Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Department of Computer Science

A

PROJECT REPORT

ON

Vulnerability Assessment and Penetration Testing

Submitted By

Group No: 05

AJEYPALSINH JADEJA – 20082291039

RIYAKUMARI PATEL – 20082291017

B.Sc. IT (CYBER SECURITY) SEMESTER-VI

U66A1IP2 - INDUSTRIAL PROJECT – II

GUIDED BY

INTERNAL: Prof. KRIMA PATEL

SUBMITTED TO

DEPARTMENT OF COMPUTER SCIENCE,

GANPAT UNIVERSITY,

GANPAT VIDHYANAGAR-384012

ACADEMY YEAR 2022-23

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Department of Computer Science

Date: 08/05/2023

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 B.Sc. IT (Cyber Security) Semester-VI have/has completed their/his project work titled **"Vulnerability Assessment and Penetration Testing"** satisfactorily and fulfill the requirement of B.Sc. IT (Cyber Security) Semester-VI, Department of Computer Science, Ganpat University in the Academic Year, 2022-2023.

Sr. No.	Student Name	Enrollment No.
1.	AJEYPALSINH JADEJA	20082291039
2.	RIYAKUMARI PATEL	20082291017

Internal Guide	Project Coordinator	Program Coordinator	Dean
Prof. Krima Patel	Prof. Deepika Patel	Dr. Ketan Patel	Dr. Nirbhay Chaubey

ACKNOWLEDGEMENT

We take this opportunity to humbly express my thankfulness to all those concerned with our project **"Vulnerability Assessment and Penetration Testing "**. We are thankful to Ganpat University for giving us opportunity to develop the Project.

Secondly, we are thankful to **Department of Computer Science, Ganpat University, Kherva** to provide the excellent environment to us for develop the project.

We express our deep sense of gratitude towards our guides; **Prof. Krima Patel** and for their keen interest in each stage of our project development, their guidance encourages us to developing the project in the right way.

Finally, we are thankful to all those people who have helped us directly or indirectly in completing this project successfully.

With Regards,

AJEYPALSINH JADEJA

RIYAKUMARI PATEL

PREFACE

This is a documentation of the project work done as part of fulfillment on completion of 6th semester in B.Sc. IT (Cyber Security) This Project is an on “Vulnerability Assessment Penetration Testing".

In this project a detail description of the requirement procedure followed and the methods implemented for the design and development are presented.

This Application Penetration Test is performed to identify and exploit vulnerabilities in an application, and the way it interacts and transfers data with the backend systems

INDEX

1. PROJECT PROFILE

PROJECT TITLE: -	Vulnerability Assessment and Penetration Testing
OBJECTIVE: -	To perform internal vulnerability assessment. To perform external vulnerability assessment.
OPERATING SYSTEM: -	Kali Linux (2023.1) Window (windows 10) Android (Android 13)
TOOLS: -	APKTool (2.7.0) Dex2jar (2.1) Burp-suite (2022.2.4) SQL Map Google Dorks Hping3 (3.a2.ds2)
PERFORM BY: -	AJEYPALSINH JADEJA (E. NO – 20082291039) RIYAKUMARI PATEL (E. NO – 20082291017)
INTERNAL GUIDE: -	Prof. Krima Patel
GROUP NO: -	05
SUBMITTED TO: -	Department of Computer Science, Ganpat University, Kherva

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.
- ✓ A Mobile Application Penetration Test is an authorized and simulated hacking attempt against a native mobile application such as Android, the purpose of this test is to identify and exploit vulnerabilities in an application, and the way it interacts and transfers data with the backend systems

2.2 BACKGROUND AND MOTIVATION

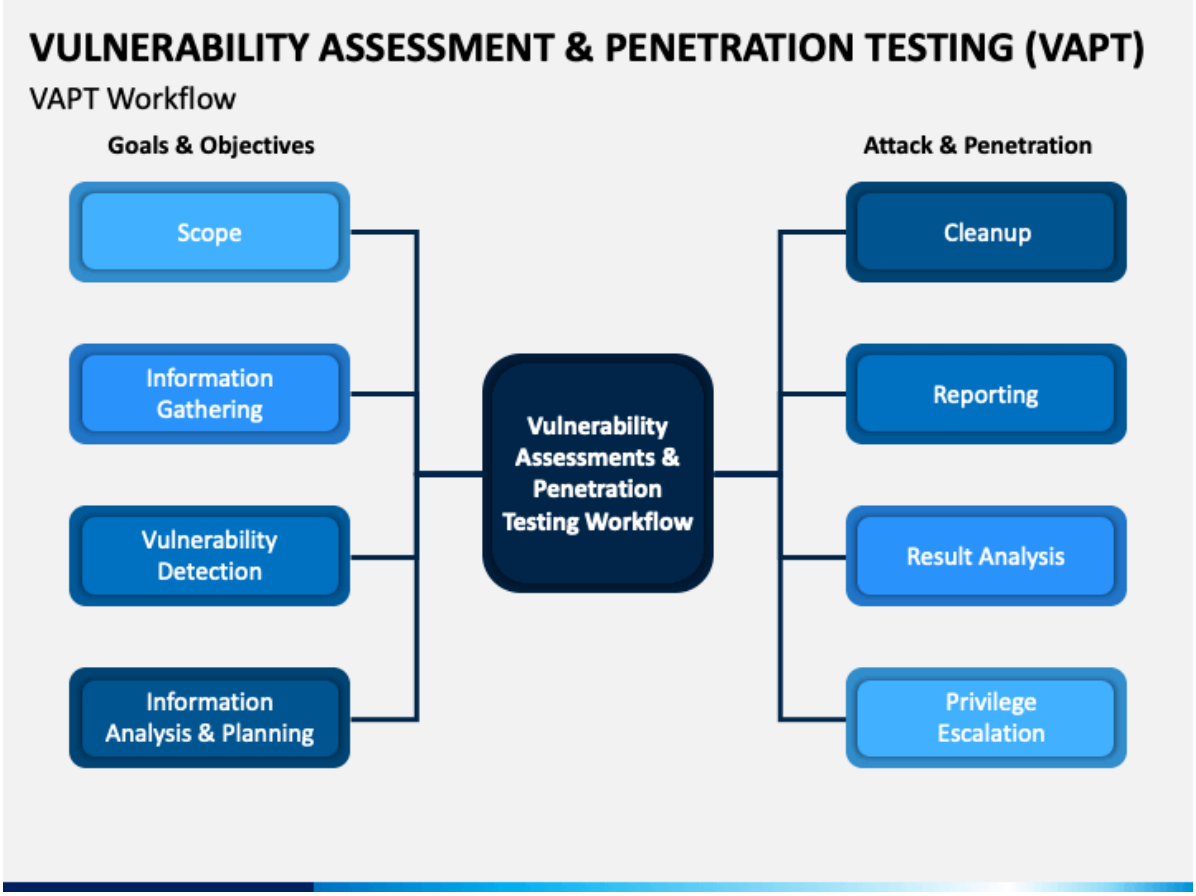
- ✓ The evolving tools, tactics and procedures used by cybercriminals to breach networks means that it is important to regularly test your organization's cyber security. VAPT helps to protect your organization by providing visibility of security weaknesses and guidance to address them. VAPT is increasingly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

- ✓ Mobile applications have become important part of day-to-day life as everyone is using smart phones now a days. Cyber security may often become false perception in case if we do not know how our apps were developed as well as penetration testing. The simplest way to identify and avoid cyber risk is to perform mobile app penetration testing.

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 REQUIRMENT

Processor	1.6 GHz
RAM	8 GB
Free Hard disk space	40 GB

SOFTWARE REQUIRMENT

Operating System	Android Linux Window
Tools	APKTool, Dex2jar, Jd-Gui, Hping3, Google Dorks, Burp-suite, SQLMap

4. TOOLS DESCRIPTION

APKTool	A tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications
Dex2jar	Dex2Jar is a freely available tool to work with Android ". dex" and Java ". class" files
Jd-Gui	JD-GUI is a standalone graphical utility that displays Java source codes of ".class" files.
Hping3	hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.
Google Dorks	Google dorking is used to find hidden information that is otherwise inaccessible through a normal Google search.
Burp-suite	Burp Suite is an integrated platform for performing security testing of applications
Sqlmap	SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.

FUNCTIONAL SPECIFICATION

5. FUNCTIONAL SPECIFICATION

Sr. No.	Vulnerability Name	Severity
01	Insecure Database Storage in Android (Reverse Engineering)	CRITICAL
02	OTP Bypassing (Brute Force)	HIGH
03	SQL Injection	HIGH
04	Cleartext Transmission of Sensitive Information	HIGH
05	No Rate Limit on Current Password Field	HIGH
06	HTML Injection	MEDIUM
07	XSS (Cross – site Scripting)	MEDIUM
08	Click Jacking	MEDIUM
09	Directory Traversal	MEDIUM
10	No Rate limiting on Admin Login page	MEDIUM
11	Dos Attack	MEDIUM
12	Css Injection	LOW
13	PHP Version Disclosure	LOW

PROOF

OF

CONCEPTS

Sr. No. Title	
01	
Description	
Insecure Database Storage in Android (Reverse Engineering)	
Affected Resource / Parameter	**Severity**
Theacher_Dairy_Base	**CRITICAL**

Impact / Consequences

Insecure data storage vulnerabilities typically lead to the following business risks for the organization that owns the risk app:

- ✓ Identity Theft
- ✓ Fraud
- ✓ Reputation Damage
- ✓ External Policy Violation (PCI); or
- ✓ Material Loss.

