

Rungta College of Engineering and Technology

Department of B.Tech CSE (Cybersecurity)

Minor-2 Project Report

Metasploitable 2 & Mutillidae II Lab

Submitted By:

Kumar Sambhava

ERP No: 6605516

3rd Semester (2025–26)

Subject: Minor-2 Project

1.Introduction

This project demonstrates the setup and configuration of an intentionally vulnerable virtual lab using Metasploitable 2 and the Mutillidae II web application. The objective is to understand vulnerable environments, perform basic Linux administrative tasks, and troubleshoot common configuration errors.

2. Environment Setup

Metasploitable 2 is an Ubuntu-based virtual machine designed for security testing and learning. The VM was imported into a virtualization platform and accessed using default credentials (username: msfadmin, password: msfadmin)

```
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun Jan  4 10:40:21 EST 2026 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo /etc/init.d/apache2 restart
[sudo] password for msfadmin:
 * Restarting web server apache2 [ OK ]
msfadmin@metasploitable:~$ sudo /etc/init.d/mysql start
 * Starting MySQL database server mysqld [ OK ]
msfadmin@metasploitable:~$
```

3. User Management

A new Linux user account was created using my own name to demonstrate system administration skills. The `adduser` command was used, followed by verification through the `/etc/passwd` file.

Commands Used:

```
sudo adduser sambhava
```

```
cat /etc/passwd | grep sambhava
```

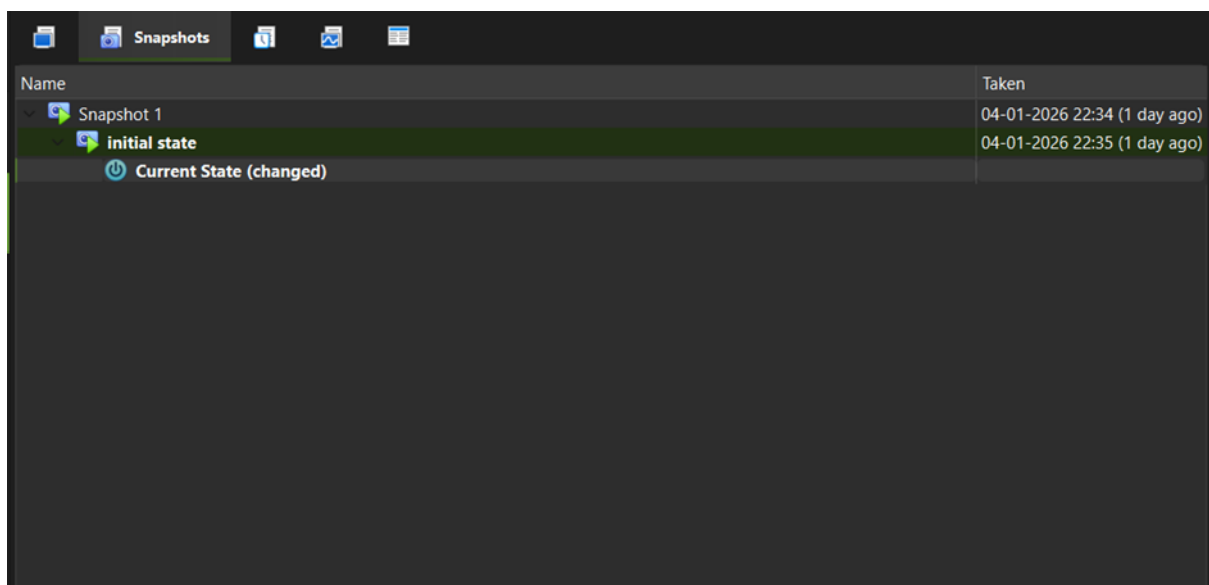
```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo adduser sambhava
[sudo] password for msfadmin:
Adding user 'sambhava' ...
Adding new group 'sambhava' (1003) ...
Adding new user 'sambhava' (1003) with group 'sambhava' ...
Creating home directory '/home/sambhava' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sambhava
Enter the new value, or press ENTER for the default
    Full Name []: Sambhava
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$ cat /etc/passwd | grep sambhava
sambhava:x:1003:1003:Sambhava,,,:/home/sambhava:/bin/bash
msfadmin@metasploitable:~$ _

```

4. Virtual Machine Snapshot

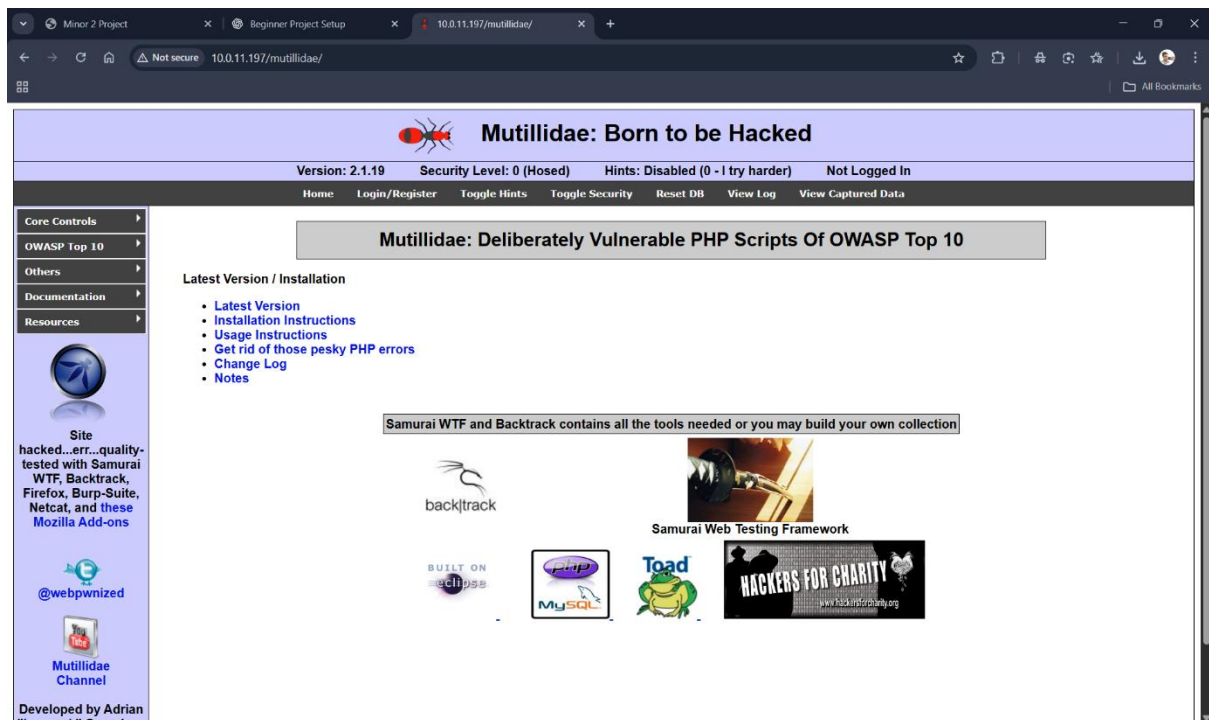
A snapshot was taken after user creation to preserve a safe system state. Snapshots allow easy rollback during testing and troubleshooting.



5. Mutillidae II Database Fix

Initially, Mutillidae II displayed database-related errors due to missing tables. The issue was resolved by using the Setup/Reset Database option within the application, which initialized the MySQL database successfully.

-Mutillidae II working.



-Mutillidae II database error.

