ShopHive-Scan-Report

Generated with ZAP on Sun 18 Dec 2022, at 20:56:12

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=High, Confidence=High (1)
  - Risk=High, Confidence=Medium (1)
  - Risk=Medium, Confidence=High (4)
  - Risk=Medium, Confidence=Medium (2)
  - Risk=Medium, Confidence=Low (1)
  - Risk=Low, Confidence=High (1)
  - Risk=Low, Confidence=Medium (7)

    - Risk=Low, Confidence=Low (1)
    - Risk=Informational, Confidence=Medium (2)
    - 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://www.shophive.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%)	1 (4.5%)	1 (4.5%)	0 (0.0%)	2 (9.1%)
	Medium	0 (0.0%)	4 (18.2%)	2 (9.1%)	1 (4.5%)	7 (31.8%)
	Low	0 (0.0%)	1 (4.5%)	7 (31.8%)	1 (4.5%)	9 (40.9%)
	Informational	0 (0.0%)	0 (0.0%)	2 (9.1%)	2 (9.1%)	4 (18.2%)
	Total	0 (0.0%)	6 (27.3%)	12 (54.5%)	4 (18.2%)	22 (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://www.shophive.com	2 (2)	7 (9)	9 (18)	4 (22)

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
Hash Disclosure - Mac OSX salted SHA-1	High	1 (4.5%)
PII Disclosure	High	3 (13.6%)
Absence of Anti-CSRF Tokens	Medium	22732 (103,327.3%)
Total		22

Alert type	Risk	Count
CSP: Wildcard Directive	Medium	7293 (33,150.0%)
CSP: script-src unsafe-inline	Medium	7293 (33,150.0%)
CSP: style-src unsafe-inline	Medium	7293 (33,150.0%)
Content Security Policy (CSP) Header Not Set	Medium	1621 (7,368.2%)
Cross-Domain Misconfiguration	Medium	8915 (40,522.7%)
Vulnerable JS Library	Medium	2 (9.1%)
Application Error Disclosure	Low	4158 (18,900.0%)
Cookie No HttpOnly Flag	Low	123 (559.1%)
Cookie Without Secure Flag	Low	62 (281.8%)
Cookie without SameSite Attribute	Low	211 (959.1%)
Cross-Domain JavaScript Source File Inclusion	Low	3025 (13,750.0%)
Secure Pages Include Mixed Content	Low	1 (4.5%)
Total		22

Alert type	Risk	Count
Strict-Transport-Security Header Not Set	Low	9117 (41,440.9%)
Timestamp Disclosure - Unix	Low	3766 (17,118.2%)
X-Content-Type-Options Header Missing	Low	280 (1,272.7%)
Information Disclosure - Suspicious Comments	Informational	3079 (13,995.5%)
Modern Web Application	Informational	8835 (40,159.1%)
Retrieved from Cache	Informational	158 (718.2%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	56 (254.5%)
Total		22

Alerts

Risk=High, Confidence=High (1)

https://www.shophive.com (1)

PII Disclosure (1)

▶ GET https://www.shophive.com/xiaomi-redmi-a1-2gb-32gb/

Risk=High, Confidence=Medium (1)

https://www.shophive.com (1)

Hash Disclosure - Mac OSX salted SHA-1 (1)

▶ GET https://www.shophive.com/media/images/cache/amasty/shopby/option_images/slider/resized/70x30/Asus.png

Risk=Medium, Confidence=High (4)

https://www.shophive.com (4)

CSP: Wildcard Directive (1)

▶ GET https://www.shophive.com/customer/account/login/

CSP: script-src unsafe-inline (1)

▶ GET https://www.shophive.com/customer/account/login/

CSP: style-src unsafe-inline (1)

▶ GET https://www.shophive.com/customer/account/login/

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

▶ POST https://www.shophive.com/checkout/cart/add/uenc/aHR0cHM6Ly93d3cuc2hvcGhpdmUuY29tL2Fua2VyLTIwdy0yLXBvcnQtdXNiLXdhbGwtY2hhcmdlcg%2C%2C/product/58477/

Risk=Medium, Confidence=Medium (2)

https://www.shophive.com (2)

Cross-Domain Misconfiguration (1)

▶ GET https://www.shophive.com/robots.txt

Vulnerable JS Library (1)

▶ GET https://www.shophive.com/static/version1666113218/_cache/merged/0418fb6577912eb099281caa88050666.min.js

Risk=Medium, Confidence=Low (1)

https://www.shophive.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.shophive.com/customer/account/login/

Risk=Low, Confidence=High (1)

https://www.shophive.com (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.shophive.com/robots.txt

Risk=Low, Confidence=Medium (7)

https://www.shophive.com (7)

Application Error Disclosure (1)

▶ GET https://www.shophive.com/tv-audio/projectors?c2c_contrast_ratio=20582

Cookie No HttpOnly Flag (1)

▶ POST https://www.shophive.com/customer/account/loginPost/

Cookie Without Secure Flag (1)

▶ POST https://www.shophive.com/customer/account/loginPost/

Cookie without SameSite Attribute (1)

▶ GET https://www.shophive.com/customer/account/login/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.shophive.com/

Secure Pages Include Mixed Content (1)

▶ GET https://www.shophive.com/a4tech-fbk11-bluetooth-2-4g-wireless-keyboard/

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

▶ GET https://www.shophive.com/sitemap.xml

Risk=Low, Confidence=Low (1)

https://www.shophive.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.shophive.com/customer/account/login/

Risk=Informational, Confidence=Medium (2)

https://www.shophive.com (2)

Modern Web Application (1)

▶ GET https://www.shophive.com/customer/account/login/

Retrieved from Cache (1)

▶ GET https://www.shophive.com/static/version1666113218/frontend/bs_complex/bs_complex1/en_US/css/print.min.css

Risk=Informational, Confidence=Low (2)

https://www.shophive.com (2)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.shophive.com/apple

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

▶ GET https://www.shophive.com/catalogsearch/result/?cat&q=legion

Appendix

Alert types

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

Hash Disclosure - Mac OSX salted SHA-1

Source	raised by a passive scanner (Hash Disclosure)
CWE ID	200
WASC ID	13
Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage ▪ http://openwall.info/wiki/john/sample-hashes

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

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/

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 (Powered by Retire.js))
CWE ID	829
Reference	▪ https://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ http://research.insecurelabs.org/jquery/test/ ▪ 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://bugs.jquery.com/ticket/11974 ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Application Error Disclosure

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

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 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

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

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

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-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)

Retrieved from Cache

Source	raised by a passive scanner (Retrieved from Cache)
Reference	▪ https://tools.ietf.org/html/rfc7234 ▪ https://tools.ietf.org/html/rfc7231 ▪ http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)

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