Recommendations

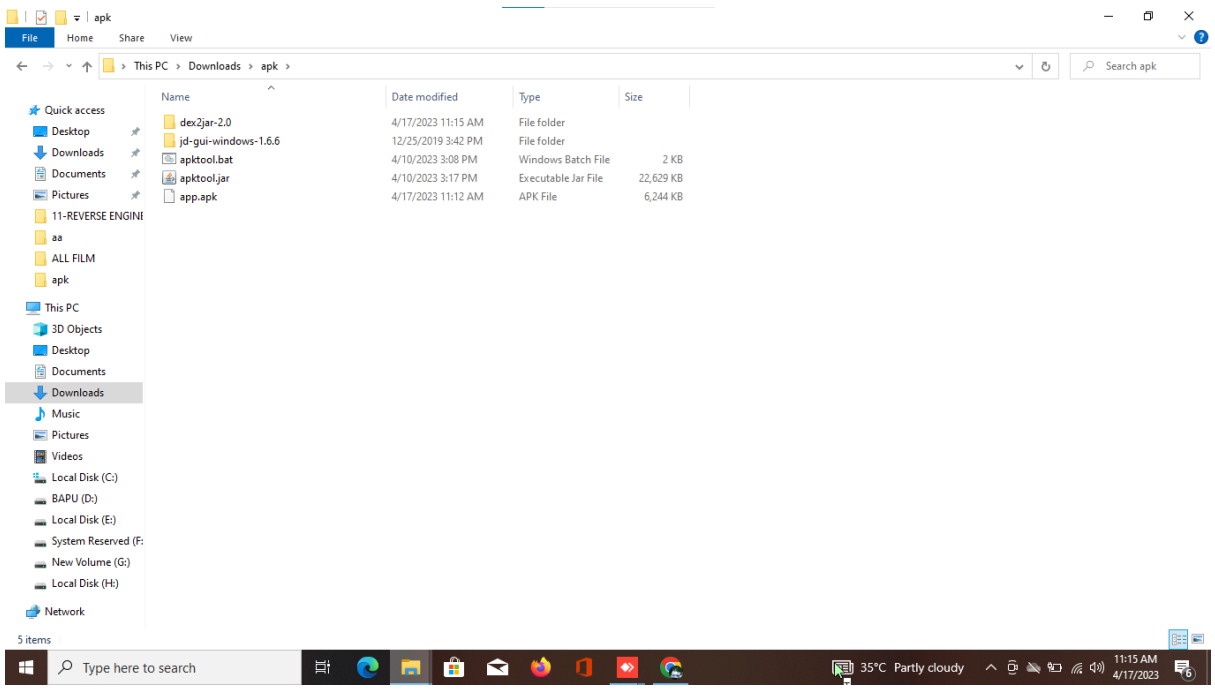
It is important to threat model your mobile app, OS, platforms, and frameworks to understand the information assets the app processes and how the APIs handle those assets. It is crucial to see how they handle the following types of features:

- ✓ URL caching (both request and response);
- ✓ Keyboard press caching;
- ✓ Copy/Paste buffer caching;
- ✓ Application back grounding;
- ✓ Intermediate data
- ✓ Logging;

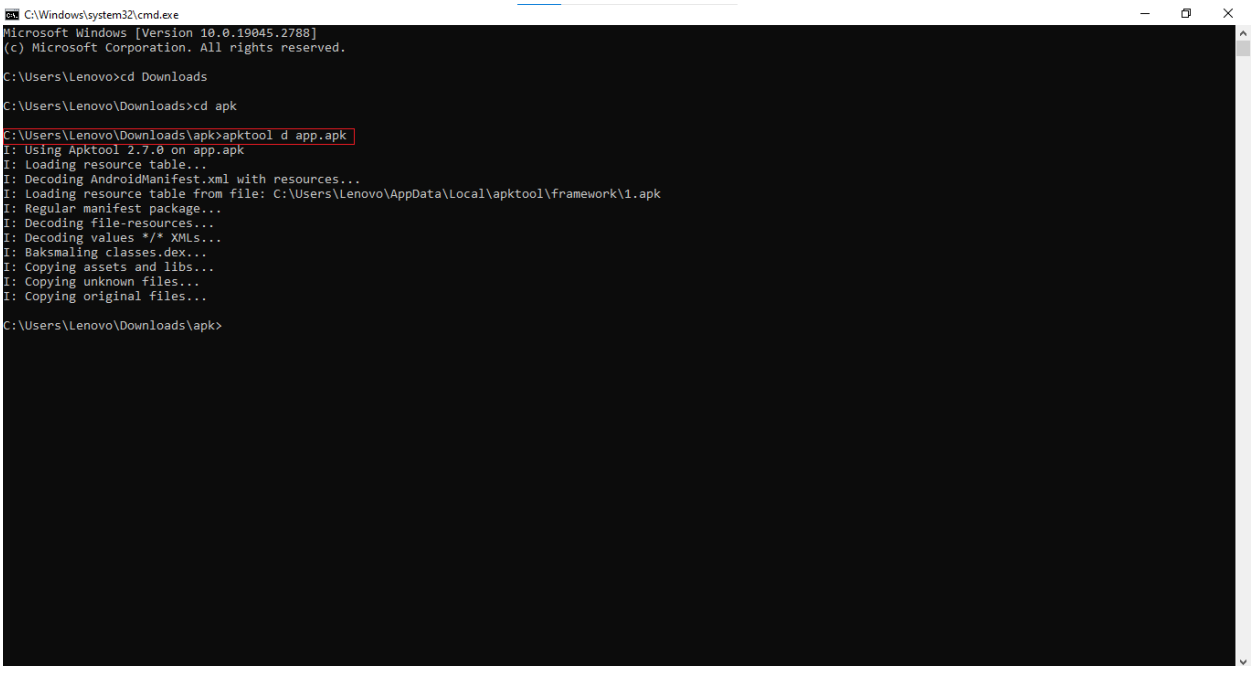
Tools Used	References
ApkTool	https://ibotpeaches.github.io/Apktool/install/
Dex2jar	https://sourceforge.net/projects/dex2jar/
Jd-GUI	http://java-decompiler.github.io/
CWE	**OWASP Top 10**
1278	M9

Proof of Vulnerability

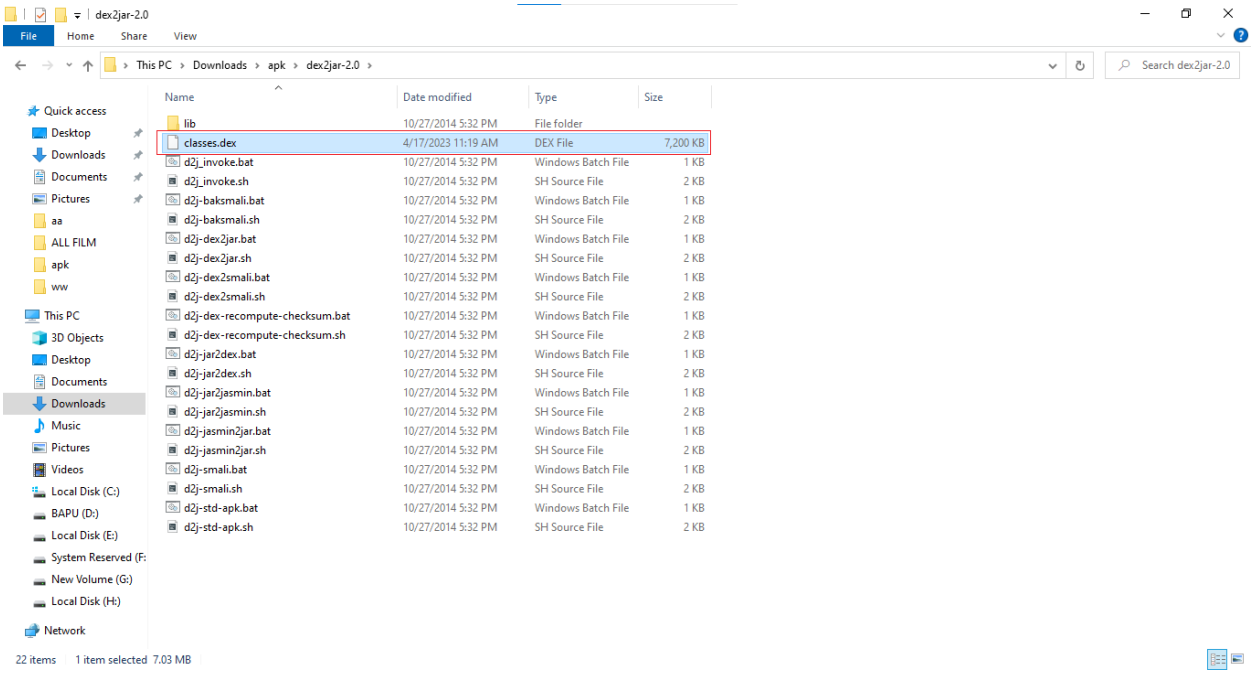
- **Step -1:** Tools we need to perform Reverse Engineering



