

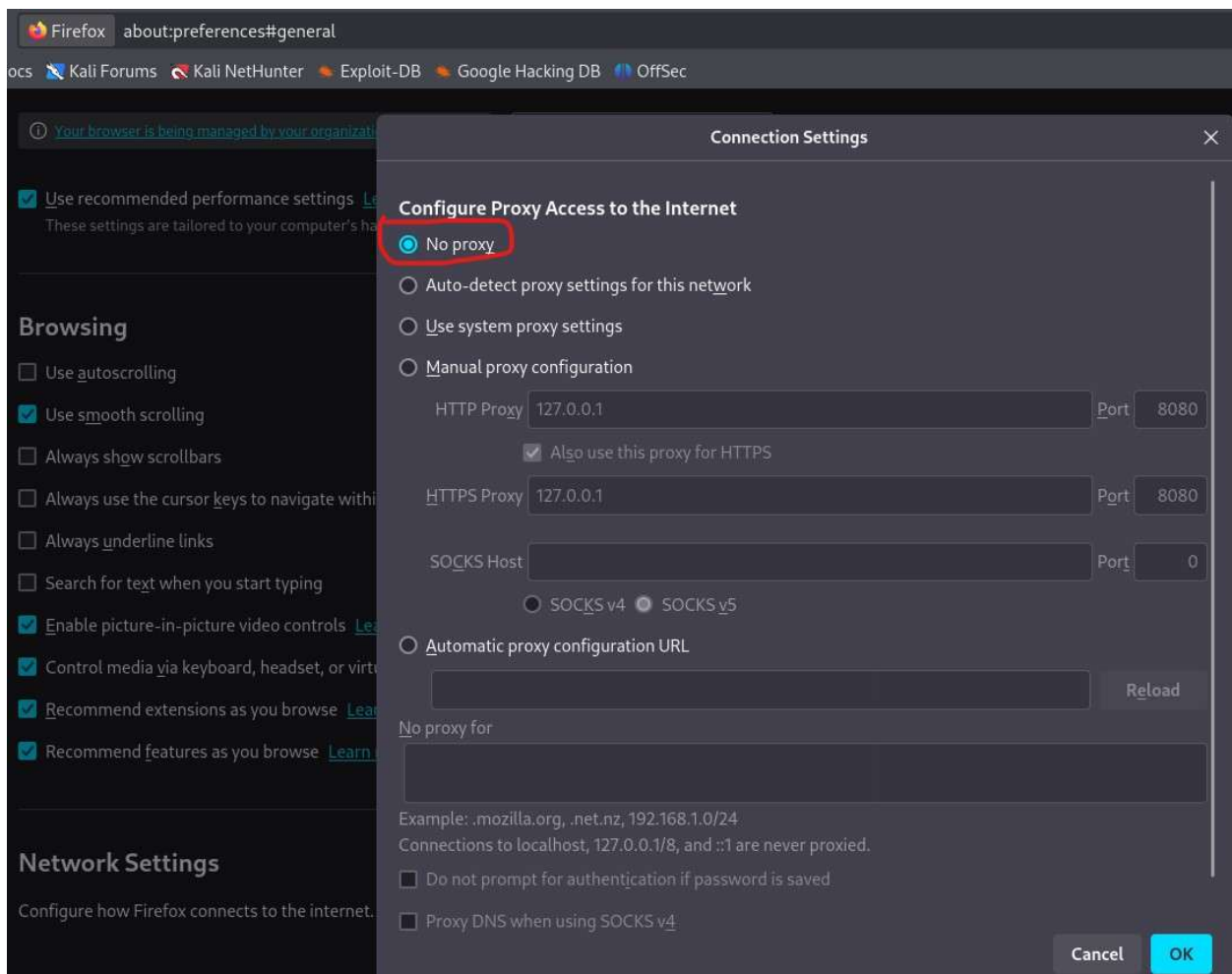
6CYSE 450: Ethical Hacking and Penetration Testing

Lab 6: DVWA vs Multillidae

Total Points: 30

Tasks:

- 1) Login to Kali Linux and Metasploitable 2. Use *msfadmin* as both username and password to login to the Metasploitable 2 VM.
- 2) Get the IP address of Metasploitable 2 using the *ifconfig* command and ping it from the Kali VM. If Kali VM cannot ping the Metasploitable 2 VM, check the network adapter setting for both machines and set “**Bridged Adapter**” as the adapter option.
- 3) In your Kali VM, make sure that there is no proxy set up for the Firefox.



- 4) Enter the following URL in your Firefox browser (in your Kali VM):
https://<Metasploitable 2 IP>/dvwa/login.php



Note that *10.254.218.172* is the IP address of my Metasploitable 2 VM.

