ZAP Scanning Report - https://vpnadmin.steps.tw

Automated report generated by OWASP ZAP Automation Framework

Site: https://vpnadmin.steps.tw

Generated on Tue, 25 Aug 2026 06:13:17

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	5
CSP: Wildcard Directive	Medium	5
CSP: script-src unsafe-inline	Medium	5
CSP: style-src unsafe-inline	Medium	5
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3
Timestamp Disclosure - Unix	Low	3
Authentication Request Identified	Informational	1
Re-examine Cache-control Directives	Informational	5
Session Management Response Identified	Informational	6

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://vpnadmin.steps.tw
Node	

Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://vpnadmin.steps.tw/
Node Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://vpnadmin.steps.tw/sitemap.xml
Node Name	https://vpnadmin.steps.tw/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
Instances	5

Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: Wildcard Directive**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://vpnadmin.steps.tw
Node Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	https://vpnadmin.steps.tw/
Node Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:

Info	img-src
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
URL	https://vpnadmin.steps.tw/sitemap.xml
Node Name	https://vpnadmin.steps.tw/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: img-src
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: script-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://vpnadmin.steps.tw
Node Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none';

	base-uri 'self'; form-action 'self'
Other Info	script-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/
Node Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	script-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	script-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	script-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/sitemap.xml
Node Name	https://vpnadmin.steps.tw/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	script-src includes unsafe-inline.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy

	https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: style-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://vpnadmin.steps.tw
Node Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/
Node Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login
Method	GET
Attack	

Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
URL	https://vpnadmin.steps.tw/sitemap.xml
Node Name	https://vpnadmin.steps.tw/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:; img-src 'self' data: blob: https:; connect-src 'self'; frame-src 'none'; object-src 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

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 indi server sent a redirect it also responded with body content (which may include sensitive details,
URL	https://vpnadmin.steps.tw/auth/google
Node Name	https://vpnadmin.steps.tw/auth/google
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 287 [https://accounts.google.com/o/oauth2/auth?client_id=425500 fvhlttpmjrtsu9o5gtrto5e076q177lp.apps.googleusercontent.com&redirect_uri=https%3A%2F%2 2Fgoogle% 2Fcallback&scope=openid+profile+email&response_type=code&state=SAkR5lxVW5rgvyJ0Re9 Predicted response size: 587. Response Body Length: 1,458.
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password ()(_token,email)
Method	POST
Attack	
Evidence	
	Location header URI length: 41 [https://vpnadmin.steps.tw/forgot-password].

Other Info	Predicted response size: 341. Response Body Length: 410.
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 31 [https://vpnadmin.steps.tw/login]. Predicted response size: 331. Response Body Length: 370.
Instances	3
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses shoul
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://vpnadmin.steps.tw
Node Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	1786329254
Other Info	1786329254, which evaluates to: 2026-08-10 02:34:14.
URL	https://vpnadmin.steps.tw/
Node Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	1786329254
Other Info	1786329254, which evaluates to: 2026-08-10 02:34:14.
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login
Method	GET
Attack	
Evidence	1786329247
Other Info	1786329247, which evaluates to: 2026-08-10 02:34:07.

Instances	3
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://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login ()(_token,email,password,remember)
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://vpnadmin.steps.tw/login csrfToken=_token
Instances	1
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	**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://vpnadmin.steps.tw
Node Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://vpnadmin.steps.tw/
Node	

Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login
Method	GET
Attack	
Evidence	no-cache, private
Other Info	
URL	https://vpnadmin.steps.tw/robots.txt
Node Name	https://vpnadmin.steps.tw/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
Instances	5
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://vpnadmin.steps.tw
Node Name	https://vpnadmin.steps.tw
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://vpnadmin.steps.tw/
Node Name	https://vpnadmin.steps.tw/
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://vpnadmin.steps.tw/auth/google
Node Name	https://vpnadmin.steps.tw/auth/google
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://vpnadmin.steps.tw/forgot-password
Node Name	https://vpnadmin.steps.tw/forgot-password ()(_token,email)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	https://vpnadmin.steps.tw/login
Node Name	https://vpnadmin.steps.tw/login ()(_token,email,password,remember)

Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
Instances	6
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