ZAP Scanning Report

Generated with ZAP on dom 5 dic 2021, at 15:39:47

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://onfeet1.herokuapp.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: `Alto`, `Medio`, `Bajo`, `Informativo`

Excluded: None

Confidence levels

Included: `User Confirmed`, `Alto`, `Medio`, `Bajo`

Excluded: `User Confirmed`, `Alto`, `Medio`, `Bajo`, `Falso positivo`

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	Alto	Medio	Bajo	Total
Risk	Alto	0 (0,0%)	0 (0,0%)	1 (3,2%)	0 (0,0%)	1 (3,2%)
	Medio	0 (0,0%)	0 (0,0%)	7 (22,6%)	0 (0,0%)	7 (22,6%)
	Bajo	0 (0,0%)	0 (0,0%)	22 (71,0%)	1 (3,2%)	23 (74,2%)
	Informativo	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Total	0 (0,0%)	0 (0,0%)	30 (96,8%)	1 (3,2%)	31 (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

		Risk			
		Alto (= Alto)	Medio (>= Medio)	Bajo (>= Bajo)	Informativo (>= Informativo)

		Alto (= Alto)	Medio (>= Medio)	Bajo (>= Bajo)	Informativo (>= Informativo)
Site	http://onfeet1.herokuapp.com	1 (1)	7 (8)	23 (31)	0 (31)

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
Cross Site Scripting (Reflected)	Alto	1 (3,2%)
X-Frame-Options Header Not Set	Medio	7 (22,6%)
Ausencia de fichas (tokens) Anti-CSRF	Bajo	4 (12,9%)
Cookie No HttpOnly Flag	Bajo	1 (3,2%)
Cookie without SameSite Attribute	Bajo	1 (3,2%)
Total		31

Alert type	Risk	Count
Cross-Domain JavaScript Source File Inclusion	Bajo	6 (19,4%)
Divulgación de la marca de hora - Unix	Bajo	1 (3,2%)
X-Content-Type-Options Header Missing	Bajo	10 (32,3%)
Total		31

Alerts

Risk=Alto, Confidence=Medio (1)

http://onfeet1.herokuapp.com (1)

Cross Site Scripting (Reflected) (1)

▶ GET http://onfeet1.herokuapp.com/product.php?p=%27%3Balert%281%29%3B%27

Risk=Medio, Confidence=Medio (7)

http://onfeet1.herokuapp.com (7)

X-Frame-Options Header Not Set (7)

▶ GET http://onfeet1.herokuapp.com

▶ GET http://onfeet1.herokuapp.com/index.php

▶ GET http://onfeet1.herokuapp.com/login.php

▶ GET http://onfeet1.herokuapp.com/login.php?e=2

▶ GET http://onfeet1.herokuapp.com/product.php?p='+data.data%5Bi%5D.IdPro+'

▶ GET http://onfeet1.herokuapp.com/signup.php

▶ POST http://onfeet1.herokuapp.com/signup.php

Risk=Bajo, Confidence=Medio (22)

http://onfeet1.herokuapp.com (22)

Ausencia de fichas (tokens) Anti-CSRF (4)

▶ GET http://onfeet1.herokuapp.com/login.php

▶ GET http://onfeet1.herokuapp.com/login.php?e=2

▶ GET http://onfeet1.herokuapp.com/signup.php

▶ POST http://onfeet1.herokuapp.com/signup.php

Cookie No HttpOnly Flag (1)

▶ GET http://onfeet1.herokuapp.com

Cookie without SameSite Attribute (1)

▶ GET http://onfeet1.herokuapp.com

Cross-Domain JavaScript Source File Inclusion (6)

▶ GET http://onfeet1.herokuapp.com

▶ GET http://onfeet1.herokuapp.com/index.php

▶ GET http://onfeet1.herokuapp.com/login.php

▶ GET http://onfeet1.herokuapp.com/login.php?e=2

▶ GET http://onfeet1.herokuapp.com/Order.php

▶ GET http://onfeet1.herokuapp.com/product.php?p='+data.data%5Bi%5D.IdPro+'

X-Content-Type-Options Header Missing (10)

▶ GET http://onfeet1.herokuapp.com

▶ GET http://onfeet1.herokuapp.com/assets/script.js

▶ GET http://onfeet1.herokuapp.com/index.php

▶ GET http://onfeet1.herokuapp.com/login.php

▶ GET http://onfeet1.herokuapp.com/login.php?e=2

▶ GET http://onfeet1.herokuapp.com/product.php?p='+data.data%5Bi%5D.IdPro+'

▶ GET http://onfeet1.herokuapp.com/resources/css/index.css

▶ GET http://onfeet1.herokuapp.com/resources/walking-solid.svg

▶ GET http://onfeet1.herokuapp.com/signup.php

▶ POST http://onfeet1.herokuapp.com/signup.php

Risk=Bajo, Confidence=Bajo (1)

http://onfeet1.herokuapp.com (1)

Divulgación de la marca de hora - Unix (1)

```
▶ GET http://onfeet1.herokuapp.com/product.php?
p='+data.data%5Bi%5D.IdPro+'
```

Appendix

Alert types

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

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ http://cwe.mitre.org/data/definitions/79.html

X-Frame-Options Header Not Set

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

Ausencia de fichas (tokens) Anti-CSRF

Source	raised by a passive scanner (Ausencia de fichas (tokens) Anti-CSRF)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Cookie without SameSite Attribute

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

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Divulgación de la marca de hora - Unix

Source	raised by a passive scanner (Divulgación de la marca de hora)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

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	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers