ZAP Scanning Report

Generated with ZAP on Sun 24 May 2026, at 18:11:52

ZAP Version: 2.17.0

ZAP by Checkmarx

Contents

About This Report

Report Parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://alfabox.hmsconsulting.it

(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%)	1 (9.1%)	1 (9.1%)	0 (0.0%)	2 (18.2%)
	Low	0 (0.0%)	3 (27.3%)	2 (18.2%)	0 (0.0%)	5 (45.5%)
	Informational	0 (0.0%)	0 (0.0%)	2 (18.2%)	2 (18.2%)	4 (36.4%)
	Total	0 (0.0%)	4 (36.4%)	5 (45.5%)	2 (18.2%)	11 (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://alfabox.hmsconsulting.it**	0 (0)	2 (2)	5 (7)	4 (11)

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
Content Security Policy (CSP) Header Not Set	Medium	5 (45.5%)
Missing Anti-clickjacking Header	Medium	4 (36.4%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	5 (45.5%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	5 (45.5%)
Strict-Transport-Security Header Not Set	Low	5 (45.5%)
X-AspNet-Version Response Header	Low	1 (9.1%)
X-Content-Type-Options Header Missing	Low	5 (45.5%)
Information Disclosure - Suspicious Comments	Informational	1 (9.1%)
Modern Web Application	Informational	2 (18.2%)
Re-examine Cache-control Directives	Informational	4 (36.4%)
User Agent Fuzzer	Informational	5 (45.5%)
Total		11

Alerts

1. **Risk=Medium, Confidence=High (1)**
    1. **https://alfabox.hmsconsulting.it (1)**
        1. **Content Security Policy (CSP) Header Not Set (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/sitemap.xml
2. **Risk=Medium, Confidence=Medium (1)**
    1. **https://alfabox.hmsconsulting.it (1)**
        1. **Missing Anti-clickjacking Header (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/
3. **Risk=Low, Confidence=High (3)**
    1. **https://alfabox.hmsconsulting.it (3)**
        1. **Server Leaks Version Information via "Server" HTTP Response Header Field (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/css/open-iconic-bootstrap.min.css
        2. **Strict-Transport-Security Header Not Set (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/css/open-iconic-bootstrap.min.css
        3. **X-AspNet-Version Response Header (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/privacy-statement.html.
4. **Risk=Low, Confidence=Medium (2)**
    1. **https://alfabox.hmsconsulting.it (2)**
        1. **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox
        2. **X-Content-Type-Options Header Missing (1)**
            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/css/open-iconic-bootstrap.min.css

5. ## Risk=Informational, Confidence=Medium (2)

    1. **https://alfabox.hmsconsulting.it (2)**

        1. **Modern Web Application (1)**

            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/

        2. **User Agent Fuzzer (1)**

            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/css

6. ## Risk=Informational, Confidence=Low (2)

    1. **https://alfabox.hmsconsulting.it (2)**

        1. **Information Disclosure - Suspicious Comments (1)**

            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/js/jquery-3.5.1.min.js

        2. **Re-examine Cache-control Directives (1)**

            1. ▶ GET https://alfabox.hmsconsulting.it/alfabox/

Appendix

Alert Types

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

1. **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	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP 2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html 3. https://www.w3.org/TR/CSP/ 4. https://w3c.github.io/webappsec-csp/ 5. https://web.dev/articles/csp 6. https://caniuse.com/#feat=contentsecuritypolicy 7. https://content-security-policy.com/

2. **Missing Anti-clickjacking Header**

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

3. **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	497
WASC ID	13
Reference	1. https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework 2. https://www.troyhunt.com/shhh-dont-let-your-response-headers/

4. **Server Leaks Version Information via "Server" HTTP Response Header Field**

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	497
WASC ID	13
Reference	1. https://httpd.apache.org/docs/current/mod/core.html#servertokens 2. https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) 3. https://www.troyhunt.com/shhh-dont-let-your-response-headers/

5. **Strict-Transport-Security Header Not Set**

Source	raised by a passive scanner (Strict-Transport-Security Header)
CWE ID	319
WASC ID	15
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html 2. https://owasp.org/www-community/Security_Headers 3. https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security 4. https://caniuse.com/stricttransportsecurity 5. https://datatracker.ietf.org/doc/html/rfc6797

6. **X-AspNet-Version Response Header**

Source	raised by a passive scanner (X-AspNet-Version Response Header)
CWE ID	933
WASC ID	14
Reference	1. https://www.troyhunt.com/shhh-dont-let-your-response-headers/ 2. https://learn.microsoft.com/en-us/archive/blogs/varunm/remove-unwanted-http-response-headers

7. **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	1. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) 2. https://owasp.org/www-community/Security_Headers

8. **Information Disclosure - Suspicious Comments**

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	615
WASC ID	13

9. **Modern Web Application**

Source	raised by a passive scanner (Modern Web Application)

10. **Re-examine Cache-control Directives**

Source	raised by a passive scanner (Re-examine Cache-control Directives)
CWE ID	525
WASC ID	13
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching 2. https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control 3. https://grayduck.mn/2021/09/13/cache-control-recommendations/

11. **User Agent Fuzzer**

Source	raised by an active scanner (User Agent Fuzzer)
Reference	1. https://owasp.org/wstg