ZAP Scanning Report DVWA

Generated with ZAP on Sun 21 Nov 2021, at 22:21:32

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=Medium, Confidence=Medium (56)
  - Risk=Low, Confidence=Medium (18)
  - Risk=Informational, Confidence=Low (2)
- Appendix
  - Alert types

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- `https://dvwa.co.uk`

(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%)	0 (0.0%)	56 (73.7%)	0 (0.0%)	56 (73.7%)
	Low	0 (0.0%)	0 (0.0%)	18 (23.7%)	0 (0.0%)	18 (23.7%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (2.6%)	2 (2.6%)
	Total	0 (0.0%)	0 (0.0%)	74 (97.4%)	2 (2.6%)	76 (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://dvwa.co.uk	0 (0)	56 (56)	18 (74)	2 (76)

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
CSP: Wildcard Directive	Medium	10 (13.2%)
CSP: style-src unsafe-inline	Medium	10 (13.2%)
Cross-Domain Misconfiguration	Medium	33 (43.4%)
Vulnerable JS Library	Medium	1 (1.3%)
X-Frame-Options Header Not Set	Medium	2 (2.6%)
Incomplete or No Cache-control Header Set	Low	2 (2.6%)
X-Content-Type-Options Header Missing	Low	16 (21.1%)
Information Disclosure - Suspicious Comments	Informational	2 (2.6%)
Total		76

Alerts

Risk=Medium, Confidence=Medium (56)

https://dvwa.co.uk (56)

CSP: Wildcard Directive (10)

▶ GET https://dvwa.co.uk/css/

▶ GET https://dvwa.co.uk/images/

▶ GET https://dvwa.co.uk/images/buttons/

▶ GET https://dvwa.co.uk/index.php

▶ GET https://dvwa.co.uk/js/

▶ GET https://dvwa.co.uk/nivo-slider/

▶ GET https://dvwa.co.uk/nivo-slider/themes/

▶ GET https://dvwa.co.uk/nivo-slider/themes/default/

▶ GET https://dvwa.co.uk/robots.txt

▶ GET https://dvwa.co.uk/sitemap.xml

CSP: style-src unsafe-inline (10)

▶ GET https://dvwa.co.uk/css/

▶ GET https://dvwa.co.uk/images/

▶ GET https://dvwa.co.uk/images/buttons/

▶ GET https://dvwa.co.uk/index.php

▶ GET https://dvwa.co.uk/js/

▶ GET https://dvwa.co.uk/nivo-slider/

▶ GET https://dvwa.co.uk/nivo-slider/themes/

▶ GET https://dvwa.co.uk/nivo-slider/themes/default/

▶ GET https://dvwa.co.uk/robots.txt

▶ GET https://dvwa.co.uk/sitemap.xml

Cross-Domain Misconfiguration (33)

▶ GET https://dvwa.co.uk

▶ GET https://dvwa.co.uk/

▶ GET https://dvwa.co.uk/css

▶ GET https://dvwa.co.uk/css/

▶ GET https://dvwa.co.uk/css/all.css

▶ GET https://dvwa.co.uk/css/lt7.css

▶ GET https://dvwa.co.uk/css/nivo-slider.css

▶ GET https://dvwa.co.uk/favicon.ico

▶ GET https://dvwa.co.uk/images

▶ GET https://dvwa.co.uk/images/

▶ GET https://dvwa.co.uk/images/buttons

▶ GET https://dvwa.co.uk/images/buttons/

▶ GET https://dvwa.co.uk/images/buttons/bugs.png

▶ GET https://dvwa.co.uk/images/buttons/download.png

▶ GET https://dvwa.co.uk/images/buttons/source.png

▶ GET https://dvwa.co.uk/images/buttons/wiki.png

▶ GET https://dvwa.co.uk/images/slider1.png

▶ GET https://dvwa.co.uk/images/slider2.png

▶ GET https://dvwa.co.uk/images/slider3.png

▶ GET https://dvwa.co.uk/index.php

▶ GET https://dvwa.co.uk/js

▶ GET https://dvwa.co.uk/js/

▶ GET https://dvwa.co.uk/js/jquery-1.6.2.min.js

▶ GET https://dvwa.co.uk/js/jquery.nivo.slider.pack.js

▶ GET https://dvwa.co.uk/nivo-slider

▶ GET https://dvwa.co.uk/nivo-slider/

▶ GET https://dvwa.co.uk/nivo-slider/themes

▶ GET https://dvwa.co.uk/nivo-slider/themes/

▶ GET https://dvwa.co.uk/nivo-slider/themes/default

▶ GET https://dvwa.co.uk/nivo-slider/themes/default/

▶ GET https://dvwa.co.uk/nivo-slider/themes/default/default.css

▶ GET https://dvwa.co.uk/robots.txt

▶ GET https://dvwa.co.uk/sitemap.xml

Vulnerable JS Library (1)

▶ GET https://dvwa.co.uk/js/jquery-1.6.2.min.js

X-Frame-Options Header Not Set (2)

▶ GET https://dvwa.co.uk

▶ GET https://dvwa.co.uk/

Risk=Low, Confidence=Medium (18)

https://dvwa.co.uk (18)

Incomplete or No Cache-control Header Set (2)

- ▶ GET https://dvwa.co.uk
- ▶ GET https://dvwa.co.uk/

X-Content-Type-Options Header Missing (16)

- ▶ GET https://dvwa.co.uk
- ▶ GET https://dvwa.co.uk/
- ▶ GET https://dvwa.co.uk/css/all.css
- ▶ GET https://dvwa.co.uk/css/lt7.css
- ▶ GET https://dvwa.co.uk/css/nivo-slider.css
- ▶ GET https://dvwa.co.uk/favicon.ico
- ▶ GET https://dvwa.co.uk/images/buttons/bugs.png
- ▶ GET https://dvwa.co.uk/images/buttons/download.png
- ▶ GET https://dvwa.co.uk/images/buttons/source.png
- ▶ GET https://dvwa.co.uk/images/buttons/wiki.png
- ▶ GET https://dvwa.co.uk/images/slider1.png
- ▶ GET https://dvwa.co.uk/images/slider2.png
- ▶ GET https://dvwa.co.uk/images/slider3.png
- ▶ GET https://dvwa.co.uk/js/jquery-1.6.2.min.js
- ▶ GET https://dvwa.co.uk/js/jquery.nivo.slider.pack.js

▶ GET https://dvwa.co.uk/nivo-slider/themes/default/default.css

Risk=Informational, Confidence=Low (2)

https://dvwa.co.uk (2)

Information Disclosure - Suspicious Comments (2)

▶ GET https://dvwa.co.uk/js/jquery-1.6.2.min.js

▶ GET https://dvwa.co.uk/js/jquery-1.6.2.min.js

Appendix

Alert types

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

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy

- http://content-security-policy.com/
- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264

WASC ID	14
Reference	▪ https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library)
CWE ID	829
Reference	▪ https://nvd.nist.gov/vuln/detail/CVE-2012-6708 ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://research.insecurelabs.org/jquery/test/ ▪ https://bugs.jquery.com/ticket/9521 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ http://bugs.jquery.com/ticket/11290 ▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 ▪ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 ▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b

- https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
- https://nvd.nist.gov/vuln/detail/CVE-2011-4969

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

Incomplete or No Cache-control Header Set

Source	raised by a passive scanner (Incomplete or No Cache-control Header Set)
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

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

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200
WASC ID	13