

Cyber Security - Minor Project

Question 1: Perform Foot printing on Amazon 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.

Answer:

I performed foot printing on amazon website and gathered information about the website using the following online websites:

<https://whois.domaintools.com/amazon.com> &

<https://sitereport.netcraft.com/?url=www.amazon.com>

The amazon website's domain is <http://www.amazon.com> with the site title: Spend less. Smile more.

The registrant of the website is Hostmaster, Amazon Legal Dept.

Registrant country is The United States of America and the Registrar is MarkMonitor Inc. It's IP Address 52.84.168.188 is hosted on a server in Sao Paulo – Amazon.com Inc.

It is 9785 days old. It was last updated on 2019.

Screenshots gathered from Whois and netcraft are attached below:

Whois:

The screenshot shows the 'Whois Record for Amazon.com' page on the DomainTools website. The page is divided into two main sections: 'Domain Profile' on the left and 'Tools' on the right. The 'Domain Profile' section contains a table with the following information:

| Domain Profile | |
|--------------------|--|
| Registrant | Hostmaster, Amazon Legal Dept. |
| Registrant Org | Amazon Technologies, Inc. |
| 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 | 9,785 days old Created on 1994-10-31 Expires on 2024-10-30 Updated on 2019-08-26 |
| Name Servers | NS1.P31.DYNECT.NET (has 227,176 domains) NS2.P31.DYNECT.NET (has 227,176 domains) NS3.P31.DYNECT.NET (has 227,176 domains) NS4.P31.DYNECT.NET (has 227,176 domains) PDNS1.ULTRADNS.NET (has 93,573 domains) PDNS6.ULTRADNS.CO.UK (has 3,221 domains) |
| Tech Contact | Hostmaster, Amazon Legal Dept. Amazon Technologies, Inc. P.O. Box 8102 Renton, WV 26050, us |

The 'Tools' section on the right includes a 'DomainTools Iris' advertisement, a 'Preview the Full Domain Report' button, and a list of tools: 'Hosting History', 'Monitor Domain Properties', 'Reverse IP Address Lookup', and 'Network Tools'. There is also a 'Visit Website' button and a small preview of the Amazon website.

whois.domaintools.com/amazon.com

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

| | |
|-------------------|--|
| Tech Contact | Hostmaster, Amazon Legal Dept. Amazon Technologies, Inc. P.O. Box 8102, Reno, NV, 89507, us hostmaster@amazon.com (n) 12062664064 (f) 12062667010 |
| IP Address | 52.84.168.188 - 2 other sites hosted on this server |
| IP Location | 🇺🇸 - Sao Paulo - Sao Paulo - Amazon.com Inc. |
| ASN | 🇺🇸 AS16509 AMAZON-02, US (registered May 04, 2000) |
| Domain Status | Registered And Active Website |
| IP History | 455 changes on 455 unique IP addresses over 17 years |
| Registrar History | 2 registrars with 1 drop |
| Hosting History | 4 changes on 4 unique name servers over 17 years |
| Website | |
| Website Title | None given. |
| Server Type | Server |
| Response Code | 200 |
| Terms | 365 (Unique: 220, Linked: 182) |
| Images | 33 (Alt tags missing: 3) |
| Links | 82 (Internal: 79, Outbound: 0) |

Whois Record (last updated on 2021-08-15)

```
Domain Name: amazon.com
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T12:19:56-0700
Creation Date: 1994-10-31T21:00:00-0800
Registrar Registration Expiration Date: 2024-10-30T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
```

whois.domaintools.com/amazon.com

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

Whois Record (last updated on 2021-08-15)

```
Domain Name: amazon.com
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T12:19:56-0700
Creation Date: 1994-10-31T21:00:00-0800
Registrar Registration Expiration Date: 2024-10-30T00:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
```

whois.domaintools.com/amazon.com

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

```
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com
Registry Admin ID:
Admin Name: Hostmaster, Amazon Legal Dept.
Admin Organization: Amazon Technologies, Inc.
Admin Street: P.O. Box 8102
Admin City: Reno
Admin State/Province: NV
Admin Postal Code: 89507
Admin Country: US
Admin Phone: +1.2062664064
Admin Phone Ext:
Admin Fax: +1.2062667010
Admin Fax Ext:
Admin Email: hostmaster@amazon.com
Registry Tech ID:
Tech Name: Hostmaster, Amazon Legal Dept.
Tech Organization: Amazon Technologies, Inc.
Tech Street: P.O. Box 8102
Tech City: Reno
Tech State/Province: NV
Tech Postal Code: 89507
Tech Country: US
Tech Phone: +1.2062664064
Tech Phone Ext:
Tech Fax: +1.2062667010
Tech Fax Ext:
Tech Email: hostmaster@amazon.com
Name Server: pdns6.ultradns.co.uk
Name Server: ns4.p31.dynect.net
Name Server: ns1.p31.dynect.net
Name Server: ns3.p31.dynect.net
Name Server: pdns1.ultradns.net
Name Server: ns2.p31.dynect.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://vdprs.internic.net/
For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes
```

Netcraft:

←→↻

sitereport.netcraft.com?url=www.amazon.com

☆🔍🌐

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ 🔍

Report FraudRequest Trial

Background

Site title

Amazon.com. Spend less. Smile more.

