ZAP by Checkmarx Scanning Report

Generated with ZAP on нд 27 квіт. 2025, at 19:35:55

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:

- `http://automationexercise.com`
- `https://automationexercise.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: `Високий`, `Середній`, `Низький`, `Відомості`

Excluded: None

Confidence levels

Included: Користувача підтверджено, Високий, Середній, Низький

Excluded: Користувача підтверджено, Високий, Середній, Низький, Помилкове спрацьовування

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				
		Користувача підтверджено	Високий	Середній	Низький	Total
Risk	Високий	0 (0,0%)	0 (0,0%)	1 (5,6%)	0 (0,0%)	1 (5,6%)
	Середній	0 (0,0%)	1 (5,6%)	1 (5,6%)	1 (5,6%)	3 (16,7%)
	Низький	0 (0,0%)	1 (5,6%)	5 (27,8%)	0 (0,0%)	6 (33,3%)
	Відомості	0 (0,0%)	1 (5,6%)	4 (22,2%)	3 (16,7%)	8 (44,4%)
	Total	0 (0,0%)	3 (16,7%)	11 (61,1%)	4 (22,2%)	18 (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			
		Високий (= Високий)	Середній (>= Середній)	Низький (>= Низький)	Відомості (>= Відомості)
Site	https://automationexercise.com	1 (1)	3 (4)	6 (10)	8 (18)

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
Вразлива бібліотека JS	Високий	1 (5,6%)
Вразлива бібліотека JS	Середній	2 (11,1%)
Відсутність токенів Anti-CSRF	Середній	2 (11,1%)
Заголовок політики безпеки вмісту (CSP) не встановлено	Середній	208 (1 155,6%)
Total		18

Alert type	Risk	Count
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Низький	272 (1 511,1%)
Включення міждоменного вихідного файлу JavaScript	Низький	188 (1 044,4%)
Заголовок Strict-Transport-Security не встановлено	Низький	271 (1 505,6%)
Прапорець HttpOnly відсутній	Низький	186 (1 033,3%)
Розкриття помилок програми	Низький	2 (11,1%)
Файл cookie без прапорця безпеки	Низький	189 (1 050,0%)
Modern Web Application	Відомості	95 (527,8%)
Визначено відповідь до керування сесією	Відомості	190 (1 055,6%)
Виявлено запит на автентифікацію	Відомості	2 (11,1%)
Відсутній заголовок Content-Type	Відомості	1 (5,6%)
Керований користувачем атрибут HTML-елемента (потенційний XSS)	Відомості	16 (88,9%)
Отримано з кешу	Відомості	19 (105,6%)
Перегляньте директиви керування кеш-пам’яттю	Відомості	98 (544,4%)
Total		18

Alert type	Risk	Count
Розголошення інформації - підозрілі коментарі	Відомості	2 (11,1%)
Total		18

Alerts

Risk=Високий, Confidence=Середній (1)

https://automationexercise.com (1)

Вразлива бібліотека JS (1)

▶ GET https://automationexercise.com/static/js/jquery.prettyPhoto.js

Risk=Середній, Confidence=Високий (1)

https://automationexercise.com (1)

Заголовок політики безпеки вмісту (CSP) не встановлено (1)

▶ GET https://automationexercise.com/

Risk=Середній, Confidence=Середній (1)

https://automationexercise.com (1)

Вразлива бібліотека JS (1)

▶ GET https://automationexercise.com/static/js/bootstrap.min.js

Risk=Середній, Confidence=Низький (1)

https://automationexercise.com (1)

Відсутність токенів Anti-CSRF (1)

▶ POST https://automationexercise.com/login

Risk=Низький, Confidence=Високий (1)

https://automationexercise.com (1)

Заголовок Strict-Transport-Security не встановлено (1)

▶ GET https://automationexercise.com/

Risk=Низький, Confidence=Середній (5)

https://automationexercise.com (5)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET https://automationexercise.com/robots.txt

Включення міждоменного вихідного файлу JavaScript (1)

▶ GET https://automationexercise.com/

Прапорець HttpOnly відсутній (1)