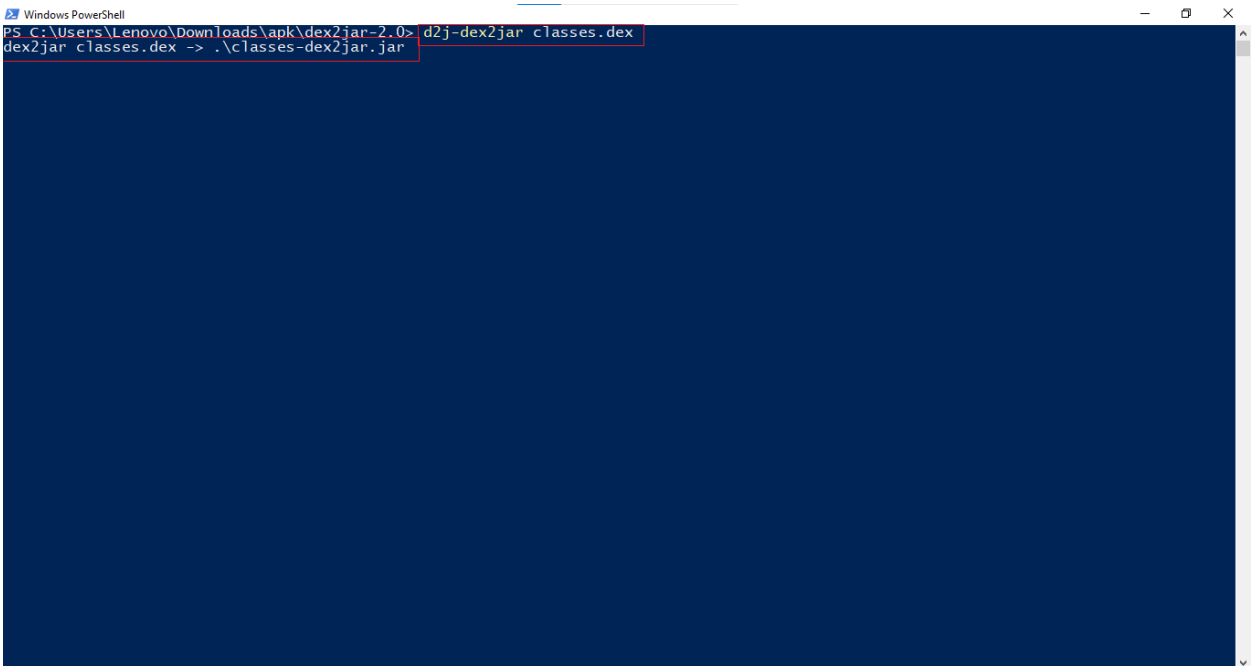
- Step – 2: Here we have the apk file of Teachers_Dairy_base. Use apk decompiler to decompile it.



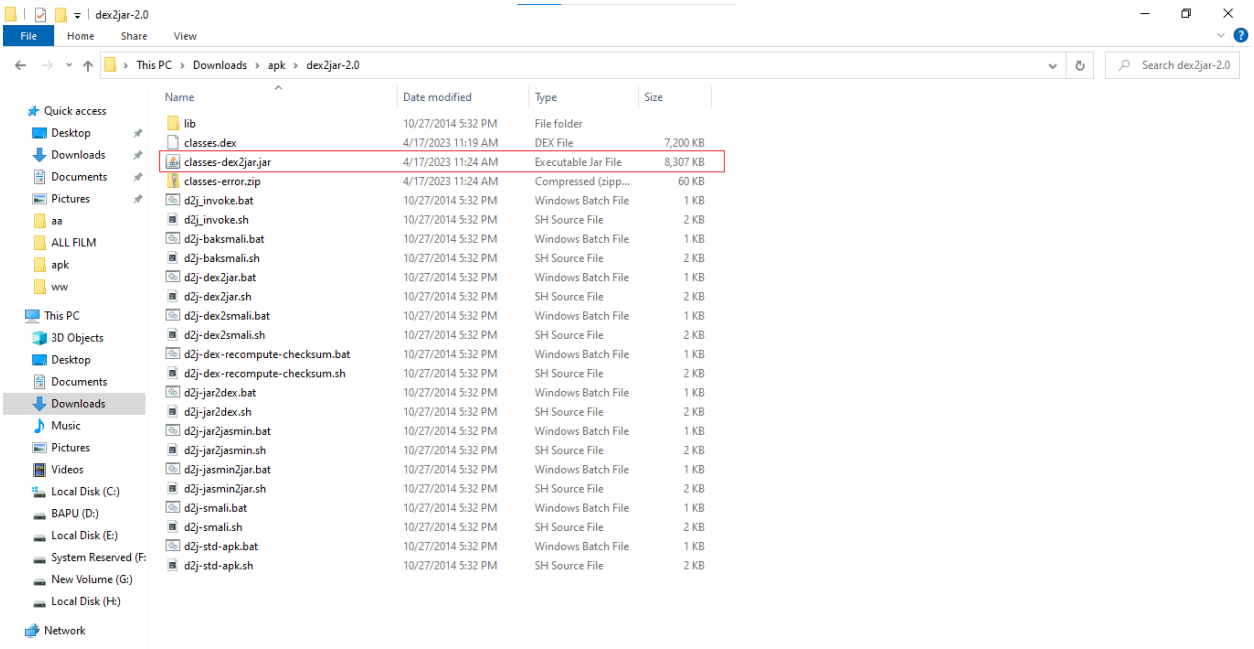
- Step – 3: After decompilation in resources folder you can see a dex file name classes.dex. Copy it and paste it in Dex2jar folder



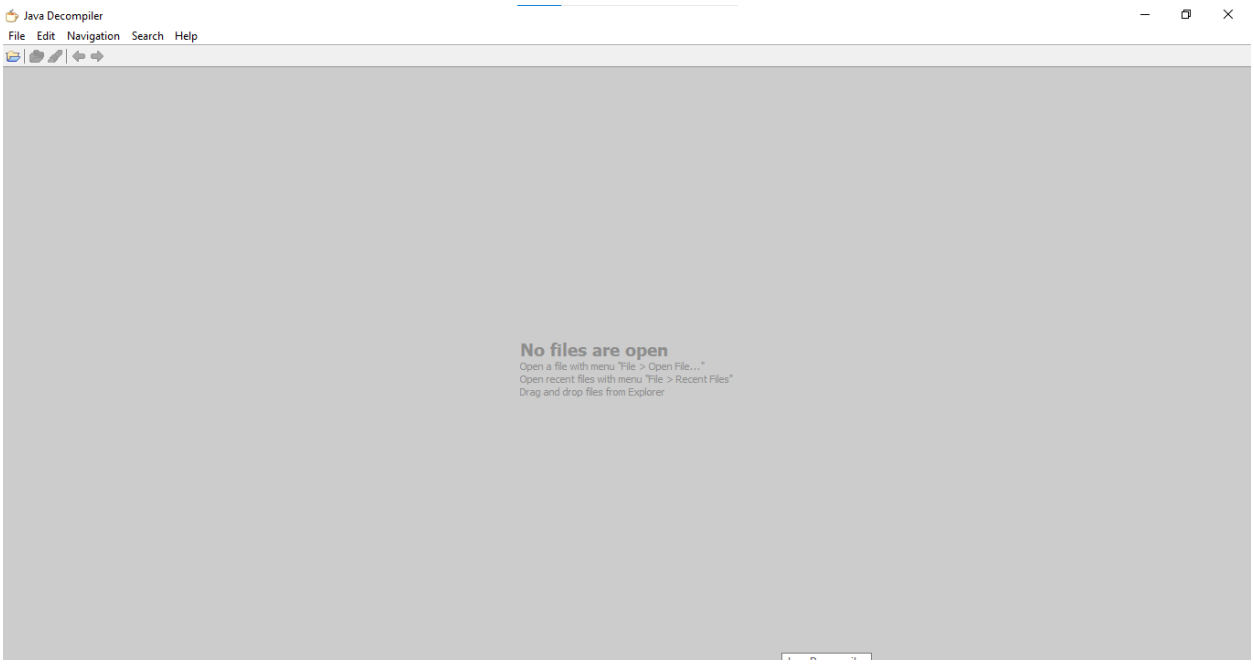
- Step – 4 : Open the folder and press shift and right click then a power shell will be there write the command inside it.



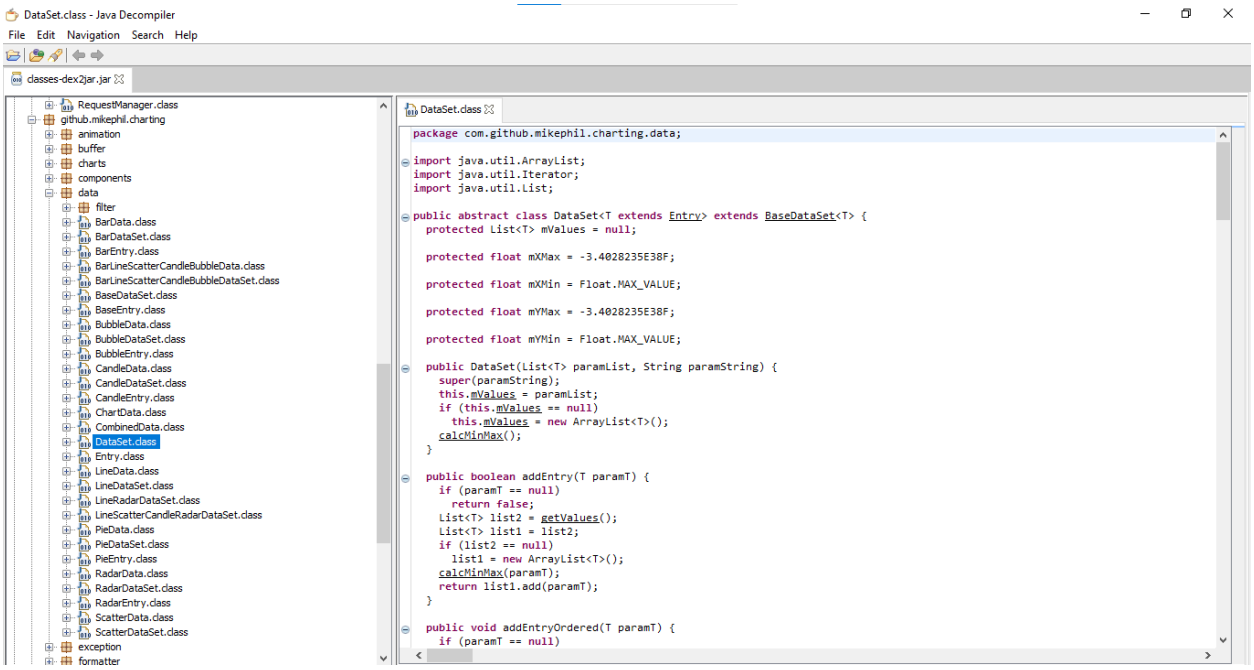
- Step – 5: After that you can see a classes-dex2jar.jar file has been create

