Diane Gilzow

April 29, 2026

CYSE 450: Ethical Hacking and Penetration Testing

Dr. Md Morshed Alam

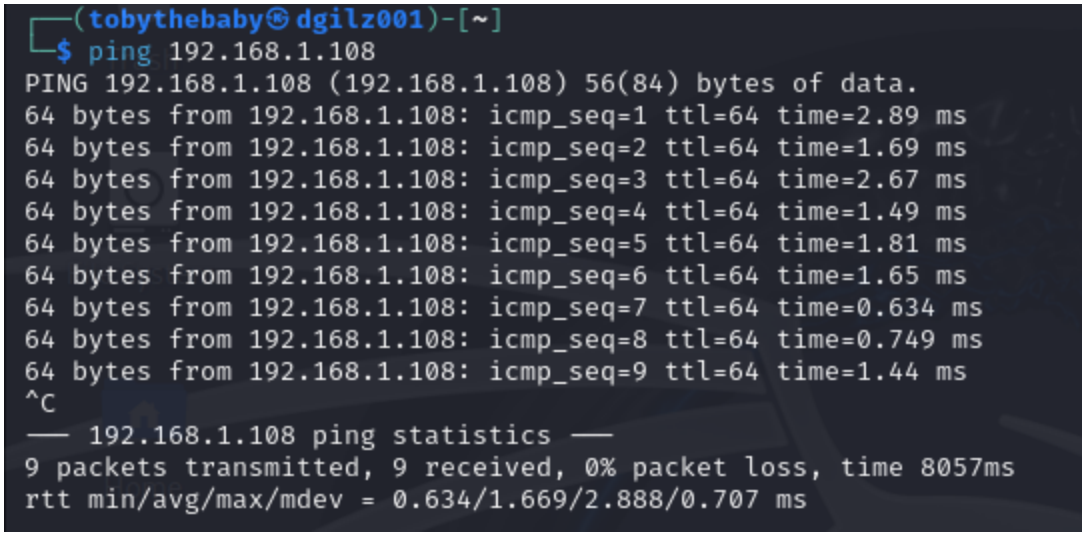
Lab 7: DVWA vs Mutillidae

1) Login to Kali Linux and Metasploitable 2. Use ***msfadmin*** as both username and password to login to the Metasploitable 2 VM.

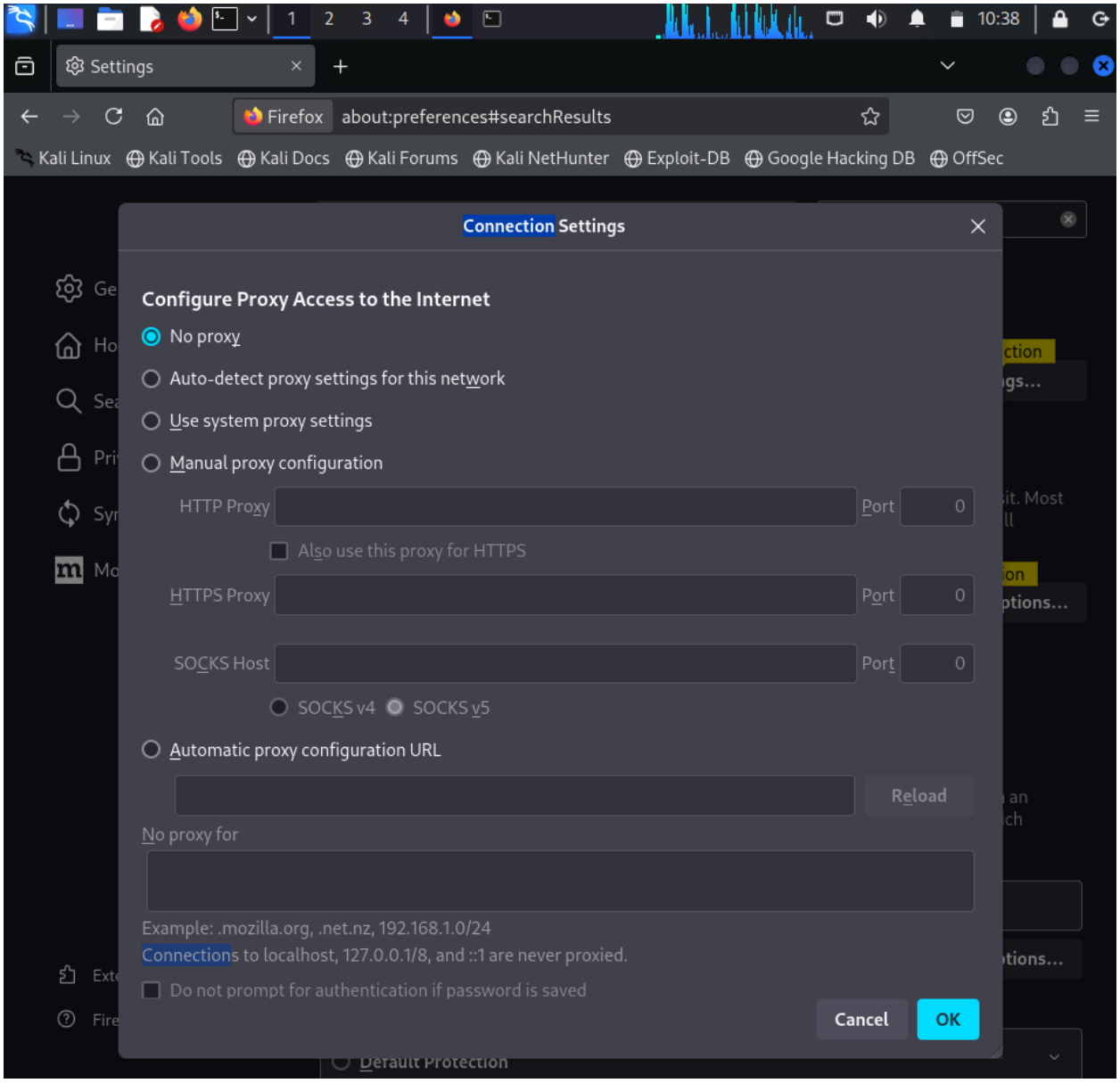
```
metasploitable login: msfadmin
Password:
Last login: Wed Jan 28 13:23:10 EST 2026 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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:~$
```

