整合平台系統

Generated with ZAP on 週一 1 6月 2026, at 00:33:41

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:

- `https://portal2.cpu.edu.tw`

(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%)	1 (9.1%)	1 (9.1%)	2 (18.2%)
	Medium	0 (0.0%)	1 (9.1%)	0 (0.0%)	0 (0.0%)	1 (9.1%)
	Low	0 (0.0%)	0 (0.0%)	2 (18.2%)	0 (0.0%)	2 (18.2%)
	Informational	0 (0.0%)	0 (0.0%)	3 (27.3%)	3 (27.3%)	6 (54.5%)
	Total	0 (0.0%)	1 (9.1%)	6 (54.5%)	4 (36.4%)	11 (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	https://portal2.cpu.edu.tw	2 (2)	1 (3)	2 (5)	6 (11)

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
Path Traversal	High	1 (9.1%)
Vulnerable JS Library	High	1 (9.1%)
Sub Resource Integrity Attribute Missing	Medium	5 (45.5%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	8 (72.7%)
X-Content-Type-Options Header Missing	Low	5 (45.5%)
Cookie Poisoning	Informational	5 (45.5%)
Total		11

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	2 (18.2%)
Re-examine Cache-control Directives	Informational	5 (45.5%)
Session Management Response Identified	Informational	11 (100.0%)
User Agent Fuzzer	Informational	5 (45.5%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	1 (9.1%)
Total		11

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Reason	Site	Description	Statistic
Low	Exceeded High	https://portal2.cpu.edu.tw	Percentage of slow responses	77 %
資訊	Informational	http://portal2.cpu.edu.tw	Percentage of responses with status code 3xx	100 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of responses with status code 2xx	51 %

Level	Reason	Site	Description	Statistic
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of responses with status code 3xx	41 %
資訊	Exceeded Low	https://portal2.cpu.edu.tw	Percentage of responses with status code 4xx	6 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with content type image/png	2 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with content type text/css	23 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with content type text/html	31 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with content type text/javascript	39 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with content type text/plain	2 %
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with method GET	84 %

Level	Reason	Site	Description	Statistic
資訊	Informational	https://portal2.cpu.edu.tw	Percentage of endpoints with method POST	15 %
資訊	Informational	https://portal2.cpu.edu.tw	Count of total endpoints	38

Alerts

Risk=High, Confidence=Medium (1)

https://portal2.cpu.edu.tw (1)

Vulnerable JS Library (1)

▶ GET https://portal2.cpu.edu.tw/vendor/handlebars/4.7.7/handlebars.runtime.js

Risk=High, Confidence=Low (1)

https://portal2.cpu.edu.tw (1)

Path Traversal (1)

▶ POST https://portal2.cpu.edu.tw/user/forget/verify

Risk=Medium, Confidence=High (1)

https://portal2.cpu.edu.tw (1)

Sub Resource Integrity Attribute Missing (1)

▶ GET https://portal2.cpu.edu.tw/

Risk=Low, Confidence=Medium (2)

https://portal2.cpu.edu.tw (2)

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET https://portal2.cpu.edu.tw/

X-Content-Type-Options Header Missing (1)

▶ GET https://portal2.cpu.edu.tw/robots.txt

Risk=Informational, Confidence=Medium (3)

https://portal2.cpu.edu.tw (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://portal2.cpu.edu.tw/vendor/handlebars/4.7.7/handlebars.runtime.js

Session Management Response Identified (1)

▶ GET https://portal2.cpu.edu.tw/

User Agent Fuzzer (1)

▶ GET https://portal2.cpu.edu.tw/

Risk=Informational, Confidence=Low (3)

https://portal2.cpu.edu.tw (3)

Cookie Poisoning (1)

▶ POST https://portal2.cpu.edu.tw/login

Re-examine Cache-control Directives (1)

▶ GET https://portal2.cpu.edu.tw/robots.txt

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET https://portal2.cpu.edu.tw/login?redirect_uri=https%3A%2F%2Fportal2.cpu.edu.tw

Appendix

Alert Types

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

Path Traversal

Source	raised by an active scanner (Path Traversal)
CWE ID	22
WASC ID	33
Reference	▪ https://owasp.org/www-community/attacks/Path_Traversal

- https://cwe.mitre.org/data/definitions/22.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	• https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Sub Resource Integrity Attribute Missing

Source	raised by a passive scanner (Sub Resource Integrity Attribute Missing)
CWE ID	345
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Big Redirect Detected (Potential Sensitive Information Leak)

Source	raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
CWE ID	201
WASC ID	13

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)

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

Cookie Poisoning

Source	raised by a passive scanner (Cookie Poisoning)
CWE ID	565
WASC ID	20
Reference	▪ https://en.wikipedia.org/wiki/HTTP_cookie ▪ https://cwe.mitre.org/data/definitions/565.html

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
WASC ID	13

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)
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/Reference/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

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

User Controllable HTML Element Attribute (Potential XSS)

Source	raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))
CWE ID	20
WASC ID	20

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html