Date first seen

October 1995

Site rank

23

Netcraft Risk Rating 🔍

0/10

Description

Free shipping on millions of items. Get the best of Shopping and Entertainment with Prime. Enjoy low prices and great deals on the largest selection of everyday essentials and other products, including fashion, home, beauty, electronics, Alexa Devices, sporting goods, toys, automotive, pets, baby, books, video games, musical instruments, office supplies, and more.

Primary language

English

Network

Site

<http://www.amazon.com> 🔗

Domain

amazon.com

Netblock Owner

Amazon.com, Inc.

Nameserver

dns-external-master.amazon.com

Hosting company

Amazon

Domain registrar

markmonitor.com

Hosting country

🇺🇸 US 🔗

Nameserver organisation

whois.markmonitor.com

IPv4 address

13.224.64.72 (VirusTotal) 🔗

Organisation

Amazon Technologies, Inc., P.O. Box 8102, Reno, 89507, United States

IPv4 autonomous systems

AS16509 🔗

DNS admin

root@amazon.com

IPv6 address

Not Present

Top Level Domain

Commercial entities (.com)

IPv6 autonomous systems

Not Present

DNS Security Extensions

unknown

Reverse DNS

server-13-224-64-72.dub2.r.cloudfront.net

Latest Performance

[Performance Graph](#) 🔗

←→↻

sitereport.netcraft.com?url=www.amazon.com

☆🔍🌐

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ 🔍

Report FraudRequest Trial

Hosting country

🇺🇸 US 🔗

Nameserver organisation

whois.markmonitor.com

IPv4 address

13.224.64.72 (VirusTotal) 🔗

Organisation

Amazon Technologies, Inc., P.O. Box 8102, Reno, 89507, United States

IPv4 autonomous systems

AS16509 🔗

DNS admin

root@amazon.com

IPv6 address

Not Present

Top Level Domain

Commercial entities (.com)

IPv6 autonomous systems

Not Present

DNS Security Extensions

unknown

Reverse DNS

server-13-224-64-72.dub2.r.cloudfront.net

Latest Performance

[Performance Graph](#) 🔗

IP delegation

IPv4 address (13.224.64.72)

| IP range | Country | Name | Description |
|-----------------------------|-------------------------------|----------|--|
| 0.0.0.0-255.255.255.255 | N/A | IANA-BLK | The whole IPv4 address space |
| 🔗 13.0.0.0-13.255.255.255 | 🇺🇸 United States | NET13 | American Registry for Internet Numbers |
| 🔗 13.200.0.0-13.239.255.255 | 🇺🇸 United States | AT-88-Z | Amazon Technologies Inc. |
| 🔗 13.224.0.0-13.227.255.255 | 🇺🇸 United States | AMAZO-CF | Amazon.com, Inc. |
| 🔗 13.224.64.72 | 🇺🇸 United States | AMAZO-CF | Amazon.com, Inc. |

IP Geolocation

We use multilateration to independently determine the location of a server. [Read more.](#)