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.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d8:36:bf
          inet addr:192.168.1.108  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed8:36bf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:88 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:18497 (18.0 KB)  TX bytes:8380 (8.1 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)
```

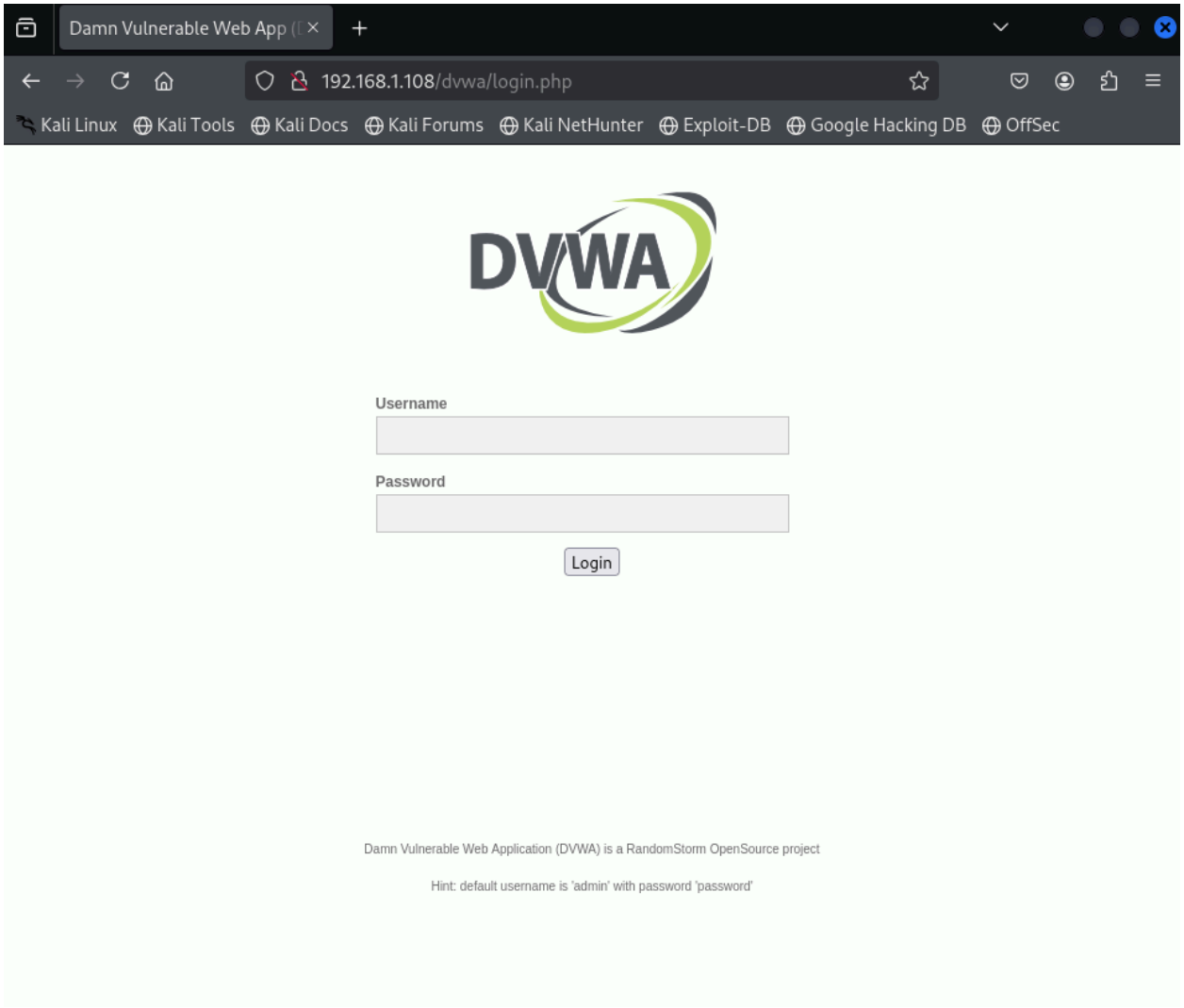


3) In your Kali VM, make sure that there is no proxy set up for the Firefox.



4) [In Kali] Enter the following URL in your Firefox browser:

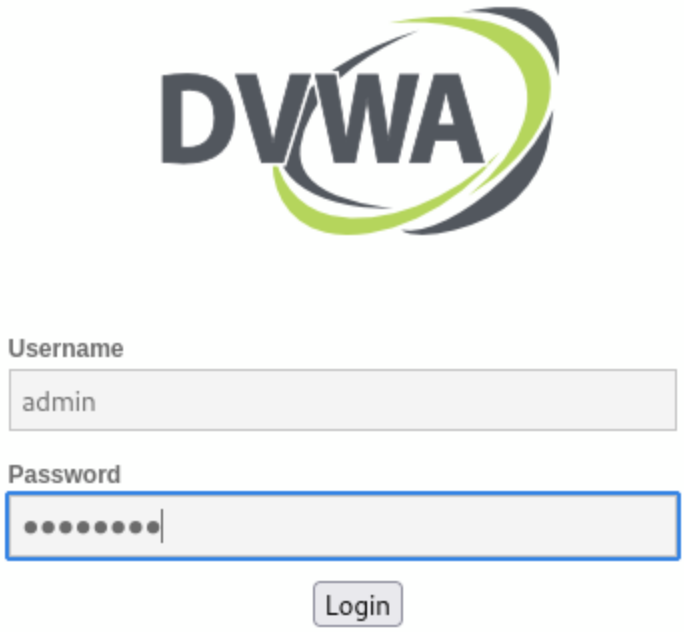
