

# Minor–2 Project Report

Project Title: Vulnerable Web Application Lab using Metasploitable and Mutillidae II

Student Name: Govind Sahu

Platform Used: VMWare Workstation Pro

## **1. Introduction**

This project is designed to create a controlled vulnerable lab environment for understanding basic web application security concepts. Metasploitable is used as a vulnerable operating system and Mutillidae II is used as a deliberately insecure web application.

## **2. Metasploitable Boot and Services**

The Metasploitable virtual machine was started successfully. During booting, multiple services such as Apache, Tomcat, and MySQL were initialized. This confirms that the system is fully operational.

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```

**Warning: Never expose this VM to an untrusted network!**

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: \_

## 3. System Login

The system was accessed using default credentials (msfadmin / msfadmin). Successful login confirmed terminal access and readiness for further configuration.

```
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
metasploitable login: msfadmin  
Password: _
```

## 4. New User Creation

To meet project requirements, a new user named 'govind' was created using Linux user management commands. This demonstrates basic system administration skills.

```
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 adduser govind
[sudo] password for msfadmin:
Adding user 'govind' ...
Adding new group 'govind' (1003) ...
Adding new user 'govind' (1003) with group 'govind' ...
Creating home directory '/home/govind' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for govind
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$
```

## 5. User Verification

The newly created user account was verified by checking the system password file. This ensures that the user was successfully added to the operating system.

```
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,,:/var/lib/mysql:/bin/false
tomcat5:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
govind:x:1003:1003:,,,,:/home/govind:/bin/bash
msfadmin@metasploitable:~$ _
```

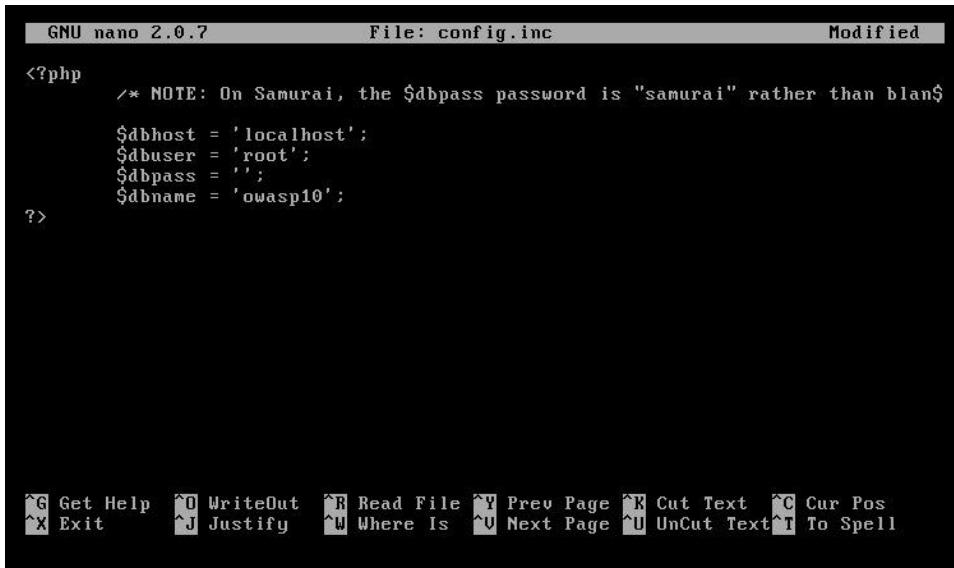
## 6. Mutillidae II Configuration Fix

Initially, Mutillidae II failed to load due to database configuration issues. The configuration file was edited to correct database credentials and database name.

```
msfadmin@metasploitable:~$ cd /var/www/mutillidae/
msfadmin@metasploitable:/var/www/mutillidae$ sudo nano config.inc
```

This screenshot shows the modification of the config.inc file of Mutillidae II. The database name was changed from **metasploit** to **owasp10** to fix the database

connection error. After updating the correct database name, the application connected successfully to the database and loaded properly in the browser.



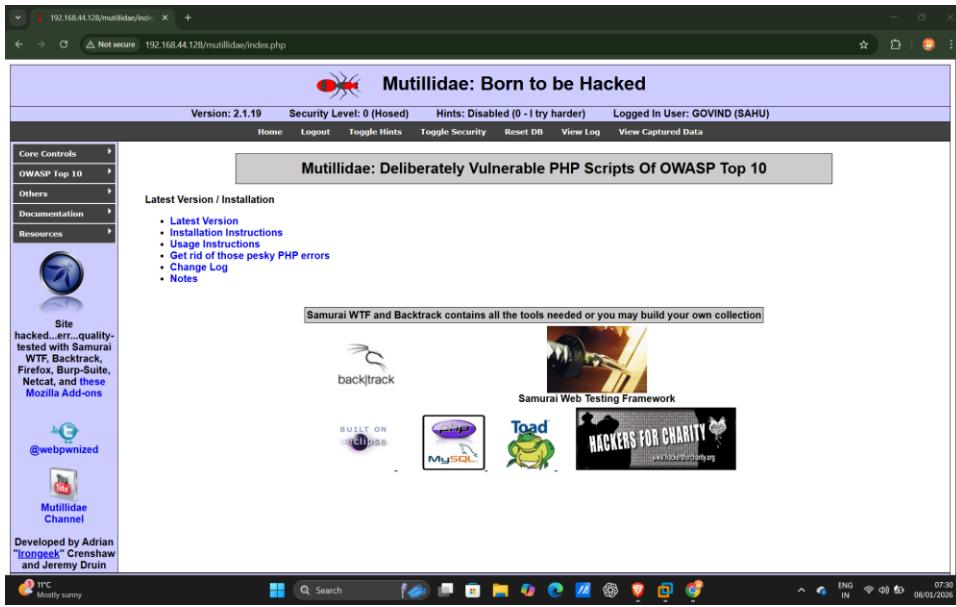
```
GNU nano 2.0.7          File: config.inc          Modified

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

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is   ^V Next Page  ^U UnCut Text  ^T To Spell
```

## 7. Successful Execution

After correcting the configuration, Mutillidae II loaded successfully in the browser without errors. This project provided hands-on experience with vulnerable systems, Linux commands, and web security labs.



## 8. Conclusion

This project successfully demonstrated the setup and configuration of the Metasploitable virtual machine for security testing purposes. System-level tasks such as user creation and verification were performed correctly. The Mutillidae II web application was configured by fixing the database connection issue, which allowed it to run without errors. Overall, the project provided practical knowledge of Linux administration, virtual machine usage, and basic web application security concepts in a controlled lab environment.