



Site: <https://hespst.mcu.edu.tw>

Generated on , 10 9 2026 15:55:25

ZAP Version: 2.17.0

ZAP by [Checkmarx](#)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	8
Informational	3

Insights

Level	Reason	Site	Description	Statistic
Info	Informational	https://hespst.mcu.edu.tw	Percentage of responses with status code 2xx	26 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of responses with status code 3xx	7 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of responses with status code 4xx	64 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of responses with status code 5xx	1 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with content type image/jpeg	3 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with	3 %

			content type image /png	
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with content type text /css	31 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with content type text /html	15 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with content type text /javascript	43 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with content type text /plain	3 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with method GET	96 %
Info	Informational	https://hespst.mcu.edu.tw	Percentage of endpoints with method POST	3 %
Info	Informational	https://hespst.mcu.edu.tw	Count of total endpoints	32
Info	Informational	https://hespst.mcu.edu.tw	Percentage of slow responses	70 %

	Risk Level	Number of Instances
Application Error Disclosure	Low	1
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1
Cookie No HttpOnly Flag	Low	5
Cookie Without Secure Flag	Low	Systemic

Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
Strict-Transport-Security Header Not Set	Low	Systemic
Timestamp Disclosure - Unix	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	5
Re-examine Cache-control Directives	Informational	3
Session Management Response Identified	Informational	5

Alert Detail

Low	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login ()(_token,captcha,captcha_key,password,uid)
	POST
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	550
WASC Id	13
Plugin Id	90022

Low	Big Redirect Detected (Potential Sensitive Information Leak)
Description	The server has responded with a redirect that seems to provide a large response. This may indicate also responded with body content (which may include sensitive details, PII, etc.).
URL	https://hespst.mcu.edu.tw/mcu/oauth
Node Name	https://hespst.mcu.edu.tw/mcu/oauth
	GET
Evidence	
Other Info	Location header URI length: 332 [https://auth.mcu.edu.tw/oauth2/authorize?response_type=code&client_id=19e9ee7686bfcff17101d81a482aec1cb12163c274c1dbbfd3d45tw&redirect_uri=https%3A%2F%2Fhespst.mcu.edu.tw%2Fmcu%2Foauth%2Fcallback&scope=openid+email+profile&state=Tur5q0yDaJonGcaGQpXYbNZDIbpTDYT&nc Predicted response size: 632. Response Body Length: 1,654.
Instances	1

Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://hespst.mcu.edu.tw/mcu/oauth
Node Name	https://hespst.mcu.edu.tw/mcu/oauth
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://hespst.mcu.edu.tw/sitemap.xml
Node Name	https://hespst.mcu.edu.tw/sitemap.xml
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login ()(_token,captcha,captcha_key,password,uid)
	POST

Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	5
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	Cookie Without Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	Set-Cookie: _session
Other Info	
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://hespst.mcu.edu.tw/sitemap.xml
Node Name	https://hespst.mcu.edu.tw/sitemap.xml
	GET
Evidence	Set-Cookie: _session
Other Info	

URL	https://hespst.mcu.edu.tw/sitemap.xml
Node Name	https://hespst.mcu.edu.tw/sitemap.xml
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	Systemic
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	Apache/2.4.65 (Ubuntu)
Other Info	
URL	https://hespst.mcu.edu.tw/css/custom.css?v=1788938435
Node Name	https://hespst.mcu.edu.tw/css/custom.css (v)
	GET
Evidence	Apache/2.4.65 (Ubuntu)
Other Info	
URL	https://hespst.mcu.edu.tw/css/jquery.tagsinput-revisited.css?v=1788938435
Node Name	https://hespst.mcu.edu.tw/css/jquery.tagsinput-revisited.css (v)
	GET
Evidence	Apache/2.4.65 (Ubuntu)
Other Info	

URL	https://hespst.mcu.edu.tw/modules/custom/css/loading-cover.css?v=1788938436
Node Name	https://hespst.mcu.edu.tw/modules/custom/css/loading-cover.css (v)
	GET
Evidence	Apache/2.4.65 (Ubuntu)
Other Info	
URL	https://hespst.mcu.edu.tw/robots.txt
Node Name	https://hespst.mcu.edu.tw/robots.txt
	GET
Evidence	Apache/2.4.65 (Ubuntu)
Other Info	
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	
Other Info	
URL	https://hespst.mcu.edu.tw/css/custom.css?v=1788938435
Node Name	https://hespst.mcu.edu.tw/css/custom.css (v)
	GET
Evidence	
Other Info	
URL	https://hespst.mcu.edu.tw/css/jquery.tagsinput-revisited.css?v=1788938435

