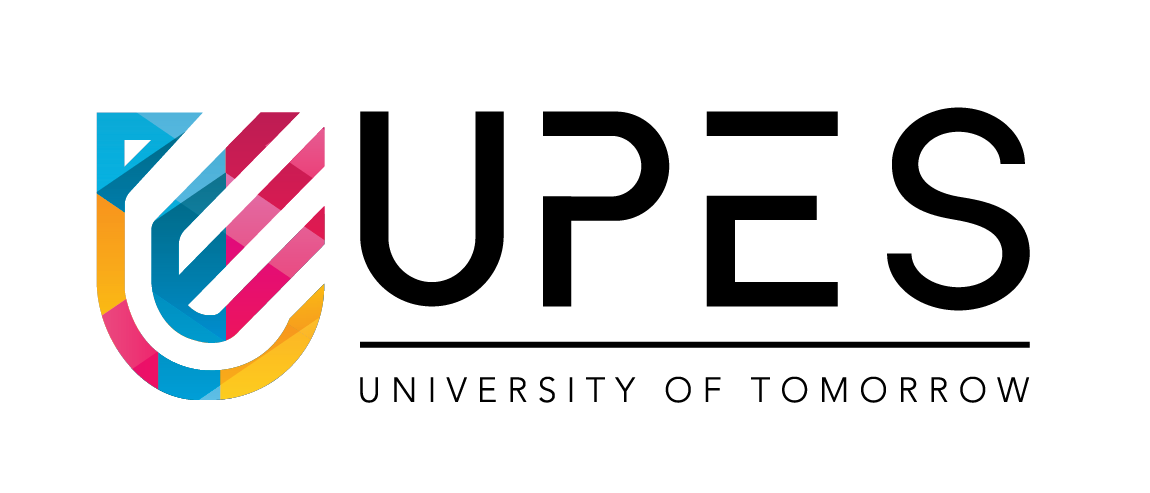
**SCHOOL OF COMPUTER SCIENCE**

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**DEHRADUN, UTTARAKHAND**



**IT DATA SECURITY LAB**

**LABORATORY FILE**

**(2024-2025)**

**For**

**Vth Semester**

**Submitted To: Submitted By:**

Prof. Abhishek Yadav Mr. Akshat Negi

Assistant Professor S.S. 500106533(SAP ID)

[Vth Semester] R2142220414(Roll No.)

School of Computer Sciences B.Tech. CSF (Batch-1)

