ZAP by Checkmarx Scanning Report

Generated with The ZAP logoZAP on Sa. 12 Sept. 2026, at 16:22:13

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://whatsapp-support.de

(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: Hoch, Mittel, Gering, Informational

Excluded: None

Confidence levels

Included: User Confirmed, Hoch, Mittel, Gering

Excluded: User Confirmed, Hoch, Mittel, Gering, Falsch Positives Ergebnis

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	**Hoch**	**Mittel**	**Gering**	**Total**
Risk	**Hoch**	0 (0,0 %)	0 (0,0 %)	1 (4,2 %)	0 (0,0 %)	1 (4,2 %)
	Mittel	0 (0,0 %)	1 (4,2 %)	1 (4,2 %)	1 (4,2 %)	3 (12,5 %)
	Gering	0 (0,0 %)	1 (4,2 %)	3 (12,5 %)	1 (4,2 %)	5 (20,8 %)
	Informational	0 (0,0 %)	1 (4,2 %)	12 (50,0 %)	2 (8,3 %)	15 (62,5 %)
	Total	0 (0,0 %)	3 (12,5 %)	17 (70,8 %)	4 (16,7 %)	24 (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			
		Hoch (= Hoch)	**Mittel (>= Mittel)**	**Gering (>= Gering)**	**Informational (>= Informational)**
Site	**https://whatsapp-support.de**	1 (1)	3 (4)	5 (9)	15 (24)

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
SQL Injection	Hoch	41 (170,8 %)
Absence of Anti-CSRF Tokens	Mittel	5 (20,8 %)
Content Security Policy (CSP) Header Not Set	Mittel	5 (20,8 %)
Directory Browsing	Mittel	5 (20,8 %)
Cookie No HttpOnly Flag	Gering	4 (16,7 %)
Cookie without SameSite Attribute	Gering	5 (20,8 %)
Strict-Transport-Security Header Not Set	Gering	5 (20,8 %)
Timestamp Disclosure - Unix	Gering	5 (20,8 %)
Total		24

Alert type	Risk	Count
X-Content-Type-Options Header Missing	Gering	5 (20,8 %)
Authentication Request Identified	Informational	2 (8,3 %)
Information Disclosure - Sensitive Information in URL	Informational	5 (20,8 %)
Information Disclosure - Suspicious Comments	Informational	105 (437,5 %)
Modern Web Application	Informational	5 (20,8 %)
Re-examine Cache-control Directives	Informational	5 (20,8 %)
Session Management Response Identified	Informational	3 (12,5 %)
Tech Detected - Apache HTTP Server	Informational	1 (4,2 %)
Tech Detected - Open Graph	Informational	1 (4,2 %)
Tech Detected - PHP	Informational	1 (4,2 %)
Tech Detected - PWA	Informational	1 (4,2 %)
Tech Detected - RSS	Informational	1 (4,2 %)
Tech Detected - React	Informational	1 (4,2 %)
Tech Detected - Woltlab Community Framework	Informational	1 (4,2 %)
User Agent Fuzzer	Informational	5 (20,8 %)
User Controllable HTML Element Attribute (Potential XSS)	Informational	79 (329,2 %)
Total		24

Insights

This table shows information that is likely to be very relevant to you, but which is not related to vulnerabilities, or potentially even related to the application in question.

Level	Grund	Site	Beschreibung	Statistic

Level	Grund	Site	Beschreibung	Statistic
Mittel	Exceeded Low		Percentage of memory used	93
Gering	Warnung		ZAP errors logged - see the zap.log file for details	3
Gering	Warnung		ZAP warnings logged - see the zap.log file for details	513
Gering	Exceeded High	https://whatsapp-support.de	Percentage of slow responses	80 %
Info	Informational	https://whatsapp-support.de	Percentage of responses with status code 2xx	67 %
Info	Informational	https://whatsapp-support.de	Percentage of responses with status code 3xx	19 %
Info	Exceeded Low	https://whatsapp-support.de	Percentage of responses with status code 4xx	12 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type application/json	24 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type application/rss+xml	1 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type application/xml	2 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type font/woff2	1 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type image/png	6 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type text/css	3 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type text/html	49 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type text/javascript	10 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with content type text/plain	2 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with method GET	86 %
Info	Informational	https://whatsapp-support.de	Percentage of endpoints with method POST	13 %
Info	Informational	https://whatsapp-support.de	Count of total endpoints	161

