ZAP by Checkmarx Scanning Report

Site: http://127.0.0.1:5000

Generated on pt., 30 sty 2026 19:10:46

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Poziom ryzyka	Number of Alerts
Wysoki	0
redni	1
Niski	2
Informacyjny	0

Insights

Level	Reason	Site	Description	Statistic
Informacje	Informacyjny	http://127.0.0.1:5000	Percentage of responses with status code 2xx	15 %
Informacje	Informacyjny	http://127.0.0.1:5000	Percentage of responses with status code 4xx	85 %
Informacje	Informacyjny	http://127.0.0.1:5000	Percentage of endpoints with content type text/html	100 %
Informacje	Informacyjny	http://127.0.0.1:5000	Percentage of endpoints with method GET	100 %
Informacje	Informacyjny	http://127.0.0.1:5000	Count of total endpoints	2
Informacje	Informacyjny	http://127.0.0.1:5000	Percentage of slow responses	5 %

Zagrozenia

Nazwa	Poziom ryzyka	Number of Instances
Content Security Policy (CSP) Header Not Set	redni	2
Server Leaks Version Information via "Server" HTTP Response Header Field	Niski	3
X-Content-Type-Options Header Missing	Niski	1

Alert Detail

redni	Content Security Policy (CSP) Header Not Set
Opis	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://127.0.0.1:5000/robots.txt
Node Name	http://127.0.0.1:5000/robots.txt
Metody	GET
Atak	
Evidence	
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Node Name	http://127.0.0.1:5000/sitemap.xml
Metody	GET
Atak	
Evidence	
Other Info	
Instances	2
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/HTTP/Guides/CSP 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

Niski	Server Leaks Version Information via "Server" HTTP Response Header Field
Opis	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://127.0.0.1:5000
Node Name	http://127.0.0.1:5000
Metody	GET
Atak	
Evidence	Werkzeug/3.1.5 Python/3.14.2
Other Info	
URL	http://127.0.0.1:5000/robots.txt
Node Name	http://127.0.0.1:5000/robots.txt
Metody	GET
Atak	
Evidence	Werkzeug/3.1.5 Python/3.14.2
Other Info	
URL	http://127.0.0.1:5000/sitemap.xml
Node Name	http://127.0.0.1:5000/sitemap.xml
Metody	GET
Atak	
Evidence	Werkzeug/3.1.5 Python/3.14.2
Other Info	
Instances	3
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

Niski	X-Content-Type-Options Header Missing
Opis	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://127.0.0.1:5000
Node Name	http://127.0.0.1:5000
Metody	GET

Atak	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021