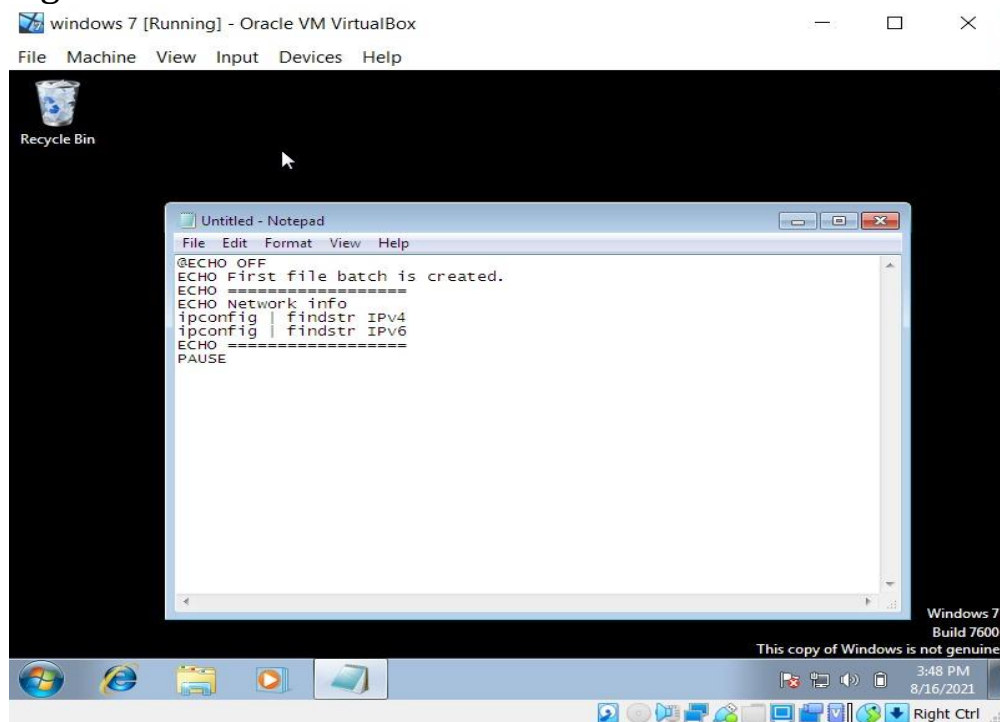
Hosting History

| Netblock owner | IP address | OS | Web server | Last seen |
|---|----------------|---------|-------------|-------------|
| Akamai | 88.221.17.57 | Linux | AkamaiGHost | 15-Aug-2021 |
| Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 | 13.224.225.29 | unknown | CloudFront | 14-Aug-2021 |
| Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB | 23.217.9.58 | Linux | AkamaiGHost | 13-Aug-2021 |
| Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 | 99.86.109.46 | unknown | CloudFront | 12-Aug-2021 |
| Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB | 23.217.9.58 | Linux | AkamaiGHost | 11-Aug-2021 |
| Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 | 99.86.109.46 | unknown | CloudFront | 10-Aug-2021 |
| Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB | 23.217.9.58 | Linux | AkamaiGHost | 9-Aug-2021 |
| Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 | 13.224.245.131 | unknown | CloudFront | 7-Aug-2021 |
| Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB | 23.217.9.58 | Linux | AkamaiGHost | 6-Aug-2021 |
| Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244 | 13.224.64.72 | Linux | CloudFront | 5-Aug-2021 |

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

Answer: I wrote a program on notepad to get the network information of the system, and saved it as .bat file.

The program I've written is in the screenshot below:

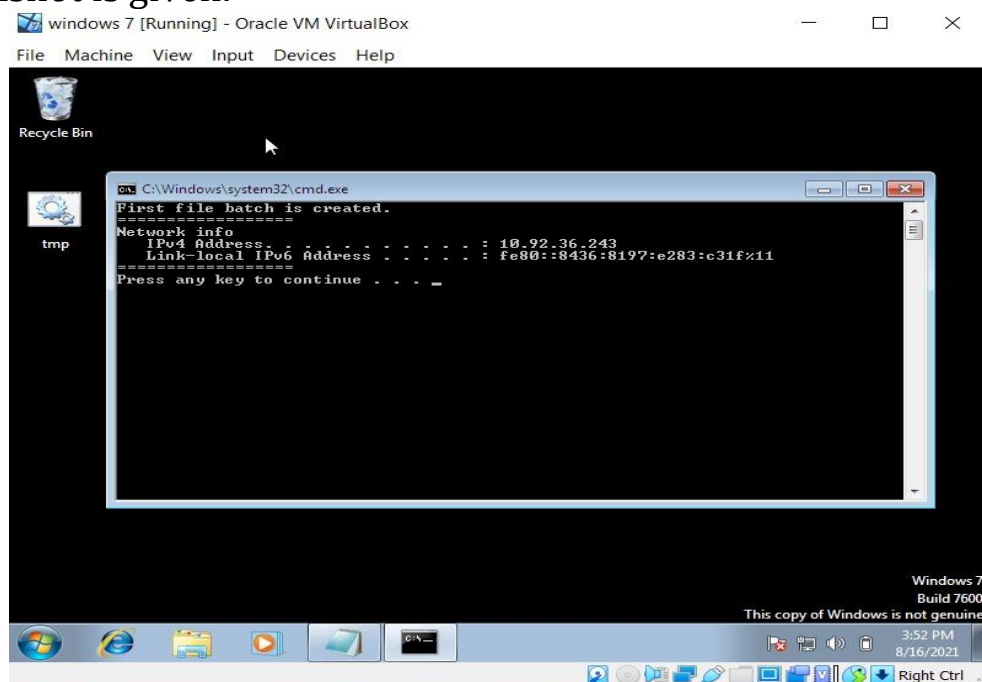


The screenshot shows a Windows 7 virtual machine running in Oracle VM VirtualBox. A Notepad window titled 'Untitled - Notepad' is open, displaying the following batch script:

```
@ECHO OFF
ECHO First file batch is created.
ECHO =====
ECHO Network info
ipconfig | findstr IPv4
ipconfig | findstr IPv6
ECHO =====
PAUSE
```

The VM desktop also shows a Recycle Bin icon and a taskbar with the system clock at 3:48 PM on 8/16/2021.

