac1fe8976956d891da3c8edbdb0dad28d621f83bdbca5
8c2a56813d6a802448d967233576f1f9107df7989250d9d3f080641d6b6d5b37e62a43751731e9e65f33b081cdcec4730e203473cb
5f42f3731b68c3bbb52ea6ff695c0c70ac32bfc58ba9fed60862802c5e0f6ed6e970cf683bec29592e68fa0efc41794c7e4e3621f8
1278f5a3de234fc6f38198e21652114b2e243d357f25466f30404cb6b3fcaf747be623e648bd67e817792543986cea10d73f69b161
f0cecf6766a43a1b00cfac7ebda78d2298a9744a5c1beed715dd43c61586df3d1c292ff178f041d846ec140fafa79389673bc49198
55eb0dfca94b28c5dbd208396185960ed0666a3286a7c3b39b00de383;
pvc_visits_1[0]=1768493482b138a1768494034b238a1768494037b520a1768494042b788a1768494045b1378a1768494048b183
4a1768494065b140a1768494065b142a1768494068b144; wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

/blog/2021/02/web%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/

Details

The following issues were detected:

- The tag **img** references the resource **http://web.hs.edu.tw/wp-content/uploads/2021/02/å-¸æ ¡ç¶²é ›å□□ä¸(é□‹ä¸SOP-V8-1.png**

Request headers

```
GET
/blog/2021/02/web%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/ HTTP/1.1
Referer: https://web.hs.edu.tw/
Cookie:
TS018c8ebf=01d5a5990ed84202002b60552b64d2eb0a64733a870fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22f76a15ea92933e38163f06e1936e50dde32147ae53d851a1cb0ec9ebdf360e8340fdf7a17d2f12a5ba398f48114b2eaa51d74ed75ff2f97395c63561377cbacdd30c48acff33dff181c1d7b2bf6bc69c227678e081ad51713d0e020c35158804a2cc2b1bcd5bea50d5efc2881eefb38c3a01879cb1906214f72a81a6f52445c6d826449db49a3e20bc9587dbb82d5b5c331d216ef75f6414ce39a303a025d1d341c9907e1239948eb07ab011e33540589dc37d4801da24a774ea95217bd7b5ec7eb6cddafbb5ad5ffc67676df7173e1e099af52b67d3a1b1f7370a2535f5834eb4287c1ddb7cf997d75254fcb8e4fc1adef60cbdb96c4edc22e51fab3a417137a04694e250457f2faafd60a917db90a7c6ba4aca07757590aab5b7db2bb0a50ef0e14fcfb19;
pvc_visits_1[0]=1768493482b138a1768494034b238a1768494037b520a1768494042b788a1768494045b1378a1768494048b1834a1768494065b140a1768494065b142a1768494068b144a1768494069b230; wordpress_test_cookie=WP%20Cookie%20check;
wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

WordPress admin accessible without HTTP authentication

Severity	**Low**
Reported by module	/Scripts/WebApps/wordpress_18.script

Description

It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.

Impact

No impact is associated with this vulnerability.

Recommendation

Add server-side password protection (such as BasicAuth) to the /wp-admin/ directory. Consult web references for more information.

References

Securing wp-admin (https://codex.wordpress.org/Hardening_WordPress)
WordPress Security Tips Part 5 | Restrict Access to wp-admin Directory (https://www.acunetix.com/blog/articles/wordpress-security-wpadmin-directory/)

Affected items

/wp-admin/
Details
Request headers

```
GET /wp-admin/ HTTP/1.1
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: web.hs.edu.tw
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://web.hs.edu.tw/
  - **CSP Value:** base-uri 'self'; connect-src 'self'; default-src 'self'; font-src 'self' data: https:; frame-src 'self' https://*.google.com https://*.googleapis.com https://www.youtube.com https://airtw.epa.gov.tw https://airtw.moenv.gov.tw https://www.facebook.com https://embed.windy.com https://weatherwidget.io; frame-ancestors 'self' https://web.hs.edu.tw; form-action 'self'; img-src * data:; media-src 'self'; object-src https:; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src https: 'unsafe-inline'; style-src-elem https: 'unsafe-inline'
  - **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 / HTTP/1.1
Referer: https://web.hs.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: web.hs.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)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Paths without CSP header: • https://web.hs.edu.tw/wp-content/themes/oceanwp/
Request headers

```
GET /wp-content/themes/oceanwp/ HTTP/1.1
Referer: https://web.hs.edu.tw/wp-content/themes/oceanwp/
Cookie:
TS018c8ebf=01d5a5990ef735c1d7aa691780dad0697ae9dcd0b60fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea9292f03bf7a56374fa063dff032b58b8cdd57dea0ce8eb22e4d0d15bfd8a714577775bb412b8409b12ac921d789e8182ed
51b8152091e49abf3146a25ca29be1da91da98d7779f991aa17e570185dc2c383d8e39136db0ba1e97db99f4c1bd2fd24eac8190e9
c3cffde2a458b161bb07329f529d4e838419d222d3dd7ee4a2523b0aff385fc2ce86b8930533edb8bdeea172a0e9d0a907b50d0696
8dc026e566320fed38c94990dcedf3752c2628a6d0ad5d70f0b16842a521a70084428080f72c0406ca6856cd4dc0dd89224fa83b64
c39df496ce0e64c34a65cde48ae90d773b09cdbf5f97d247f886b0a468f3b321f6d42e9ef94f4fe8a34c9d37f8c18c41c9751e9c1d
a5925db726b9c98d601c7917118af33667df0adf5e2643988ae9af7fd; pvc_visits_1[0]=1768493482b138;
wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

Generic Email Address Disclosure

Severity	**Informational**
Reported by module	/target/404_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://web.hs.edu.tw/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E6%9C%8D%E5%8B%99%E5%96%AE%E4%BD%8D/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/page/2/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/sitemap/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%9A%B1%E7%A7%81%E6%AC%8A%E6%94%BF%E7%AD%96/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/page/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/search/the/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E8%87%A8%E6%99%82%E6%B8%AC%E8%A9%A6%E7%94%A8%E9%A0%81%E9%9D%A2/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/2/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E6%A5%AD%E5%8B%99%E8%81%B7%E6%8E%8C/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/search/feed/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/page/3/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%A6%96%E9%A0%81/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/3/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E9%98%B2%E8%AD%B7/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/page/4/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/4/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E9%98%B2%E8%AD%B7/2/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E9%98%B2%E8%AD%B7/3/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E9%98%B2%E8%AD%B7/4/
  dnsweb@hs.edu.tw
- https://web.hs.edu.tw/search/1/
  dnsweb@hs.edu.tw

Request headers