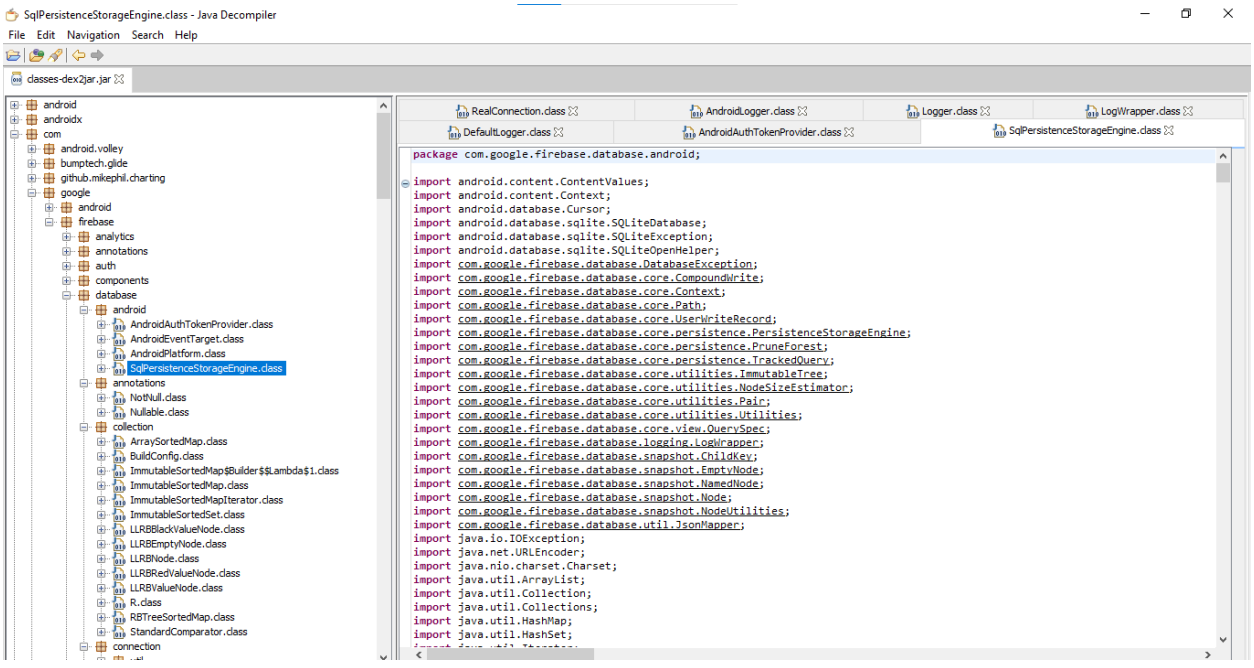


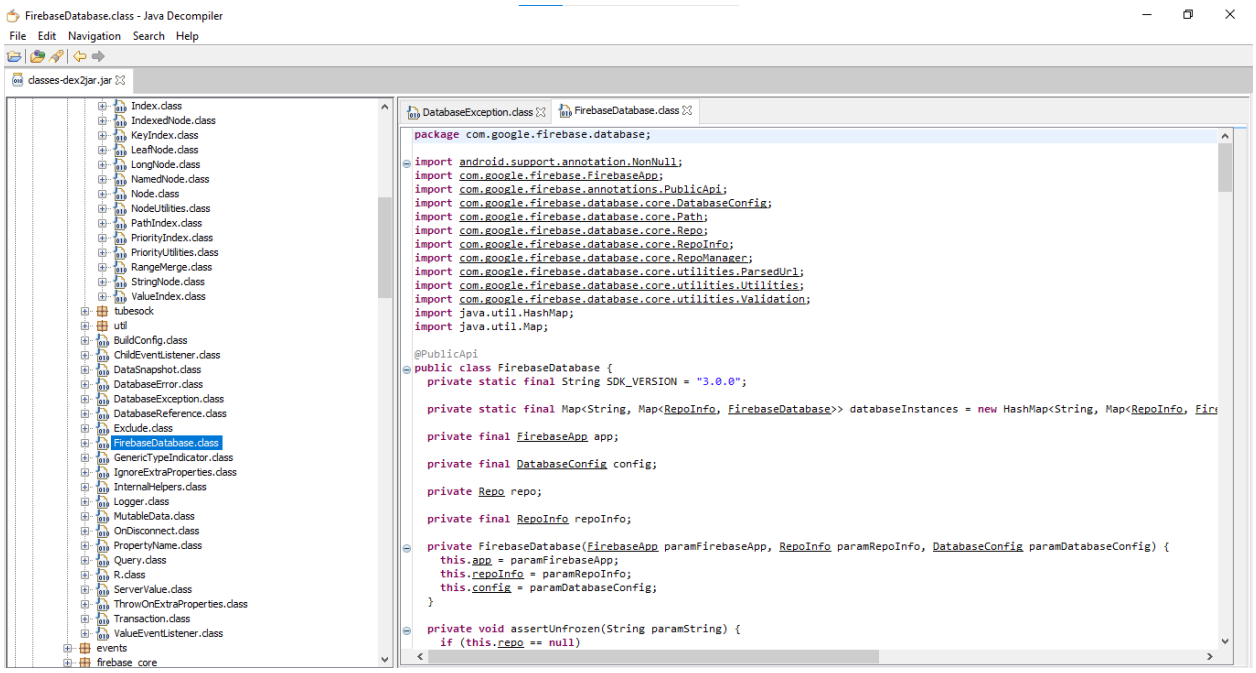
- Step – 6: Then open jd-gui.



- Step – 7: We can see all the file present in this app.