- 5) Login to DVWA using the following credentials:

Username: admin

Password: password

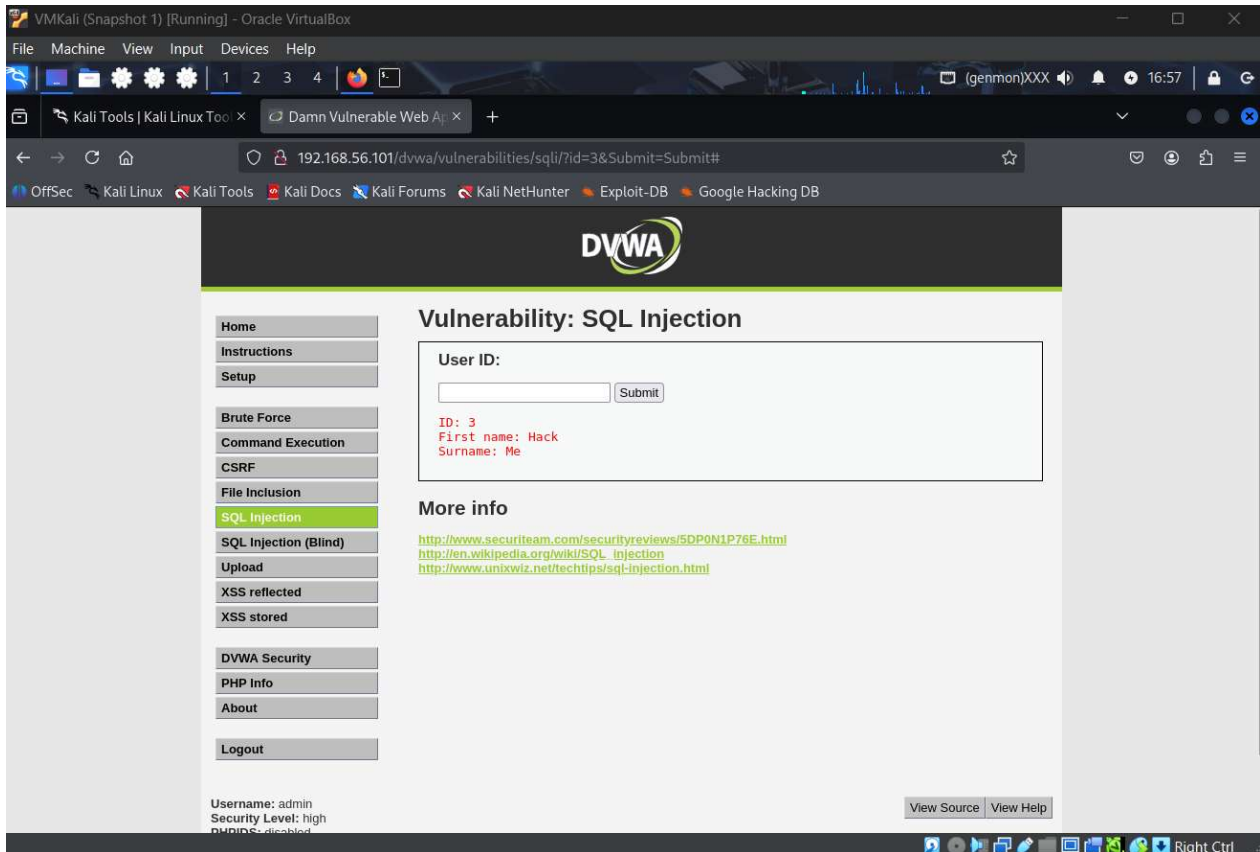


Username

Password

Login

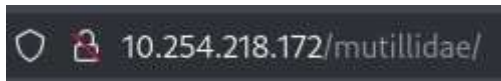
- 6) Select **SQL Injection** from the menu and enter **any value other than 2** as the User ID. Submit the user id and take a screenshot like the attached one showing the result. Briefly explain how SQL Injection can be implemented to get the same result. Give the relevant SQL query you need to use. **10 points**



An SQL query could be used to give the same result by essentially making the server execute the code that the user puts into a text box because the code is not properly sanitized. An SQL query to find this would be `3' OR '3'='3'#`

7) In Firefox, go the following URL:

`http://<Metasploitable 2 IP>/multillidae/`



You will get a page like this. Click multiple times on the buttons **“Toggle Security”** and **“Toggle Hints”**. Briefly explain what happens when you change these settings. Take relevant screenshots to attach to your submission. **4 points**



When you click the Toggle security button, the hints disappear and the level of security at the top changes. When you click the hints button when you are on security level 0, the level of hints

change from level 0-2

VMKali (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

192.168.50.132/mutillidae/ x multillidae hacking websi x Settings

192.168.50.132/mutillidae/index.php?page=home.php

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Enabled (2 - Noob) 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