```
GET / HTTP/1.1
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: web.hs.edu.tw
Connection: Keep-alive
```

Insecure Referrer Policy

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

Description

Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

Impact

In some situations, an attacker may leak a user's private data

Recommendation

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

References

Referrer-Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

Affected items

Web Server
Details

URLs where Referrer Policy configuration is insecure:

- https://web.hs.edu.tw/
- https://web.hs.edu.tw/blog/2020/10/%E5%90%91%E4%B8%8A%E9%9B%86%E4%B8%AD%E6%A8%99%E6%BA%96%E4%BD%9C%E6%A5%AD%E6%B5%81%E7%A8%8B/
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E6%9C%8D%E5%8B%99%E5%96%AE%E4%BD%8D/
- https://web.hs.edu.tw/blog/category/news/inform/
- https://web.hs.edu.tw/page/2/
- https://web.hs.edu.tw/wp-login.php
- https://web.hs.edu.tw/sitemap/
- https://web.hs.edu.tw/%E9%9A%B1%E7%A7%81%E6%AC%8A%E6%94%BF%E7%AD%96/
- https://web.hs.edu.tw/page/
- https://web.hs.edu.tw/wp-admin/images/
- https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/hamburgers/types/
- https://web.hs.edu.tw/blog/tag/dns/
- https://web.hs.edu.tw/blog/tag/dns/page/2/
- https://web.hs.edu.tw/wp-admin/includes/
- https://web.hs.edu.tw/search/the/
- https://web.hs.edu.tw/%E8%87%A8%E6%99%82%E6%B8%AC%E8%A9%A6%E7%94%A8%E9%A0%81%E9%9D%A2/
- https://web.hs.edu.tw/2/
- https://web.hs.edu.tw/wp-content/uploads/2020/10/
- https://web.hs.edu.tw/wp-includes/assets/
- https://web.hs.edu.tw/blog/author/chiachi/
- https://web.hs.edu.tw/%E9%97%9C%E6%96%BC%E6%88%91%E5%80%91/%E6%A5%AD%E5%8B%99%E8%81%B7%E6%8E%8C/

Request headers

```
GET / HTTP/1.1
Referer: https://web.hs.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: web.hs.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)
Permissions Policy (W3C) (https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server
Details
Locations without Permissions-Policy header: • https://web.hs.edu.tw/wp-content/themes/oceanwp/
Request headers

```
GET /wp-content/themes/oceanwp/ HTTP/1.1
Referer: https://web.hs.edu.tw/wp-content/themes/oceanwp/
Cookie:
TS018c8ebf=01d5a5990ef735c1d7aa691780dad0697ae9dcd0b60fab0f309530a1d5abb79e1fa4323b5249a6bf4bde78305f43a22
f76a15ea9292f03bf7a56374fa063dff032b58b8cdd57dea0ce8eb22e4d0d15bfd8a714577775bb412b8409b12ac921d789e8182ed
51b8152091e49abf3146a25ca29be1da91da98d7779f991aa17e570185dc2c383d8e39136db0ba1e97db99f4c1bd2fd24eac8190e9
c3cffde2a458b161bb07329f529d4e838419d222d3dd7ee4a2523b0aff385fc2ce86b8930533edb8bdeea172a0e9d0a907b50d0696
8dc026e566320fed38c94990dcedf3752c2628a6d0ad5d70f0b16842a521a70084428080f72c0406ca6856cd4dc0dd89224fa83b64
c39df496ce0e64c34a65cde48ae90d773b09cdbf5f97d247f886b0a468f3b321f6d42e9ef94f4fe8a34c9d37f8c18c41c9751e9c1d
a5925db726b9c98d601c7917118af33667df0adf5e2643988ae9af7fd; pvc_visits_1[0]=1768493482b138;
wordpress_test_cookie=WP%20Cookie%20check; wp_lang=en_US
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: web.hs.edu.tw
Connection: Keep-alive
```

Reverse Proxy Detected

Severity	**Informational**
Reported by module	/target/RevProxy_Detection.js

Description

This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.

