HammerCorpEcom.html

Generated with ZAP on Wed 8 Nov 2023, at 14:56:19

ZAP Version: 2.14.0

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://172.16.1.114

(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%)	1 (5.9%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	1 (5.9%)	1 (5.9%)	1 (5.9%)	3 (17.6%)
	Low	0 (0.0%)	0 (0.0%)	5 (29.4%)	1 (5.9%)	6 (35.3%)
	Informational	0 (0.0%)	1 (5.9%)	4 (23.5%)	2 (11.8%)	7 (41.2%)
	Total	0 (0.0%)	2 (11.8%)	11 (64.7%)	4 (23.5%)	17 (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://172.16.1.11 4**	1 (1)	3 (4)	6 (10)	7 (17)

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
Cross Site Scripting (Reflected)	High	8 (47.1%)
Absence of Anti-CSRF Tokens	Medium	137 (805.9%)
Total		17

Alert type	Risk	Count
Content Security Policy (CSP) Header Not Set	Medium	63 (370.6%)
Vulnerable JS Library	Medium	3 (17.6%)
Cookie No HttpOnly Flag	Low	4 (23.5%)
Cookie without SameSite Attribute	Low	6 (35.3%)
Cross-Domain JavaScript Source File Inclusion	Low	108 (635.3%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	67 (394.1%)
Timestamp Disclosure - Unix	Low	92 (541.2%)
X-Content-Type-Options Header Missing	Low	115 (676.5%)
Authentication Request Identified	Informational	2 (11.8%)
Information Disclosure - Sensitive Information in URL	Informational	1 (5.9%)
Information Disclosure - Suspicious Comments	Informational	29 (170.6%)
Total		17

Alert type	Risk	Count
Modern Web Application	Informational	55 (323.5%)
Session Management Response Identified	Informational	5 (29.4%)
User Agent Fuzzer	Informational	809 (4,758.8%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	84 (494.1%)
Total		17

Alerts

Risk=High, Confidence=Medium (1)

http://172.16.1.114 (1)

Cross Site Scripting (Reflected) (1)

▶ GET http://172.16.1.114/index.php?email=%27%3Balert%281%29%3B%27&rt=account%2Fsubscriber&rt=account%2Fsubscriber

Risk=Medium, Confidence=High (1)

http://172.16.1.114 (1)

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

▶ GET http://172.16.1.114/sitemap.xml

Risk=Medium, Confidence=Medium (1)

http://172.16.1.114 (1)

Vulnerable JS Library (1)

▶ GET http://172.16.1.114/storefront/view/default/javascript/jquery-migrate-1.2.1.min.js.pagespeed.jm.mhpNjdU8Wl.js

Risk=Medium, Confidence=Low (1)

http://172.16.1.114 (1)

Absence of Anti-CSRF Tokens (1)

▶ GET http://172.16.1.114

Risk=Low, Confidence=Medium (5)

http://172.16.1.114 (5)

Cookie No HttpOnly Flag (1)

▶ GET http://172.16.1.114

Cookie without SameSite Attribute (1)

▶ GET http://172.16.1.114

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET http://172.16.1.114

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

▶ GET http://172.16.1.114/core/

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

▶ GET http://172.16.1.114/robots.txt

Risk=Low, Confidence=Low (1)

http://172.16.1.114 (1)

Timestamp Disclosure - Unix (1)

▶ GET http://172.16.1.114

Risk=Informational, Confidence=High (1)

http://172.16.1.114 (1)

Authentication Request Identified (1)

▶ POST http://172.16.1.114/index.php?rt=account/login

Risk=Informational, Confidence=Medium (4)

http://172.16.1.114 (4)

Information Disclosure - Sensitive Information in URL (1)

▶ GET http://172.16.1.114
/index.php?email=zaproxy%40example.com&
rt=account%2Fsubscriber&rt=account/subscriber

Modern Web Application (1)

▶ GET http://172.16.1.114

Session Management Response Identified (1)

▶ GET http://172.16.1.114

User Agent Fuzzer (1)

▶ POST http://172.16.1.114/index.php?form_id=2&rt=content
/contact

Risk=Informational, Confidence=Low (2)

http://172.16.1.114 (2)

Information Disclosure - Suspicious Comments (1)

▶ GET http://172.16.1.114/index.php?product_id=127&
rt=product/product

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

▶ GET http://172.16.1.114/index.php?product_id=127&
rt=product/product

Appendix

Alert types

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

Cross Site Scripting (Reflected)

Source	raised by an active scanner (Cross Site Scripting (Reflected))
CWE ID	79
WASC ID	8
Reference	▪ http://projects.webappsec.org/Cross-Site-Scripting ▪ https://cwe.mitre.org/data/definitions/79.html

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 ▪ https://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/

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829

Reference	▪ http://research.insecurelabs.org/jquery/test/ ▪ http://bugs.jquery.com/ticket/11290

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

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 (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

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

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

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg

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