K. J. Somaiya College of Engineering, Mumbai
(A Constituent College of Somaiya Vidyavihar University)

Information Security

IA-2

By-

Paras Jain - 16010121071

Aditya Mishra - 16010121111

Knowledge Alone Liberates
ज्ञानादेव तु केवलम्
Somaiya Vidyavihar
SOMAIYA
VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering

Somaiya
TRUST

K. J. Somaiya College of Engineering, Mumbai
(A Constituent College of Somaiya Vidyavihar University)

Title: Implementation of SQL Map using DVWA through Metasploitable 2

SOMAIYA VIDYAVIHAR UNIVERSITY
K J Somaiya College of Engineering
Somaiya TRUST

Contents:

1. **Introduction**
2. **Sql Map**
3. **DVWA**
4. **Metasploitable 2**
5. **Stepwise demonstration of tool**

1. Introduction

- Kali Linux, a Debian-based Linux distribution, is tailored for conducting penetration testing and digital forensics, managed and maintained by Offensive Security.

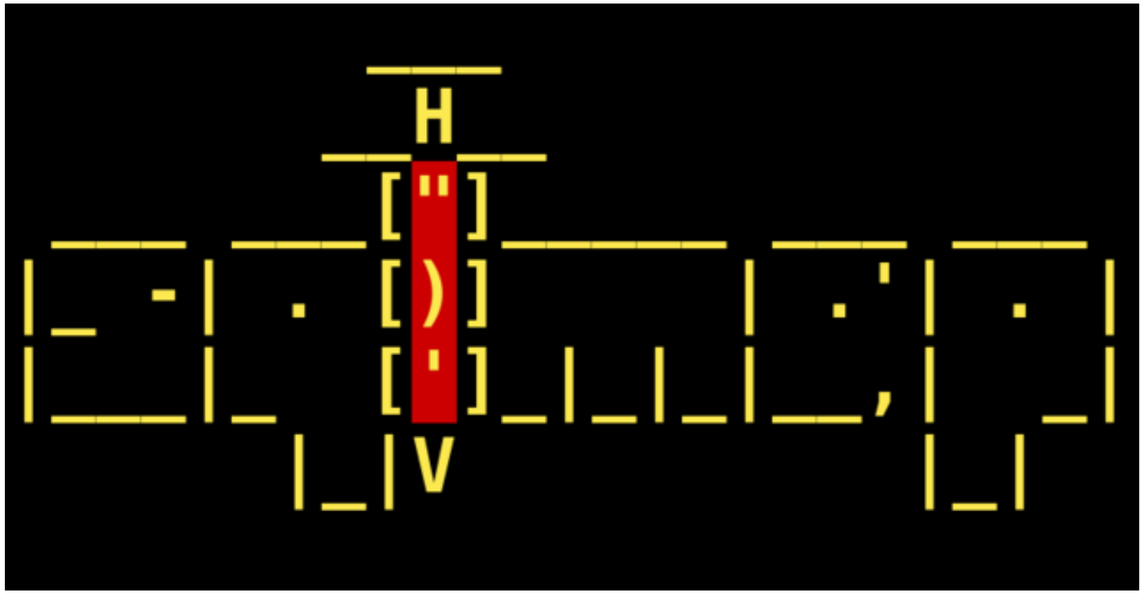
- Offering a suite of 600 penetration-testing tools, Kali Linux includes applications such as Armitage, Nmap, Wireshark, John the Ripper, sqlmap, Aircrack-ng, Burp, and OWASP ZAP.

- The brainchild of Offensive Security are Mati Aharoni and Devon Kearns, Kali Linux emerged from the redevelopment of BackTrack, a previously utilized Linux distribution for information security testing based on Knoppix. The choice of the name "Kali" drew inspiration from the Hindu goddess Kali.

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

2. SQL Map



SOMAIYA VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Somaiya TRUST

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Detecting and exploiting SQL injection vulnerabilities in online applications is streamlined through the utilization of the open-source penetration testing tool SQLmap. Besides managing the tool's operations, it facilitates data retrieval from databases and execution of commands on the underlying system.

SOMAIYA VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Somaiya TRUST

However, it's imperative to employ SQLmap in a controlled environment and with explicit permission from the application's owner. Unauthorized usage of SQLmap on a live website is strictly prohibited and may lead to legal consequences.

3. DVWA

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

Detecting and exploiting SQL injection vulnerabilities in online applications is streamlined through the utilization of the open-source penetration testing tool SQLmap. Besides managing the tool's operations, it facilitates data retrieval from databases and execution of commands on the underlying system.

However, it's imperative to employ SQLmap in a controlled environment and with explicit permission from the application's owner. Unauthorized usage of SQLmap on a live website is strictly prohibited and may lead to legal consequences.

4. Metasploitable 2

K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

```
 * 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:
```

SOMAIYA VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Somaiya TRUST

A testing environment provides a secure space for conducting security analysis and penetration testing. This controlled environment ensures that security professionals can experiment with various tools and techniques without compromising live systems or networks. To set up such an environment, you'll need a Metasploit instance capable of accessing a vulnerable target.