After saving this and opening, it was executed. The following screenshot is given:



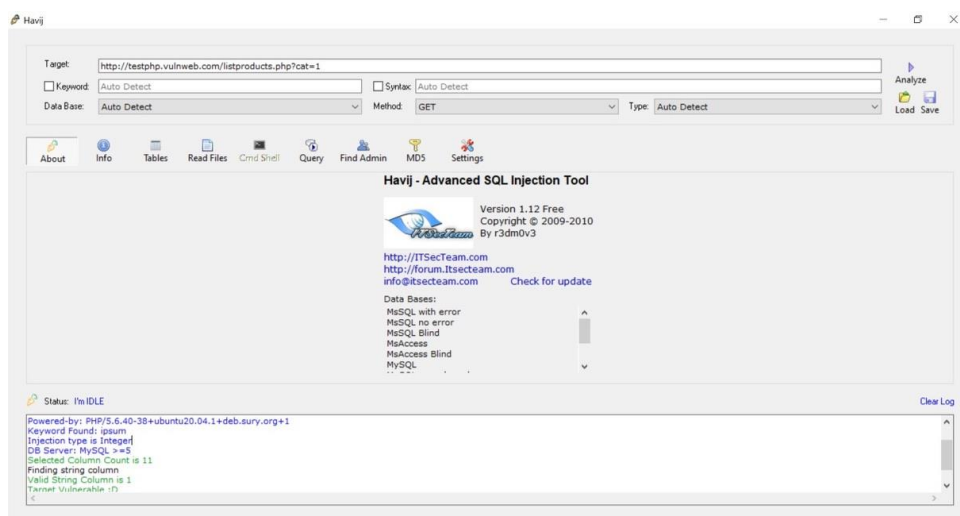
The screenshot shows the same Windows 7 virtual machine, but now a Command Prompt window titled 'C:\Windows\system32\cmd.exe' is open. It displays the output of the batch script:

```
First file batch is created.
=====
Network info
IPv4 Address . . . . . : 10.92.36.243
Link-local IPv6 Address . . . . . : fe80::8436:8197:e283:c31f%11
=====
Press any key to continue . . . .
```

The taskbar now shows the system clock at 3:52 PM on 8/16/2021.

Question 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.

Answer: SQL injections are one of the most utilized web attack vectors used with the goal of retrieving sensitive data from organizations. I installed Havij tool. I opened the given link of the demo website and from categories, I chose a link. Then, I copied the link and pasted it in the target site bar in Havij tool, and analysed it. The screenshot is attached below.



Steps to avoid SQL injections:

1. Everyone involved in building the web application must be aware of the risks associated with SQL injections.
2. Do not trust any user input.
3. Use the latest version of the development environment and language and the latest technologies.
4. Employ verified mechanisms.
5. You should regularly scan your web applications using any web application scanners.

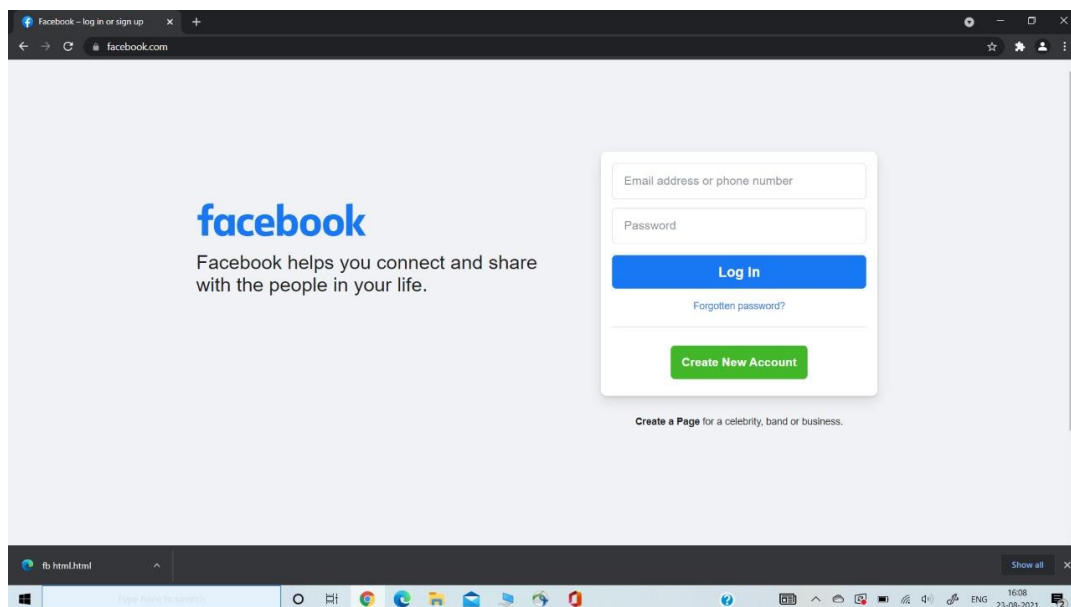
Question 6: Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials and write the document along with screenshots and suggest the solution to avoid from phishing.

