ZAP Scanning Report

Sites: http://localhost:8084 http://localhost:8083 http://localhost:8082 http://localhost:8081 http://localhost:8080

Generated on Sun, 7 Jul 2024 14:40:09

ZAP Version: 2.15.0

ZAP is supported by the [Crash Override Open Source Fellowship]()

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	10
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	10
Authentication Request Identified	Informational	2

Alert Detail

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://localhost:8081/api/products/search?id%5B%5D=1&id%5B%5D=2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8082/api/orders
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.20

Other Info	
URL	http://localhost:8084/api/orders
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8080/api/login
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8080/api/users/create
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8081/api/categories
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8081/api/products
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8082/api/orders
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
URL	http://localhost:8083/api/webhook/ml/pix
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	

URL	http://localhost:8084/api/orders/666caee86f2fe5907b03a832
Method	PUT
Attack	
Evidence	X-Powered-By: PHP/8.2.20
Other Info	
Instances	10
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	200
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://localhost:8081/api/products/search?id%5B%5D=1&id%5B%5D=2
Method	GET
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8082/api/orders
Method	GET
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8084/api/orders
Method	GET
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8080/api/login
Method	POST
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8080/api/users/create

Method	POST
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8081/api/categories
Method	POST
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8081/api/products
Method	POST
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8082/api/orders
Method	POST
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8083/api/webhook/ml/pix
Method	POST
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
URL	http://localhost:8084/api/orders/666caee86f2fe5907b03a832
Method	PUT
Attack	
Evidence	Apache/2.4.59 (Debian)
Other Info	
Instances	10
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	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://localhost:8080/api/users/create
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=user3@example.com passwordParam=password
URL	http://localhost:8080/api/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=mario@mario.com passwordParam=password
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/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111