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

back|track

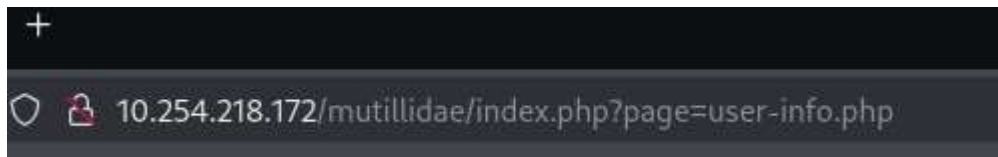
Samurai Web Testing Framework

BUILT ON PHP

Toad

RAVENS FOR CHARITY

8) Navigate: OWASP Top 10 → A1 - Injection → SQLi - Extract Data → User Info.





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](#)

View your details

**Please enter username and password
to view account details**

Name

Password

Dont have an account? [Please register here](#)

Enter **“admin”** as Name and **“cyse-450”** as Password. Click on the button **“View Account Details”**.

- 9) Similar to the following screenshot, show the SQL query that has been executed. **Note that you used the password “cyse-450”, not “password”**. If you get an error message like the message shown in the screenshot, explain the reason behind this error. If there is no error message, take screenshots of the resultant output. **6 points**

I got an error message like the screenshot. This is because the account I am inputting does not exist


```
VMKali (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
(genmon)XXX 18:22
kali@vbox: ~
Session Actions Edit View Help
[18:07:34] [INFO] testing 'Oracle stacked queries (USER_LOCK,SLEEP)''
[18:07:34] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)''
[18:07:37] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (SLEEP)''
[18:07:40] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (SLEEP - comment)''
[18:07:42] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP - comment)''
[18:07:44] [INFO] testing 'MySQL > 5.0.12 RLIKE time-based blind''
[18:07:47] [INFO] testing 'MySQL > 5.0.12 RLIKE time-based blind (comment)''
[18:07:49] [INFO] testing 'MySQL > 5.0.12 RLIKE time-based blind (query SLEEP)''
[18:07:52] [INFO] testing 'MySQL > 5.0.12 RLIKE time-based blind (query SLEEP - comment)''
[18:07:54] [INFO] testing 'MySQL AND time-based blind (ELT)''
[18:07:57] [INFO] testing 'MySQL AND time-based blind (ELT - comment)''
[18:07:59] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind''
[18:08:02] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind (comment)''
[18:08:04] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)''
[18:08:07] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)''
[18:08:09] [INFO] testing 'Oracle AND time-based blind''
[18:08:12] [INFO] testing 'Oracle AND time-based blind (comment)''
[18:08:14] [INFO] testing 'ClickHouse AND time-based blind (heavy query)''
[18:08:16] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace''
[18:08:16] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)''
[18:08:16] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)''
[18:08:16] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)''
[18:08:16] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)''
[18:08:16] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace''
[18:08:16] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK,SLEEP)''
[18:08:16] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)''
[18:08:17] [INFO] testing 'MySQL > 5.0.12 time-based blind - ORDER BY, GROUP BY clause''
[18:08:17] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause''
[18:08:17] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK,SLEEP)''
[18:08:17] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)''
[18:08:17] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns''
[18:08:22] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns''
[18:08:27] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns''
[18:08:31] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns''
[18:08:36] [WARNING] parameter 'Host' does not seem to be injectable
[18:08:36] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 18:08:36 /2025-11-25/
kali@vbox:~$
kali@vbox:~$
```

11) Explore different features of the **Multillidae** application and provide a brief comparison with the DVWA application. Make sure you discuss the features of both applications in

your comparative discussion.

6 points

The screenshot shows a web browser window with the URL `192.168.50.132/mutillidae/index.php?page=user-info.php&username=admin&password=cyse-450&user-info-php-submit-button=View+Account+Details#&username=adr`. The page title is "Mutillidae: Born to be Hacked". The interface includes a navigation menu with "Home", "Login/Register", "Toggle Hints", "Toggle Security", "Reset DB", "View Log", and "View". A "Core Controls" dropdown menu is open, listing OWASP Top 10 categories (A1-A10) and other security-related items. The main content area has a "View your details" section with a form for "Please enter username and password to view account details". Below the form is an error message: "Error: Failure is always an option and this situation". The error details are as follows:

Error: Failure is always an option and this situation	
Line	126
Code	0
File	:/var/www/mutillidae/user-info.php
Message	Error executing query: Table 'metasploit.accounts'
Trace	:#0 /var/www/mutillidae/index.php(469): include()



DVWA and mutillitude both have plenty of tools for testing different kinds of attacks as shown by the highlighted tools above, but they both have mostly different tools. For example, DVWA and Mutillitude both have XSS and SQL Injection, but DVWA does not have things like CSRF, or insecure cryptographic storage.