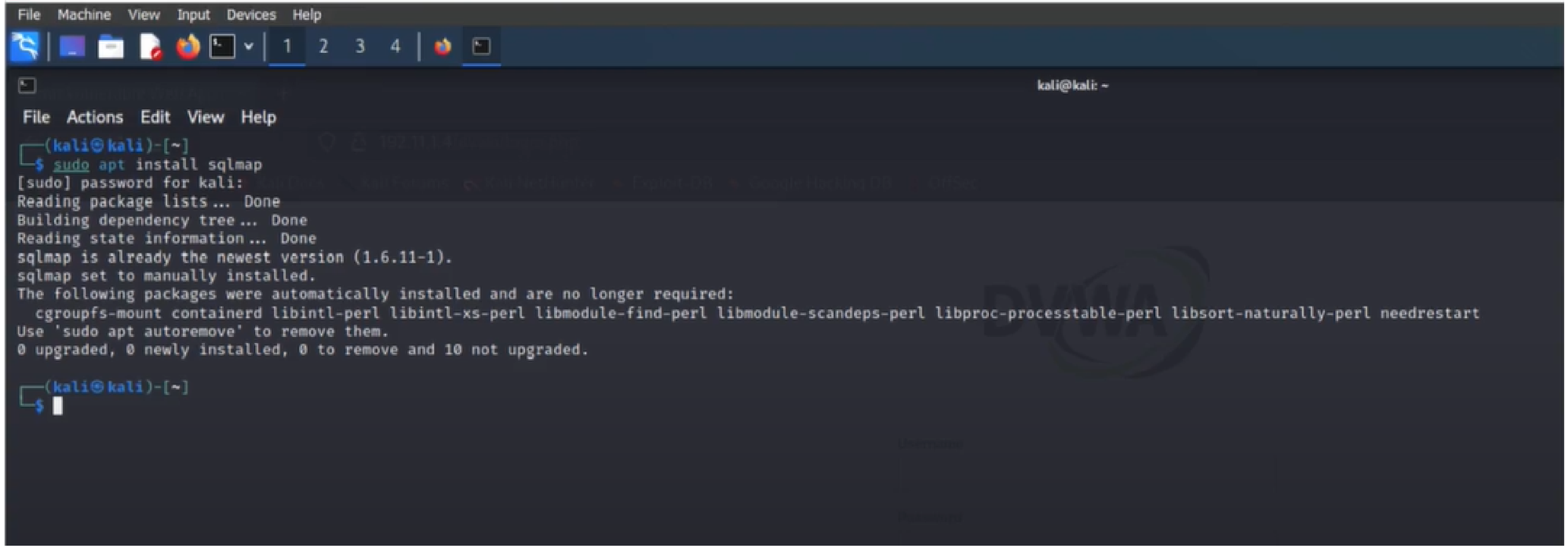
Metasploitable 2 is an intentionally vulnerable Ubuntu Linux virtual machine designed specifically for testing common vulnerabilities. It serves as an ideal target system, allowing security practitioners to simulate real-world attack scenarios and practice defensive strategies. Moreover, Metasploitable 2 is compatible with popular virtualization platforms like VirtualBox, VMware, and others, making it accessible and easy to integrate into diverse testing environments.

5. Step wise Demonstration

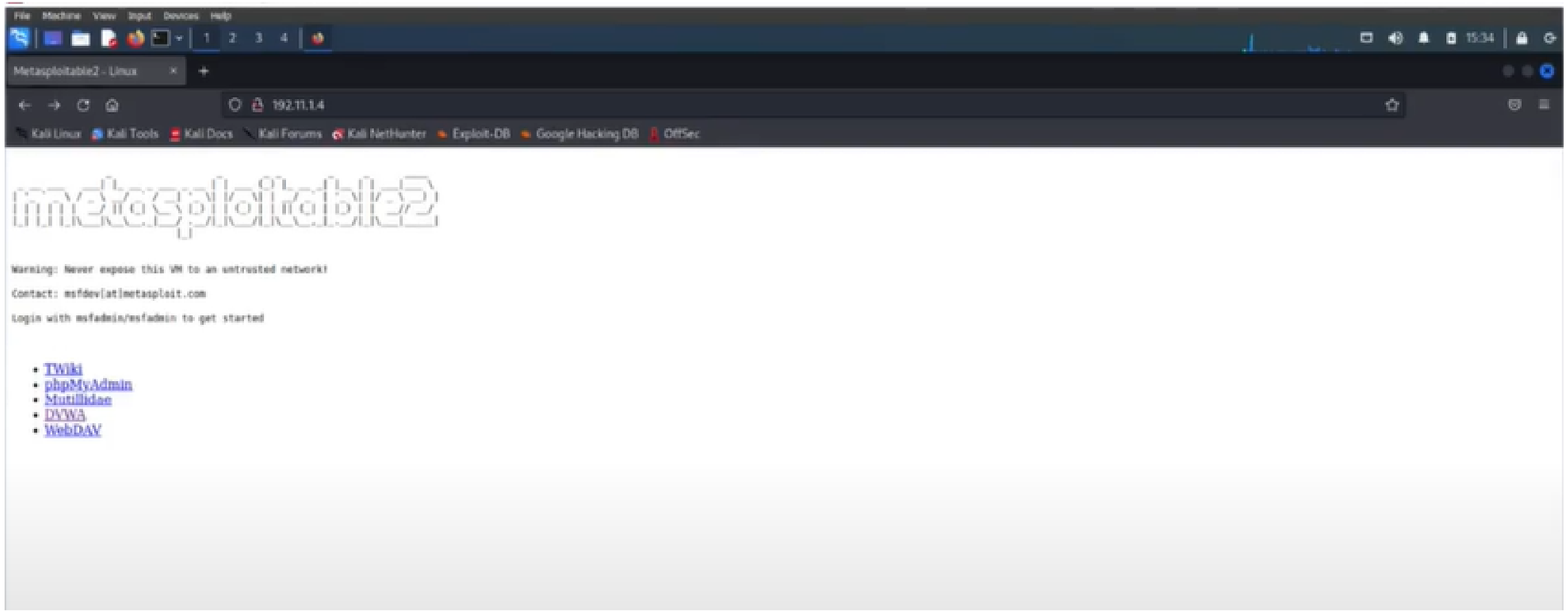
K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

