iShopping.pk-Scan-Report

Generated with ZAP on Tue 20 Dec 2022, at 06:46:05

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://www.ishopping.pk`
- `https://www.ishopping.pk`

(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 (6.2%)	0 (0.0%)	0 (0.0%)	1 (6.2%)
	Medium	0 (0.0%)	1 (6.2%)	2 (12.5%)	1 (6.2%)	4 (25.0%)
	Low	0 (0.0%)	1 (6.2%)	5 (31.2%)	1 (6.2%)	7 (43.8%)
	Informational	0 (0.0%)	0 (0.0%)	2 (12.5%)	2 (12.5%)	4 (25.0%)
	Total	0 (0.0%)	3 (18.8%)	9 (56.2%)	4 (25.0%)	16 (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.ishopping.pk	1 (1)	4 (5)	7 (12)	4 (16)

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	6 (37.5%)
Absence of Anti-CSRF Tokens	Medium	11786 (73,662.5%)
Content Security Policy (CSP) Header Not Set	Medium	1479 (9,243.8%)
Cross-Domain Misconfiguration	Medium	9 (56.2%)
Total		16

Alert type	Risk	Count
Missing Anti-clickjacking Header	Medium	1359 (8,493.8%)
Cookie No HttpOnly Flag	Low	47 (293.8%)
Cookie with SameSite Attribute None	Low	6893 (43,081.2%)
Cross-Domain JavaScript Source File Inclusion	Low	68845 (430,281.2%)
Strict-Transport-Security Header Not Set	Low	1613 (10,081.2%)
Timestamp Disclosure - Unix	Low	4089 (25,556.2%)
X-Backend-Server Header Information Leak	Low	3499 (21,868.8%)
X-Content-Type-Options Header Missing	Low	1492 (9,325.0%)
Information Disclosure - Suspicious Comments	Informational	4667 (29,168.8%)
Modern Web Application	Informational	1362 (8,512.5%)
Retrieved from Cache	Informational	244 (1,525.0%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	139 (868.8%)
Total		16

Alerts

Risk=High, Confidence=High (1)

https://www.ishopping.pk (1)

PII Disclosure (1)

▶ GET https://www.ishopping.pk/fanci-mall-ultimate-eye-shadow-palette-super-star-es001-1-price-in-pakistan-322815.html

Risk=Medium, Confidence=High (1)

https://www.ishopping.pk (1)

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

▶ GET https://www.ishopping.pk/

Risk=Medium, Confidence=Medium (2)

https://www.ishopping.pk (2)

Cross-Domain Misconfiguration (1)

▶ GET https://www.ishopping.pk/media/wysiwyg/CMS_Blocks/Block_For_MakeUp/Jordana-1.png

Missing Anti-clickjacking Header (1)

▶ GET https://www.ishopping.pk/

Risk=Medium, Confidence=Low (1)

https://www.ishopping.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.ishopping.pk/

Risk=Low, Confidence=High (1)

https://www.ishopping.pk (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.ishopping.pk/robots.txt

Risk=Low, Confidence=Medium (5)

https://www.ishopping.pk (5)

Cookie No HttpOnly Flag (1)

▶ POST https://www.ishopping.pk/checkout/cart/add/uenc/aHR0cHM6Ly93d3cuaXNob3BwaW5nLnBrL2JyYXVuLWJlYXV0eS13ZXQtZHJ5LWVwaWxhdG9yLXNlcy05OTg1LXByaWNlLWluLXBha2lzdGFuLmh0bWw,/product/579910/form_key/1M92WLoOzYk2fwPJ/

Cookie with SameSite Attribute None (1)

▶ GET https://www.ishopping.pk/customer/account/

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.ishopping.pk/

X-Backend-Server Header Information Leak (1)

▶ GET https://www.ishopping.pk/robots.txt

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

▶ GET https://www.ishopping.pk/

Risk=Low, Confidence=Low (1)

https://www.ishopping.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.ishopping.pk/

Risk=Informational, Confidence=Medium (2)

https://www.ishopping.pk (2)

Modern Web Application (1)

▶ GET https://www.ishopping.pk/

Retrieved from Cache (1)

▶ GET https://www.ishopping.pk/

Risk=Informational, Confidence=Low (2)

https://www.ishopping.pk (2)

Information Disclosure - Suspicious Comments (1)

▶ `GET https://www.ishopping.pk/`

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

▶ `GET https://www.ishopping.pk/health-beauty.html?dir=asc&order=price`

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

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

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

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 with SameSite Attribute None

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

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-Backend-Server Header Information Leak

Source	raised by a passive scanner (X-Backend-Server Header Information Leak)
CWE ID	200
WASC ID	13

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