ZAP Scanning Report - http://120.126.223.31/

Automated report generated by OWASP ZAP Automation Framework

Site: http://120.126.223.31

Generated on Tue, 25 Aug 2026 03:59:13

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Big Redirect Detected (Potential Sensitive Information Leak)	Low	4
Cookie No HttpOnly Flag	Low	Systemic
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
Information Disclosure - Suspicious Comments	Informational	2
Session Management Response Identified	Informational	9

Alert Detail

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	http://120.126.223.31/login/dedicated_tutor
Node Name	http://120.126.223.31/login/dedicated_tutor ()(_token,action,captcha,password,uid)
Method	POST
Attack	

Evidence	
Other Info	Location header URI length: 43 [http://120.126.223.31/login/dedicated_tutor]. Predicted response size: 343. Response Body Length: 418.
URL	http://120.126.223.31/login/manager
Node Name	http://120.126.223.31/login/manager ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 35 [http://120.126.223.31/login/manager]. Predicted response size: 335. Response Body Length: 386.
URL	http://120.126.223.31/login/mentor
Node Name	http://120.126.223.31/login/mentor ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 34 [http://120.126.223.31/login/mentor]. Predicted response size: 334. Response Body Length: 382.
URL	http://120.126.223.31/login/student
Node Name	http://120.126.223.31/login/student ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 35 [http://120.126.223.31/login/student]. Predicted response size: 335. Response Body Length: 386.
Instances	4
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	http://120.126.223.31/
Node Name	http://120.126.223.31/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/dedicated_tutor
Node Name	http://120.126.223.31/login/dedicated_tutor
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/manager
Node Name	http://120.126.223.31/login/manager
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/mentor
Node Name	http://120.126.223.31/login/mentor
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/student
Node Name	http://120.126.223.31/login/student
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	**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://120.126.223.31/
Node Name	http://120.126.223.31/
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/css/theme/frontend/style.min.css
Node Name	http://120.126.223.31/css/theme/frontend/style.min.css
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/css/alert.css
Node Name	http://120.126.223.31/modules/custom/css/alert.css
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/robots.txt
Node Name	http://120.126.223.31/robots.txt
Method	GET
Attack	
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/sitemap.xml
Node Name	http://120.126.223.31/sitemap.xml
Method	GET
Attack	

Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
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

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://120.126.223.31/js/jquery.tagsinput-revisited.js
Node Name	http://120.126.223.31/js/jquery.tagsinput-revisited.js
Method	GET
Attack	
Evidence	// If a user types a delimiter c
Other Info	The following pattern was used: \bUSER\b and was detected 3 times, the first in likely comment: "// If a user types a delimiter create a new tag", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/vendor/handlebars/4.7.9/handlebars.runtime.min.js
Node Name	http://120.126.223.31/vendor/handlebars/4.7.9/handlebars.runtime.min.js
Method	GET
Attack	
Evidence	OTHERWISE, ARISING FROM, OUT OF OR IN CONNE
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "/**! @license handlebars v4.7.9 Copyright (C) 2011-2019 by Yehuda Katz Permission is hereby granted, free of charge, to any", 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	**Session Management Response Identified**
	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

Description	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://120.126.223.31/
Node Name	http://120.126.223.31/
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/dedicated_tutor
Node Name	http://120.126.223.31/login/dedicated_tutor
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/manager
Node Name	http://120.126.223.31/login/manager
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/mentor
Node Name	http://120.126.223.31/login/mentor
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/student
Node Name	http://120.126.223.31/login/student
Method	GET
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN

URL	http://120.126.223.31/login/dedicated_tutor
Node Name	http://120.126.223.31/login/dedicated_tutor ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/manager
Node Name	http://120.126.223.31/login/manager ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/mentor
Node Name	http://120.126.223.31/login/mentor ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/student
Node Name	http://120.126.223.31/login/student ()(_token,action,captcha,password,uid)
Method	POST
Attack	
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
Instances	9
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