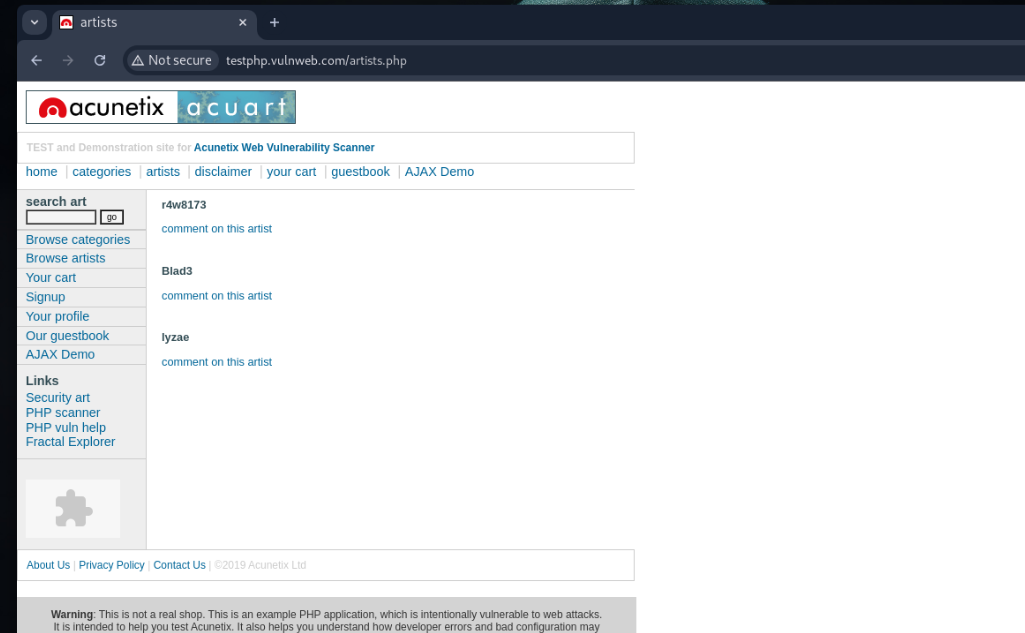
**LAB EXPERIMENT – 4**

**SQL MAP**

SQL map is a open vulnerable penetration test tool that automates the process of detecting and exploiting weaknesses in SQL injection(sqli) and taking over the server database SQL injection is a hacking technique where an attacker can insert SQL commands with a URL to be executed by the database located in the backend ,A database is a collection of information stored on a computer or a web server that is accessed by a front end client used for obtaining information from the database.

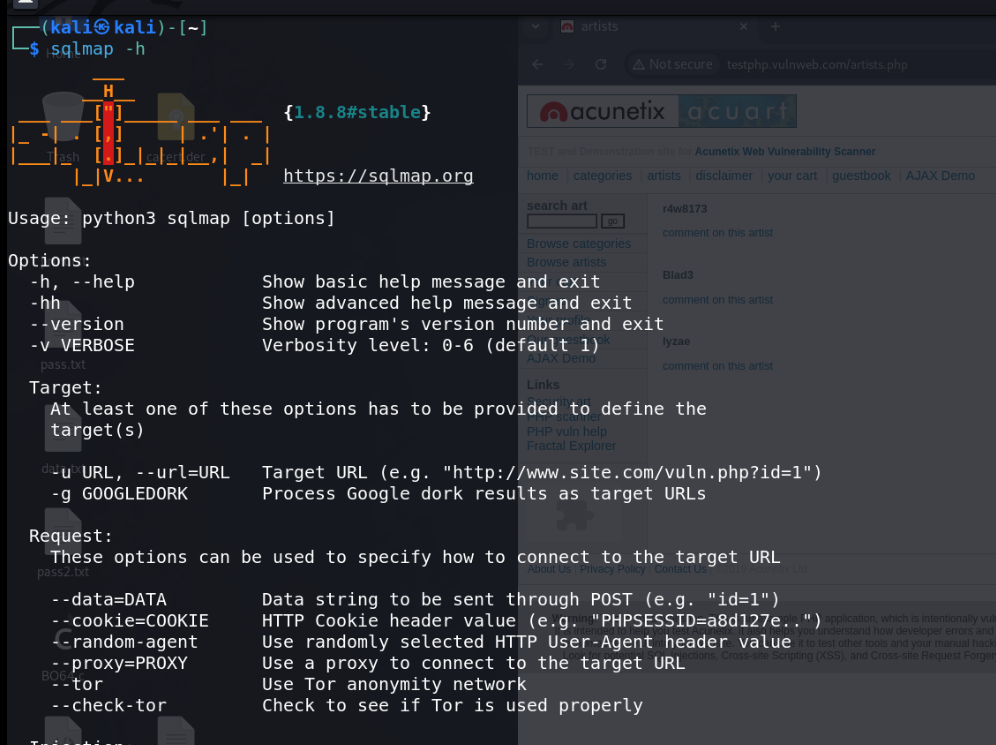
Use acunetix for web application vulnerability for SQL injection.

