ZAP Scanning Report

Generated with The ZAP logoZAP on Wed 20 Nov 2024, at 19:03:54

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

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://10.1.2.6

(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 (2.7%)	4 (10.8%)	0 (0.0%)	5 (13.5%)
	Medium	0 (0.0%)	1 (2.7%)	7 (18.9%)	1 (2.7%)	9 (24.3%)
	Low	0 (0.0%)	2 (5.4%)	9 (24.3%)	1 (2.7%)	12 (32.4%)
	Informational	0 (0.0%)	2 (5.4%)	5 (13.5%)	4 (10.8%)	11 (29.7%)
	Total	0 (0.0%)	6 (16.2%)	25 (67.6%)	6 (16.2%)	37 (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://10.1.2.6	5 (5)	9 (14)	12 (26)	11 (37)

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 (DOM Based)	High	13 (35.1%)
Cross Site Scripting (Persistent)	High	3 (8.1%)
Cross Site Scripting (Reflected)	High	4 (10.8%)
Remote OS Command Injection	High	1 (2.7%)
SQL Injection - MySQL	High	1 (2.7%)
Absence of Anti-CSRF Tokens	Medium	342 (924.3%)
Application Error Disclosure	Medium	1 (2.7%)
Buffer Overflow	Medium	2 (5.4%)
Content Security Policy (CSP) Header Not Set	Medium	451 (1,218.9%)
Directory Browsing	Medium	14 (37.8%)
HTTP to HTTPS Insecure Transition in Form Post	Medium	1 (2.7%)
Missing Anti-clickjacking Header	Medium	409 (1,105.4%)
Vulnerable JS Library	Medium	11 (29.7%)
Weak Authentication Method	Medium	1 (2.7%)
Application Error Disclosure	Low	7 (18.9%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	3 (8.1%)
Cookie No HttpOnly Flag	Low	71 (191.9%)
Cookie without SameSite Attribute	Low	86 (232.4%)
Cross-Domain JavaScript Source File Inclusion	Low	52 (140.5%)
Information Disclosure - Debug Error Messages	Low	3 (8.1%)
Private IP Disclosure	Low	5 (13.5%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	351 (948.6%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	823 (2,224.3%)
Timestamp Disclosure - Unix	Low	15 (40.5%)
X-AspNet-Version Response Header	Low	47 (127.0%)
X-Content-Type-Options Header Missing	Low	652 (1,762.2%)
Authentication Request Identified	Informational	10 (27.0%)
Cookie Poisoning	Informational	2 (5.4%)
GET for POST	Informational	2 (5.4%)
Information Disclosure - Sensitive Information in URL	Informational	2 (5.4%)
Information Disclosure - Suspicious Comments	Informational	285 (770.3%)
Loosely Scoped Cookie	Informational	20 (54.1%)
Modern Web Application	Informational	158 (427.0%)
Session Management Response Identified	Informational	824 (2,227.0%)
User Agent Fuzzer	Informational	288 (778.4%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	122 (329.7%)
User Controllable JavaScript Event (XSS)	Informational	2 (5.4%)
Total		37

