

# AmericanBank-Scan-Report

Generated with  ZAP on Wed 16 Nov 2022, at 15:54:20

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

- <https://fonts.googleapis.com>
- <https://cdn.jsdelivr.net>
- <http://localhost:3000>

(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%)	2 (16.7%)	2 (16.7%)	0 (0.0%)	4 (33.3%)
	Low	0 (0.0%)	0 (0.0%)	3 (25.0%)	1 (8.3%)	4 (33.3%)
	Informational	0 (0.0%)	0 (0.0%)	3 (25.0%)	1 (8.3%)	4 (33.3%)
	1	0 (0.0%)	0 (0.0%)	3 (25.0%)	1 (8.3%)	4 (33.3%)
Total		0 (0.0%)	2 (16.7%)	8 (66.7%)	2 (16.7%)	12 (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			Informational
	High (= High)	Medium (>= Medium)	Low (>= Low)	(>= Informational)
Site <a href="https://cdn.jsdelivr.net">https://cdn.jsdelivr.net</a>	0 (0)	0 (0)	0 (0)	2 (2)
<a href="http://localhost:3000">http://localhost:3000</a>	0 (0)	4 (4)	4 (8)	2 (10)

### 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
<a href="#">CSP: Wildcard Directive</a>	Medium	6 (50.0%)
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	4 (33.3%)
<a href="#">Cross-Domain Misconfiguration</a>	Medium	33 (275.0%)
<a href="#">Missing Anti-clickjacking Header</a>	Medium	4 (33.3%)
Total		12

Alert type	Risk	Count
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	3 (25.0%)
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	29 (241.7%)
<a href="#">Timestamp Disclosure - Unix</a>	Low	1 (8.3%)
<a href="#">X-Content-Type-Options Header Missing</a>	Low	23 (191.7%)
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	13 (108.3%)
<a href="#">Modern Web Application</a>	Informational	4 (33.3%)
<a href="#">Retrieved from Cache</a>	Informational	2 (16.7%)
<a href="#">User Agent Fuzzer</a>	Informational	12 (100.0%)
Total		12

## Alerts

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

<http://localhost:3000> (2)

**CSP: Wildcard Directive (1)**

► GET http://localhost:3000/sitemap.xml

### **Content Security Policy (CSP) Header Not Set (1)**

► GET http://localhost:3000/

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

http://localhost:3000 (2)

### **Cross-Domain Misconfiguration (1)**

► GET http://localhost:3000/

### **Missing Anti-clickjacking Header (1)**

► GET http://localhost:3000/

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

http://localhost:3000 (3)

### **Cross-Domain JavaScript Source File Inclusion (1)**

► GET http://localhost:3000/

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

► GET http://localhost:3000/

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

► GET http://localhost:3000/

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

<http://localhost:3000> (1)

**Timestamp Disclosure - Unix (1)**

► GET <http://localhost:3000/static/js/bundle.js>

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

<https://cdn.jsdelivr.net> (1)

**Retrieved from Cache (1)**

► GET

<https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.min.js>

<http://localhost:3000> (2)

**Modern Web Application (1)**

► GET <http://localhost:3000/>

**User Agent Fuzzer (1)**

► GET <http://localhost:3000/info>

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

<https://cdn.jsdelivr.net> (1)

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

► GET

`https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/js/bootstrap.bundle.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 ( <a href="#">CSP</a> )
CWE ID	<a href="#">693</a>
WASC ID	15
Reference	<ul style="list-style-type: none"><li>▪ <a href="http://www.w3.org/TR/CSP2/">http://www.w3.org/TR/CSP2/</a></li><li>▪ <a href="http://www.w3.org/TR/CSP/">http://www.w3.org/TR/CSP/</a></li><li>▪ <a href="http://caniuse.com/#search=content+security+policy">http://caniuse.com/#search=content+security+policy</a></li><li>▪ <a href="http://content-security-policy.com/">http://content-security-policy.com/</a></li><li>▪ <a href="https://github.com/shapesecurity/salvation">https://github.com/shapesecurity/salvation</a></li><li>▪ <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a></li></ul>



## Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner ( <a href="#">Content Security Policy (CSP) Header Not Set</a> )
CWE ID	<a href="#">693</a>
WASC ID	15
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a></li><li>▪ <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a></li><li>▪ <a href="http://www.w3.org/TR/CSP/">http://www.w3.org/TR/CSP/</a></li><li>▪ <a href="http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html">http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html</a></li><li>▪ <a href="http://www.html5rocks.com/en/tutorials/security/content-security-policy/">http://www.html5rocks.com/en/tutorials/security/content-security-policy/</a></li><li>▪ <a href="http://caniuse.com/#feat=contentsecuritypolicy">http://caniuse.com/#feat=contentsecuritypolicy</a></li><li>▪ <a href="http://content-security-policy.com/">http://content-security-policy.com/</a></li></ul>

## 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**

- [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)

## Missing Anti-clickjacking Header

**Source** raised by a passive scanner ([Anti-clickjacking Header](#))

**CWE ID** [1021](#)

**WASC ID** 15

**Reference**

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

## Cross-Domain JavaScript Source File Inclusion

**Source** raised by a passive scanner ([Cross-Domain JavaScript Source File Inclusion](#))

**CWE ID** [829](#)

**WASC ID** 15

## 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** [200](#)

**WASC ID** 13

## Reference

- <http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx>
- <http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

## Timestamp Disclosure - Unix

Source	raised by a passive scanner ( <a href="#">Timestamp Disclosure</a> )
CWE ID	<a href="#">200</a>
WASC ID	13
Reference	▪ <a href="http://projects.webappsec.org/w/page/13246936/Information%20Leakage">http://projects.webappsec.org/w/page/13246936/Information%20Leakage</a>

## 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	▪ <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> ▪ <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>

## Information Disclosure - Suspicious Comments

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

## Modern Web Application

<b>Source</b>	raised by a passive scanner ( <a href="#">Modern Web Application</a> )
---------------	--

## Retrieved from Cache

<b>Source</b>	raised by a passive scanner ( <a href="#">Retrieved from Cache</a> )
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://tools.ietf.org/html/rfc7234">https://tools.ietf.org/html/rfc7234</a></li><li>▪ <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a></li><li>▪ <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html">http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html</a> (obsoleted by rfc7234).</li></ul>

## User Agent Fuzzer

<b>Source</b>	raised by an active scanner ( <a href="#">User Agent Fuzzer</a> )
<b>Reference</b>	<ul style="list-style-type: none"><li>▪ <a href="https://owasp.org/wstg">https://owasp.org/wstg</a></li></ul>