ZAP by Checkmarx Scanning Report

Site: http://10.100.104.100

Generated on Tue, 12 Aug 2025 15:59:59

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	4

Alerts

Name	Risk Level	Number of Instances
.env Information Leak	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	4
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	2
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4
Authentication Request Identified	Informational	1
Session Management Response Identified	Informational	1
User Agent Fuzzer	Informational	24
User Controllable HTML Element Attribute (Potential XSS)	Informational	2

Alert Detail

Medium	.env Information Leak
Description	One or more .env files seems to have been located on the server. These files often expose infrastructure or administrative account credentials, API or APP keys, or other sensitive configuration information.
URL	http://10.100.104.100/Capstone_01-main/.env

Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	1
Solution	Ensure the .env file is not accessible.
Reference	https://www.google.com/search?q=db_password+filetype%3Aenv https://mobile.twitter.com/svblxyz/status/1045013939904532482
CWE Id	215
WASC Id	13
Plugin Id	40034

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://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.100.104.100/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.100.104.100/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	POST
Attack	
Evidence	
Other Info	
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://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
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	**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	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/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	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
Instances	2
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/2012/02/shhh-dont-let-your-response-headers.html
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	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	http://10.100.104.100/robots.txt
Method	GET
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	http://10.100.104.100/sitemap.xml
Method	GET
Attack	

Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	POST
Attack	
Evidence	Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Other Info	
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	497
WASC Id	13
Plugin Id	10036

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	http://10.100.104.100/Capstone_01-main/login.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=root passwordParam=password referer=http://10.100.104.100/Capstone_01-main/login.php csrfToken=csrf_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	**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://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	
Evidence	PHPSESSID
Other Info	cookie:PHPSESSID

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

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)

Attack	Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	24
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	**User Controllable HTML Element Attribute (Potential XSS)**
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://10.100.104.100/Capstone_01-

Other Info	main/login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: csrf_token=c8b702372bef8c58728ab03dc6160369a6190a20409d432e208ce398bc2c8b3b The user-controlled value was: c8b702372bef8c58728ab03dc6160369a6190a20409d432e208ce398bc2c8b3b
URL	http://10.100.104.100/Capstone_01-main/login.php
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://10.100.104.100/Capstone_01-main/login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: username=root The user-controlled value was: root
Instances	2
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031