Impact

No impact is associated with this vulnerability.

Recommendation

None

References

What is a reverse proxy? | Proxy servers explained (https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/)

Affected items

Web Server
Details
Detected reverse proxy: Apache httpd
Request headers

```
GET / HTTP/1.1
Max-Forwards: 0
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: web.hs.edu.tw
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://web.hs.edu.tw/
  - **CSP Value:** base-uri 'self'; connect-src 'self'; default-src 'self'; font-src 'self' data: https:; frame-src 'self' https://*.google.com https://*.googleapis.com https://www.youtube.com https://airtw.epa.gov.tw https://airtw.moenv.gov.tw https://www.facebook.com https://embed.windy.com https://weatherwidget.io; frame-ancestors 'self' https://web.hs.edu.tw; form-action 'self'; img-src * data:; media-src 'self'; object-src https:; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src https: 'unsafe-inline'; style-src-elem https: 'unsafe-inline'
  - **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 / HTTP/1.1
Referer: https://web.hs.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: web.hs.edu.tw
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://web.hs.edu.tw/ Script SRC: **https://cdnjs.cloudflare.com/ajax/libs/twbs-pagination/1.4.2/jquery.twbsPagination.min.js** • https://web.hs.edu.tw/wp-login.php Script SRC: **https://www.google.com/recaptcha/api.js?onload=c4wp_onloadCallback&render=explicit&hl=zh-TW**
Request headers
GET / HTTP/1.1 Referer: https://web.hs.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: web.hs.edu.tw Connection: Keep-alive

Wildcard Detected in Domain Portion of 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

- **Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive**
  - **First observed on:** https://web.hs.edu.tw/
  - **CSP Value:** base-uri 'self'; connect-src 'self'; default-src 'self'; font-src 'self' data: https:; frame-src 'self' https://*.google.com https://*.googleapis.com https://www.youtube.com https://airtw.epa.gov.tw https://airtw.moenv.gov.tw https://www.facebook.com https://embed.windy.com https://weatherwidget.io; frame-ancestors 'self' https://web.hs.edu.tw; form-action 'self'; img-src * data:; media-src 'self'; object-src https:; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src https: 'unsafe-inline'; style-src-elem https: 'unsafe-inline'
  - **CSP Source:** header
  - **Summary:** Acunetix detected that wildcard was used in domain portion of a CSP directive.
  - **Impact:** This means you trust all of the subdomains of this domain, if this is the case there is no impact.
  - **Remediation:** If you trust all of the subdomains and if this is necessary then you do not need to take any actions. However if this is not the case replace the wildcard with the only subdomain that you trust.
  - **References:**
    - N/A

Request headers

```
GET / HTTP/1.1
Referer: https://web.hs.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: web.hs.edu.tw
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://web.hs.edu.tw/
  - **CSP Value:** base-uri 'self'; connect-src 'self'; default-src 'self'; font-src 'self' data: https:; frame-src 'self' https://*.google.com https://*.googleapis.com https://www.youtube.com https://airtw.epa.gov.tw https://airtw.moenv.gov.tw https://www.facebook.com https://embed.windy.com https://weatherwidget.io; frame-ancestors 'self' https://web.hs.edu.tw; form-action 'self'; img-src * data:; media-src 'self'; object-src https:; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src https: 'unsafe-inline'; style-src-elem https: 'unsafe-inline'
  - **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 / HTTP/1.1
Referer: https://web.hs.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: web.hs.edu.tw
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://web.hs.edu.tw/
  - **CSP Value:** base-uri 'self'; connect-src 'self'; default-src 'self'; font-src 'self' data: https:; frame-src 'self' https://*.google.com https://*.googleapis.com https://www.youtube.com https://airtw.epa.gov.tw https://airtw.moenv.gov.tw https://www.facebook.com https://embed.windy.com https://weatherwidget.io; frame-ancestors 'self' https://web.hs.edu.tw; form-action 'self'; img-src * data:; media-src 'self'; object-src https:; script-src https: 'unsafe-inline' 'unsafe-eval'; style-src https: 'unsafe-inline'; style-src-elem https: 'unsafe-inline'
  - **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 / HTTP/1.1
Referer: https://web.hs.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: web.hs.edu.tw
Connection: Keep-alive
```

Scanned items (coverage report)

https://web.hs.edu.tw/
https://web.hs.edu.tw/臨時測試用頁面/
https://web.hs.edu.tw/關於我們/
https://web.hs.edu.tw/關於我們/服務單位/
https://web.hs.edu.tw/關於我們/業務職掌/
https://web.hs.edu.tw/關於我們/資通安全防護/
https://web.hs.edu.tw/關於我們/資通安全防護/2/
https://web.hs.edu.tw/關於我們/資通安全防護/3/
https://web.hs.edu.tw/關於我們/資通安全防護/4/
https://web.hs.edu.tw/隱私權政策/
https://web.hs.edu.tw/首頁/
https://web.hs.edu.tw/2/
https://web.hs.edu.tw/3/
https://web.hs.edu.tw/4/
https://web.hs.edu.tw/blog/
https://web.hs.edu.tw/blog/2020/
https://web.hs.edu.tw/blog/2020/07/
https://web.hs.edu.tw/blog/2020/07/109年7月22日1000-1700-國立高中職資訊系統學校-dns、學校網頁/
https://web.hs.edu.tw/blog/2020/10/
https://web.hs.edu.tw/blog/2020/10/向上集中標準作業流程/
https://web.hs.edu.tw/blog/2020/10/系統使用說明/
https://web.hs.edu.tw/blog/2020/10/系統運作原理/
https://web.hs.edu.tw/blog/2020/10/dns常見記錄/
https://web.hs.edu.tw/blog/2020/10/dns進階記錄設定/
https://web.hs.edu.tw/blog/2020/10/dns-faq/
https://web.hs.edu.tw/blog/2020/11/
https://web.hs.edu.tw/blog/2020/11/109年11月20日19002100-dns管理系統進行不斷線維護，可能發生/
https://web.hs.edu.tw/blog/2020/11/109年11月27日19002100-dns管理系統進行不斷線維護/
https://web.hs.edu.tw/blog/2020/11/109年12月5日六20時至24時，台南區網骨幹網路設備進行/
https://web.hs.edu.tw/blog/2020/12/
https://web.hs.edu.tw/blog/2020/12/109年12月15日-1030-1600-國立高級中等以下-dns、學校網頁向上集/
https://web.hs.edu.tw/blog/2020/page/
https://web.hs.edu.tw/blog/2020/page/1/
https://web.hs.edu.tw/blog/2020/page/2/
https://web.hs.edu.tw/blog/2021/
https://web.hs.edu.tw/blog/2021/01/
https://web.hs.edu.tw/blog/2021/01/新增dns-faq：gsuite信箱收發信延遲，收不到信是哪裡有問/
https://web.hs.edu.tw/blog/2021/02/
https://web.hs.edu.tw/blog/2021/02/新網站web-hs-edu-tw成立/
https://web.hs.edu.tw/blog/2021/02/110年3月1日-08001700-國立成功大學高壓電力設備停電檢驗、/
https://web.hs.edu.tw/blog/2021/02/110年3月4日0900-1230-110-年度國立高級中等以下學校網頁向上/
https://web.hs.edu.tw/blog/2021/02/web向上集中標準作業流程/
https://web.hs.edu.tw/blog/2021/03/
https://web.hs.edu.tw/blog/2021/03/110年4月1日1330-1720-110-年度前導學校公版網頁建置實務操作/
https://web.hs.edu.tw/blog/2021/03/web-faq/
https://web.hs.edu.tw/blog/2021/04/
https://web.hs.edu.tw/blog/2021/04/110年4月20日930-1230-110-年度國立高級中等以下學校網頁向上/
https://web.hs.edu.tw/blog/2021/05/
https://web.hs.edu.tw/blog/2021/05/緊急公告-為防治嚴重特殊傳染性肺炎，110年5月17日/
https://web.hs.edu.tw/blog/2021/05/110年5月17日930-1730-110年dns、學校網頁向上集中期中交流會議/
https://web.hs.edu.tw/blog/2021/05/5-19-5-28因異地辦公，請以mail為主要聯繫工具/
https://web.hs.edu.tw/blog/2021/05/5-31-6-4-維運團隊因異地辦公，請以mail為主要聯繫工具/