Alerts

1. **Risk=Hoch, Confidence=Mittel (1)**
    1. **https://whatsapp-support.de (1)**
        1. **SQL Injection (1)**
            1. ► POST https://whatsapp-support.de/acp/index.php?login/
2. **Risk=Mittel, Confidence=Hoch (1)**
    1. **https://whatsapp-support.de (1)**
        1. **Content Security Policy (CSP) Header Not Set (1)**
            1. ► GET https://whatsapp-support.de/sitemap.xml
3. **Risk=Mittel, Confidence=Mittel (1)**
    1. **https://whatsapp-support.de (1)**
        1. **Directory Browsing (1)**
            1. ► GET https://whatsapp-support.de/acp/images/
4. **Risk=Mittel, Confidence=Gering (1)**
    1. **https://whatsapp-support.de (1)**
        1. **Absence of Anti-CSRF Tokens (1)**
            1. ► GET https://whatsapp-support.de
5. **Risk=Gering, Confidence=Hoch (1)**
    1. **https://whatsapp-support.de (1)**
        1. **Strict-Transport-Security Header Not Set (1)**
            1. ► GET https://whatsapp-support.de/robots.txt
6. **Risk=Gering, Confidence=Mittel (3)**
    1. **https://whatsapp-support.de (3)**
        1. **Cookie No HttpOnly Flag (1)**

1. ► GET https://whatsapp-support.de

2. **Cookie without SameSite Attribute** (1)

    1. ► GET https://whatsapp-support.de

3. **X-Content-Type-Options Header Missing** (1)

    1. ► GET https://whatsapp-support.de/robots.txt

7. Risk=Gering, Confidence=Gering (1)

1. **https://whatsapp-support.de (1)**

    1. **Timestamp Disclosure - Unix** (1)

        1. ► GET https://whatsapp-support.de

8. Risk=Informational, Confidence=Hoch (1)

1. **https://whatsapp-support.de (1)**

    1. **Authentication Request Identified** (1)

        1. ► POST https://whatsapp-support.de/acp/index.php?login/

9. Risk=Informational, Confidence=Mittel (12)

1. **https://whatsapp-support.de (12)**

    1. **Information Disclosure - Sensitive Information in URL** (1)

        1. ► GET https://whatsapp-support.de/index.php?lost-password/

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

        1. ► GET https://whatsapp-support.de

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

        1. ► GET https://whatsapp-support.de

    4. **Session Management Response Identified** (1)

        1. ► GET https://whatsapp-support.de

    5. **Tech Detected - Apache HTTP Server** (1)

1. ► GET https://whatsapp-support.de/robots.txt

6. **Tech Detected - Open Graph** (1)

    1. ► GET https://whatsapp-support.de

7. **Tech Detected - PHP** (1)

    1. ► GET https://whatsapp-support.de/acp/index.php?index/

8. **Tech Detected - PWA** (1)

    1. ► GET https://whatsapp-support.de

9. **Tech Detected - RSS** (1)

    1. ► GET https://whatsapp-support.de

10. **Tech Detected - React** (1)

    1. ► GET https://whatsapp-support.de

11. **Tech Detected - Woltlab Community Framework** (1)

    1. ► GET https://whatsapp-support.de

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

    1. ► GET https://whatsapp-support.de/forum/

10. **Risk=Informational, Confidence=Gering (2)**

    1. **https://whatsapp-support.de (2)**

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

            1. ► GET https://whatsapp-support.de/robots.txt

        2. **User Controllable HTML Element Attribute (Potential XSS)** (1)

            1. ► GET https://whatsapp-support.de/acp/index.php?login/&url=https%3A%2F%2Fwhatsapp-support.de%2Facp%2F

Appendix

Alert Types

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

1. **SQL Injection**

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

2. **Absence of Anti-CSRF Tokens**

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	1. https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html 2. https://cwe.mitre.org/data/definitions/352.html

3. **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/

4. **Directory Browsing**

Source	raised by an active scanner (Directory Browsing)
CWE ID	548
WASC ID	48
Reference	1. https://httpd.apache.org/docs/current/mod/core.html#options

5. **Cookie No HttpOnly Flag**

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	1. https://owasp.org/www-community/HttpOnly

6. **Cookie without SameSite Attribute**

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	1. https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

7. **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

8. **Timestamp Disclosure - Unix**

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	1. https://cwe.mitre.org/data/definitions/200.html

9. **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

10. **Authentication Request Identified**

Source	raised by a passive scanner (Authentication Request Identified)
Reference	1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

11. **Information Disclosure - Sensitive Information in URL**

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	598
WASC ID	13

12. **Information Disclosure - Suspicious Comments**

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

13. **Modern Web Application**

Source raised by a passive scanner (Modern Web Application)

14. **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/

15. **Session Management Response Identified**

Source	raised by a passive scanner (Session Management Response Identified)
Reference	1. https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/

16. **Tech Detected - Apache HTTP Server**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://httpd.apache.org/

17. **Tech Detected - Open Graph**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://ogp.me

18. **Tech Detected - PHP**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://php.net

19. **Tech Detected - PWA**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://web.dev/progressive-web-apps/

20. **Tech Detected - RSS**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://www.rssboard.org/rss-specification

21. **Tech Detected - React**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://reactjs.org

22. **Tech Detected - Woltlab Community Framework**

Source	raised by other tools/functionalities in ZAP (for example, fuzzer, HTTPS Info add-on, custom scripts...) (plugin ID: 10004)
WASC ID	13
Reference	1. https://www.woltlab.com

23. **User Agent Fuzzer**

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

24. **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	1. https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html