▶ GET https://automationexercise.com/

Розкриття помилок програми (1)

▶ POST https://automationexercise.com/login

Файл cookie без прапорця безпеки (1)

▶ GET https://automationexercise.com/

Risk=Відомості, Confidence=Високий (1)

https://automationexercise.com (1)

Виявлено запит на автентифікацію (1)

▶ POST https://automationexercise.com/login

Risk=Відомості, Confidence=Середній (4)

https://automationexercise.com (4)

Modern Web Application (1)

▶ GET https://automationexercise.com/

Визначено відповідь до керування сесією (1)

▶ GET https://automationexercise.com/

Відсутній заголовок Content-Type (1)

▶ GET https://automationexercise.com/cdn-cgi/l/email-protection

Отримано з кешу (1)

▶ GET https://automationexercise.com/static/css/font-awesome.min.css

Risk=Відомості, Confidence=Низький (3)

https://automationexercise.com (3)

Керований користувачем атрибут HTML-елемента (потенційний XSS) (1)

▶ POST https://automationexercise.com/contact_us

Перегляньте директиви керування кеш-пам’яттю (1)

▶ GET https://automationexercise.com/

Розголошення інформації - підозрілі коментарі (1)

▶ GET https://automationexercise.com/static/js/jquery.js

Appendix

Alert types

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

Вразлива бібліотека JS

Source	raised by a passive scanner (Вразлива бібліотека JS (на основі Retire.js))
CWE ID	1395
Reference	• https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Вразлива бібліотека JS

Source	raised by a passive scanner (Вразлива бібліотека JS (на основі Retire.js))

CWE ID	1395
Reference	▪ https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Відсутність токенів Anti-CSRF

Source	raised by a passive scanner (Відсутність токенів Anti-CSRF)
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

Заголовок політики безпеки вмісту (CSP) не встановлено

Source	raised by a passive scanner (Заголовок політики безпеки вмісту (CSP) не встановлено)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ 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/

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
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/2012/02/shhh-dont-let-your-response-headers.html

Включення міждоменного вихідного файлу JavaScript

Source	raised by a passive scanner (Включення міждоменного вихідного файлу JavaScript)
CWE ID	829
WASC ID	15

Заголовок Strict-Transport-Security не встановлено

Source	raised by a passive scanner (Заголовок Strict-Transport-Security)
CWE ID	319
WASC ID	15
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/html/rfc6797

Прапорець HttpOnly відсутній

Source	raised by a passive scanner (Прапорець HttpOnly відсутній)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Розкриття помилок програми

Source	raised by a passive scanner (Розкриття помилок програми)
CWE ID	550
WASC ID	13

Файл cookie без прапорця безпеки

Source	raised by a passive scanner (Файл cookie без прапорця безпеки)
CWE ID	614
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Визначено відповідь до керування сесією

Source	raised by a passive scanner (Визначено відповідь до керування сесією)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

Виявлено запит на автентифікацію

Source	raised by a passive scanner (Виявлено запит на автентифікацію)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

Відсутній заголовок Content-Type

Source	raised by a passive scanner (Відсутній заголовок Content-Type)
CWE ID	345
WASC ID	12
Reference	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)

Керований користувачем атрибут HTML-елемента (потенційний XSS)

Source	raised by a passive scanner (Керований користувачем атрибут HTML-елемента (потенційний XSS))
CWE ID	20
WASC ID	20
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Отримано з кешу

Source	raised by a passive scanner (Отримано з кешу)

Reference	▪ https://tools.ietf.org/html/rfc7234 ▪ https://tools.ietf.org/html/rfc7231 ▪ https://www.rfc-editor.org/rfc/rfc9110.html

Перегляньте директиви керування кеш-пам’яттю

Source	raised by a passive scanner (Перегляньте директиви керування кеш-пам’яттю)
CWE ID	525
WASC ID	13
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

Розголошення інформації - підозрілі коментарі

Source	raised by a passive scanner (Розголошення інформації - підозрілі коментарі)
CWE ID	615
WASC ID	13