https://web.hs.edu.tw/blog/2021/06/

https://web.hs.edu.tw/blog/2021/06/110年6月16日930-1230-110-年度國立高級中等以下學校網頁向上/
https://web.hs.edu.tw/blog/2021/06/110年7月18日8001700-為配合台電後甲變電所之架空地線全面/
https://web.hs.edu.tw/blog/2021/06/6-15-6-28-維運團隊因異地辦公，請以mail為主要聯繫工具/
https://web.hs.edu.tw/blog/2021/06/6-29-7-12-維運團隊因異地辦公，請以mail為主要聯繫工具/
https://web.hs.edu.tw/blog/2021/07/
https://web.hs.edu.tw/blog/2021/07/110年7月14日1330-1730-110年度國立高級中等以下學校公版網站/
https://web.hs.edu.tw/blog/2021/07/110年8月11日1330-1730-110年度國立高級中等以下學校公版網站/
https://web.hs.edu.tw/blog/2021/08/
https://web.hs.edu.tw/blog/2021/08/110年9月12日日8001200-國立成功大學進行校園骨幹網路設備/
https://web.hs.edu.tw/blog/2021/09/
https://web.hs.edu.tw/blog/2021/09/110年10月6日0930-1730-110年dns、學校網頁向上集中期末交流會議/
https://web.hs.edu.tw/blog/2021/11/
https://web.hs.edu.tw/blog/2021/11/110年11月22日一-1700-2300-進行公版系統更新維運/
https://web.hs.edu.tw/blog/2021/page/
https://web.hs.edu.tw/blog/2021/page/1/
https://web.hs.edu.tw/blog/2021/page/2/
https://web.hs.edu.tw/blog/2021/page/3/
https://web.hs.edu.tw/blog/2022/
https://web.hs.edu.tw/blog/2022/02/
https://web.hs.edu.tw/blog/2022/02/email-faq/
https://web.hs.edu.tw/blog/2022/03/
https://web.hs.edu.tw/blog/2022/03/11年3月27日9001800成大向上集中機房設備維護作業，已集/
https://web.hs.edu.tw/blog/2022/03/111年3月8日1000-1730國立高級中等以下學校向上集中資通安/
https://web.hs.edu.tw/blog/2022/03/111年4月10日8001700-國立成功大學高壓電力設備停電檢驗、/
https://web.hs.edu.tw/blog/2022/06/
https://web.hs.edu.tw/blog/2022/06/111年6月1日18002200成大向上集中設備臨時維護作業，已集/
https://web.hs.edu.tw/blog/2022/07/
https://web.hs.edu.tw/blog/2022/07/111年7月23日13001700成大向上集中機房進行設備韌體升級作/
https://web.hs.edu.tw/blog/2022/07/dns-faq更新q5、q17、q18/
https://web.hs.edu.tw/blog/2022/08/
https://web.hs.edu.tw/blog/2022/08/111年9月6日1330-1730-111年dns、學校網頁向上集中新任業務承辦/
https://web.hs.edu.tw/blog/2022/09/
https://web.hs.edu.tw/blog/2022/09/111年10月6日930-1730-111年dns、學校網頁及電子郵件系統向上集/
https://web.hs.edu.tw/blog/2022/10/
https://web.hs.edu.tw/blog/2022/10/111年10月16日（日）08002400及111年10月18日（二）08001800成大向上集/
https://web.hs.edu.tw/blog/2022/12/
https://web.hs.edu.tw/blog/2022/12/111年12月15日（五）17002100成大向上集中出口端防火牆維護/
https://web.hs.edu.tw/blog/2022/page/
https://web.hs.edu.tw/blog/2022/page/1/
https://web.hs.edu.tw/blog/2022/page/2/
https://web.hs.edu.tw/blog/2023/
https://web.hs.edu.tw/blog/2023/01/
https://web.hs.edu.tw/blog/2023/01/112年1月13日（五）17002400-設備維護更新，因有備援機制，/
https://web.hs.edu.tw/blog/2023/03/
https://web.hs.edu.tw/blog/2023/03/112年03月17日（五）16002100成大向上集中設備韌體維護更新/
https://web.hs.edu.tw/blog/2023/04/
https://web.hs.edu.tw/blog/2023/04/test/
https://web.hs.edu.tw/blog/2023/07/
https://web.hs.edu.tw/blog/2023/07/112年7月8日（六）-0800-2400成大向上集中維護作業，原則上/
https://web.hs.edu.tw/blog/2023/11/
https://web.hs.edu.tw/blog/2023/11/112-11-28二-1800-2400學校網頁集中化管理系統維護作業/
https://web.hs.edu.tw/blog/2024/
https://web.hs.edu.tw/blog/2024/03/
https://web.hs.edu.tw/blog/2024/03/【國教署-dnsweb向上集中】113-03-13三-1800-2400公版網站維護作業/
https://web.hs.edu.tw/blog/2024/03/dnsupdate/
https://web.hs.edu.tw/blog/2024/07/

https://web.hs.edu.tw/blog/2024/07/113年7月13日（六）-0800-2400-進行設備升級作業，因有備援機/
https://web.hs.edu.tw/blog/2024/12/
https://web.hs.edu.tw/blog/2024/12/113年12月28日六0800-2400-進行核心設備升級作業，將影響學/
https://web.hs.edu.tw/blog/2024/12/114-1-4六0800-1800-進行dns集中化管理系統升級作業，不影響集/
https://web.hs.edu.tw/blog/2025/
https://web.hs.edu.tw/blog/2025/02/
https://web.hs.edu.tw/blog/2025/02/dns-faq更新q5、q17/
https://web.hs.edu.tw/blog/2025/06/
https://web.hs.edu.tw/blog/2025/06/114年6月21日六-08002400-團隊將進行「公版-web-維護」，原則不/
https://web.hs.edu.tw/blog/author/
https://web.hs.edu.tw/blog/author/chiachi/
https://web.hs.edu.tw/blog/author/chiachi/feed/
https://web.hs.edu.tw/blog/author/chiachi/page/
https://web.hs.edu.tw/blog/author/chiachi/page/1/
https://web.hs.edu.tw/blog/author/chiachi/page/2/
https://web.hs.edu.tw/blog/author/chiachi/page/3/
https://web.hs.edu.tw/blog/author/chiachi/page/4/
https://web.hs.edu.tw/blog/author/chiachi/page/5/
https://web.hs.edu.tw/blog/author/dnsweb_poster/
https://web.hs.edu.tw/blog/author/dnsweb_poster/feed/
https://web.hs.edu.tw/blog/author/kevin/
https://web.hs.edu.tw/blog/author/kevin/feed/
https://web.hs.edu.tw/blog/author/ncku11112017/
https://web.hs.edu.tw/blog/author/ncku11112017/feed/
https://web.hs.edu.tw/blog/author/z11109022/
https://web.hs.edu.tw/blog/author/z11109022/feed/
https://web.hs.edu.tw/blog/category/
https://web.hs.edu.tw/blog/category/dns-system/
https://web.hs.edu.tw/blog/category/dns-system/feed/
https://web.hs.edu.tw/blog/category/email-system/
https://web.hs.edu.tw/blog/category/email-system/feed/
https://web.hs.edu.tw/blog/category/news/
https://web.hs.edu.tw/blog/category/news/feed/
https://web.hs.edu.tw/blog/category/news/inform/
https://web.hs.edu.tw/blog/category/news/inform/feed/
https://web.hs.edu.tw/blog/category/news/meeting/
https://web.hs.edu.tw/blog/category/news/meeting/feed/
https://web.hs.edu.tw/blog/category/news/meeting/page/
https://web.hs.edu.tw/blog/category/news/meeting/page/1/
https://web.hs.edu.tw/blog/category/news/meeting/page/2/
https://web.hs.edu.tw/blog/category/news/notice/
https://web.hs.edu.tw/blog/category/news/notice/feed/
https://web.hs.edu.tw/blog/category/news/notice/page/
https://web.hs.edu.tw/blog/category/news/notice/page/1/
https://web.hs.edu.tw/blog/category/news/notice/page/2/
https://web.hs.edu.tw/blog/category/news/notice/page/3/
https://web.hs.edu.tw/blog/category/news/page/
https://web.hs.edu.tw/blog/category/news/page/1/
https://web.hs.edu.tw/blog/category/news/page/2/
https://web.hs.edu.tw/blog/category/news/page/3/
https://web.hs.edu.tw/blog/category/news/page/4/
https://web.hs.edu.tw/blog/category/news/page/5/
https://web.hs.edu.tw/blog/category/web-system/
https://web.hs.edu.tw/blog/category/web-system/feed/
https://web.hs.edu.tw/blog/tag/
https://web.hs.edu.tw/blog/tag/dns/
https://web.hs.edu.tw/blog/tag/dns/feed/
https://web.hs.edu.tw/blog/tag/dns/page/
https://web.hs.edu.tw/blog/tag/dns/page/1/
https://web.hs.edu.tw/blog/tag/dns/page/2/

https://web.hs.edu.tw/blog/tag/dns/page/3/
https://web.hs.edu.tw/blog/tag/dns/page/4/
https://web.hs.edu.tw/blog/tag/email/
https://web.hs.edu.tw/blog/tag/email/feed/
https://web.hs.edu.tw/blog/tag/web/
https://web.hs.edu.tw/blog/tag/web/feed/
https://web.hs.edu.tw/blog/tag/web/page/
https://web.hs.edu.tw/blog/tag/web/page/1/
https://web.hs.edu.tw/blog/tag/web/page/2/
https://web.hs.edu.tw/blog/tag/web/page/3/
https://web.hs.edu.tw/blog/tag/web/page/4/
https://web.hs.edu.tw/feed/
https://web.hs.edu.tw/license.txt
https://web.hs.edu.tw/page/
https://web.hs.edu.tw/page/1/
https://web.hs.edu.tw/page/2/
https://web.hs.edu.tw/page/3/
https://web.hs.edu.tw/page/4/
https://web.hs.edu.tw/robots.txt
https://web.hs.edu.tw/search/
https://web.hs.edu.tw/search/1/
https://web.hs.edu.tw/search/1/feed/
https://web.hs.edu.tw/search/1/feed/rss2/
https://web.hs.edu.tw/search/1/page/
https://web.hs.edu.tw/search/1/page/1/
https://web.hs.edu.tw/search/1/page/2/
https://web.hs.edu.tw/search/1/page/3/
https://web.hs.edu.tw/search/1/page/4/
https://web.hs.edu.tw/search/1/page/feed/
https://web.hs.edu.tw/search/1/page/feed/rss2/
https://web.hs.edu.tw/search/feed/
https://web.hs.edu.tw/search/feed/feed/
https://web.hs.edu.tw/search/feed/feed/rss2/
https://web.hs.edu.tw/search/feed/rss2/
https://web.hs.edu.tw/search/the/
https://web.hs.edu.tw/search/the/feed/
https://web.hs.edu.tw/search/the/feed/rss2/
https://web.hs.edu.tw/sitemap/
https://web.hs.edu.tw/wp-admin/
https://web.hs.edu.tw/wp-admin/css/
https://web.hs.edu.tw/wp-admin/css/forms.min.css
https://web.hs.edu.tw/wp-admin/css/l10n.min.css
https://web.hs.edu.tw/wp-admin/css/login.min.css
https://web.hs.edu.tw/wp-admin/images/
https://web.hs.edu.tw/wp-admin/includes/
https://web.hs.edu.tw/wp-admin/js/
https://web.hs.edu.tw/wp-admin/js/password-strength-meter.min.js
https://web.hs.edu.tw/wp-admin/js/user-profile.min.js
https://web.hs.edu.tw/wp-admin/user/
https://web.hs.edu.tw/wp-admin/wp-admin/
https://web.hs.edu.tw/wp-admin/wp-content/
https://web.hs.edu.tw/wp-admin/wp-includes/
https://web.hs.edu.tw/wp-content/
https://web.hs.edu.tw/wp-content/languages/
https://web.hs.edu.tw/wp-content/plugins/
https://web.hs.edu.tw/wp-content/plugins/advanced-nocaptcha-recaptcha/
https://web.hs.edu.tw/wp-content/plugins/advanced-nocaptcha-recaptcha/assets/
https://web.hs.edu.tw/wp-content/plugins/advanced-nocaptcha-recaptcha/assets/css/
