ZAP Scanning Report - https://exam.manco.tw

Automated report generated by OWASP ZAP Automation Framework

Site: https://exam.manco.tw

Generated on Thu, 29 Oct 2026 08:52:42

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	3
Informational	4
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Sub Resource Integrity Attribute Missing	Medium	2
Big Redirect Detected (Potential Sensitive Information Leak)	Low	7
Cross-Domain JavaScript Source File Inclusion	Low	2
Timestamp Disclosure - Unix	Low	1
Authentication Request Identified	Informational	2
Information Disclosure - Suspicious Comments	Informational	1
Re-examine Cache-control Directives	Informational	Systemic
Session Management Response Identified	Informational	14

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://exam.manco.tw
Node Name	https://exam.manco.tw
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exam.manco.tw/privacy
Node Name	https://exam.manco.tw/privacy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exam.manco.tw/sitemap.xml
Node Name	https://exam.manco.tw/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
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	**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://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login
Method	GET
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client" async defer onload="initGoogleSignIn()"></script>
Other Info	
URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login
Method	GET
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client" async defer onload="initGoogleSignIn()"></script>
Other Info	
Instances	2
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://exam.manco.tw/candidate/products
Node Name	https://exam.manco.tw/candidate/products
Method	GET
Attack	

Evidence	
Other Info	Location header URI length: 37 [https://exam.manco.tw/candidate/login]. Predicted response size: 337. Response Body Length: 394.
URL	https://exam.manco.tw/exams
Node Name	https://exam.manco.tw/exams
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://exam.manco.tw/login]. Predicted response size: 327. Response Body Length: 354.
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 37 [https://exam.manco.tw/candidate/login]. Predicted response size: 337. Response Body Length: 394.
URL	https://exam.manco.tw/candidate/login/google
Node Name	https://exam.manco.tw/candidate/login/google ()(_token,credential)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 37 [https://exam.manco.tw/candidate/login]. Predicted response size: 337. Response Body Length: 394.
URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://exam.manco.tw/login]. Predicted response size: 327. Response Body Length: 354.
URL	https://exam.manco.tw/login/google

Node Name	https://exam.manco.tw/login/google ()(_token,credential)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 27 [https://exam.manco.tw/login]. Predicted response size: 327. Response Body Length: 354.
URL	https://exam.manco.tw/register
Node Name	https://exam.manco.tw/register ()(_token,email,name,password,password_confirmation)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 30 [https://exam.manco.tw/register]. Predicted response size: 330. Response Body Length: 366.
Instances	7
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	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login
Method	GET
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client" async defer onload="initGoogleSignIn()"></script>
Other Info	
URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login
Method	GET
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client" async defer onload="initGoogleSignIn()"></script>
Other Info	

Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login
Method	GET
Attack	
Evidence	1791860839
Other Info	1791860839, which evaluates to: 2026-10-13 03:07:19.
Instances	1
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

Informational	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://exam.manco.tw/candidate/login csrfToken=_token
URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login ()(_token,email,password,remember)
Method	POST

Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://exam.manco.tw/login csrfToken=_token
Instances	2
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/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://exam.manco.tw/vendor/marked.min.js
Node Name	https://exam.manco.tw/vendor/marked.min.js
Method	GET
Attack	
Evidence	s file is generated from files in ./src/ */
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "/** * DO NOT EDIT THIS FILE * The code in this file is generated from files in ./src/ */", see evidence field for the suspicious comment/snippet.
Instances	1
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://exam.manco.tw
Node Name	https://exam.manco.tw
Method	GET
Attack	

Evidence	no-cache, private
Other Info	
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://exam.manco.tw/manifest.json
Node Name	https://exam.manco.tw/manifest.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exam.manco.tw/privacy
Node Name	https://exam.manco.tw/privacy
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://exam.manco.tw/robots.txt
Node Name	https://exam.manco.tw/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
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://exam.manco.tw
Node Name	https://exam.manco.tw
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/
Node Name	https://exam.manco.tw/
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/candidate/products
Node Name	https://exam.manco.tw/candidate/products
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/exams
Node Name	https://exam.manco.tw/exams
Method	GET
Attack	
Evidence	XSRF-TOKEN

Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/practice
Node Name	https://exam.manco.tw/practice
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/privacy
Node Name	https://exam.manco.tw/privacy
Method	GET
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/candidate/login
Node Name	https://exam.manco.tw/candidate/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/candidate/login/google
Node Name	https://exam.manco.tw/candidate/login/google ()(_token,credential)
Method	POST
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session

URL	https://exam.manco.tw/login
Node Name	https://exam.manco.tw/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/login/google
Node Name	https://exam.manco.tw/login/google ()(_token,credential)
Method	POST
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw/register
Node Name	https://exam.manco.tw/register ()(_token,email,name,password,password_confirmation)
Method	POST
Attack	
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN cookie:-session
URL	https://exam.manco.tw
Node Name	https://exam.manco.tw
Method	GET
Attack	
Evidence	-session
Other Info	cookie:-session
Instances	14
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