Not secure 10.0.11.197/mutillidae/index.php?page=login.php

Error: Failure is always an option and this situation proves it	
Line	49
Code	0
File	/var/www/mutillidae/process-login-attempt.php
Message	Error executing query: Table 'metasploit.accounts' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(96): include() #1 (main)
Diagnostic Information	SELECT * FROM accounts WHERE username='shajh' AND password='hgahgs'


Did you [setup/reset the DB?](#)

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 148

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 254

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 255

Warning: Cannot modify header information - headers already sent by (output started at /var/www/mutillidae/process-login-attempt.php:97) in /var/www/mutillidae/index.php on line 256




Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls
OWASP Top 10
Others
Documentation
Resources

 Back

Login

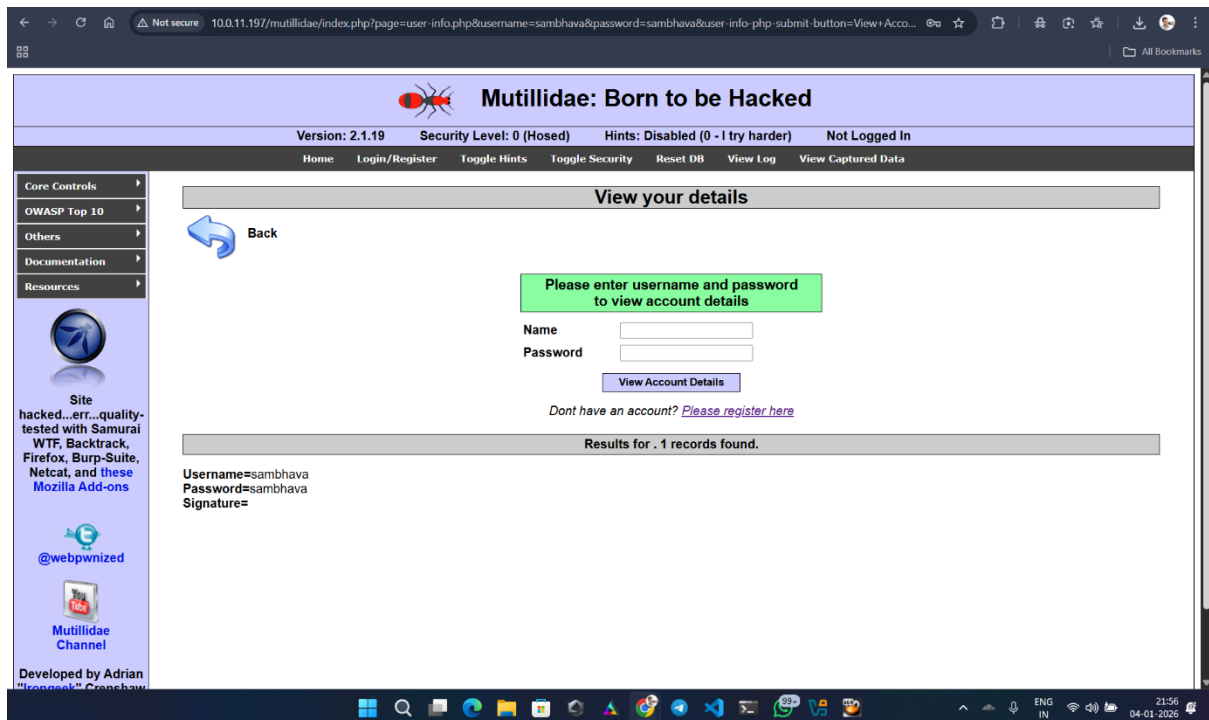
Please sign-in

-Mutillidae II database fixed.

```
<?php
/* NOTE: On Samurai, the $dbpass password is "samurai" rather than blank
$dbhost = 'localhost';
$dbuser = 'root';
$dbpass = '';
$dbname = 'owasp10';
?>
```

[Wrote 8 lines]

```
msfadmin@metasploitable:/var/www/mutillidae$
msfadmin@metasploitable:/var/www/mutillidae$
```



6.Conclusion

This project successfully demonstrated the setup of a vulnerable lab using Metasploitable2 and the troubleshooting of a real-world configuration issue in Mutillidae II. It enhanced practical understanding of Linux administration, virtualization safety, and web application deployment issues, which are essential skills in cybersecurity.

Appendix: Linux Commands Used

- ifconfig
- sudo adduser sambhava
- cat /etc/passwd | grep sambhava
- service mysql start
- Accessing http://[IP]/mutillidae/