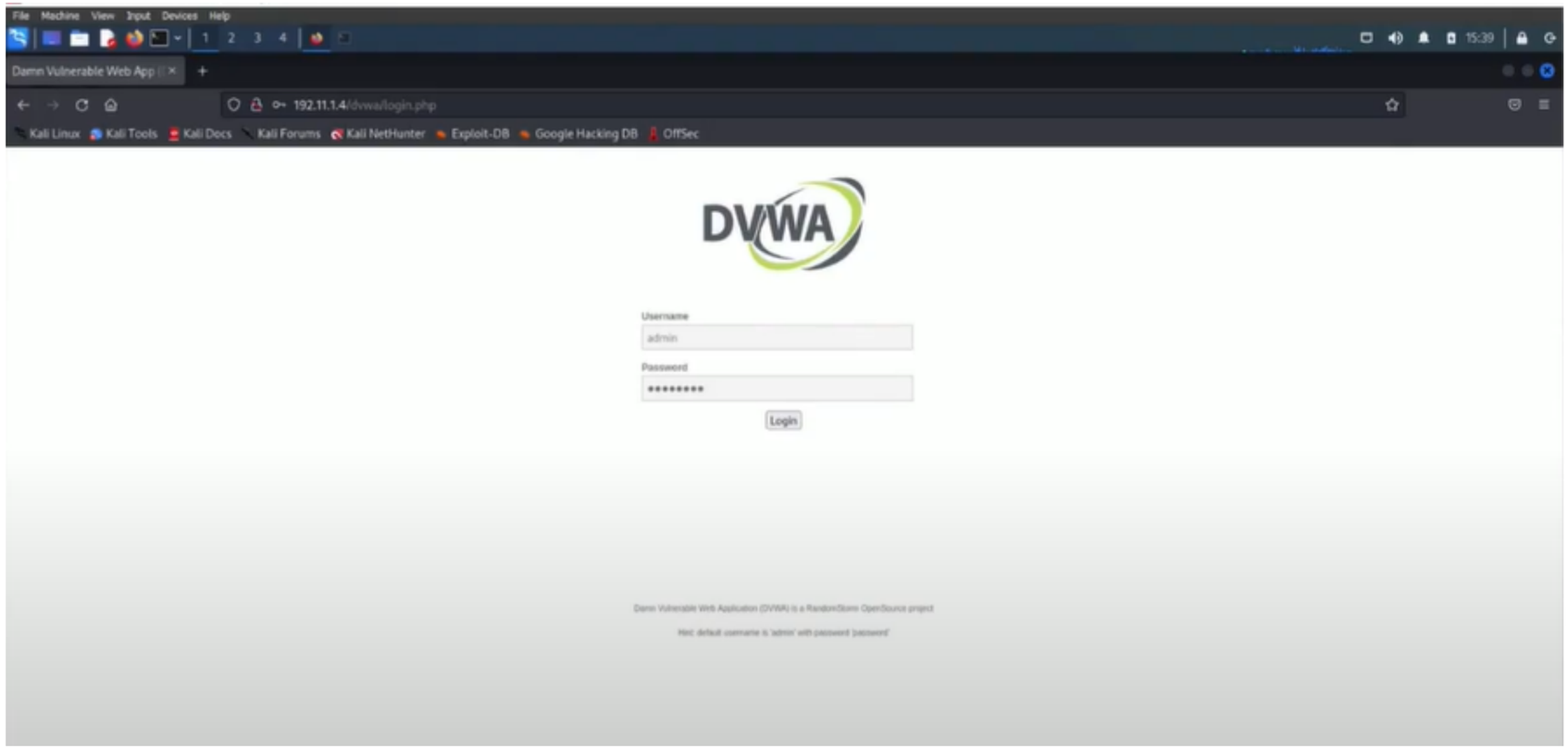
1. First we need to download SQL Map using the following command: sudo apt install sqlmap



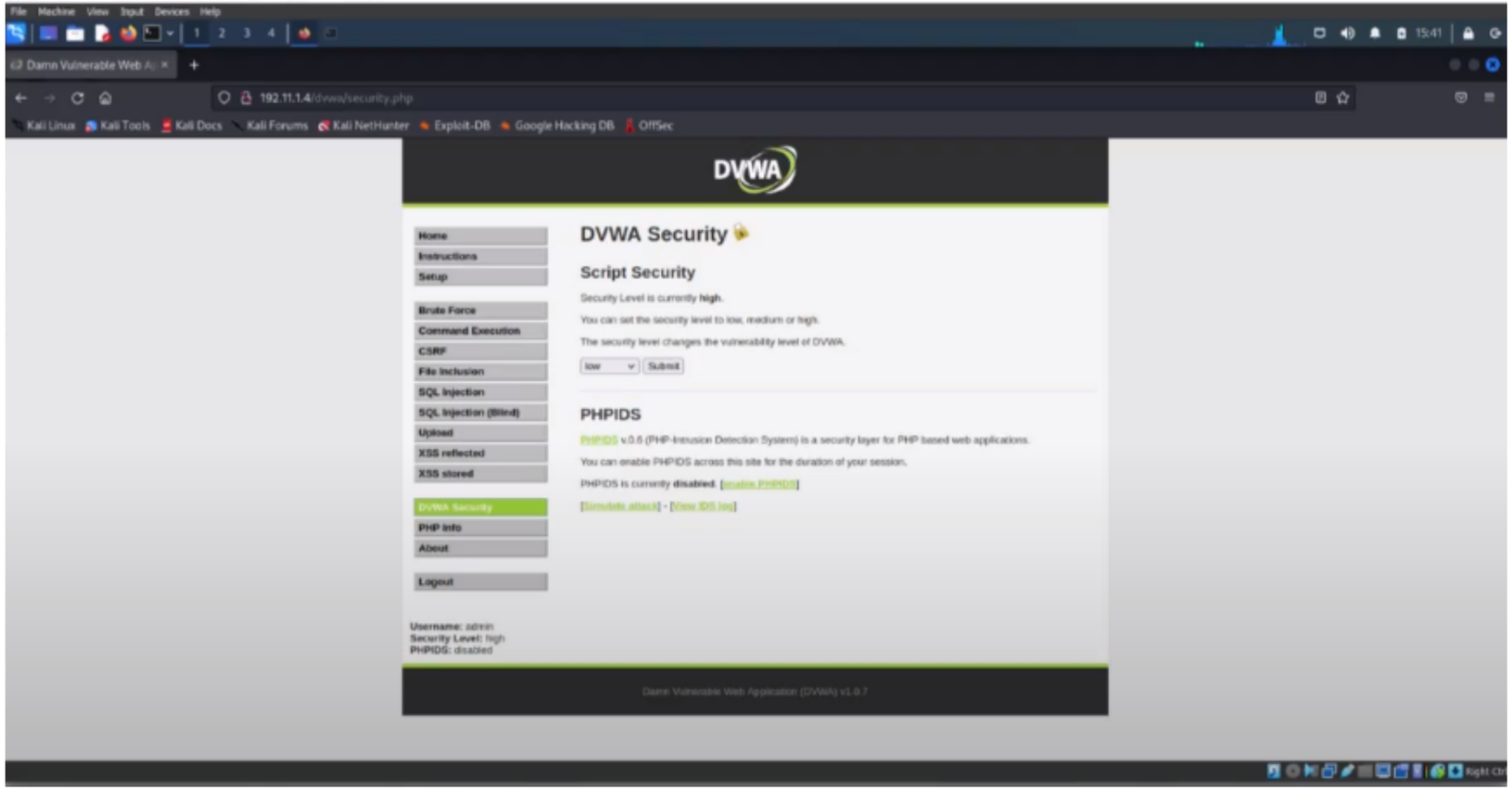
2. To setup DVWA for SQL Map we are using Metasploitable 2. Here is the demonstration for the same.



