Phishing Detector - OWASP ZAP Scan Report

Generated with ZAP on Tue 20 Jan 2026, at 16:38:58

ZAP Version: 2.17.0

ZAP by Checkmarx

Contents

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- `http://127.0.0.1:5000`

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: `High`, `Medium`, `Low`, `Informational`

Excluded: None

Confidence levels

Included: `User Confirmed`, `High`, `Medium`, `Low`

Excluded: `User Confirmed`, `High`, `Medium`, `Low`, `False Positive`

Summaries

Alert Counts by Risk and Confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	2 (25.0%)	0 (0.0%)	1 (12.5%)	3 (37.5%)
	Low	0 (0.0%)	1 (12.5%)	1 (12.5%)	0 (0.0%)	2 (25.0%)
	Informational	0 (0.0%)	1 (12.5%)	2 (25.0%)	0 (0.0%)	3 (37.5%)
	Total	0 (0.0%)	4 (50.0%)	3 (37.5%)	1 (12.5%)	8 (100%)

Alert Counts by Site and Risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

			Risk		
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	http://127.0.0.1:5000	0 (0)	3 (3)	2 (5)	3 (8)

Alert Counts by Alert Type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	4 (50.0%)
CSP: Failure to Define Directive with No Fallback	Medium	5 (62.5%)
CSP: style-src unsafe-inline	Medium	5 (62.5%)
Cookie without SameSite Attribute	Low	2 (25.0%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (62.5%)
Authentication Request Identified	Informational	1 (12.5%)
Total		8

Alert type	Risk	Count
Session Management Response Identified	Informational	2 (25.0%)
User Agent Fuzzer	Informational	5 (62.5%)
Total		8

Alerts

Risk=Medium, Confidence=High (2)

http://127.0.0.1:5000 (2)

CSP: Failure to Define Directive with No Fallback (1)

▶ GET http://127.0.0.1:5000/robots.txt

CSP: style-src unsafe-inline (1)

▶ GET http://127.0.0.1:5000/robots.txt

Risk=Medium, Confidence=Low (1)

http://127.0.0.1:5000 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://127.0.0.1:5000/login

Risk=Low, Confidence=High (1)

http://127.0.0.1:5000 (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://127.0.0.1:5000/static/styles.css

Risk=Low, Confidence=Medium (1)

http://127.0.0.1:5000 (1)

Cookie without SameSite Attribute (1)

▶ POST http://127.0.0.1:5000/register

Risk=Informational, Confidence=High (1)

http://127.0.0.1:5000 (1)

Authentication Request Identified (1)

▶ POST http://127.0.0.1:5000/login

Risk=Informational, Confidence=Medium (2)

http://127.0.0.1:5000 (2)

Session Management Response Identified (1)

▶ POST http://127.0.0.1:5000/register

User Agent Fuzzer (1)

▶ POST http://127.0.0.1:5000/login

Appendix

Alert Types

This section contains additional information on the types of alerts in the report.

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html ▪ https://cwe.mitre.org/data/definitions/352.html

CSP: Failure to Define Directive with No Fallback

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy

	- https://content-security-policy.com/ - https://github.com/HtmlUnit/htmlunit-csp - https://web.dev/articles/csp#resource-options

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	- https://www.w3.org/TR/CSP/ - https://caniuse.com/#search=content+security+policy - https://content-security-policy.com/ - https://github.com/HtmlUnit/htmlunit-csp - https://web.dev/articles/csp#resource-options

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	- https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

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

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
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/

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	- https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg