OnlineBankingSystemHtdocs-Scan-Report

Generated with ZAP on Wed 16 Nov 2022, at 15:16:52

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://localhost

(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%)	1 (3.3%)	0 (0.0%)	0 (0.0%)	1 (3.3%)
	Medium	0 (0.0%)	4 (13.3%)	4 (13.3%)	1 (3.3%)	9 (30.0%)
	Low	0 (0.0%)	1 (3.3%)	8 (26.7%)	1 (3.3%)	10 (33.3%)
	Informational	0 (0.0%)	3 (10.0%)	3 (10.0%)	4 (13.3%)	10 (33.3%)
	Total	0 (0.0%)	9 (30.0%)	15 (50.0%)	6 (20.0%)	30 (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	http://localhost	1 (1)	9 (10)	9 (19)	10 (29)

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
PII Disclosure	High	16 (53.3%)
Absence of Anti-CSRF Tokens	Medium	25101 (83,670.0%)
Application Error Disclosure	Medium	251 (836.7%)
CSP: Wildcard Directive	Medium	6838 (22,793.3%)
CSP: script-src unsafe-inline	Medium	6838 (22,793.3%)
CSP: style-src unsafe-inline	Medium	6837
Total		30

Alert type	Risk	Count (22,790.0%)
Content Security Policy (CSP) Header Not Set	Medium	383 (1,276.7%)
Directory Browsing - Apache 2	Medium	144 (480.0%)
Missing Anti-clickjacking Header	Medium	208 (693.3%)
Vulnerable JS Library	Medium	2 (6.7%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	457 (1,523.3%)
Cookie No HttpOnly Flag	Low	1 (3.3%)
Cookie without SameSite Attribute	Low	1 (3.3%)
Cross-Domain JavaScript Source File Inclusion	Low	25 (83.3%)
Information Disclosure - Debug Error Messages	Low	586 (1,953.3%)
Private IP Disclosure	Low	6 (20.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	7396 (24,653.3%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	8192 (27,306.7%)
Total		30

Alert type	Risk	Count
Timestamp Disclosure - Unix	Low	481 (1,603.3%)
X-Content-Type-Options Header Missing	Low	577 (1,923.3%)
CSP: X-Content-Security-Policy	Informational	6838 (22,793.3%)
CSP: X-WebKit-CSP	Informational	6838 (22,793.3%)
Content-Type Header Missing	Informational	20 (66.7%)
Information Disclosure - Sensitive Information in URL	Informational	770 (2,566.7%)
Information Disclosure - Suspicious Comments	Informational	6971 (23,236.7%)
Loosely Scoped Cookie	Informational	11464 (38,213.3%)
Modern Web Application	Informational	7035 (23,450.0%)
User Controllable Charset	Informational	2 (6.7%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	44745 (149,150.0%)
Username Hash Found	Informational	48 (160.0%)
Total		30

Alerts

Risk=High, Confidence=High (1)

http://localhost (1)

PII Disclosure (1)

▶ GET http://localhost/dashboard/docs/install-wordpress.pdf

Risk=Medium, Confidence=High (4)

http://localhost (4)

CSP: Wildcard Directive (1)

▶ GET http://localhost/phpmyadmin/

CSP: script-src unsafe-inline (1)

▶ GET http://localhost/phpmyadmin/

CSP: style-src unsafe-inline (1)

▶ GET http://localhost/phpmyadmin/

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

▶ GET http://localhost/banking

Risk=Medium, Confidence=Medium (4)

http://localhost (4)

Application Error Disclosure (1)

▶ GET http://localhost/Online-Banking-System/t&c.php

Directory Browsing - Apache 2 (1)

▶ GET http://localhost/xampp/

Missing Anti-clickjacking Header (1)

▶ GET http://localhost/Online-Banking-System/

Vulnerable JS Library (1)

▶ GET http://localhost/phpmyadmin/js/vendor/jquery/jquery-ui.min.js?v=5.2.0

Risk=Medium, Confidence=Low (1)

http://localhost (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://localhost/Online-Banking-System/

Risk=Low, Confidence=High (1)

http://localhost (1)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET http://localhost/banking

Risk=Low, Confidence=Medium (8)

http://localhost (7)

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

▶ GET http://localhost/Online-Banking-System

Cookie No HttpOnly Flag (1)

▶ GET http://localhost/Online-Banking-System/

Cookie without SameSite Attribute (1)

▶ GET http://localhost/Online-Banking-System/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://localhost

Information Disclosure - Debug Error Messages (1)

▶ GET http://localhost/phpmyadmin/doc/html/config.html

Private IP Disclosure (1)

▶ GET http://localhost/phpmyadmin/doc/html/config.html

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

▶ GET http://localhost/Online-Banking-System/

Risk=Low, Confidence=Low (1)

http://localhost (1)

Timestamp Disclosure - Unix (1)

▶ GET http://localhost/dashboard/phpinfo.php

Risk=Informational, Confidence=High (3)

http://localhost (3)

CSP: X-Content-Security-Policy (1)

▶ GET http://localhost/phpmyadmin/

CSP: X-WebKit-CSP (1)

▶ GET http://localhost/phpmyadmin/

Username Hash Found (1)

▶ GET http://localhost/phpmyadmin/index.php?db=bank_db&lang=en&route=/database/structure

Risk=Informational, Confidence=Medium (3)

http://localhost (3)

Content-Type Header Missing (1)

▶ GET http://localhost/dashboard/docs/access-phpmyadmin-remotely.pdfmarks

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://localhost/phpmyadmin/index.php?db&lang=en&route=/&table&token=4861494f40495829477b22522f3d5543

Modern Web Application (1)

▶ GET http://localhost/Online-Banking-System/

Risk=Informational, Confidence=Low (4)

http://localhost (4)

Information Disclosure - Suspicious Comments (1)

▶ GET http://localhost/dashboard/javascripts/modernizr.js

Loosely Scoped Cookie (1)

▶ GET http://localhost/Online-Banking-System/

User Controllable Charset (1)

▶ POST http://localhost/phpmyadmin/index.php?route=/export

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

▶ GET http://localhost/phpmyadmin/index.php?lang=en

Appendix

Alert types

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

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352

WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

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: script-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

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

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	• https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy • https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html • http://www.w3.org/TR/CSP/ • http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html • http://www.html5rocks.com/en/tutorials/security/content-security-policy/ • http://caniuse.com/#feat=contentsecuritypolicy • http://content-security-policy.com/

Directory Browsing - Apache 2

Source	raised by a passive scanner (Directory Browsing)
CWE ID	548

WASC ID	16
Reference	▪ https://cwe.mitre.org/data/definitions/548.html

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://nvd.nist.gov/vuln/detail/CVE-2022-31160 ▪ https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9

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

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

Information Disclosure - Debug Error Messages

Source	raised by a passive scanner (Information Disclosure - Debug Error Messages)
CWE ID	200
WASC ID	13

Private IP Disclosure

Source	raised by a passive scanner (Private IP Disclosure)

CWE ID	200
WASC ID	13
Reference	▪ https://tools.ietf.org/html/rfc1918

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

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007

- 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 (Timestamp Disclosure)
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

CSP: X-Content-Security-Policy

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: X-WebKit-CSP

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

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

Information Disclosure - Suspicious Comments

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

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1

- https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Modern Web Application

Source raised by a passive scanner (Modern Web Application)

User Controllable Charset

Source raised by a passive scanner (User Controllable Charset)

CWE ID 20

WASC ID 20

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

- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute

Username Hash Found

Source raised by a passive scanner (Username Hash Found)

CWE ID	284
WASC ID	2
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References.html