SmartShop-Scan-Report

Generated with ZAP on Fri 11 Nov 2022, at 17:47:18

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://demo.smartstore.com
- https://demo.smartstore.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				
		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%)	3 (16.7%)	1 (5.6%)	1 (5.6%)	5 (27.8%)
	Low	0 (0.0%)	3 (16.7%)	5 (27.8%)	1 (5.6%)	9 (50.0%)
	Informational	0 (0.0%)	0 (0.0%)	1 (5.6%)	3 (16.7%)	4 (22.2%)
	Total	0 (0.0%)	6 (33.3%)	7 (38.9%)	5 (27.8%)	18 (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://demo.smartstore.com	0 (0)	5 (5)	9 (14)	4 (18)

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
Absence of Anti-CSRF Tokens	Medium	2333 (12,961.1%)
CSP: Wildcard Directive	Medium	16077 (89,316.7%)
CSP: script-src unsafe-inline	Medium	16076 (89,311.1%)
CSP: style-src unsafe-inline	Medium	16075 (89,305.6%)
Vulnerable JS Library	Medium	3 (16.7%)
Total		18

Alert type	Risk	Count
Cookie Without Secure Flag	Low	2 (11.1%)
Cookie without SameSite Attribute	Low	1 (5.6%)
Secure Pages Include Mixed Content	Low	2 (11.1%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	17076 (94,866.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	17076 (94,866.7%)
Strict-Transport-Security Header Not Set	Low	2382 (13,233.3%)
Timestamp Disclosure - Unix	Low	249 (1,383.3%)
X-AspNet-Version Response Header	Low	34047 (189,150.0%)
X-Content-Type-Options Header Missing	Low	2361 (13,116.7%)
Information Disclosure - Suspicious Comments	Informational	2738 (15,211.1%)
Modern Web Application	Informational	1369 (7,605.6%)
Re-examine Cache-control Directives	Informational	1364
Total		18

Alert type	Risk	Count
		(7,577.8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	800 (4,444.4%)
Total		18

Alerts

Risk=Medium, Confidence=High (3)

https://demo.smartstore.com (3)

CSP: Wildcard Directive (1)

▶ GET https://demo.smartstore.com/robots.txt

CSP: script-src unsafe-inline (1)

▶ GET https://demo.smartstore.com/robots.txt

CSP: style-src unsafe-inline (1)

▶ GET https://demo.smartstore.com/robots.txt

Risk=Medium, Confidence=Medium (1)

https://demo.smartstore.com (1)

Vulnerable JS Library (1)

▶ GET https://demo.smartstore.com/BACKEND/bundles/js/w7ar7xaahjxetk7y541-liwb0fnuimdqdas0qtmrxoa1?v=8Ywxgy-xHzt53KjDA9qzUGP_Uv0gvVwf0iyEcYxaCGY1

Risk=Medium, Confidence=Low (1)

https://demo.smartstore.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://demo.smartstore.com/backend/en/login

Risk=Low, Confidence=High (3)

https://demo.smartstore.com (3)

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

▶ GET https://demo.smartstore.com/robots.txt

Strict-Transport-Security Header Not Set (1)

▶ GET https://demo.smartstore.com/robots.txt

X-AspNet-Version Response Header (1)

▶ GET https://demo.smartstore.com/backend/changelanguage/1?returnUrl=login

Risk=Low, Confidence=Medium (5)

https://demo.smartstore.com (5)

Cookie Without Secure Flag (1)

▶ GET https://demo.smartstore.com/backend/en/cart

Cookie without SameSite Attribute (1)

▶ GET https://demo.smartstore.com/backend/en/register

Secure Pages Include Mixed Content (1)

▶ GET https://demo.smartstore.com/backend/en/bauhaus-furniture

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

▶ GET https://demo.smartstore.com/sitemap.xml

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

▶ GET https://demo.smartstore.com/backend/en/login

Risk=Low, Confidence=Low (1)

https://demo.smartstore.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://demo.smartstore.com/backend/en/contactus

Risk=Informational, Confidence=Medium (1)

https://demo.smartstore.com (1)

Modern Web Application (1)

▶ GET https://demo.smartstore.com/backend/en/login

Risk=Informational, Confidence=Low (3)

https://demo.smartstore.com (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://demo.smartstore.com/backend/en/login

Re-examine Cache-control Directives (1)

▶ GET https://demo.smartstore.com/backend/en/login

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

▶ GET https://demo.smartstore.com/backend/en/login?returnUrl=%2Fbackend%2Fen%2Flogin

Appendix

Alert types

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

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

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	• https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	• 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

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

Secure Pages Include Mixed Content

Source raised by a passive scanner (Secure Pages Include Mixed Content)

CWE ID 311

WASC ID 4

Reference
- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

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

Strict-Transport-Security Header Not Set

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

- https://owasp.org/www-community/Security_Headers
- http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- http://caniuse.com/stricttransportsecurity
- http://tools.ietf.org/html/rfc6797

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-AspNet-Version Response Header

Source	raised by a passive scanner (X-AspNet-Version Response Header)
CWE ID	933
WASC ID	14
Reference	- https://www.troyhunt.com/shhh-dont-let-your-response-headers/ - https://blogs.msdn.microsoft.com/varunm/2013/

04/23/remove-unwanted-http-response-headers/

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source	raised by a passive scanner (Re-examine Cache-control Directives)

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 ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

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