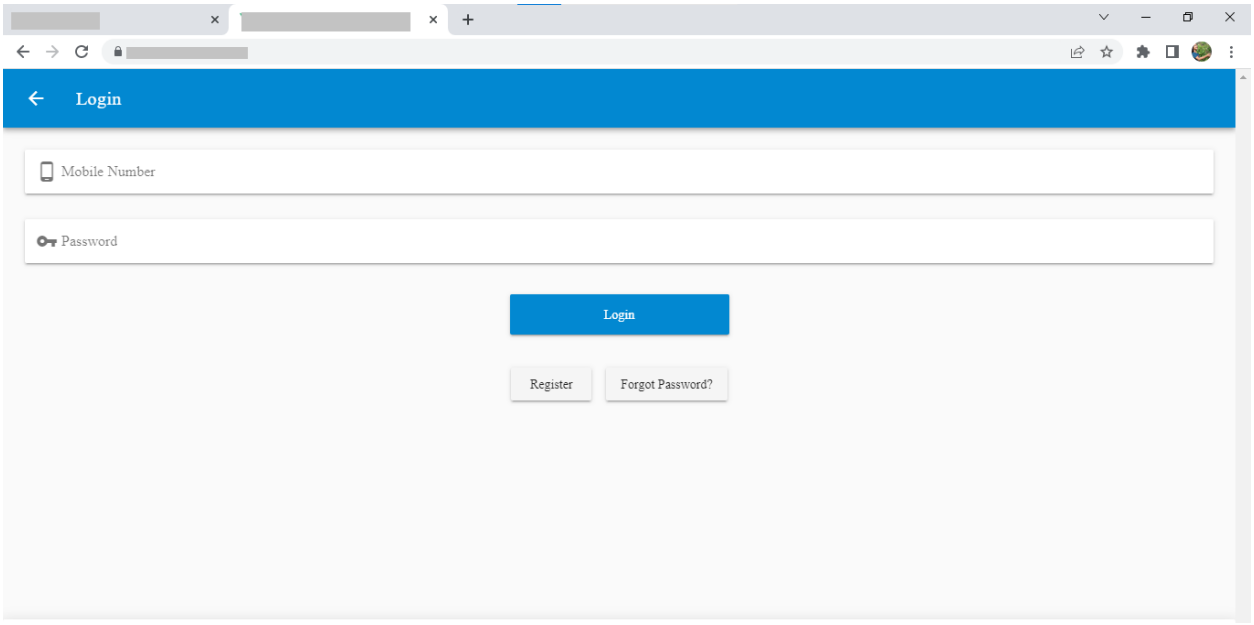


Observation

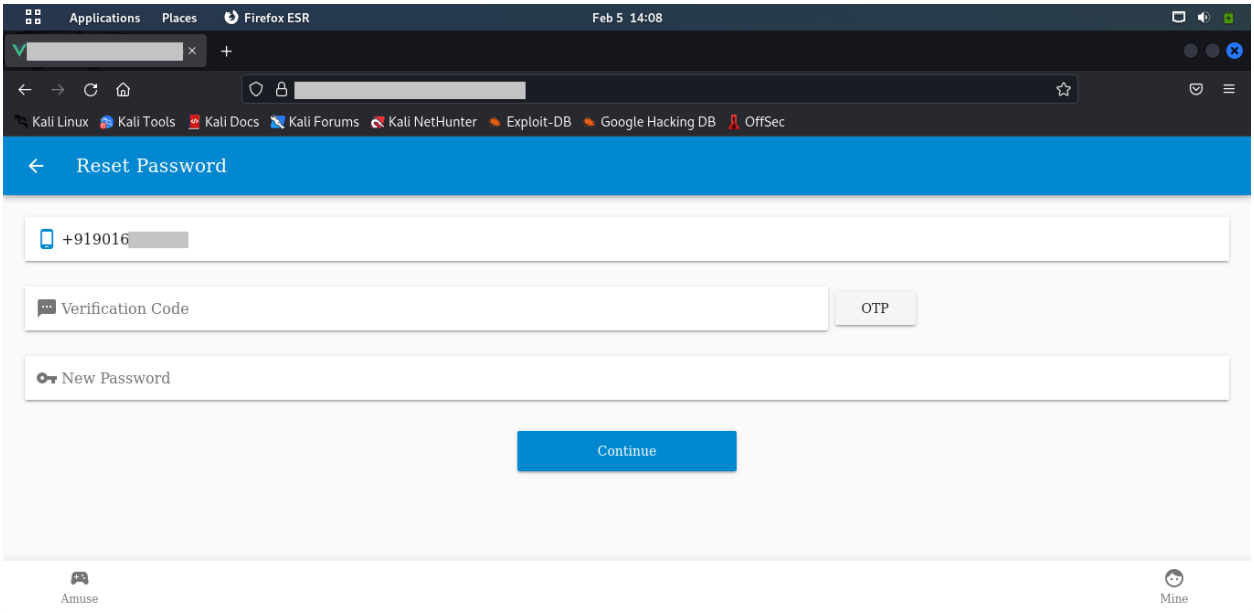
Reverse engineering involves analyzing the code of a product or system, understanding its underlying technology, identifying patterns, and testing for vulnerabilities. It requires technical expertise, analytical skills, and attention to detail. The goal is to ensure the security of software and systems.

Sr. No. Title	
02	
Description	
OTP BYPASSING (BRUTE FORCE)	
Affected Resource / Parameter	**Severity**
https://colorwiz.in/#/login	**HIGH**
Impact / Consequences	
Unauthorized access to any User account.	
Recommendations	
The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator.	
Tools Used	**References**
Burp-suit	https://portswigger.net/burp/communitydownload
CWE	**OWASP Top 10**
307	-
Proof of Vulnerability	

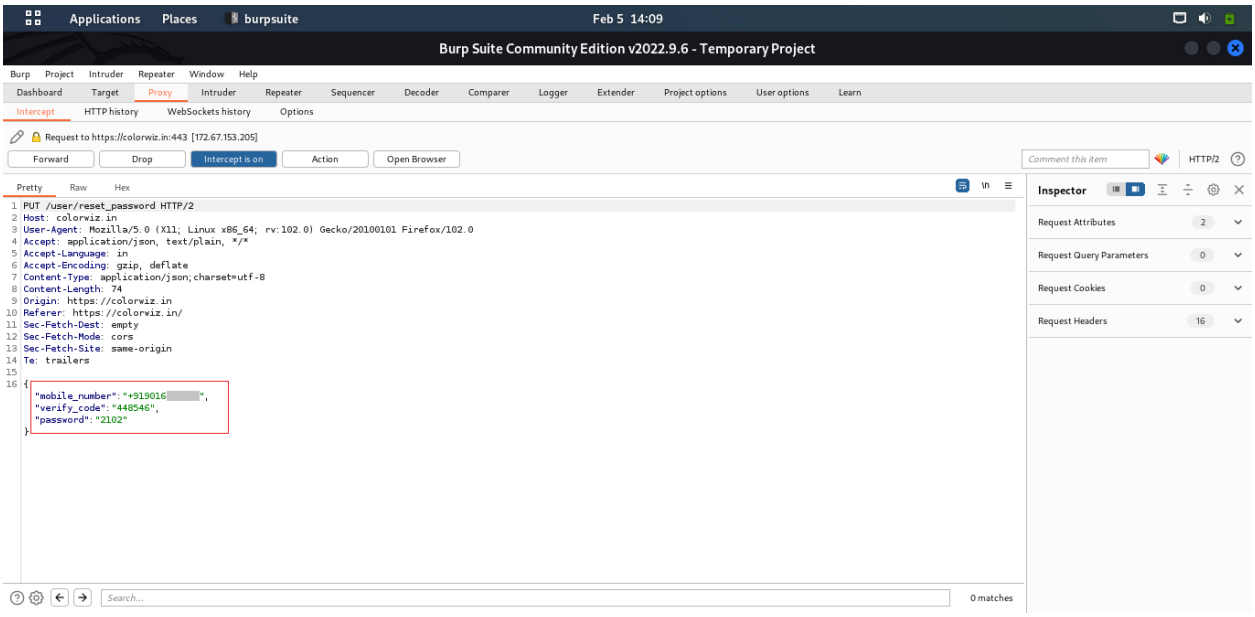
- Step – 1: Visit



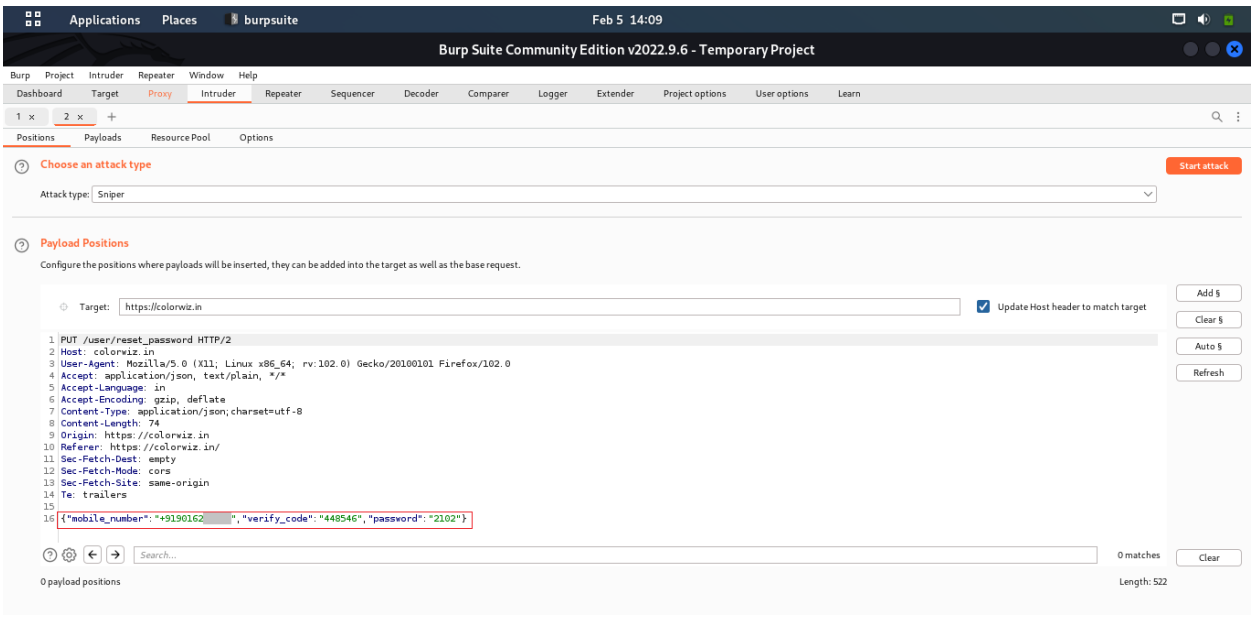
- Step – 2: Enter Phone Number and Click on OTP



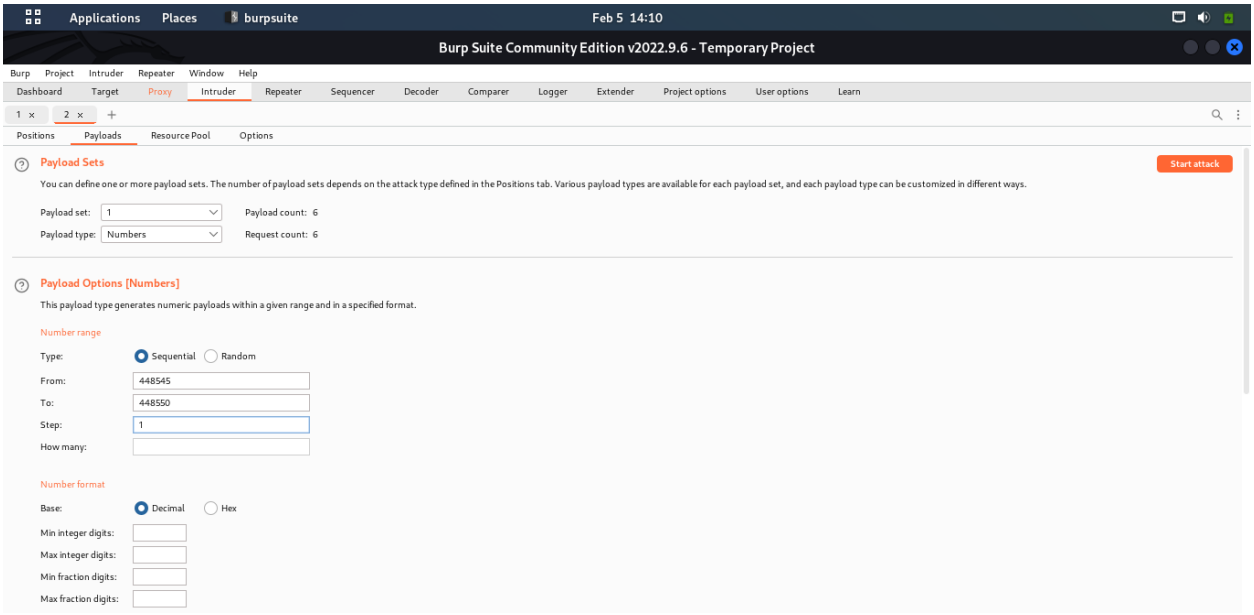
- Step – 3: It Requires 6 Digit of OTP An attacker can also bypass this using response manipulation that will uses in the coming steps.
- Step – 4: After we get this response



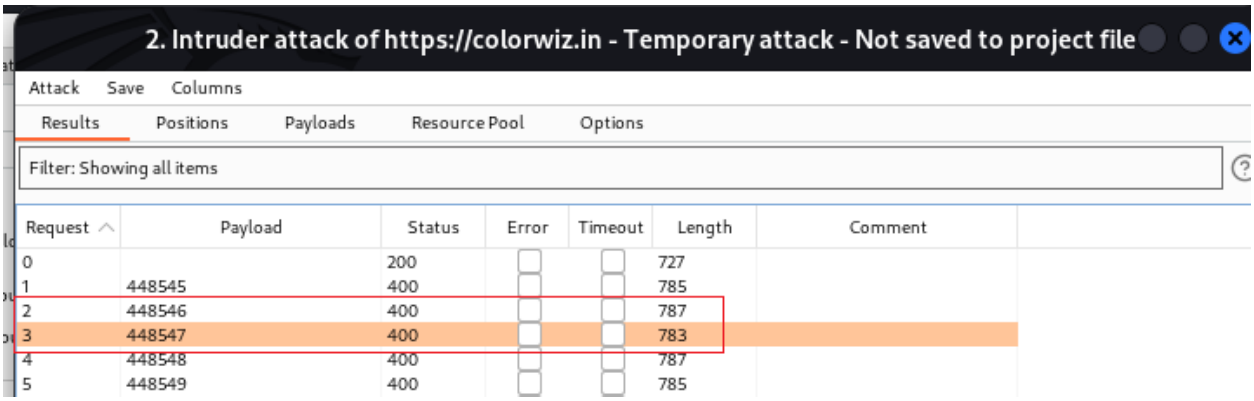
- Step – 5: In this we can see that there is a parameter “verify code” in this code there is a code there we enter incorrect code



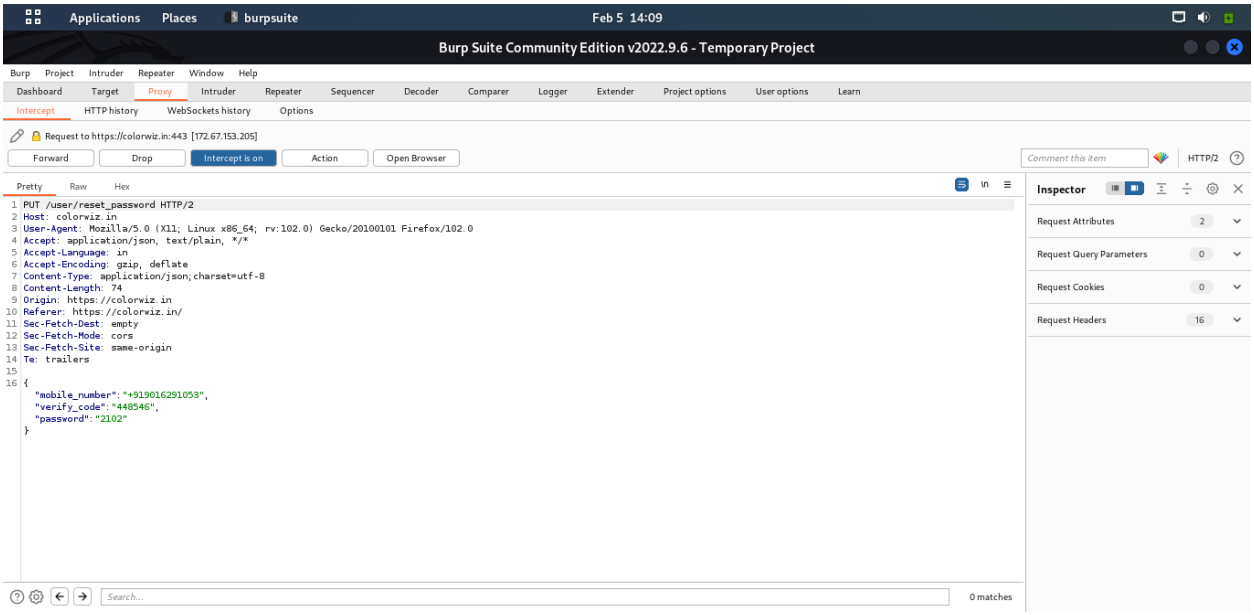
- Step – 6: I send this in the Intruder and put payload of six digit and start attack



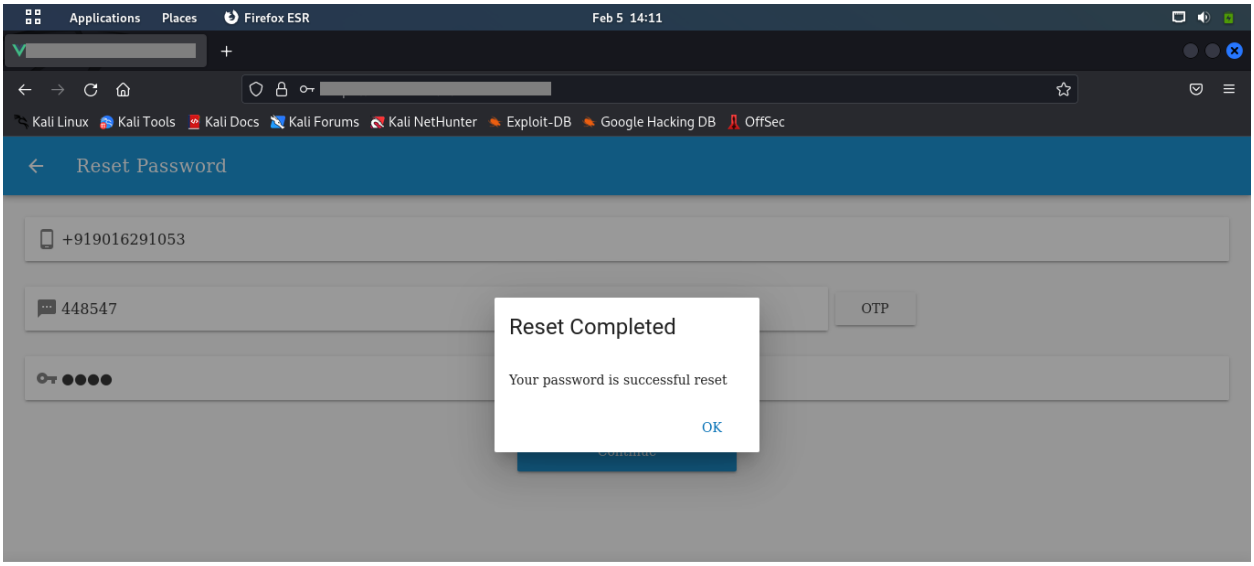
- Step – 7: In this we get result there is OTP ******



- Step – 8: I put this OTP in the parameter verify code and manipulate this and press Forward



- Result: Here password has been reset successful.



Observation
Brute force attacks are used to break through security measures so they can reach the intended data target. While this may seem like something only hackers can use to their advantage, many security firms use brute force attacks to help test their clients'

Sr. No. Title	
03	
Description	
SQL INJECTION	
Affected Resource / Parameter	**Severity**
https://science-med.com	**HIGH**

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!!