testphp.vulnweb.com/index.php

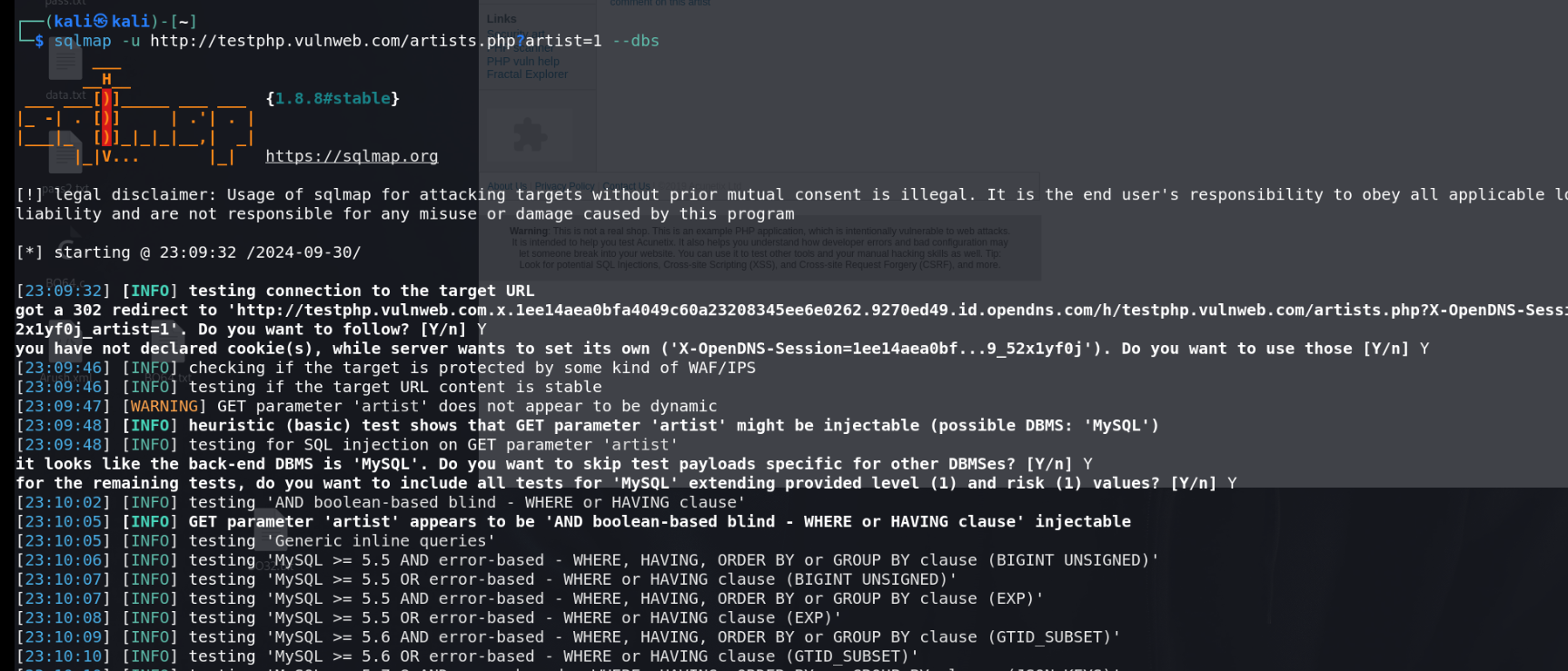


Type sqlmap -h, It will list all the available services.

Now you can see all the different switches that you can use with sqlmap and since we know that acunetix website is vulnerable to a sql injection we can now attempt to find the databases ,what is and how many sql type are running on the server.



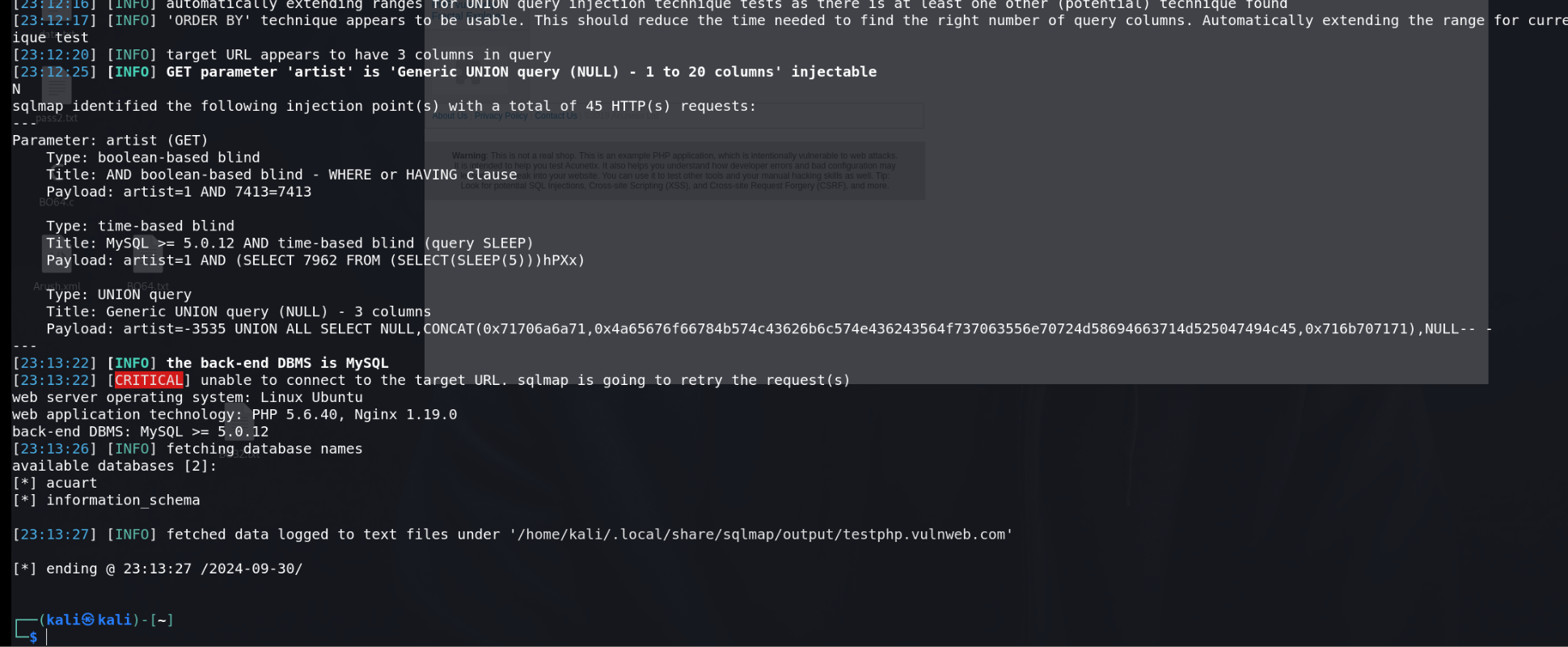
For accessing database type this command.



