ZAP Scanning Report

Site: http://192.168.254.209

Generated on Thu, 12 Oct 2023 21:20:54

ZAP Version: 2.13.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	4
Informational	1
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
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	2
Session Management Response Identified	Informational	2

Alert Detail

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://192.168.254.209/portal.php/
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	Set-Cookie: PHPSESSID
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://192.168.254.209/portal.php/
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	Set-Cookie: PHPSESSID
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://192.168.254.209/portal.php/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
URL	http://192.168.254.209/portal.php/login.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.5.9-1ubuntu4.14
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

	Server Leaks Version Information via "Server" HTTP Response Header Field

Low	
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://192.168.254.209/portal.php/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.7 (Ubuntu)
URL	http://192.168.254.209/portal.php/login.php
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.7 (Ubuntu)
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
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://192.168.254.209/portal.php/
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	jjf330q5pav0oajk278j8ihal7
URL	http://192.168.254.209/portal.php/
Method	GET
Parameter	PHPSESSID
Attack	
Evidence	jjf330q5pav0oajk278j8ihal7
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/session-mgmt-id
CWE Id	

WASC Id	
Plugin Id	10112