ZAP by Checkmarx Scanning Report

Generated with ZAP on вс 16 нояб. 2025, at 15:47:02

ZAP Version: 2.16.1

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:

- https://www.google.com
- https://accounts.google.com
- http://clients2.google.com
- http://testphp.vulnweb.com

(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: Высокий, Средний, Низкий, Информационный

Excluded: None

Confidence levels

Included: Пользователь подтвержден , Высокий, Средний, Низкий

Excluded: Пользователь подтвержден , Высокий, Средний, Низкий, Ложно-положительное

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				
		Пользователь подтвержден	Высокий	Средний	Низкий	Total
Risk	Высокий	0 (0,0 %)	0 (0,0 %)	2 (14,3 %)	0 (0,0 %)	2 (14,3 %)
	Средний	0 (0,0 %)	1 (7,1 %)	3 (21,4 %)	1 (7,1 %)	5 (35,7 %)
	Низкий	0 (0,0 %)	1 (7,1 %)	2 (14,3 %)	0 (0,0 %)	3 (21,4 %)
	Информационный	0 (0,0 %)	0 (0,0 %)	1 (7,1 %)	3 (21,4 %)	4 (28,6 %)
	Total	0 (0,0 %)	2 (14,3 %)	8 (57,1 %)	4 (28,6 %)	14 (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			
		Высокий (= Высокий)	Средний (>= Средний)	Низкий (>= Низкий)	Информационный (>= Информационный)
Site	http://testphp.vulnweb.com	2 (2)	5 (7)	3 (10)	4 (14)

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
SQL Injection - MySQL	Высокий	11 (78,6 %)
SQL-инъекция	Высокий	1 (7,1 %)
XSLT Инъекция	Средний	2 (14,3 %)
Заголовок Content Security Policy (CSP) не задан	Средний	73 (521,4 %)
Отсутствует заголовок (Header) для защиты от кликджекинга	Средний	53 (378,6 %)
Отсутствуют токены против CSRF атак	Средний	42 (300,0 %)
Просмотр каталогов	Средний	3 (21,4 %)
Total		14

Alert type	Risk	Count
Заголовок X-Content-Type-Options отсутствует	Низкий	81 (578,6 %)
Сервер утекает информацию через поля заголовка HTTP-ответа "X-Powered-By"	Низкий	74 (528,6 %)
Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»	Низкий	108 (771,4 %)
Authentication Request Identified	Информационный	2 (14,3 %)
Charset Mismatch (Header Versus Meta Content-Type Charset)	Информационный	35 (250,0 %)
Атрибут элемента HTML, управляемый пользователем (потенциальный XSS)	Информационный	4 (28,6 %)
Современное веб-приложение	Информационный	10 (71,4 %)
Total		14

Alerts

Risk=Высокий, Confidence=Средний (2)

http://testphp.vulnweb.com (2)

SQL Injection - MySQL (1)

▶ GET http://testphp.vulnweb.com/AJAX/infoartist.php?id=%27

SQL-инъекция (1)

▶ POST http://testphp.vulnweb.com/secured/newuser.php

Risk=Средний, Confidence=Высокий (1)

http://testphp.vulnweb.com (1)

Заголовок Content Security Policy (CSP) не задан (1)

▶ GET http://testphp.vulnweb.com

Risk=Средний, Confidence=Средний (3)

http://testphp.vulnweb.com (3)

XSLT Инъекция (1)

▶ GET http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E

Отсутствует заголовок (Header) для защиты от кликджекинга (1)

▶ GET http://testphp.vulnweb.com

Просмотр каталогов (1)

▶ GET http://testphp.vulnweb.com/Flash/

Risk=Средний, Confidence=Низкий (1)

http://testphp.vulnweb.com (1)

Отсутствуют токены против CSRF атак (1)

▶ GET http://testphp.vulnweb.com

Risk=Низкий, Confidence=Высокий (1)

http://testphp.vulnweb.com (1)

Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server» (1)

▶ GET http://testphp.vulnweb.com

Risk=Низкий, Confidence=Средний (2)

http://testphp.vulnweb.com (2)

Заголовок X-Content-Type-Options отсутствует (1)

▶ GET http://testphp.vulnweb.com

Сервер утекает информацию через поля заголовка HTTP-ответа "X-Powered-By" (1)

▶ GET http://testphp.vulnweb.com

Risk=Информационный, Confidence=Средний (1)

http://testphp.vulnweb.com (1)

Современное веб-приложение (1)

▶ GET http://testphp.vulnweb.com/artists.php

Risk=Информационный, Confidence=Низкий (3)

http://testphp.vulnweb.com (3)

Authentication Request Identified (1)

▶ POST http://testphp.vulnweb.com/secured/newuser.php

Charset Mismatch (Header Versus Meta Content-Type Charset) (1)

▶ GET http://testphp.vulnweb.com

Атрибут элемента HTML, управляемый пользователем (потенциальный XSS) (1)

▶ POST http://testphp.vulnweb.com/search.php?test=query

Appendix

Alert Types

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

SQL Injection - MySQL

Source	raised by an active scanner (SQL-инъекция)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL-инъекция

Source	raised by an active scanner (SQL-инъекция)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

XSLT Инъекция

Source	raised by an active scanner (XSLT Инъекция)
CWE ID	91
WASC ID	23

Reference	▪ https://book.hacktricks.wiki/en/pentesting-web/xslt-server-side-injection-extensible-stylesheet-language-transformations.html

Заголовок Content Security Policy (CSP) не задан

Source	raised by a passive scanner (Заголовок Content Security Policy (CSP) не задан)
CWE ID	693
WASC ID	15
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/

Отсутствует заголовок (Header) для защиты от кликджекинга

Source	raised by a passive scanner (Заголовок против кликджекинга)
CWE ID	1021
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

Отсутствуют токены против CSRF атак

Source	raised by a passive scanner (Отсутствуют токены против CSRF атак)
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

Просмотр каталогов

Source	raised by a passive scanner (Просмотр каталогов)
CWE ID	548
WASC ID	16
Reference	▪ https://cwe.mitre.org/data/definitions/548.html

Заголовок X-Content-Type-Options отсутствует

Source	raised by a passive scanner (Заголовок X-Content-Type-Options отсутствует)
CWE ID	693
WASC ID	15
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

Сервер утекает информацию через поля заголовка HTTP-ответа "X-Powered-By"

Source	raised by a passive scanner (Сервер утекает информацию через поля заголовка HTTP-ответа "X-Powered-By")
CWE ID	497
WASC ID	13
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/shhh-dont-let-your-response-headers/

Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»

Source	raised by a passive scanner (Заголовок ответа HTTP-сервера)
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/

Charset Mismatch (Header Versus Meta Content-Type Charset)

Source	raised by a passive scanner (Несоответствие кодировки)
CWE ID	436
WASC ID	15
Reference	▪ https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

Атрибут элемента HTML, управляемый пользователем (потенциальный XSS)

Source	raised by a passive scanner (Атрибут элемента HTML, управляемый пользователем (потенциальный XSS))
CWE ID	20
WASC ID	20
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Современное веб-приложение

Source	raised by a passive scanner (Современное веб-приложение)