Node Name	https://hespst.mcu.edu.tw/css/jquery.tagsinput-revisited.css (v)
	GET
Evidence	
Other Info	
URL	https://hespst.mcu.edu.tw/modules/custom/css/loading-cover.css?v=1788938436
Node Name	https://hespst.mcu.edu.tw/modules/custom/css/loading-cover.css (v)
	GET
Evidence	
Other Info	
URL	https://hespst.mcu.edu.tw/robots.txt
Node Name	https://hespst.mcu.edu.tw/robots.txt
	GET
Evidence	
Other Info	
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security-Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	1788938435
Other Info	1788938435, which evaluates to: 2026-09-09 15:20:35.
URL	https://hespst.mcu.edu.tw/

Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	1788938436
Other Info	1788938436, which evaluates to: 2026-09-09 15:20:36.
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login
	GET
Evidence	1788938435
Other Info	1788938435, which evaluates to: 2026-09-09 15:20:35.
URL	https://hespst.mcu.edu.tw/sitemap.xml
Node Name	https://hespst.mcu.edu.tw/sitemap.xml
	GET
Evidence	1788938435
Other Info	1788938435, which evaluates to: 2026-09-09 15:20:35.
URL	https://hespst.mcu.edu.tw/sitemap.xml
Node Name	https://hespst.mcu.edu.tw/sitemap.xml
	GET
Evidence	1788938436
Other Info	1788938436, which evaluates to: 2026-09-09 15:20:36.
Instances	Systemic
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://hespst.mcu.edu.tw/
Node	

Name	https://hespst.mcu.edu.tw/
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hespst.mcu.edu.tw/css/custom.css?v=1788938435
Node Name	https://hespst.mcu.edu.tw/css/custom.css (v)
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hespst.mcu.edu.tw/css/jquery.taginput-revisited.css?v=1788938435
Node Name	https://hespst.mcu.edu.tw/css/jquery.taginput-revisited.css (v)
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hespst.mcu.edu.tw/modules/custom/css/loading-cover.css?v=1788938436
Node Name	https://hespst.mcu.edu.tw/modules/custom/css/loading-cover.css (v)
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://hespst.mcu.edu.tw/robots.txt
Node Name	https://hespst.mcu.edu.tw/robots.txt
	GET
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	Systemic

Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://hespst.mcu.edu.tw/js/jquery.tagsinput-revisited.js?v=1788938435
Node Name	https://hespst.mcu.edu.tw/js/jquery.tagsinput-revisited.js (v)
	GET
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// If a user types a delimiter create a new tag", see evidence field for the suspicious comment/snippet.
URL	https://hespst.mcu.edu.tw/js/jquery/jquery-3.5.1.min.js?v=1788938435
Node Name	https://hespst.mcu.edu.tw/js/jquery/jquery-3.5.1.min.js (v)
	GET
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//, Rt={},Mt={},It="*".concat(""),Wt=E.createElement("a");function Ft(o){return function(e,t){\"string\"!=typeof e&&(t=e,e="*");v", see evidence field for the suspicious comment/snippet.
URL	https://hespst.mcu.edu.tw/js/theme/sidebar/bootstrap/5.1.3/bootstrap.bundle.min.js?v=1788938435
Node Name	https://hespst.mcu.edu.tw/js/theme/sidebar/bootstrap/5.1.3/bootstrap.bundle.min.js (v)
	GET
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper.js.org)"); let e = this._element; \"parent\" === this._config.reference ? e = t : o(this._config.reference) ? e = r(this._", see evidence field for the suspicious comment/snippet.
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login
	GET
Evidence	user
Other	The following pattern was used: \bUSER\b and was detected in likely comment: "//hespst.

Info	mcu.edu.tw/modules/user/js/login.js?v=1788938436"></script>", see evidence field for the suspicious comment/snippet.
URL	https://hespst.mcu.edu.tw/vendor/handlebars/4.7.7/handlebars.runtime.js?v=1788938435
Node Name	https://hespst.mcu.edu.tw/vendor/handlebars/4.7.7/handlebars.runtime.js (v)
	GET
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// Sourced from lodash", see evidence field for the suspicious comment/snippet.
Instances	5
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	no-cache, private
Other Info	
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login
	GET
Evidence	no-cache, private
Other Info	
URL	https://hespst.mcu.edu.tw/robots.txt
Node Name	https://hespst.mcu.edu.tw/robots.txt
	GET
Evidence	
Other Info	

Instances	3
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://hespst.mcu.edu.tw/
Node Name	https://hespst.mcu.edu.tw/
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://hespst.mcu.edu.tw/mcu/oauth
Node Name	https://hespst.mcu.edu.tw/mcu/oauth
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://hespst.mcu.edu.tw/sitemap.xml
Node Name	https://hespst.mcu.edu.tw/sitemap.xml
	GET
Evidence	_session

Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://hespst.mcu.edu.tw/login
Node Name	https://hespst.mcu.edu.tw/login ()(_token,captcha,captcha_key,password,uid)
	POST
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
Instances	5
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112