ZAP Scanning Report - https://is.ypu.edu.tw

Automated report generated by OWASP ZAP Automation Framework

Site: https://is.ypu.edu.tw

Generated on Tue, 25 Aug 2026 03:38:24

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	7
Informational	3
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Missing Anti-clickjacking Header	Medium	3
Sub Resource Integrity Attribute Missing	Medium	Systemic
Big Redirect Detected (Potential Sensitive Information Leak)	Low	6
Cookie No HttpOnly Flag	Low	Systemic
Cookie Without Secure Flag	Low	Systemic
Cookie without SameSite Attribute	Low	Systemic
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	Systemic
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
X-Content-Type-Options Header Missing	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	2
Re-examine Cache-control Directives	Informational	4
Session Management Response Identified	Informational	8

Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
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. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Sub Resource Integrity Attribute Missing**
Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	<link href="https://fonts.googleapis.com/css?family=Raleway:100,600" rel="stylesheet" type="text/css">

Other Info	
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	<link href="https://use.fontawesome.com/releases/v5.8.2/css/all.css" rel="stylesheet" type="text/css">
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	<link href="https://fonts.googleapis.com/css?family=Raleway:100,600" rel="stylesheet" type="text/css">
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	<link href="https://use.fontawesome.com/releases/v5.8.2/css/all.css" rel="stylesheet" type="text/css">
Other Info	
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget
Method	GET
Attack	
Evidence	<link href="https://fonts.googleapis.com/css?family=Raleway:100,600" rel="stylesheet" type="text/css">
Other Info	
Instances	Systemic
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Defenses/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

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 that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://is.ypu.edu.tw/login]. Predicted response size: 327. Response Body Length: 354.
URL	https://is.ypu.edu.tw/google/login
Node Name	https://is.ypu.edu.tw/google/login
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 372 [https://accounts.google.com/o/oauth2/auth?response_type=code&access_type=offline&client_id=860657235902-i19dkdd2lvegurjj0bp5hnknplordqu7.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fis.ypu.edu.tw%2Fgoogle%2Flogin&state&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.email%20https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fuserinfo.profile&approval_prompt=auto]. Predicted response size: 672. Response Body Length: 1,830.
URL	https://is.ypu.edu.tw/sitemap.xml
Node Name	https://is.ypu.edu.tw/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://is.ypu.edu.tw/login]. Predicted response size: 327. Response Body Length: 354.
URL	https://is.ypu.edu.tw/sso
Node Name	https://is.ypu.edu.tw/sso
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://is.ypu.edu.tw/login]. Predicted response size: 327. Response Body Length: 354.

URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login ()(_token,captcha,captcha_key,password,uid)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://is.ypu.edu.tw/login]. Predicted response size: 327. Response Body Length: 354.
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget ()(_token,phone,submit,uid)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 33 [https://is.ypu.edu.tw/user/forget]. Predicted response size: 333. Response Body Length: 378.
Instances	6
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
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://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/google/login
Node Name	https://is.ypu.edu.tw/google/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN

Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/sso
Node Name	https://is.ypu.edu.tw/sso
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	Systemic
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://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	Set-Cookie: _session
Other Info	
URL	https://is.ypu.edu.tw
Node	

Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	Set-Cookie: _session
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/sso
Node Name	https://is.ypu.edu.tw/sso
Method	GET
Attack	
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	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw

Method	GET
Attack	
Evidence	Set-Cookie: _session
Other Info	
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	Set-Cookie: _session
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	https://is.ypu.edu.tw/sso
Node Name	https://is.ypu.edu.tw/sso
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	Systemic
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	https://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	X-Powered-By: PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/google/login
Node Name	https://is.ypu.edu.tw/google/login
Method	GET
Attack	
Evidence	X-Powered-By: PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	X-Powered-By: PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/sitemap.xml
Node Name	https://is.ypu.edu.tw/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/sso
Node Name	https://is.ypu.edu.tw/sso
Method	GET
Attack	
Evidence	X-Powered-By: PHP/7.4.8
Other Info	
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10037

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://is.ypu.edu.tw/css/custom.css
Node Name	https://is.ypu.edu.tw/css/custom.css
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/css/layout.css
Node Name	https://is.ypu.edu.tw/css/layout.css
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/images/logo.png
Node Name	https://is.ypu.edu.tw/images/logo.png
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/modules/user/css/login.css
Node Name	https://is.ypu.edu.tw/modules/user/css/login.css
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/7.4.8
Other Info	
URL	https://is.ypu.edu.tw/robots.txt
Node Name	https://is.ypu.edu.tw/robots.txt

Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/7.4.8
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	**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://is.ypu.edu.tw/css/custom.css
Node Name	https://is.ypu.edu.tw/css/custom.css
Method	GET
Attack	
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://is.ypu.edu.tw/css/layout.css
Node Name	https://is.ypu.edu.tw/css/layout.css
Method	GET
Attack	
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://is.ypu.edu.tw/images/logo.png
Node Name	https://is.ypu.edu.tw/images/logo.png
Method	GET
Attack	
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://is.ypu.edu.tw/modules/user/css/login.css
Node Name	https://is.ypu.edu.tw/modules/user/css/login.css
Method	GET
Attack	
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://is.ypu.edu.tw/robots.txt
Node Name	https://is.ypu.edu.tw/robots.txt
Method	GET
Attack	
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://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	tps://is.ypu.edu.tw/user/forget"></a-->
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "<!--a class="btn btn-outline-dark btn-block" href="https://is.ypu.edu.tw/user/forget"></a-->", see evidence field for the suspicious comment/snippet.

URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	tps://is.ypu.edu.tw/user/forget"></a-->
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "<!--a class="btn btn-outline-dark btn-block" href="https://is.ypu.edu.tw/user/forget"></a-->", see evidence field for the suspicious comment/snippet.
Instances	2
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://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://is.ypu.edu.tw/robots.txt
Node Name	https://is.ypu.edu.tw/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://is.ypu.edu.tw/user/forget

Node Name	https://is.ypu.edu.tw/user/forget
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
Instances	4
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://is.ypu.edu.tw
Node Name	https://is.ypu.edu.tw
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/google/login
Node Name	https://is.ypu.edu.tw/google/login
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	_session

Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/sso
Node Name	https://is.ypu.edu.tw/sso
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login ()(_token,captcha,captcha_key,password,uid)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/user/forget
Node Name	https://is.ypu.edu.tw/user/forget ()(_token,phone,submit,uid)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://is.ypu.edu.tw/login
Node Name	https://is.ypu.edu.tw/login
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session
Instances	8

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