Alerts

1. **Risk=High, Confidence=High (1)**
    1. **http://10.1.2.6 (1)**
        1. Cross Site Scripting (DOM Based) (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/piccheck.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
2. **Risk=High, Confidence=Medium (4)**
    1. **http://10.1.2.6 (4)**
        1. Cross Site Scripting (Persistent) (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/guestbook.php
        2. Cross Site Scripting (Reflected) (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/guestbook.php
        3. Remote OS Command Injection (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/passcheck.php
        4. SQL Injection - MySQL (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/users/login.php
3. **Risk=Medium, Confidence=High (1)**
    1. **http://10.1.2.6 (1)**
        1. Content Security Policy (CSP) Header Not Set (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
4. **Risk=Medium, Confidence=Medium (7)**
    1. **http://10.1.2.6 (7)**
        1. Application Error Disclosure (1)
            1. ▶ GET http://10.1.2.6/wivet/pages/
        2. Buffer Overflow (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/admin/index.php?page=login
        3. Directory Browsing (1)
            1. ▶ GET http://10.1.2.6/wivet/pages/
        4. HTTP to HTTPS Insecure Transition in Form Post (1)
            1. ▶ GET http://10.1.2.6/gtd-php/donate.php
        5. Missing Anti-clickjacking Header (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
        6. Vulnerable JS Library (1)
            1. ▶ GET http://10.1.2.6/jquery.min.js
        7. Weak Authentication Method (1)
            1. ▶ GET http://10.1.2.6/WebGoat/attack
5. **Risk=Medium, Confidence=Low (1)**
    1. **http://10.1.2.6 (1)**
        1. Absence of Anti-CSRF Tokens (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
6. **Risk=Low, Confidence=High (2)**
    1. **http://10.1.2.6 (2)**
        1. Server Leaks Version Information via "Server" HTTP Response Header Field (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
        2. X-AspNet-Version Response Header (1)
            1. ▶ GET http://10.1.2.6/webgoat.net/
7. **Risk=Low, Confidence=Medium (9)**
    1. **http://10.1.2.6 (9)**
        1. Application Error Disclosure (1)
            1. ▶ GET http://10.1.2.6/redmine
        2. Big Redirect Detected (Potential Sensitive Information Leak) (1)
            1. ▶ GET http://10.1.2.6/webcal/
        3. Cookie No HttpOnly Flag (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
        4. Cookie without SameSite Attribute (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
        5. Cross-Domain JavaScript Source File Inclusion (1)
            1. ▶ GET http://10.1.2.6/owaspbricks/
        6. Information Disclosure - Debug Error Messages (1)
            1. ▶ GET http://10.1.2.6/mutillidae/
        7. Private IP Disclosure (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/guestbook.php
        8. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
        9. X-Content-Type-Options Header Missing (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
8. **Risk=Low, Confidence=Low (1)**
    1. **http://10.1.2.6 (1)**
        1. Timestamp Disclosure - Unix (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/calendar.php
9. **Risk=Informational, Confidence=High (2)**
    1. **http://10.1.2.6 (2)**
        1. Authentication Request Identified (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/users/login.php
        2. GET for POST (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/pic'%20+%20'check'%20+%20'.php
10. **Risk=Informational, Confidence=Medium (5)**
    1. **http://10.1.2.6 (5)**
        1. Information Disclosure - Sensitive Information in URL (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/users/sample.php?userid=1
        2. Information Disclosure - Suspicious Comments (1)
            1. ▶ GET http://10.1.2.6/
        3. Modern Web Application (1)
            1. ▶ GET http://10.1.2.6/hackxor_intro.php
        4. Session Management Response Identified (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/
        5. User Agent Fuzzer (1)
            1. ▶ POST http://10.1.2.6/WackoPicko/cart/action.php?action=delete
11. **Risk=Informational, Confidence=Low (4)**
    1. **http://10.1.2.6 (4)**
        1. Cookie Poisoning (1)
            1. ▶ POST http://10.1.2.6/ghost/submit.php
        2. Loosely Scoped Cookie (1)
            1. ▶ GET http://10.1.2.6/phpBB2/
        3. User Controllable HTML Element Attribute (Potential XSS) (1)
            1. ▶ GET http://10.1.2.6/WackoPicko/pictures/search.php?query=ZAP
        4. User Controllable JavaScript Event (XSS) (1)
            1. ▶ GET http://10.1.2.6/ESAPI-Java-SwingSet-Interactive/main?function=XSS&lab

Appendix

Alert types

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

1. **Cross Site Scripting (DOM Based)**

    Source raised by an active scanner (Cross Site Scripting (DOM Based))
    CWE ID 79
    WASC ID 8
    Reference
    1. https://owasp.org/www-community/attacks/xss/
    2. https://cwe.mitre.org/data/definitions/79.html

2. **Cross Site Scripting (Persistent)**

    Source raised by an active scanner (Cross Site Scripting (Persistent))
    CWE ID 79
    WASC ID 8
    Reference
    1. https://owasp.org/www-community/attacks/xss/
    2. https://cwe.mitre.org/data/definitions/79.html

3. **Cross Site Scripting (Reflected)**

    Source raised by an active scanner (Cross Site Scripting (Reflected))
    CWE ID 79
    WASC ID 8
    Reference
    1. https://owasp.org/www-community/attacks/xss/
    2. https://cwe.mitre.org/data/definitions/79.html

4. **Remote OS Command Injection**

    Source raised by an active scanner (Remote OS Command Injection)
    CWE ID 78
    WASC ID 31
    Reference
    1. https://cwe.mitre.org/data/definitions/78.html
    2. https://owasp.org/www-community/attacks/Command_Injection