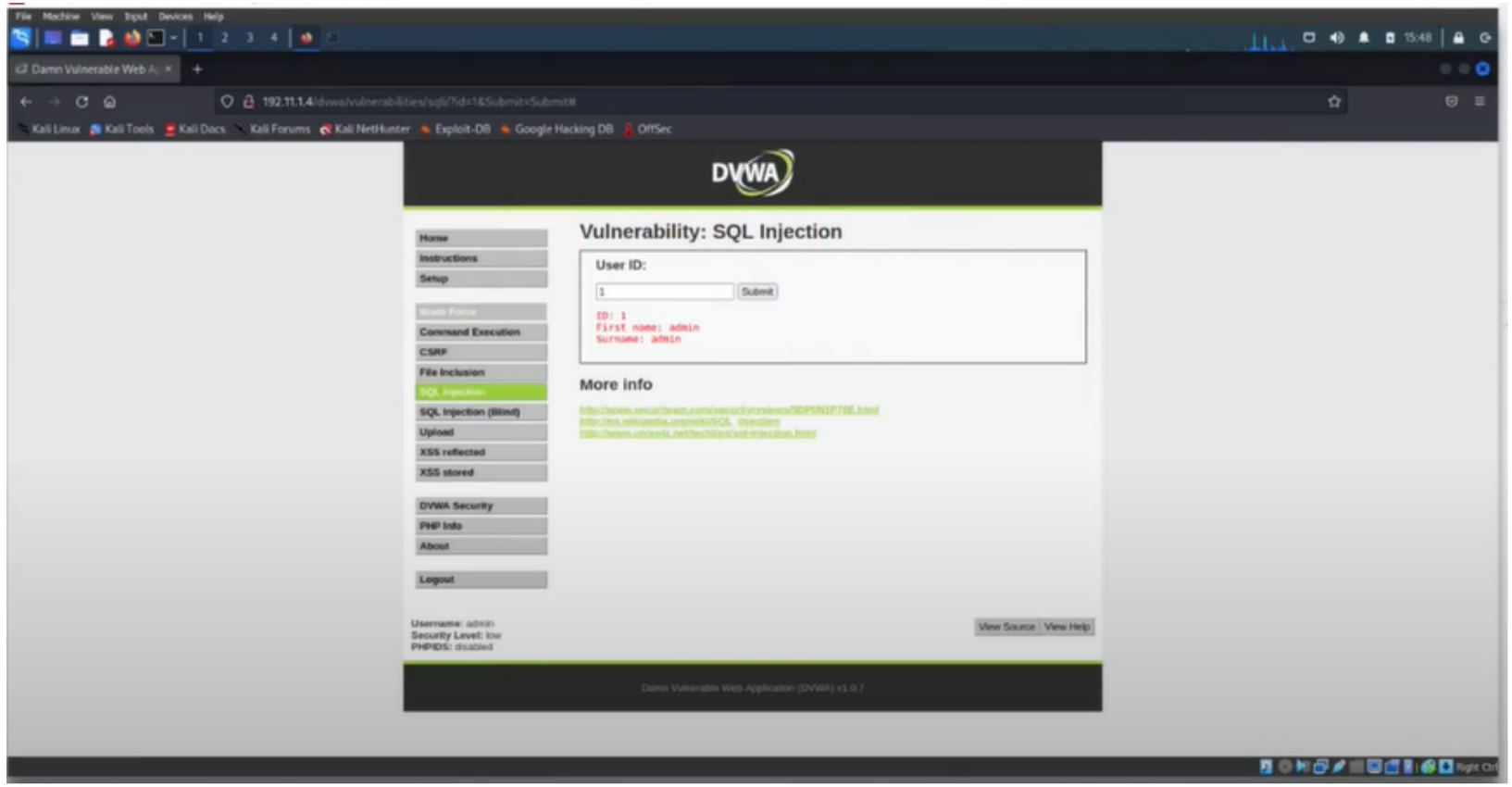
3. We get access to DVWA



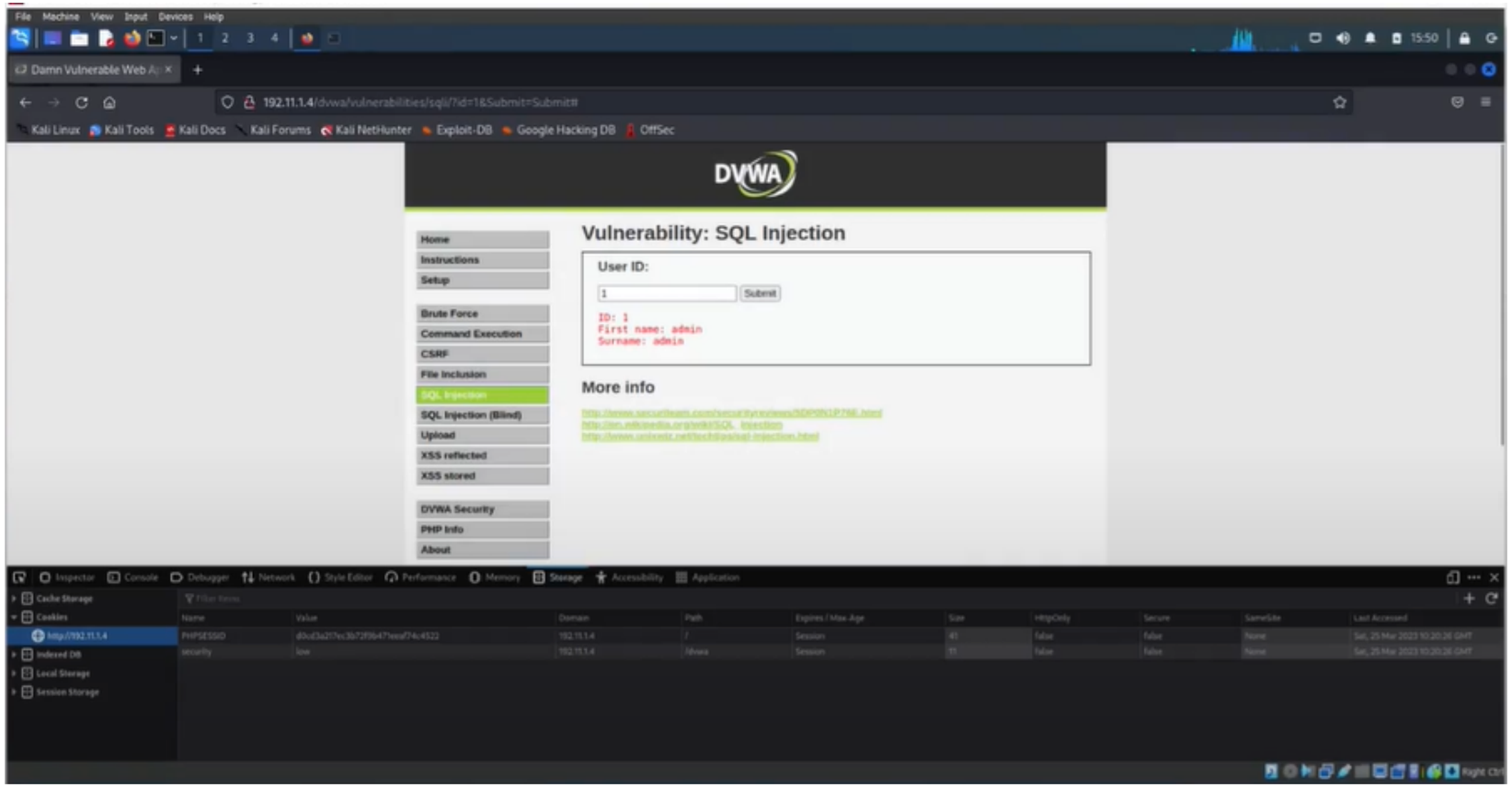
4. Setting the DVWA settings to low.