https://web.hs.edu.tw/wp-content/plugins/advanced-nocaptcha-recaptcha/assets/css/style.css
https://web.hs.edu.tw/wp-content/plugins/disable-comments/
https://web.hs.edu.tw/wp-content/plugins/ilc-barrier-free/

https://web.hs.edu.tw/wp-content/plugins/ilc-barrier-free/js/
https://web.hs.edu.tw/wp-content/plugins/ilc-barrier-free/js/oceanwp-category-a11y.js
https://web.hs.edu.tw/wp-content/plugins/ilc-barrier-free/js/px-to-rem-converter.js
https://web.hs.edu.tw/wp-content/plugins/import-users-from-csv/
https://web.hs.edu.tw/wp-content/plugins/limit-login-attempts-reloaded/
https://web.hs.edu.tw/wp-content/plugins/limit-login-attempts-reloaded/assets/
https://web.hs.edu.tw/wp-content/plugins/limit-login-attempts-reloaded/assets/css/
https://web.hs.edu.tw/wp-content/plugins/limit-login-attempts-reloaded/assets/css/login-page-styles.css
https://web.hs.edu.tw/wp-content/plugins/post-views-counter/
https://web.hs.edu.tw/wp-content/plugins/post-views-counter/css/
https://web.hs.edu.tw/wp-content/plugins/post-views-counter/css/frontend.min.css
https://web.hs.edu.tw/wp-content/plugins/wordpress-importer/
https://web.hs.edu.tw/wp-content/plugins/wp-fastest-cache/
https://web.hs.edu.tw/wp-content/plugins/wp-mail-smtp/
https://web.hs.edu.tw/wp-content/themes/
https://web.hs.edu.tw/wp-content/themes/oceanwp/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/style.min.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/hamburgers/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/hamburgers/hamburgers.min.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/hamburgers/types/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/hamburgers/types/collapse-r.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/magnific-popup.min.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/simple-line-icons.min.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/css/third/slick.min.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/fontawesome/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/fontawesome/css/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/fontawesome/css/all.min.css
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/fontawesome/webfonts/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/simple-line-icons/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/fonts/slick/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/js/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/js/main.min.js
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/js/third/
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/js/third/html5.min.js
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/js/third/lightbox.min.js
https://web.hs.edu.tw/wp-content/themes/oceanwp/assets/js/third/magnific-popup.min.js
https://web.hs.edu.tw/wp-content/uploads/
https://web.hs.edu.tw/wp-content/uploads/2020/
https://web.hs.edu.tw/wp-content/uploads/2020/10/
https://web.hs.edu.tw/wp-content/uploads/2020/11/
https://web.hs.edu.tw/wp-content/uploads/2021/
https://web.hs.edu.tw/wp-content/uploads/2021/02/
https://web.hs.edu.tw/wp-content/uploads/2022/
https://web.hs.edu.tw/wp-content/uploads/2022/01/
https://web.hs.edu.tw/wp-content/uploads/2022/02/
https://web.hs.edu.tw/wp-content/uploads/2024/
https://web.hs.edu.tw/wp-content/uploads/2024/03/
https://web.hs.edu.tw/wp-content/uploads/2025/
https://web.hs.edu.tw/wp-content/uploads/2025/01/
https://web.hs.edu.tw/wp-content/uploads/2025/02/
https://web.hs.edu.tw/wp-content/wp-admin/
https://web.hs.edu.tw/wp-content/wp-content/
https://web.hs.edu.tw/wp-content/wp-includes/
https://web.hs.edu.tw/wp-includes/
https://web.hs.edu.tw/wp-includes/assets/
https://web.hs.edu.tw/wp-includes/css/
https://web.hs.edu.tw/wp-includes/css/buttons.min.css

https://web.hs.edu.tw/wp-includes/css/dashicons.min.css
https://web.hs.edu.tw/wp-includes/css/dist/
https://web.hs.edu.tw/wp-includes/css/dist/block-library/
https://web.hs.edu.tw/wp-includes/css/dist/block-library/style.min.css
https://web.hs.edu.tw/wp-includes/css/dist/editor/
https://web.hs.edu.tw/wp-includes/fonts/
https://web.hs.edu.tw/wp-includes/images/
https://web.hs.edu.tw/wp-includes/js/