Answer: Phishing is a social engineering attack often used to steal data like login credentials, credit card details, etc.

Three files that are required in phishing are html file(of a genuine website), php file(to execute the malicious code) and text file(that saves the username and password).

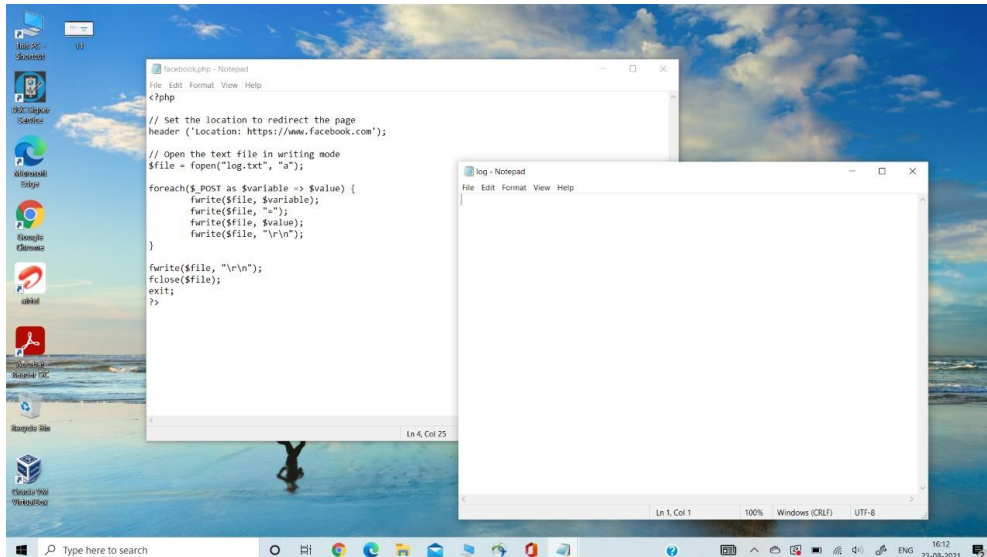
Here, the target is www.facebook.com.

First, I opened a facebook page and saved it as an html file.

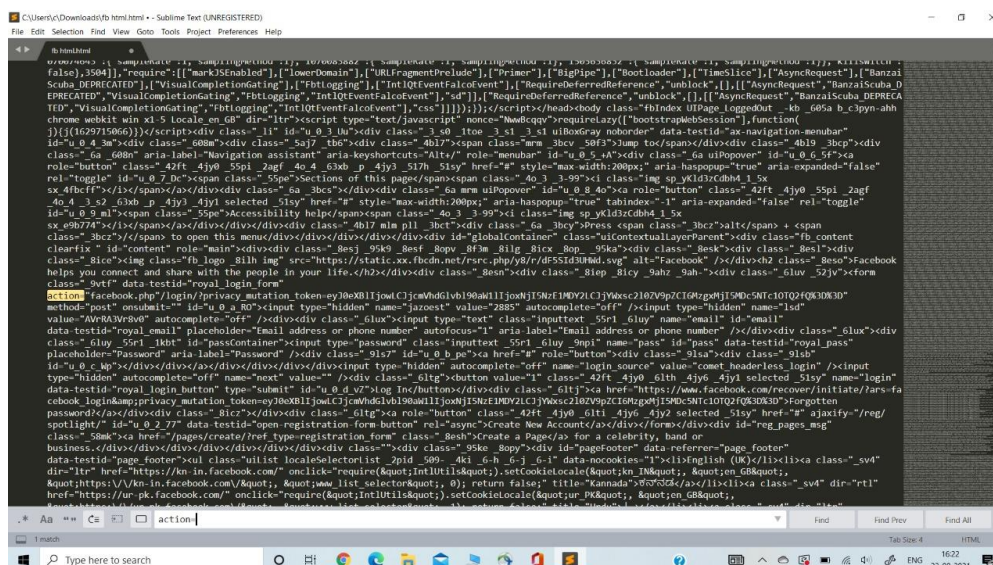


Next, I got a phishing code from geeksforgeeks website. I copied that code in notepad and saved it as a php file.