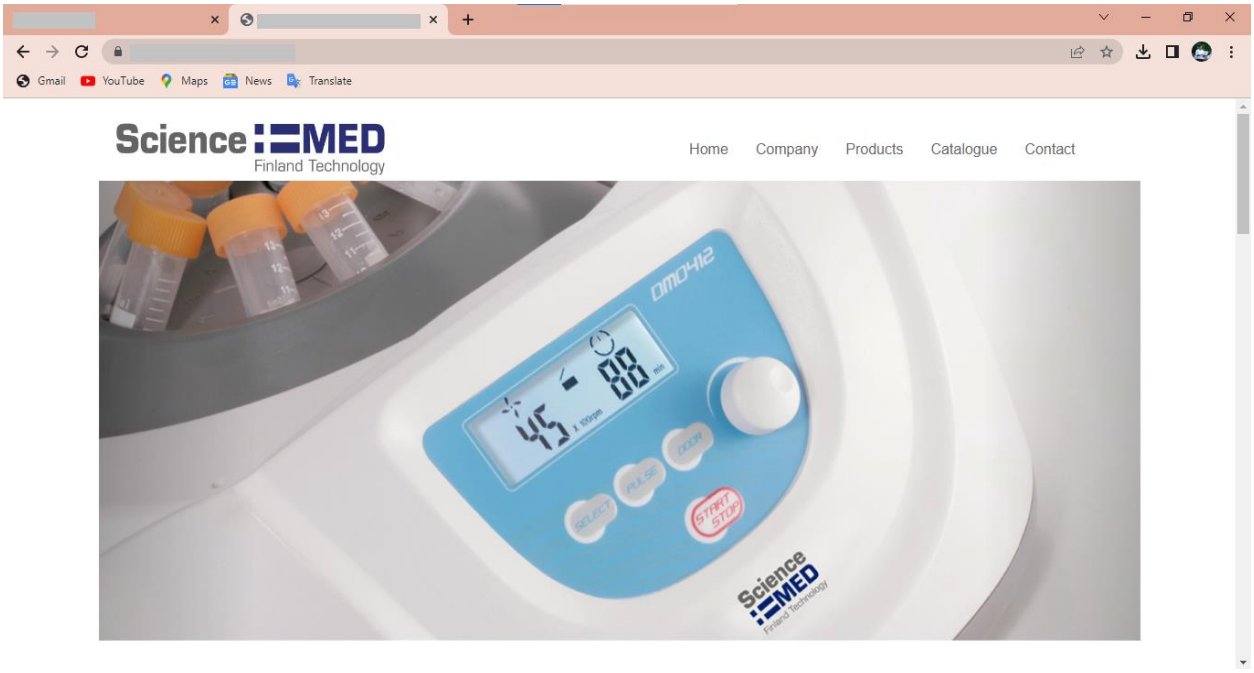
Recommendations

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.

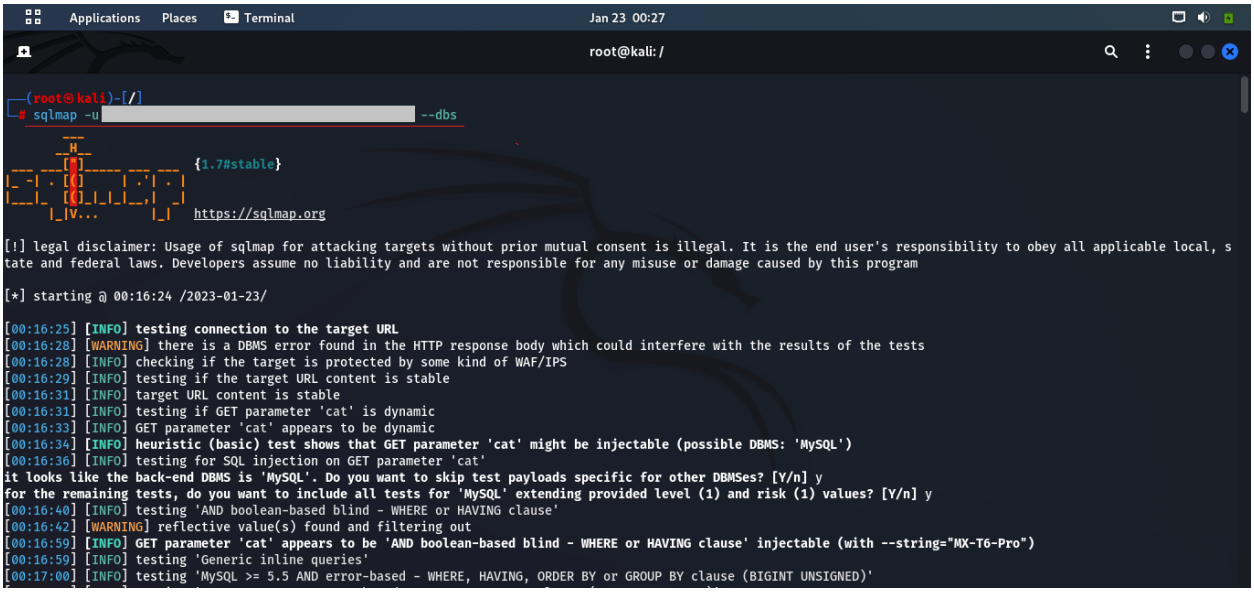
Tools Used	References
Sqlmap	https://sqlmap.org/
CWE	**OWASP Top 10**
89	WSTG-INPV-05

Proof of Vulnerability

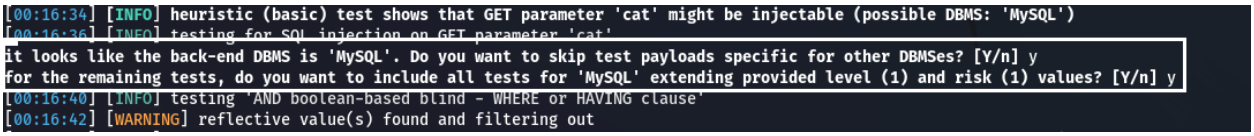
- Step – 1: Visit:



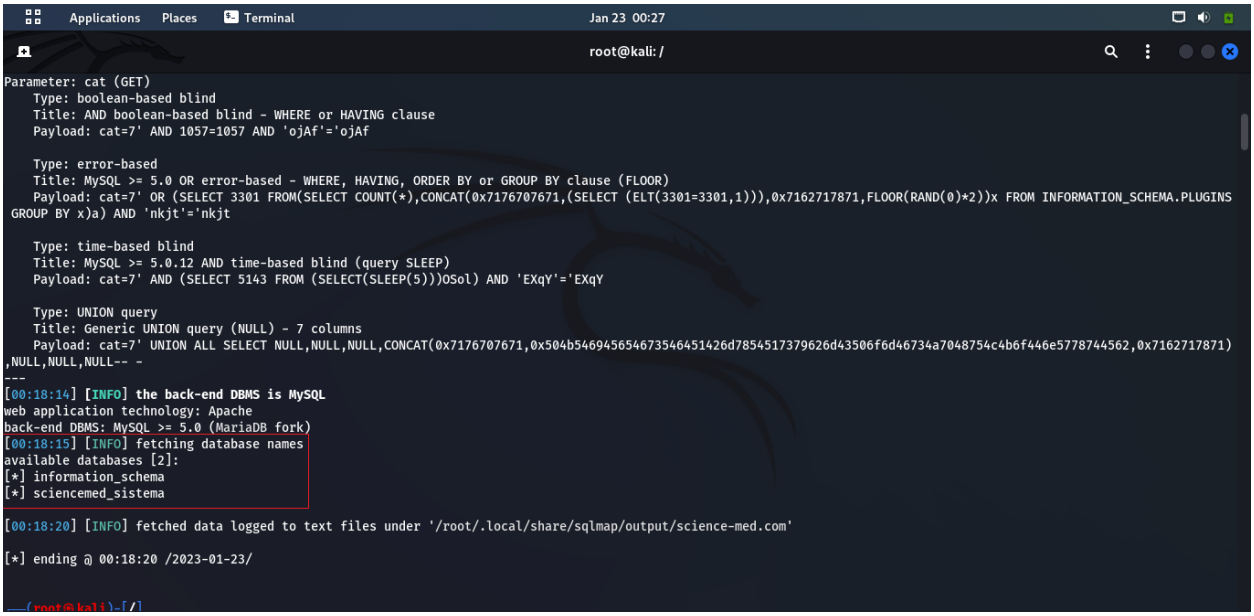
- Step – 2: use SQLMap tool in kali Linux and put –u for URL and provide URL and then use –dbs. for getting the database control and use –risk 1 for increasing the risk level.



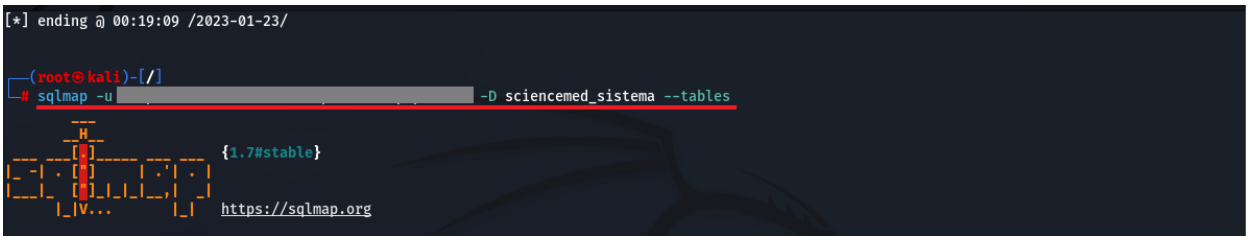
- Step – 3: here you can see that we founded the backend database is MySQL It asks you want to use MySQL payload then put y for 'yes' and it will ask for increase the risk level and put again y for 'yes'



