OWASP ZAP Scan Report

Target: http://3.110.88.164/

All scanned sites: http://3.110.88.164

Javascript included from: http://3.110.88.164

Generated on Mon, 10 Jun 2024 09:10:01

ZAP Version: 2.15.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	2
Informational	1

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
Cookie No HttpOnly Flag	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4
Session Management Response Identified	Informational	1

Passing Rules

Name	Rule Type	Threshold	Strength
Verification Request Identified	Passive	MEDIUM	-
Private IP Disclosure	Passive	MEDIUM	-
Session ID in URL Rewrite	Passive	MEDIUM	-
Insecure JSF ViewState	Passive	MEDIUM	-
Vulnerable JS Library (Powered by Retire.js)	Passive	MEDIUM	-
Charset Mismatch	Passive	MEDIUM	-
Cookie Without Secure Flag	Passive	MEDIUM	-
Re-examine Cache-control Directives	Passive	MEDIUM	-
Cross-Domain JavaScript Source File Inclusion	Passive	MEDIUM	-
Content-Type Header Missing	Passive	MEDIUM	-
Anti-clickjacking Header	Passive	MEDIUM	-

X-Content-Type-Options Header Missing	Passive	MEDIUM	-
Application Error Disclosure	Passive	MEDIUM	-
Information Disclosure - Debug Error Messages	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in URL	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in HTTP Referrer Header	Passive	MEDIUM	-
Information Disclosure - Suspicious Comments	Passive	MEDIUM	-
Open Redirect	Passive	MEDIUM	-
Cookie Poisoning	Passive	MEDIUM	-
User Controllable Charset	Passive	MEDIUM	-
WSDL File Detection	Passive	MEDIUM	-
User Controllable HTML Element Attribute (Potential XSS)	Passive	MEDIUM	-
Loosely Scoped Cookie	Passive	MEDIUM	-
Viewstate	Passive	MEDIUM	-
Directory Browsing	Passive	MEDIUM	-
Heartbleed OpenSSL Vulnerability (Indicative)	Passive	MEDIUM	-
Strict-Transport-Security Header	Passive	MEDIUM	-
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Passive	MEDIUM	-
X-Backend-Server Header Information Leak	Passive	MEDIUM	-
Secure Pages Include Mixed Content	Passive	MEDIUM	-
HTTP to HTTPS Insecure Transition in Form Post	Passive	MEDIUM	-
HTTPS to HTTP Insecure Transition in Form Post	Passive	MEDIUM	-
User Controllable JavaScript Event (XSS)	Passive	MEDIUM	-
Big Redirect Detected (Potential Sensitive Information Leak)	Passive	MEDIUM	-
Retrieved from Cache	Passive	MEDIUM	-
X-ChromeLogger-Data (XCOLD) Header Information Leak	Passive	MEDIUM	-
Cookie without SameSite Attribute	Passive	MEDIUM	-
CSP	Passive	MEDIUM	-
X-Debug-Token Information Leak	Passive	MEDIUM	-
Username Hash Found	Passive	MEDIUM	-
X-AspNet-Version Response Header	Passive	MEDIUM	-
PII Disclosure	Passive	MEDIUM	-
Script Passive Scan Rules	Passive	MEDIUM	-
Stats Passive Scan Rule	Passive	MEDIUM	-
Absence of Anti-CSRF Tokens	Passive	MEDIUM	-
Timestamp Disclosure	Passive	MEDIUM	-
Hash Disclosure	Passive	MEDIUM	-
Cross-Domain Misconfiguration	Passive	MEDIUM	-
Weak Authentication Method	Passive	MEDIUM	-
Reverse Tabnabbing	Passive	MEDIUM	-
Modern Web Application	Passive	MEDIUM	-
Authentication Request Identified	Passive	MEDIUM	-

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	http://3.110.88.164/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://3.110.88.164/login/
Method	GET
Parameter	
Attack	
Evidence	
URL	http://3.110.88.164/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	http://3.110.88.164/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Instances	4
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/Security/CSP/Introducing_Content_Security_Policy 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

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	http://3.110.88.164/login/
Method	GET
Parameter	csrftoken

Attack	
Evidence	Set-Cookie: csrftoken
Instances	1
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	**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	http://3.110.88.164/
Method	GET
Parameter	
Attack	
Evidence	WSGIServer/0.2 CPython/3.12.3
URL	http://3.110.88.164/login/
Method	GET
Parameter	
Attack	
Evidence	WSGIServer/0.2 CPython/3.12.3
URL	http://3.110.88.164/robots.txt
Method	GET
Parameter	
Attack	
Evidence	WSGIServer/0.2 CPython/3.12.3
URL	http://3.110.88.164/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	WSGIServer/0.2 CPython/3.12.3
Instances	4
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	200
WASC Id	13
Plugin Id	10036

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	http://3.110.88.164/login/
Method	GET
Parameter	csrftoken
Attack	
Evidence	GfDnv7o7VmF49TENkek6xgFV1XAPIGp9
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/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112