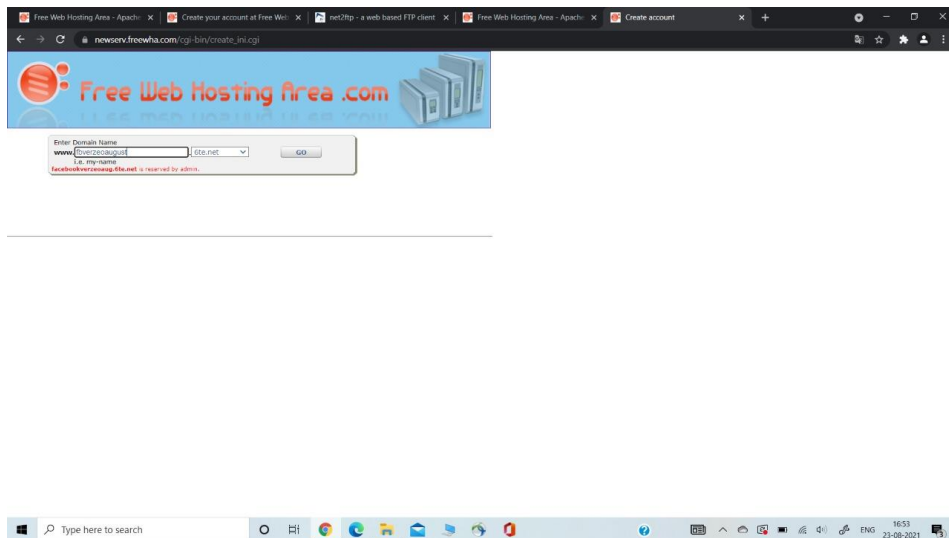
After doing this, I created an empty text file and saved it as log.txt, as this will save all the usernames and passwords at the end.



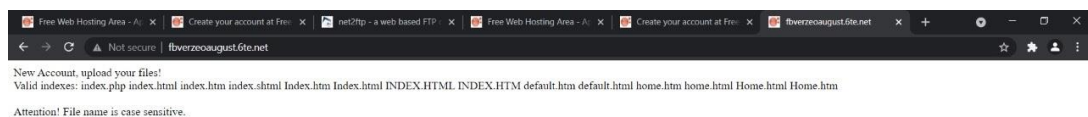
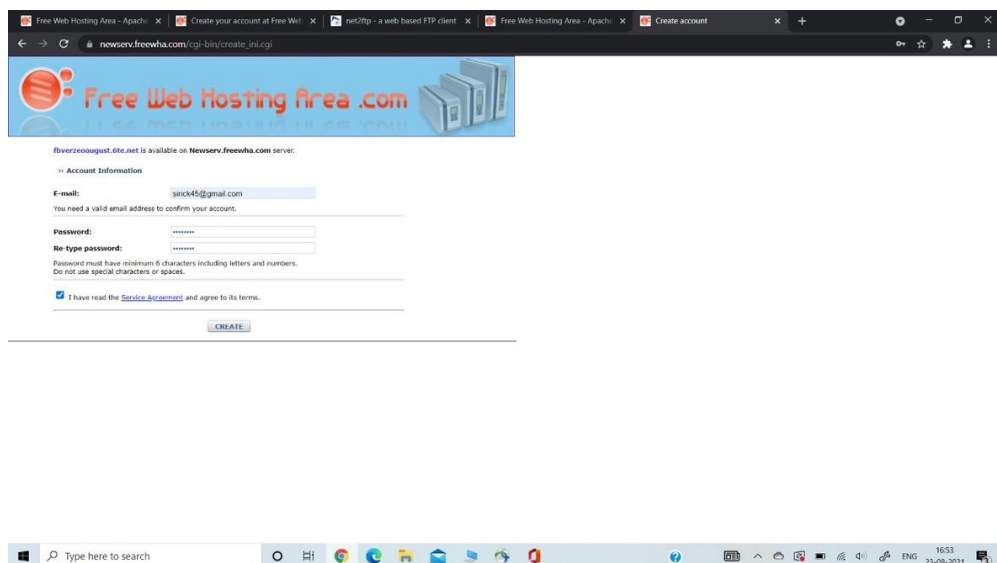
Once I had all the three files with me, I modified the html file by finding the keyword “action=” and replacing original link with facebook.php.



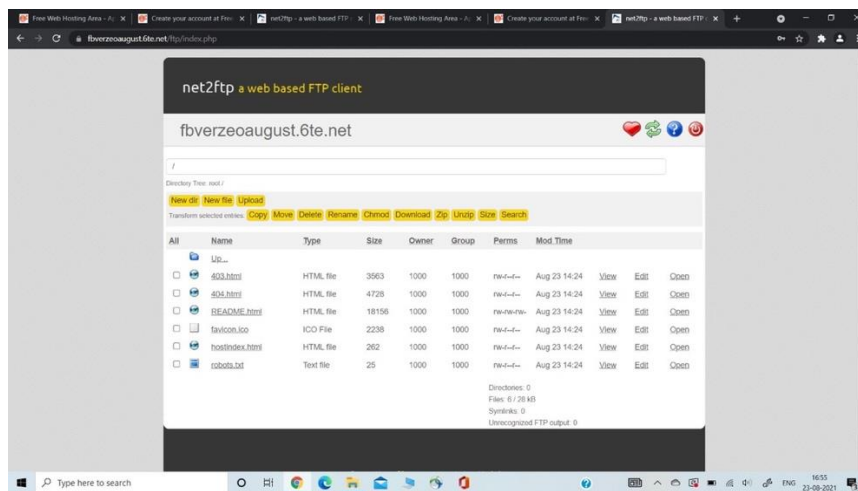
I used an online temporary website creator and hosted a new web page of my choice.



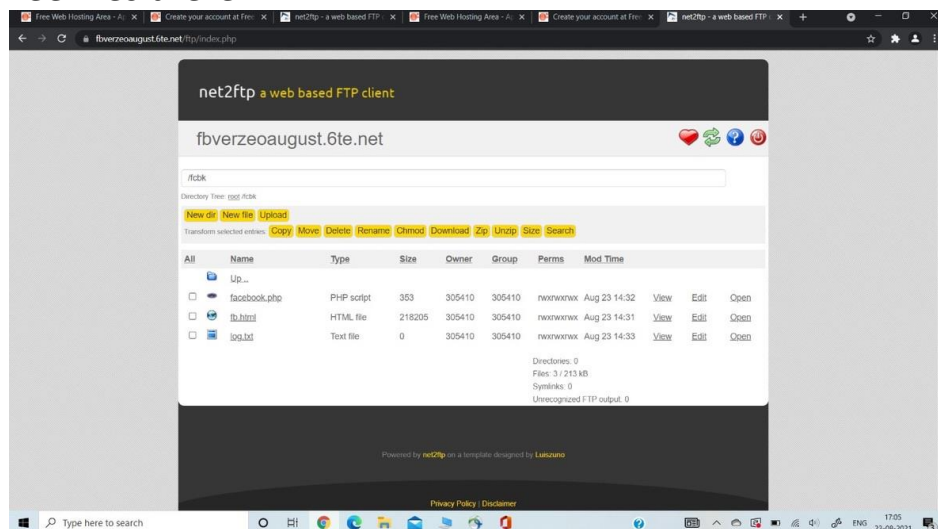
I chose a subdomain called fbverzeoaugust.6te.net. I had to create an account following which the website is created.



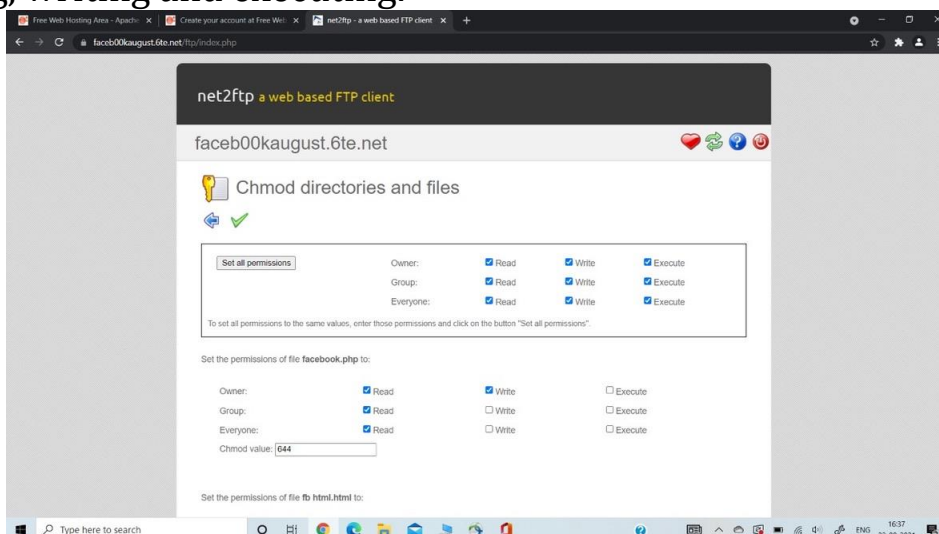
Next, I went to fbverzeoaugust.6te.net/ftp.



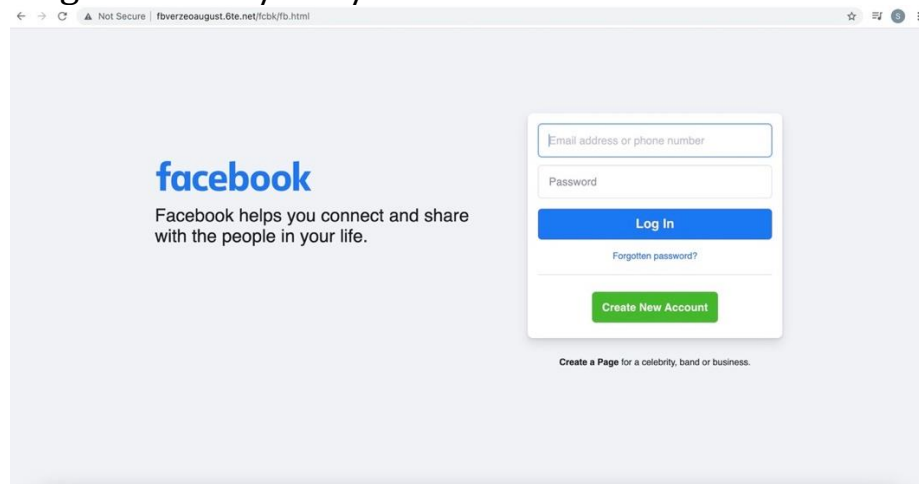
After this step, I created a new directory called “fcbk”, and added the initial three files there.



For granting permissions, I went to chmod and got the permissions for reading, writing and executing.



The next step was to access the website which is fbverzeoaugust.6te.net/fcbk/facebook.html



I typed random email addresses and passwords and each time I clicked on sign in, the same log in page opened. The email addresses and passwords were saved in log.txt file.

```
jazoest=2958
lsd=AVp0X1st3y0
email=vvvvcwkk
pass=cwncon
login_source=comet_headerless_login
next=

jazoest=2958
lsd=AVp0X1st3y0
email=sirelaciacc
pass=wicwicwc
login_source=comet_headerless_login
next=
```

Therefore, I have successfully cloned a facebook page.

Methods to avoid phishing:

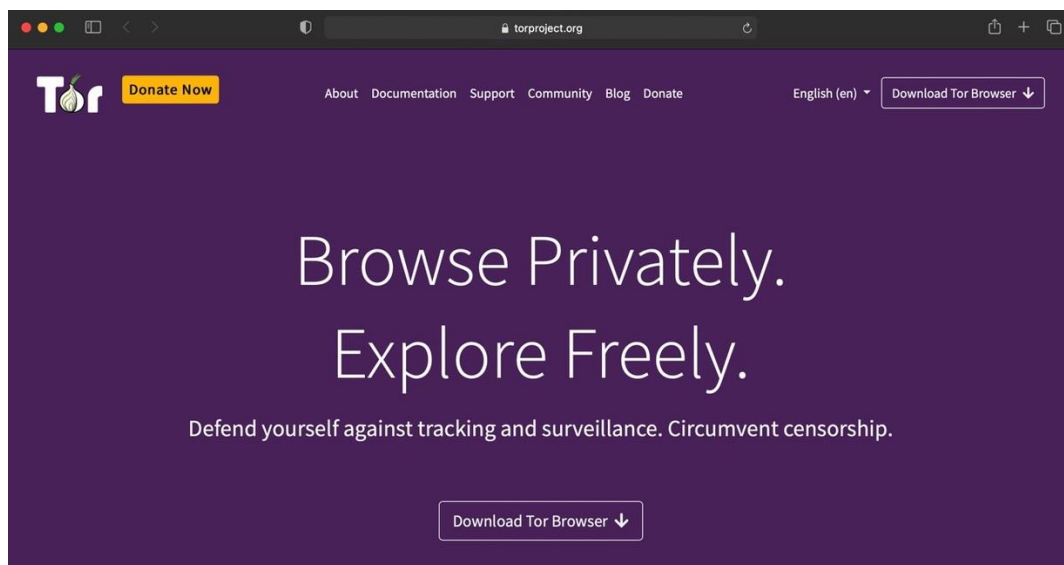
1. One of the most simplest methods to prevent phishing is for internet users to be cautious before clicking on any random links given by fake websites.
2. Be wary of fake links, such as bit.ly, that may be altered to look like a genuine website link.
3. Typically, these links are sent via email. Do not open any emails that do not appear to be legitimate, since they may contain harmful malware that can steal personal information when you visit the website linked in the email.

Question 7: Write article on how to change the IP address by using proxies and mention the differences between proxies and VPN.

Answer:

Changing IP address is a simple task. Normally, it is done through an online browser, but the best option is to use software, and the best Proxy software to use is Tor, which can be obtained from the following link.

<https://www.torproject.org>



After that, we log in and begin browsing in private mode.

VPNs and proxies both give a higher level of privacy than would be possible, allowing us to browse the internet anonymously in a number of ways by concealing our IP address. However, how they go about doing so is a much more difficult process.

A proxy acts as a gateway and is ideal for simple activities such as anonymous online browsing and content restriction management. Proxy servers excel at IP masking and misdirection, making them excellent for viewing regionally restricted content. They allow users to access content restrictions and monitoring, as well as impose content restrictions on websites, such as the inability to view specific web pages during business hours.

The computer's virtual private network (VPN) creates a secure tunnel with the VPN server, changing your local IP address. VPN connections,

like proxy servers, encrypt and protect all the network interactions from browser.

To put it more simply, a proxy just changes IP address, whereas a VPN or Virtual Private Network, temporarily changes whole network. VPN can be downloaded straight to a local machine or a virtual machine. We can also get a VPN for free. For example, from seed4me or cyber ghost.