5. **SQL Injection - MySQL**

    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

6. **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

7. **Application Error Disclosure**

    Source raised by a passive scanner (Application Error Disclosure)
    CWE ID 200
    WASC ID 13

8. **Buffer Overflow**

    Source raised by an active scanner (Buffer Overflow)
    CWE ID 120
    WASC ID 7
    Reference
    1. https://owasp.org/www-community/attacks/Buffer_overflow_attack

9. **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/Security/CSP/Introducing_Content_Security_Policy
    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/

10. **Directory Browsing**

    Source raised by a passive scanner (Directory Browsing)
    CWE ID 548
    WASC ID 16
    Reference
    1. https://cwe.mitre.org/data/definitions/548.html

11. **HTTP to HTTPS Insecure Transition in Form Post**

    Source raised by a passive scanner (HTTP to HTTPS Insecure Transition in Form Post)
    CWE ID 319
    WASC ID 15

12. **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/Headers/X-Frame-Options

13. **Vulnerable JS Library**

    Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
    CWE ID 829
    Reference
    1. https://nvd.nist.gov/vuln/detail/CVE-2012-6708
    2. http://research.insecurelabs.org/jquery/test/
    3. https://bugs.jquery.com/ticket/9521
    4. http://bugs.jquery.com/ticket/11290
    5. https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/
    6. https://nvd.nist.gov/vuln/detail/CVE-2019-11358
    7. https://github.com/advisories/GHSA-q4m3-2j7h-f7xw
    8. https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b
    9. https://github.com/jquery/jquery.com/issues/162
    10. https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    11. https://nvd.nist.gov/vuln/detail/CVE-2020-7656
    12. https://nvd.nist.gov/vuln/detail/CVE-2011-4969

14. **Weak Authentication Method**

    Source raised by a passive scanner (Weak Authentication Method)
    CWE ID 326
    WASC ID 4
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

15. **Application Error Disclosure**

    Source raised by a passive scanner (Application Error Disclosure)
    CWE ID 200
    WASC ID 13

16. **Big Redirect Detected (Potential Sensitive Information Leak)**

    Source raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
    CWE ID 201
    WASC ID 13

17. **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

18. **Cookie without SameSite Attribute**

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

19. **Cross-Domain JavaScript Source File Inclusion**

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

20. **Information Disclosure - Debug Error Messages**

    Source raised by a passive scanner (Information Disclosure - Debug Error Messages)
    CWE ID 200
    WASC ID 13

21. **Private IP Disclosure**

    Source raised by a passive scanner (Private IP Disclosure)
    CWE ID 200
    WASC ID 13
    Reference
    1. https://tools.ietf.org/html/rfc1918

22. **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
    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/2012/02/shhh-dont-let-your-response-headers.html

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

    Source raised by a passive scanner (HTTP Server Response Header)
    CWE ID 200
    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/

24. **Timestamp Disclosure - Unix**

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

25. **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://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

26. **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

27. **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/

28. **Cookie Poisoning**

    Source raised by a passive scanner (Cookie Poisoning)
    CWE ID 565
    WASC ID 20
    Reference
    1. https://en.wikipedia.org/wiki/HTTP_cookie
    2. https://cwe.mitre.org/data/definitions/565.html

29. **GET for POST**

    Source raised by an active scanner (GET for POST)
    CWE ID 16
    WASC ID 20

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

    Source raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
    CWE ID 200
    WASC ID 13

31. **Information Disclosure - Suspicious Comments**

    Source raised by a passive scanner (Information Disclosure - Suspicious Comments)
    CWE ID 200
    WASC ID 13

32. **Loosely Scoped Cookie**

    Source raised by a passive scanner (Loosely Scoped Cookie)
    CWE ID 565
    WASC ID 15
    Reference
    1. https://tools.ietf.org/html/rfc6265#section-4.1
    2. 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
    3. https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

33. **Modern Web Application**

    Source raised by a passive scanner (Modern Web Application)

34. **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

35. **User Agent Fuzzer**

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

36. **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

37. **User Controllable JavaScript Event (XSS)**

    Source raised by a passive scanner (User Controllable JavaScript Event (XSS))
    CWE ID 20
    WASC ID 20
    Reference
    1. https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html