It will show 2 databases

1. acurat

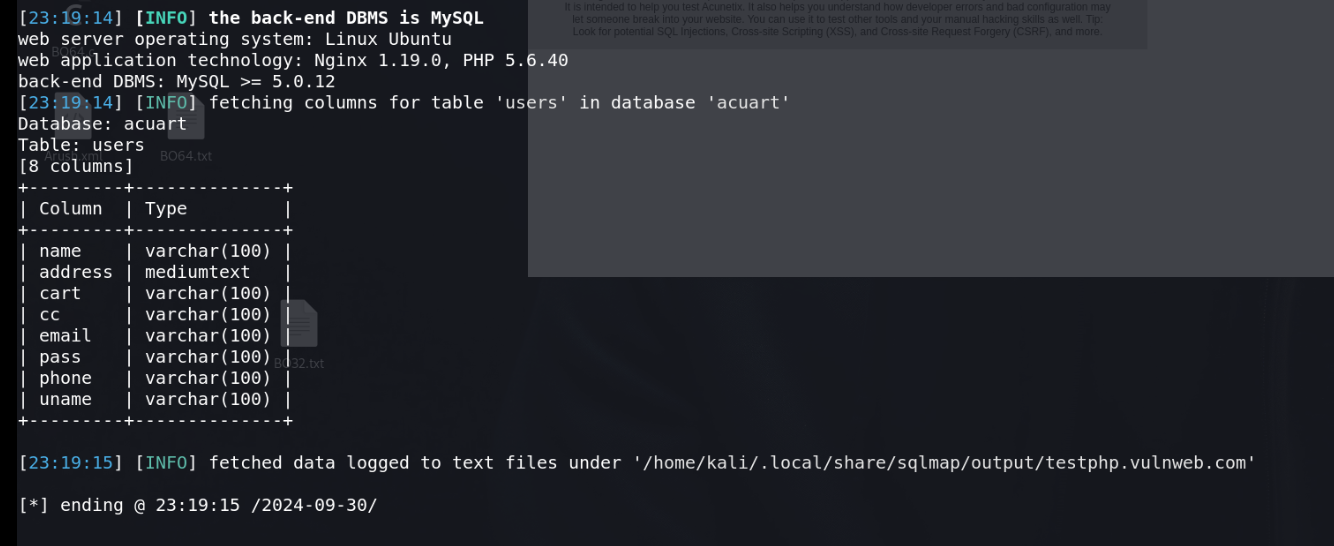
2. Information\_schema



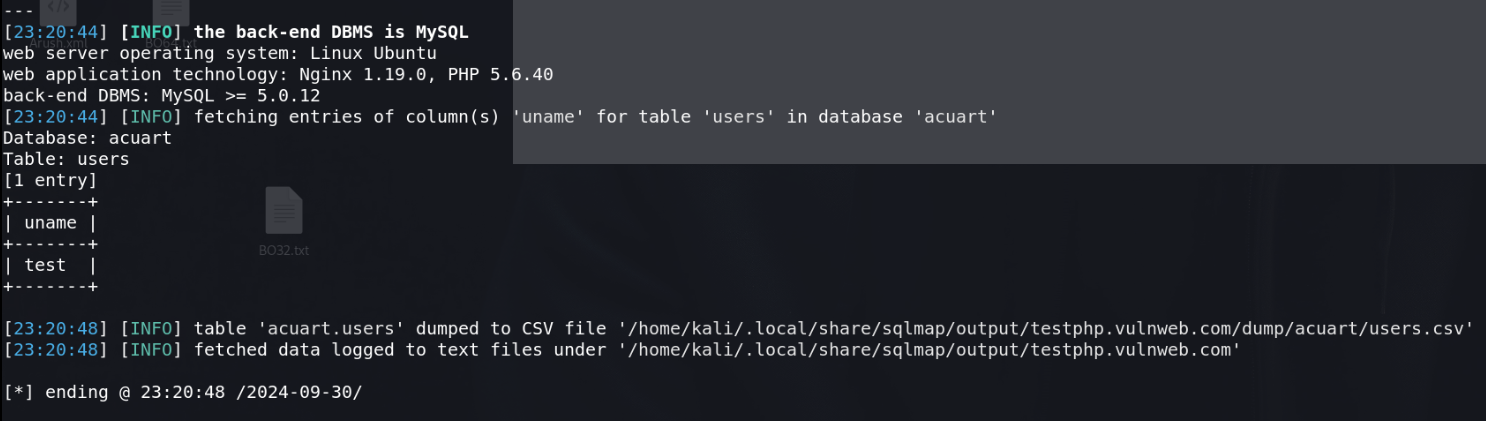
For accessing tables in database



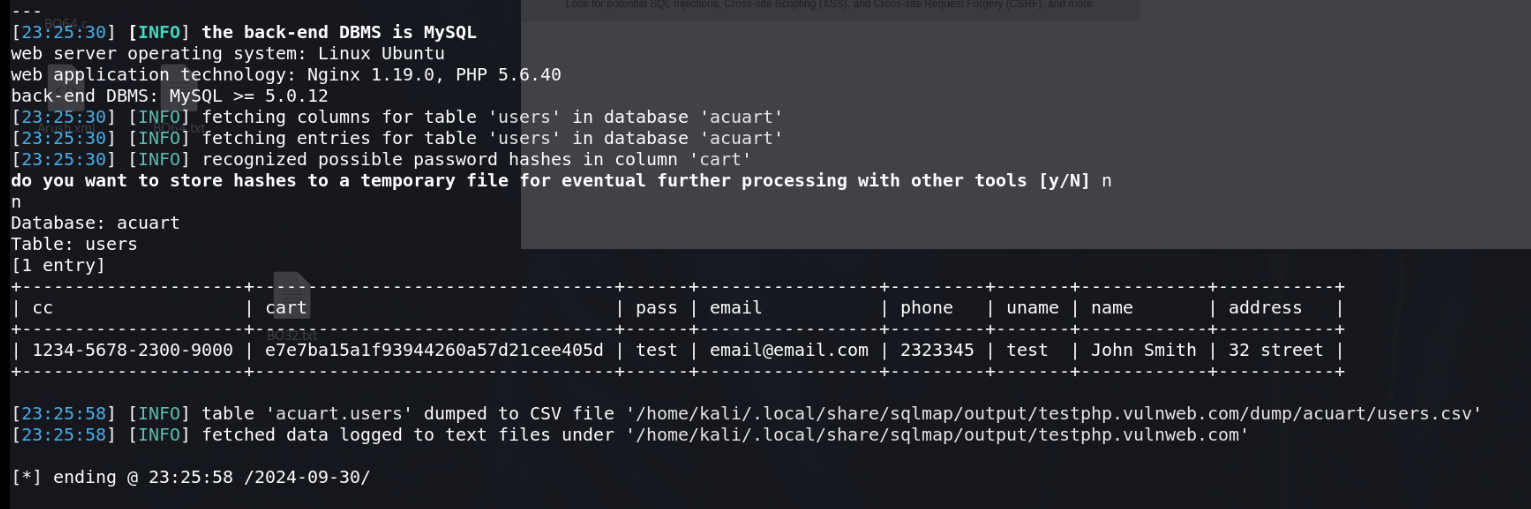
It will show all the present columns.



It will show the entry in uname column



For altering the complete table



**NETBIOS ENUMERATION**

Network basic input output system,

NetBIOS is used to communicate over a Lan, file share, connect printers

TCP/IP devices identification

Netbios (windows) ,System in windows are known through netbios

Network - Unique and limit 16 char , 15 char are reserved for devices name .

16- identify services

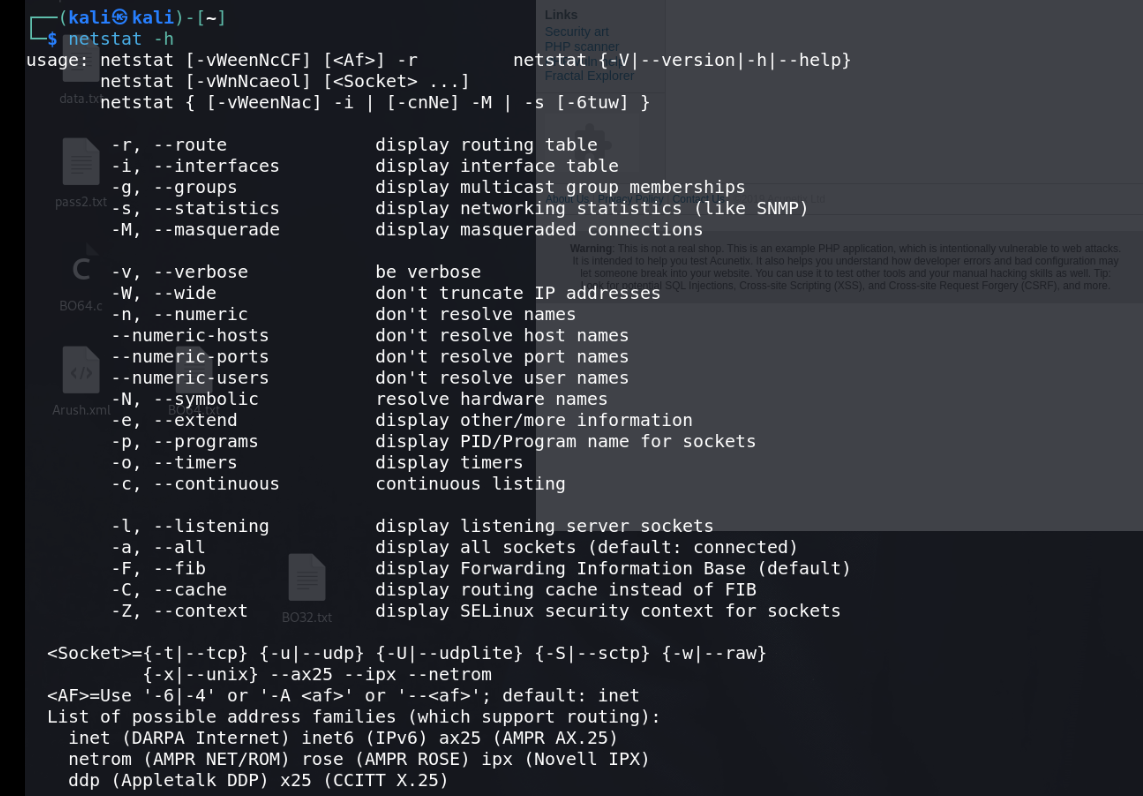
Netbios enumeration tools – Netstat tool

Functions - Tells us about the established connection

**Commands**

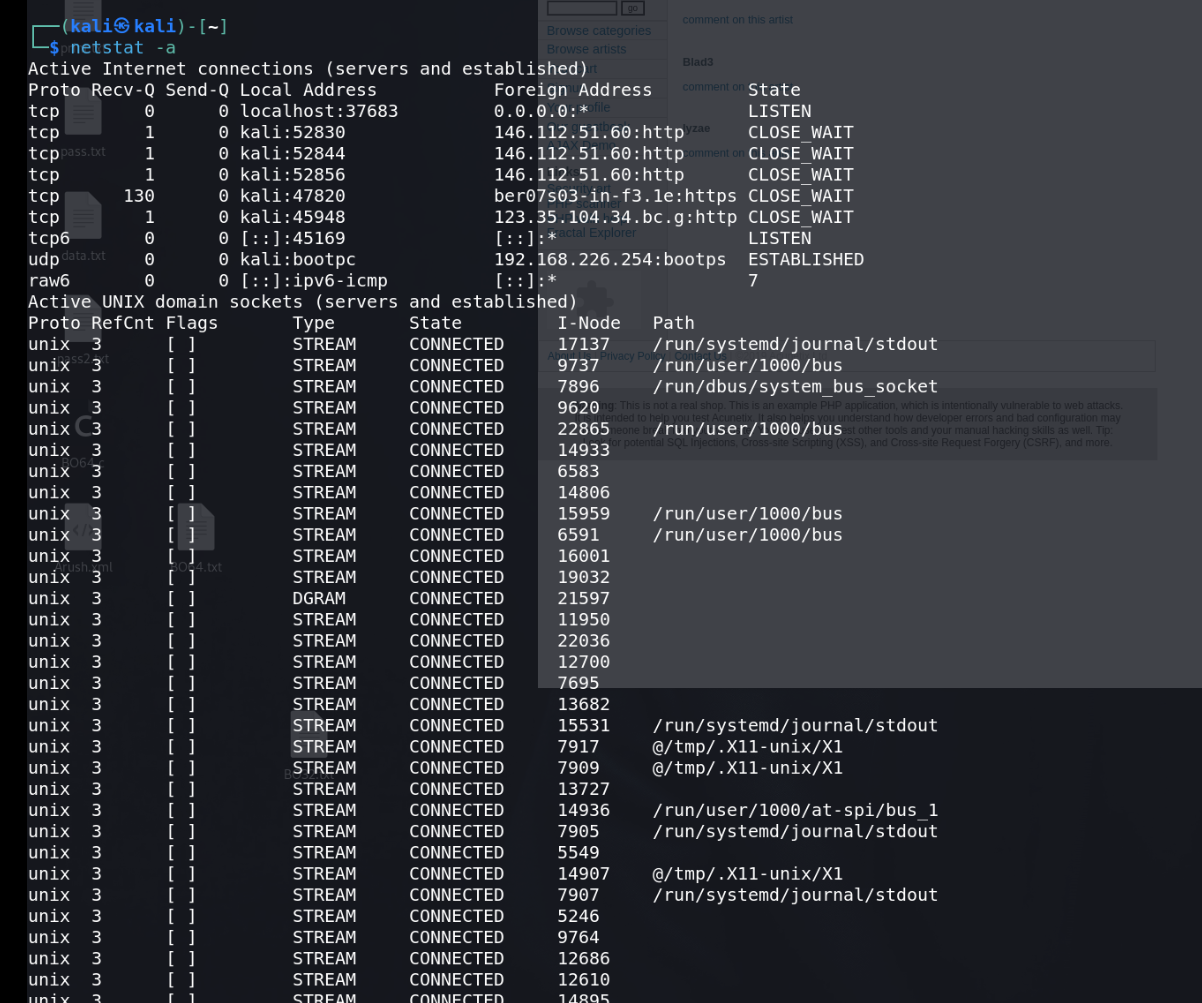
netstat -h

It will tells us about all the flags.



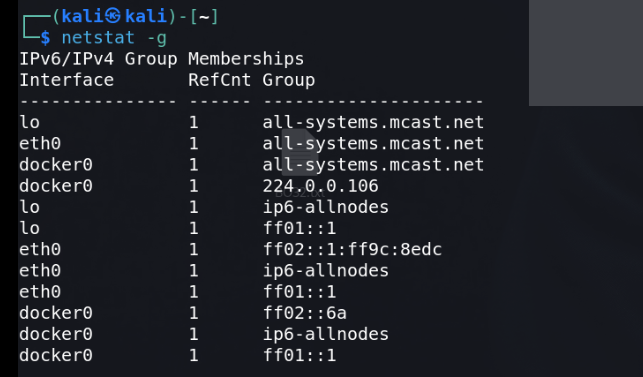
netstat -a

It will tells us about main tables



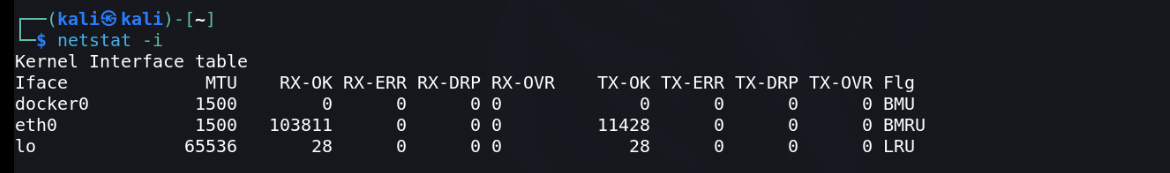
netstat -g

It will tells us about groups regarding ipv4/ipv6



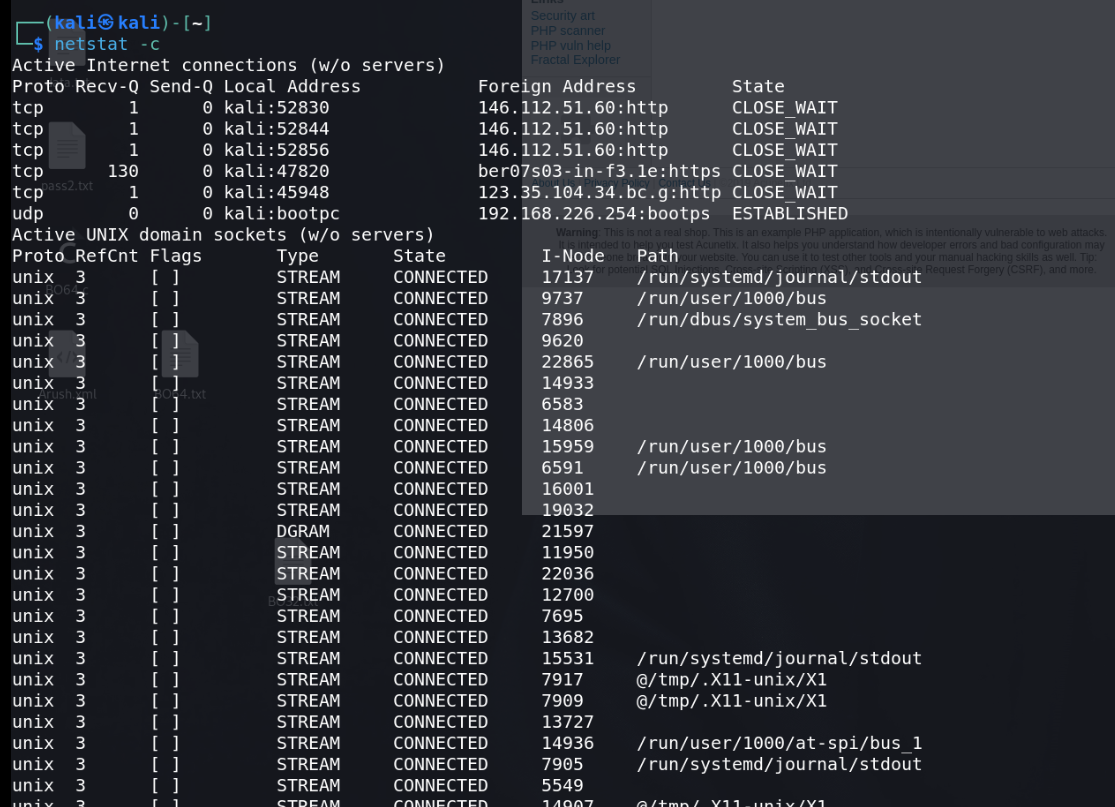
netstat -i

It will tells us about kernel interface table



netstat -c

It will tells us about system cache information.



v