https://web.hs.edu.tw/wp-includes/js/dist/
https://web.hs.edu.tw/wp-includes/js/dist/hooks.min.js
https://web.hs.edu.tw/wp-includes/js/dist/i18n.min.js
https://web.hs.edu.tw/wp-includes/js/dist/vendor/
https://web.hs.edu.tw/wp-includes/js/dist/vendor/lodash.min.js
https://web.hs.edu.tw/wp-includes/js/dist/vendor/regenerator-runtime.min.js
https://web.hs.edu.tw/wp-includes/js/dist/vendor/wp-polyfill.min.js
https://web.hs.edu.tw/wp-includes/js/imagesloaded.min.js
https://web.hs.edu.tw/wp-includes/js/jquery/
https://web.hs.edu.tw/wp-includes/js/jquery/jquery-migrate.min.js
https://web.hs.edu.tw/wp-includes/js/jquery/jquery.min.js
https://web.hs.edu.tw/wp-includes/js/plupload/
https://web.hs.edu.tw/wp-includes/js/wp-emoji-release.min.js
https://web.hs.edu.tw/wp-includes/js/wp-util.min.js
https://web.hs.edu.tw/wp-includes/js/zxcvbn-async.min.js
https://web.hs.edu.tw/wp-includes/js/zxcvbn.min.js
https://web.hs.edu.tw/wp-includes/wlwmanifest.xml
https://web.hs.edu.tw/wp-includes/wp-admin/
https://web.hs.edu.tw/wp-includes/wp-content/
https://web.hs.edu.tw/wp-includes/wp-includes/
https://web.hs.edu.tw/wp-json/
https://web.hs.edu.tw/wp-json/oembed/
https://web.hs.edu.tw/wp-json/oembed/1.0/
https://web.hs.edu.tw/wp-json/oembed/1.0/embed
https://web.hs.edu.tw/wp-json/wp/
https://web.hs.edu.tw/wp-json/wp/v2/
https://web.hs.edu.tw/wp-json/wp/v2/categories/
https://web.hs.edu.tw/wp-json/wp/v2/categories/15
https://web.hs.edu.tw/wp-json/wp/v2/categories/26
https://web.hs.edu.tw/wp-json/wp/v2/categories/3
https://web.hs.edu.tw/wp-json/wp/v2/categories/5
https://web.hs.edu.tw/wp-json/wp/v2/categories/7
https://web.hs.edu.tw/wp-json/wp/v2/categories/8
https://web.hs.edu.tw/wp-json/wp/v2/categories/9
https://web.hs.edu.tw/wp-json/wp/v2/pages/
https://web.hs.edu.tw/wp-json/wp/v2/pages/1436
https://web.hs.edu.tw/wp-json/wp/v2/pages/160
https://web.hs.edu.tw/wp-json/wp/v2/pages/162
https://web.hs.edu.tw/wp-json/wp/v2/pages/190
https://web.hs.edu.tw/wp-json/wp/v2/pages/203
https://web.hs.edu.tw/wp-json/wp/v2/pages/224
https://web.hs.edu.tw/wp-json/wp/v2/pages/390
https://web.hs.edu.tw/wp-json/wp/v2/pages/87
https://web.hs.edu.tw/wp-json/wp/v2/posts/
https://web.hs.edu.tw/wp-json/wp/v2/posts/1004
https://web.hs.edu.tw/wp-json/wp/v2/posts/1006
https://web.hs.edu.tw/wp-json/wp/v2/posts/1232
https://web.hs.edu.tw/wp-json/wp/v2/posts/1378
https://web.hs.edu.tw/wp-json/wp/v2/posts/138
https://web.hs.edu.tw/wp-json/wp/v2/posts/140
https://web.hs.edu.tw/wp-json/wp/v2/posts/142
https://web.hs.edu.tw/wp-json/wp/v2/posts/144
https://web.hs.edu.tw/wp-json/wp/v2/posts/1834

https://web.hs.edu.tw/wp-json/wp/v2/posts/230
https://web.hs.edu.tw/wp-json/wp/v2/posts/2315
https://web.hs.edu.tw/wp-json/wp/v2/posts/238
https://web.hs.edu.tw/wp-json/wp/v2/posts/2384
https://web.hs.edu.tw/wp-json/wp/v2/posts/2420
https://web.hs.edu.tw/wp-json/wp/v2/posts/2664
https://web.hs.edu.tw/wp-json/wp/v2/posts/344
https://web.hs.edu.tw/wp-json/wp/v2/posts/362
https://web.hs.edu.tw/wp-json/wp/v2/posts/369
https://web.hs.edu.tw/wp-json/wp/v2/posts/520
https://web.hs.edu.tw/wp-json/wp/v2/posts/540
https://web.hs.edu.tw/wp-json/wp/v2/posts/630
https://web.hs.edu.tw/wp-json/wp/v2/posts/632
https://web.hs.edu.tw/wp-json/wp/v2/posts/644
https://web.hs.edu.tw/wp-json/wp/v2/posts/653
https://web.hs.edu.tw/wp-json/wp/v2/posts/660
https://web.hs.edu.tw/wp-json/wp/v2/posts/662
https://web.hs.edu.tw/wp-json/wp/v2/posts/788
https://web.hs.edu.tw/wp-json/wp/v2/posts/821
https://web.hs.edu.tw/wp-json/wp/v2/posts/878
https://web.hs.edu.tw/wp-json/wp/v2/posts/900
https://web.hs.edu.tw/wp-json/wp/v2/posts/926
https://web.hs.edu.tw/wp-json/wp/v2/posts/934
https://web.hs.edu.tw/wp-json/wp/v2/tags/
https://web.hs.edu.tw/wp-json/wp/v2/tags/18
https://web.hs.edu.tw/wp-json/wp/v2/tags/19
https://web.hs.edu.tw/wp-json/wp/v2/tags/27
https://web.hs.edu.tw/wp-json/wp/v2/users/
https://web.hs.edu.tw/wp-json/wp/v2/users/1436
https://web.hs.edu.tw/wp-json/wp/v2/users/1651
https://web.hs.edu.tw/wp-json/wp/v2/users/4
https://web.hs.edu.tw/wp-json/wp/v2/users/5
https://web.hs.edu.tw/wp-json/wp/v2/users/961
https://web.hs.edu.tw/wp-login.php
https://web.hs.edu.tw/xmlrpc.php