

# ZAP Scanning Report

Generated with  ZAP on Tue 14 Jun 2022, at 16:12:10

## 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 \(3\)](#)
  - [Risk=Low, Confidence=Medium \(2\)](#)
  - [Risk=Informational, Confidence=Low \(1\)](#)
- [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:

- <http://zero.webappsecurity.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: [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				
Risk		User Confirmed	High	Medium	Low	Total
	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	0 (0.0%)	3 (50.0%)	0 (0.0%)	3 (50.0%)
	Low	0 (0.0%)	0 (0.0%)	2 (33.3%)	0 (0.0%)	2 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (16.7%)	1 (16.7%)
	1					
Total	0 (0.0%)	0 (0.0%)	5 (83.3%)	1 (16.7%)	6 (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			Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)
http://zero.webappsec	0	3	2	1
curiety.com	(0)	(3)	(5)	(6)

## 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
<u>Cross-Domain Misconfiguration</u>	Medium	15 (250.0%)
<u>Vulnerable JS Library</u>	Medium	1 (16.7%)
<u>X-Frame-Options Header Not Set</u>	Medium	4 (66.7%)
<u>Absence of Anti-CSRF Tokens</u>	Low	4 (66.7%)
Total		6

Alert type	Risk	Count
<a href="#">X-Content-Type-Options Header Missing</a>	Low	13 (216.7%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	3 (50.0%)
Total		6

## Alerts

**Risk=Medium, Confidence=Medium (3)**

<http://zero.webappsecurity.com> (3)

### [Cross-Domain Misconfiguration \(1\)](#)

► GET <http://zero.webappsecurity.com>

### [Vulnerable JS Library \(1\)](#)

► GET <http://zero.webappsecurity.com/resources/js/jquery-1.8.2.min.js>

### [X-Frame-Options Header Not Set \(1\)](#)

► GET <http://zero.webappsecurity.com>

**Risk=Low, Confidence=Medium (2)**

<http://zero.webappsecurity.com> (2)

### [Absence of Anti-CSRF Tokens \(1\)](#)

► GET http://zero.webappsecurity.com

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

► GET http://zero.webappsecurity.com

**Risk=Informational, Confidence=Low (1)**

http://zero.webappsecurity.com (1)

### **Information Disclosure - Suspicious Comments (1)**

► GET

http://zero.webappsecurity.com/resources/js/bootstrap.min.js

## Appendix

### **Alert types**

---

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

#### **Cross-Domain Misconfiguration**

Source	raised by a passive scanner ( <a href="#">Cross-Domain Misconfiguration</a> )
CWE ID	<a href="#">264</a>
WASC ID	14
Reference	▪ <a href="https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy">https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy</a>

## Vulnerable JS Library

Source	raised by a passive scanner ( <a href="#">Vulnerable JS Library</a> )
CWE ID	<a href="#">829</a>
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://nvd.nist.gov/vuln/detail/CVE-2012-6708">https://nvd.nist.gov/vuln/detail/CVE-2012-6708</a></li><li>▪ <a href="https://github.com/jquery/jquery/issues/2432">https://github.com/jquery/jquery/issues/2432</a></li><li>▪ <a href="http://research.insecurelabs.org/jquery/test/">http://research.insecurelabs.org/jquery/test/</a></li><li>▪ <a href="http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/">http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/</a></li><li>▪ <a href="http://bugs.jquery.com/ticket/11290">http://bugs.jquery.com/ticket/11290</a></li><li>▪ <a href="https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/">https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/</a></li><li>▪ <a href="https://nvd.nist.gov/vuln/detail/CVE-2019-11358">https://nvd.nist.gov/vuln/detail/CVE-2019-11358</a></li><li>▪ <a href="https://nvd.nist.gov/vuln/detail/CVE-2015-9251">https://nvd.nist.gov/vuln/detail/CVE-2015-9251</a></li><li>▪ <a href="https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b">https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b</a></li><li>▪ <a href="https://bugs.jquery.com/ticket/11974">https://bugs.jquery.com/ticket/11974</a></li><li>▪ <a href="https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/">https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/</a></li></ul>

## X-Frame-Options Header Not Set

Source	raised by a passive scanner ( <a href="#">Anti-clickjacking Header</a> )
CWE ID	<a href="#">1021</a>
WASC ID	15
Reference	<ul style="list-style-type: none"> <li>▪ <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a></li> </ul>

### Absence of Anti-CSRF Tokens

Source	raised by a passive scanner ( <a href="#">Absence of Anti-CSRF Tokens</a> )
CWE ID	<a href="#">352</a>
WASC ID	9
Reference	<ul style="list-style-type: none"> <li>▪ <a href="http://projects.webappsec.org/Cross-Site-Request-Forgery">http://projects.webappsec.org/Cross-Site-Request-Forgery</a></li> <li>▪ <a href="http://cwe.mitre.org/data/definitions/352.html">http://cwe.mitre.org/data/definitions/352.html</a></li> </ul>

### X-Content-Type-Options Header Missing

Source	raised by a passive scanner ( <a href="#">X-Content-Type-Options Header Missing</a> )
CWE ID	<a href="#">693</a>
WASC ID	15
Reference	<ul style="list-style-type: none"> <li>▪ <a href="http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx">http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx</a></li> <li>▪ <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a></li> </ul>



## Information Disclosure - Suspicious Comments

Source	raised by a passive scanner ( <a href="#">Information Disclosure - Suspicious Comments</a> )
CWE ID	<a href="#">200</a>
WASC ID	13