5. Then click on SQL injection and set the ID as 1.



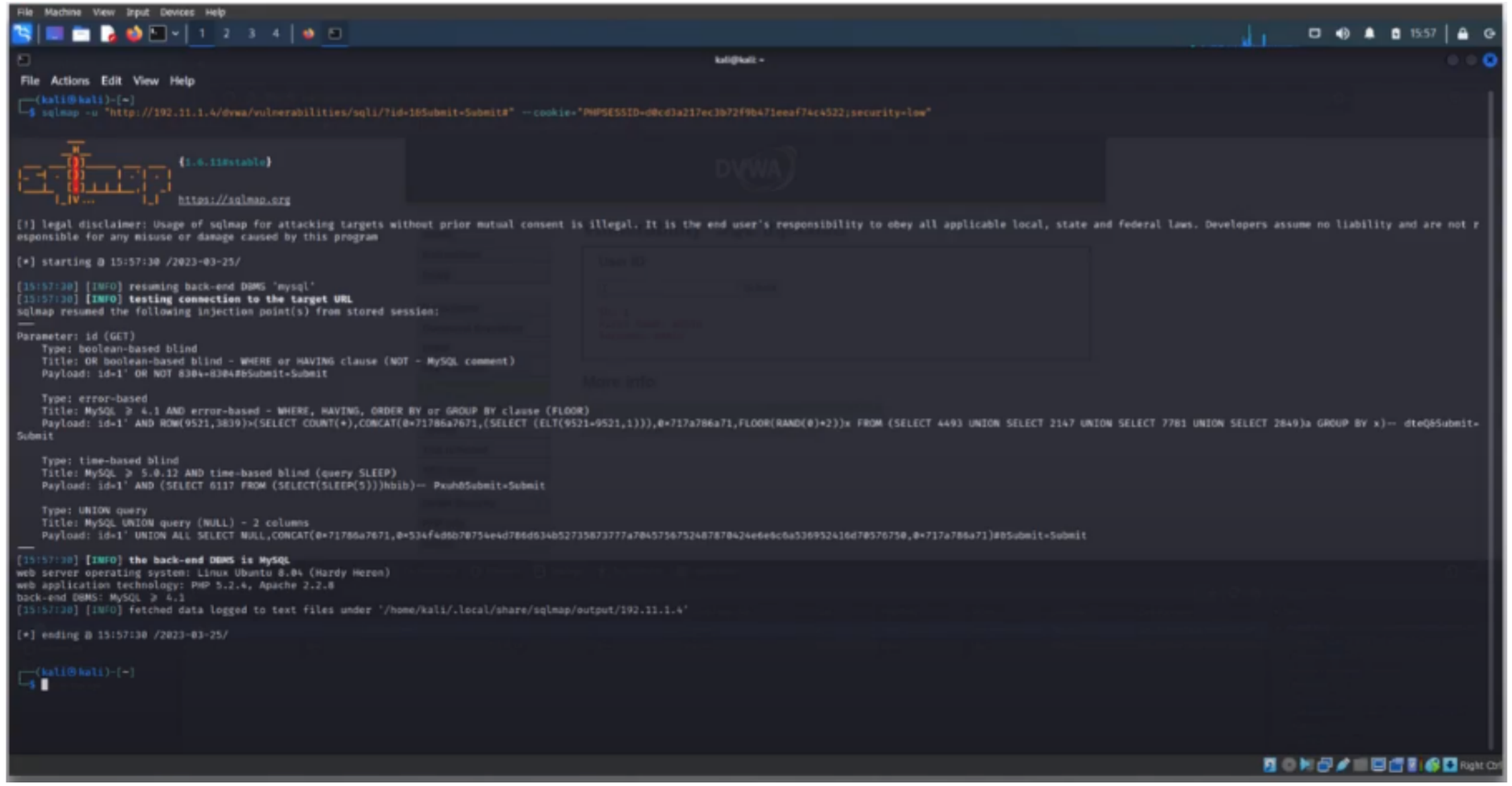
6. Click on inspect to view the php session ID.



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

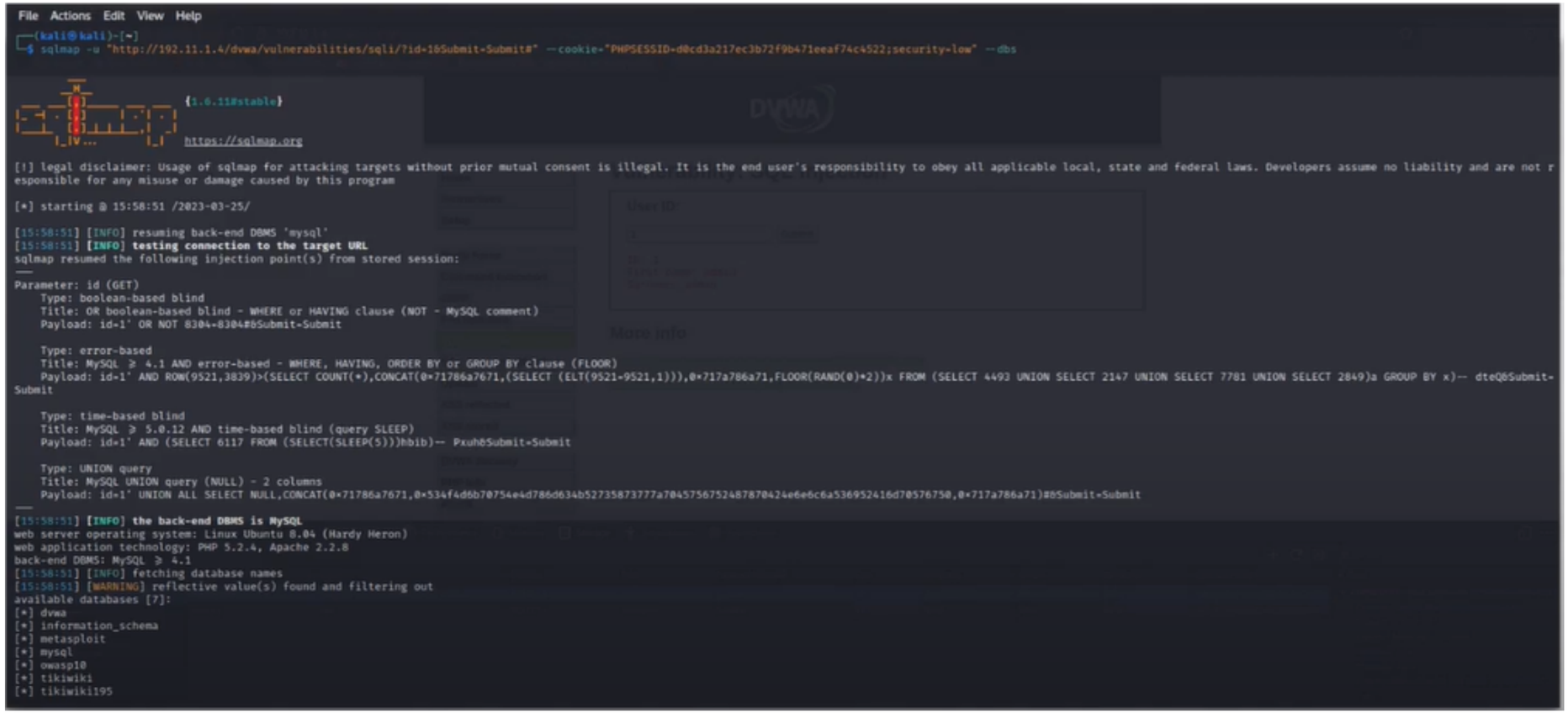
7. sqlmap -u “url” --cookie “php session id and security”



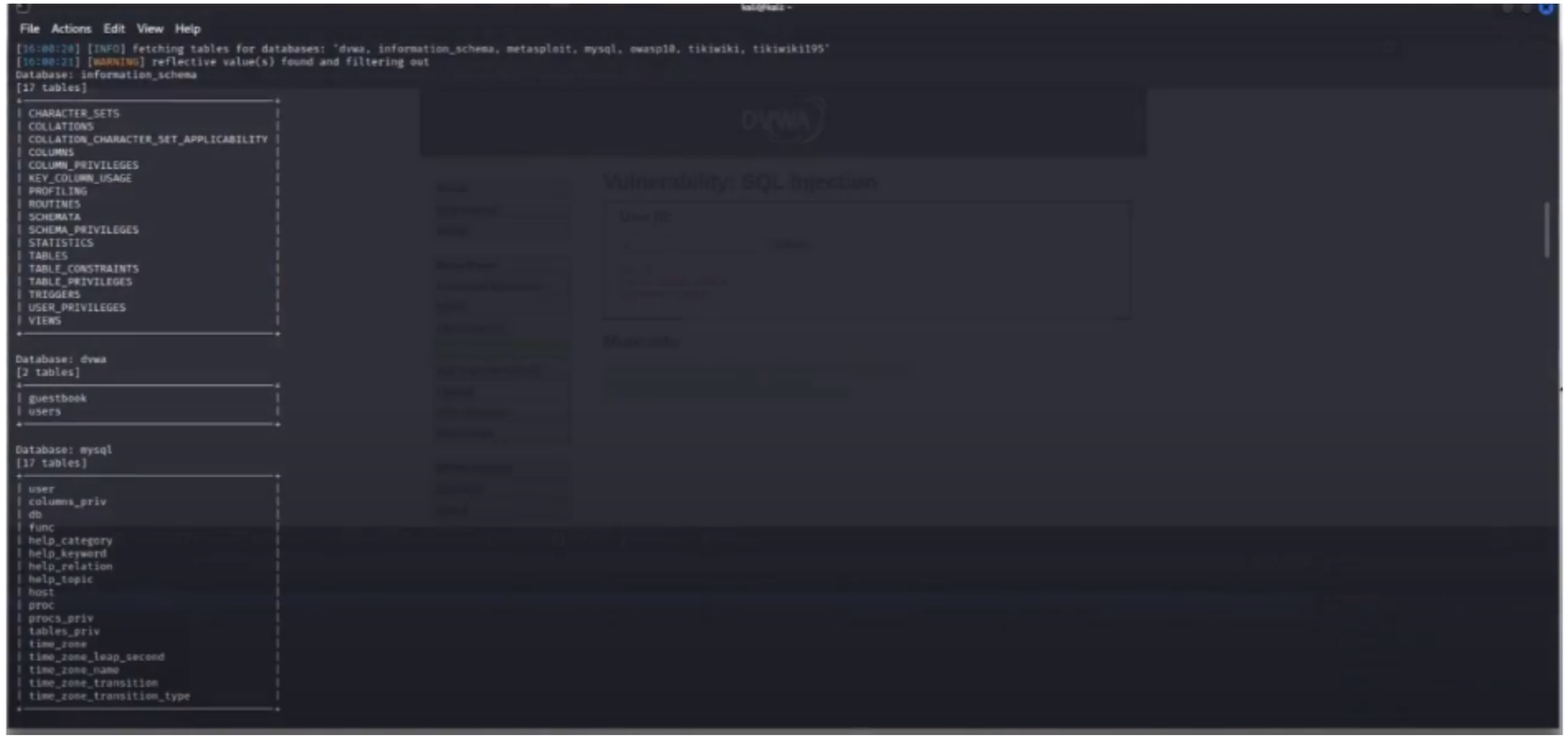
K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

8. sqlmap -u “url” --cookie “php session id and security” --dbs

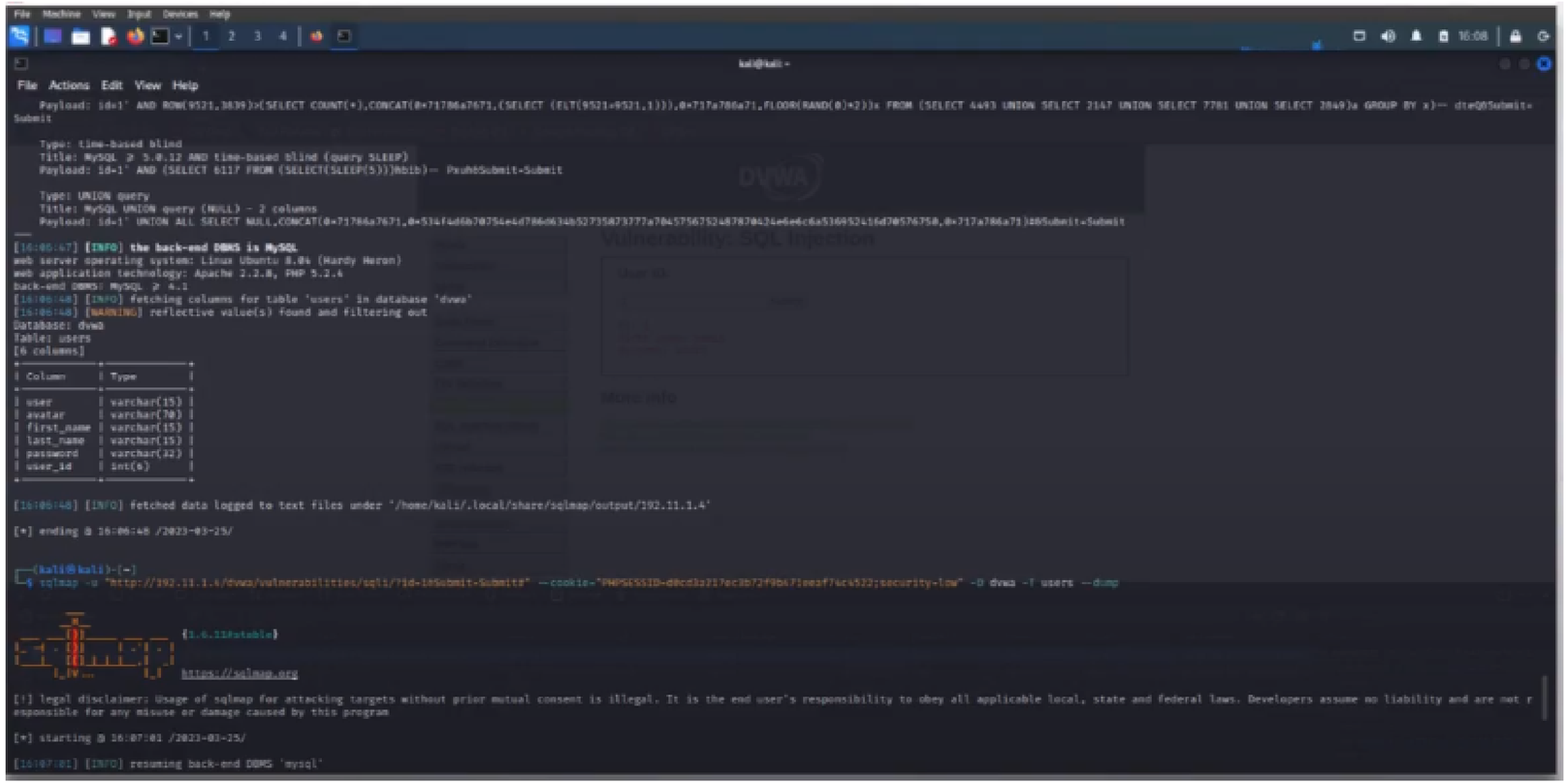


9. sqlmap -u “url” --cookie “php session id and security” --tables
it will display all the tables in the database.



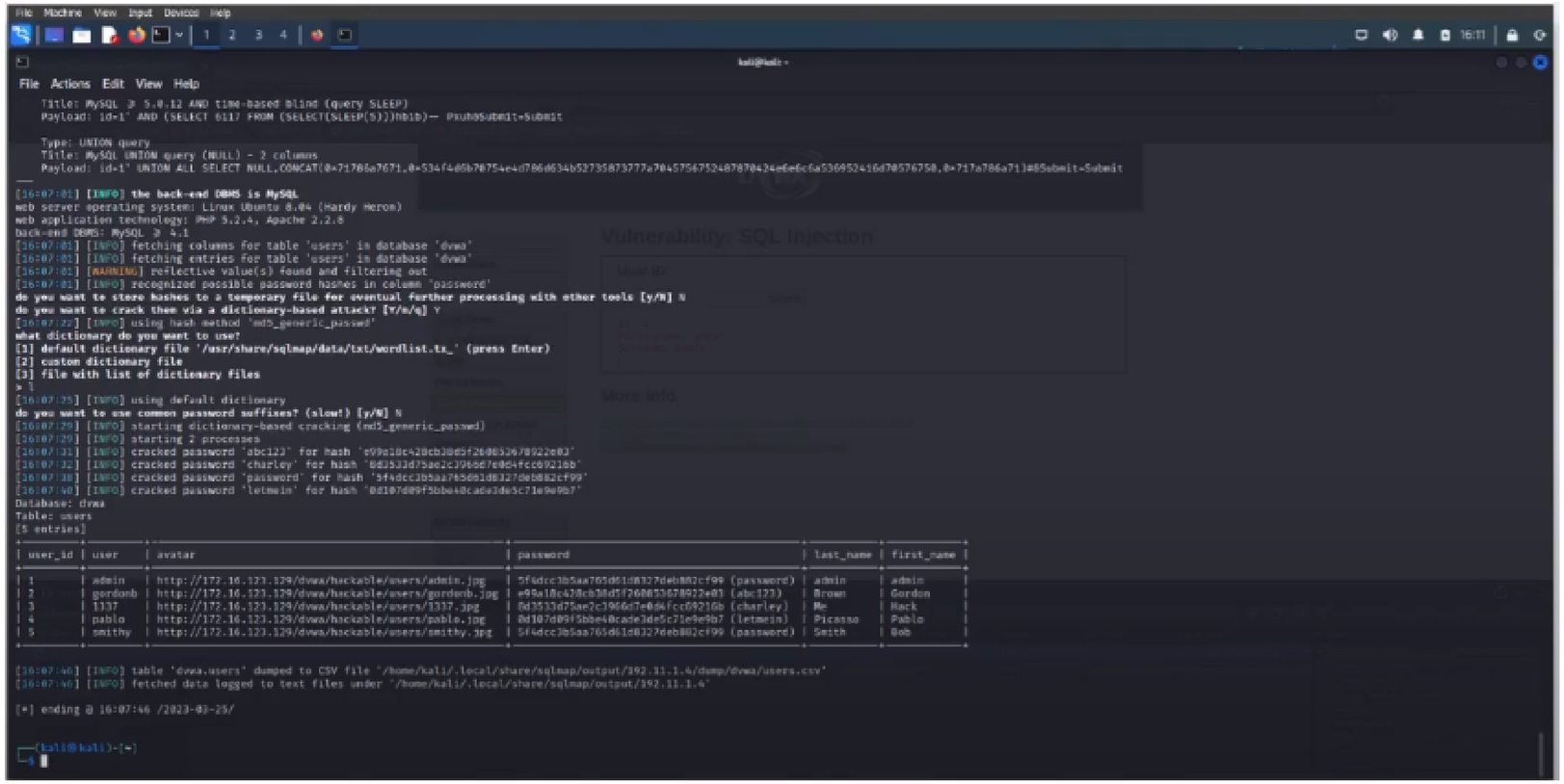
10. sqlmap -u “url” --cookie “php session id and security” --D DVWA _T users --columns

It will display all the coluns of the table user in the database.



11. sqlmap -u “url” --cookie “php session id and security” --D dvwa -T users --dump

It will display all the values of columns of the able user in a tex file locally.



K. J. Somaiya College of Engineering, Mumbai

(A Constituent College of Somaiya Vidyavihar University)

SOMAIYA VIDYAVIHAR UNIVERSITY

K J Somaiya College of Engineering

Somaiya TRUST