http://<IP of your Metasploitable 2 VM>/dvwa/login.php



5) Login to DVWA using the following credentials:

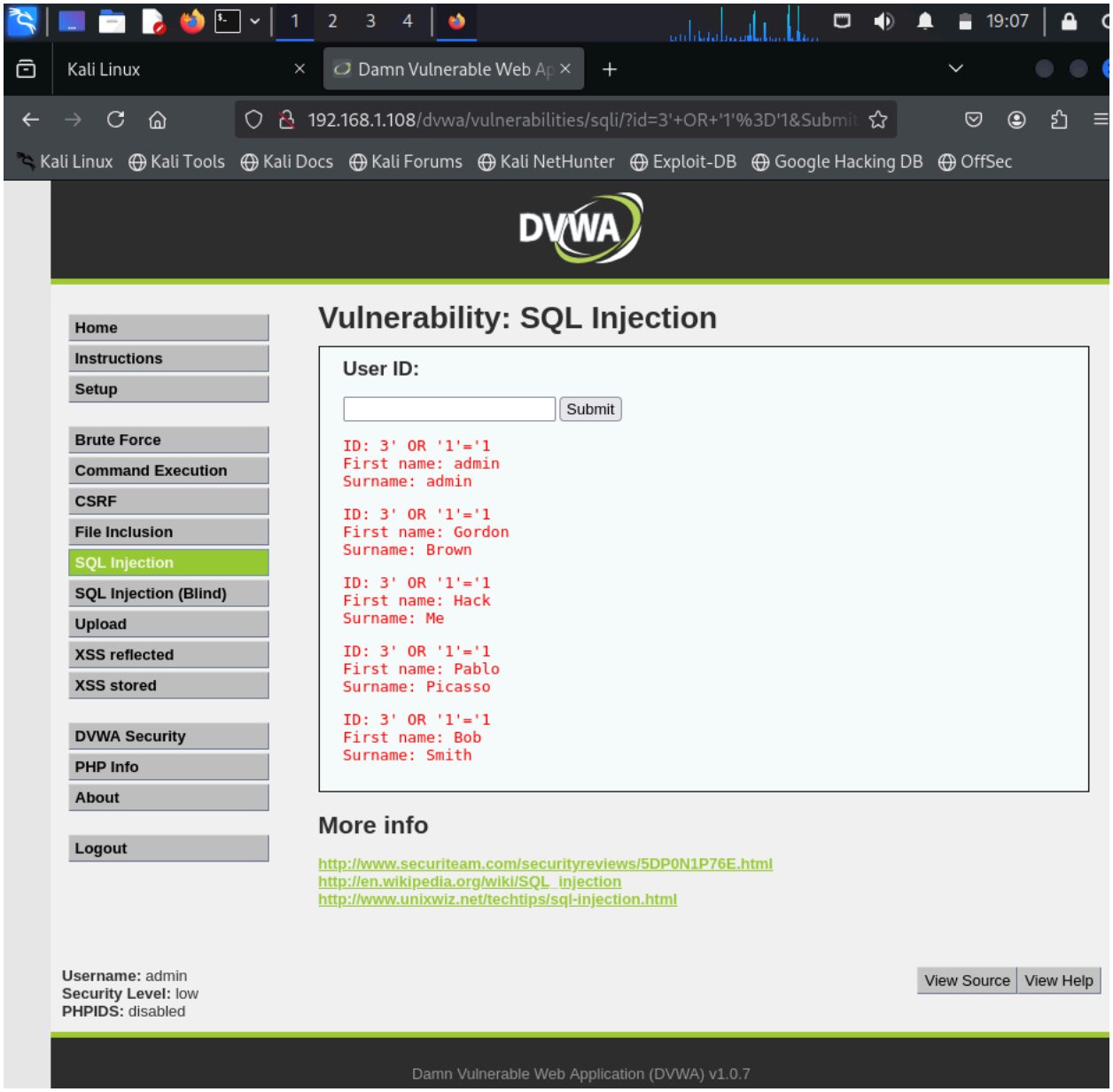
Username: admin

Password: password



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 showing the result.

7) Implement an SQL Injection attack to retrieve information for all users. Take screenshots showing the SQL query used as an input and the corresponding results.



8) Explain the SQL Injection attack performed in **step #7.**

I used 3’ OR ‘1’=’1 as input to launch the SQL injection attack. What this input does is breaks out of the original SQL query condition and injects a logical statement that is always true. This results in all of the user records being returned instead of only the intended user with ID 3.

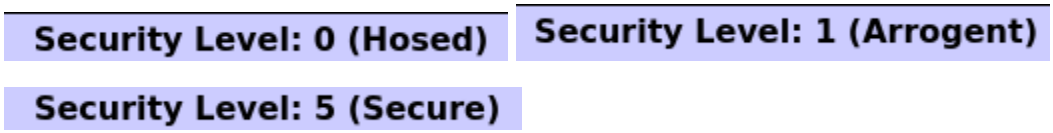
9) [In Kali] In Firefox, go to the following URL:

http://< IP of your Metasploitable 2 VM >/mutillidae/

You will get a page like the following. Explore the buttons **“Toggle Security”** and **“Toggle**

Hints”. Briefly explain what happens when you change these settings. Take relevant screenshots to attach to your submission.

When I press the **“Toggle Security”** button, it would change the security level from Security Level: 0 (Hosed), Security Level: 1 (Arrogant), and Security Level: 5 (Secure)



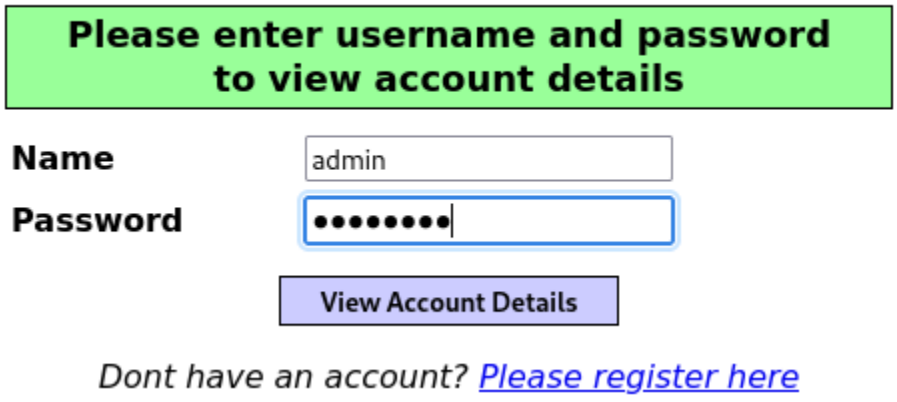
As for when I press the **“Toggle Hints”** button, it would either enable or disable hints. There’s two levels for enabled hints, one being 5cr1pt K1dd1e and the other being Noob.

Hints: Disabled (0 - I try harder)

Hints: Enabled (1 - 5cr1pt K1dd1e) Hints: Enabled (2 - Noob)

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

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



11) 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.

Please enter username and password to view account details

Name

Password

View Account Details

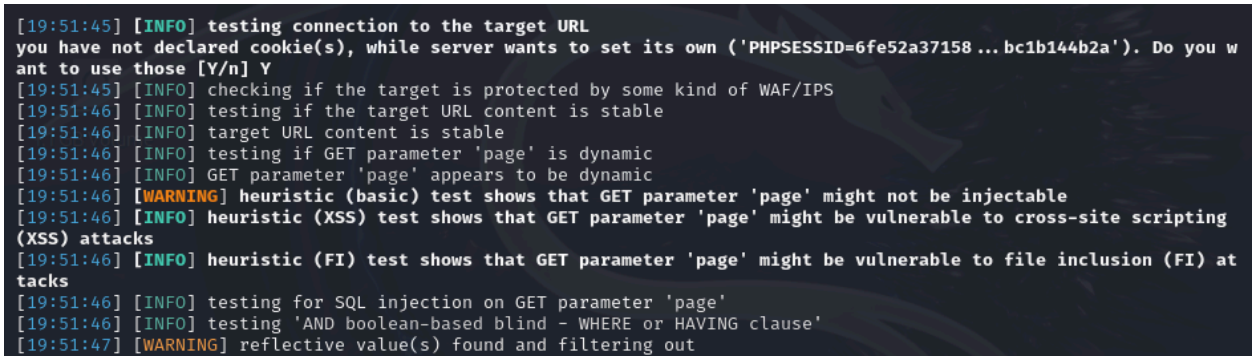
Dont have an account? Please register here

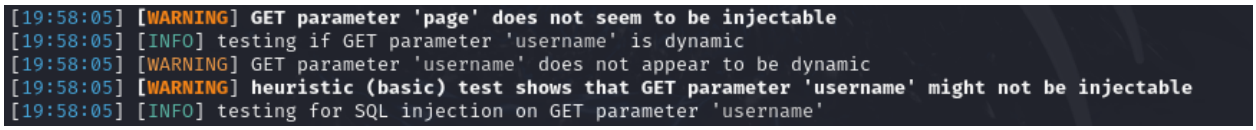
Error: Failure is always an option and this situation proves it	
Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: Table 'metasploit.accounts' doesn't exist
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='admin' AND password='cyse-450'
Did you setup/reset the DB?	

The reason behind this error is that the 'metasploit.accounts' table either doesn't exist or couldn't be found. The database has either not been properly initialized or that the required schema has not been created.

12) [In Kali] Run the ***sqlmap*** command shown in the following screenshot. **Make sure the IP address 10.254.218.172 is replaced with the IP address of your Metasploitable 2 VM.** Interact with ***sqlmap*** and perform attack discovery. Take a screenshot showing the execution of the command.

13) When ***sqlmap*** performs attack discovery, it will attempt to identify possible injection points and relevant payloads. Take necessary screenshots showing the injections points and payloads found by ***sqlmap.***





14) Explore different features of the ***Mutillidae*** application and provide a brief comparison with the DVWA application. Make sure you discuss the features of both applications in your comparative discussion.

Mutillidae provides a hint toggle button whereas one isn't present in DVWA. Additionally, it seems like DVWA has a focus primarily on web-based vulnerabilities, like SQL injection and XSS. Mutillidae on the other hand includes a wider range of vulnerabilities along with built-in guidance features. Besides that, both of these applications share similarities in having adjustable security difficulty levels, being written in PHP, and being an intentionally vulnerable environment for practice.