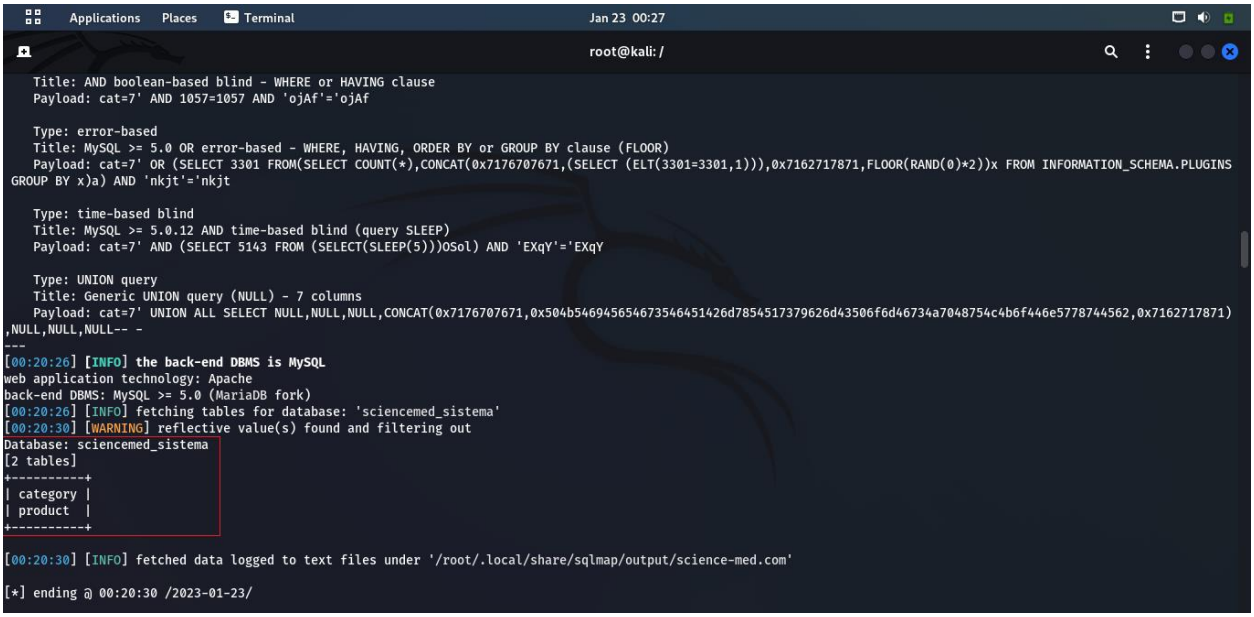
- Step – 4: After this we get this response and, we get the Database name.



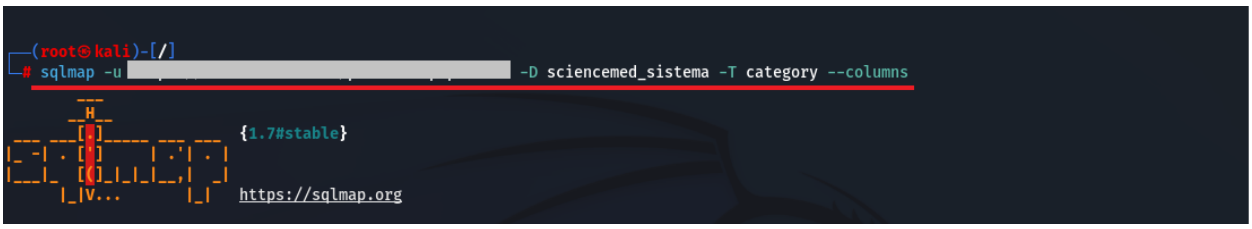
- Step – 5: After getting the database name use –tables in command for retrieve all the tables name.



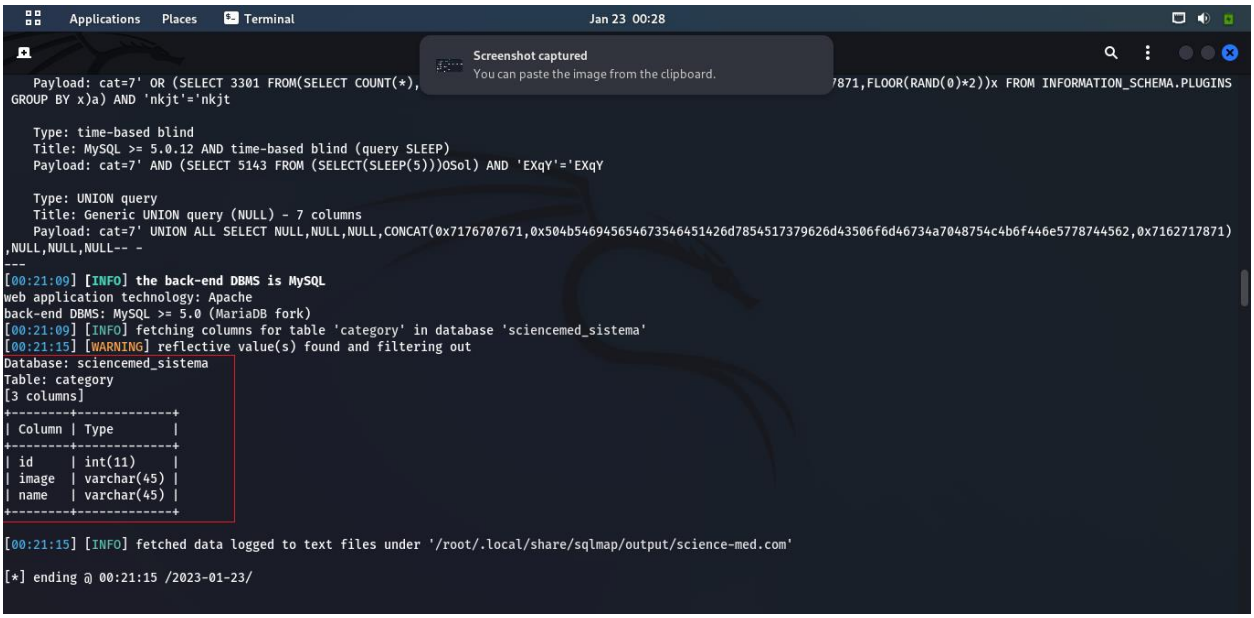
- Step – 6: As a result, we able to retrieve all the tables name and also access the table data of database.



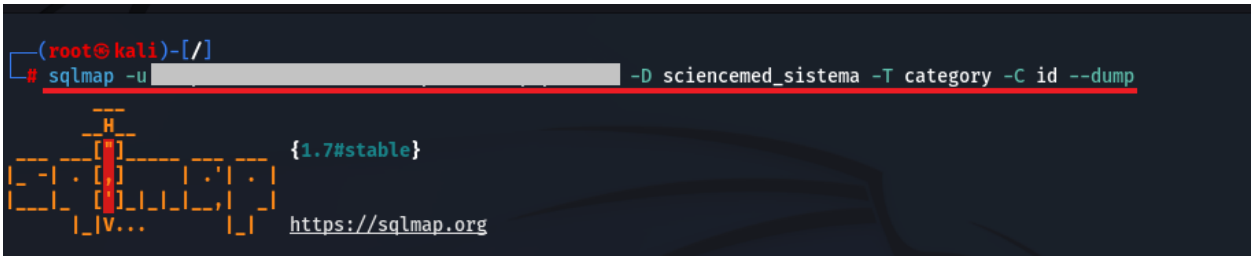
- Step – 7: find out h column of those tables using – column command.



- Step – 8: As a result of that –column command is like.



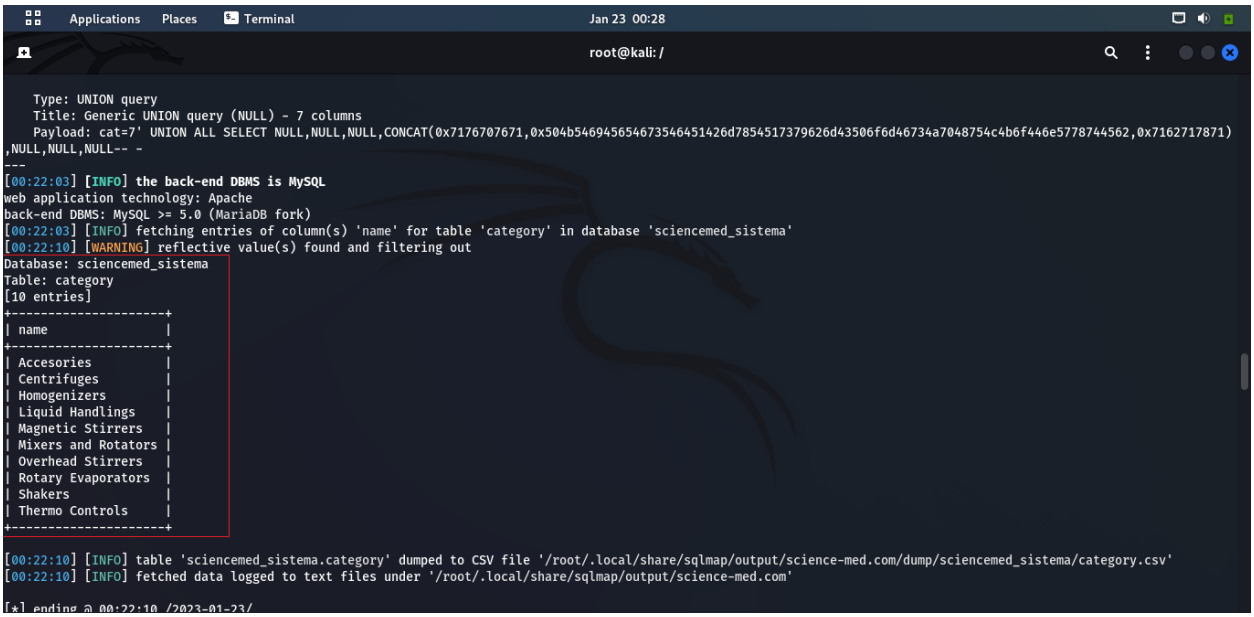
- Step – 9: After getting the column of that table use – dump for retrieve the data of that table.



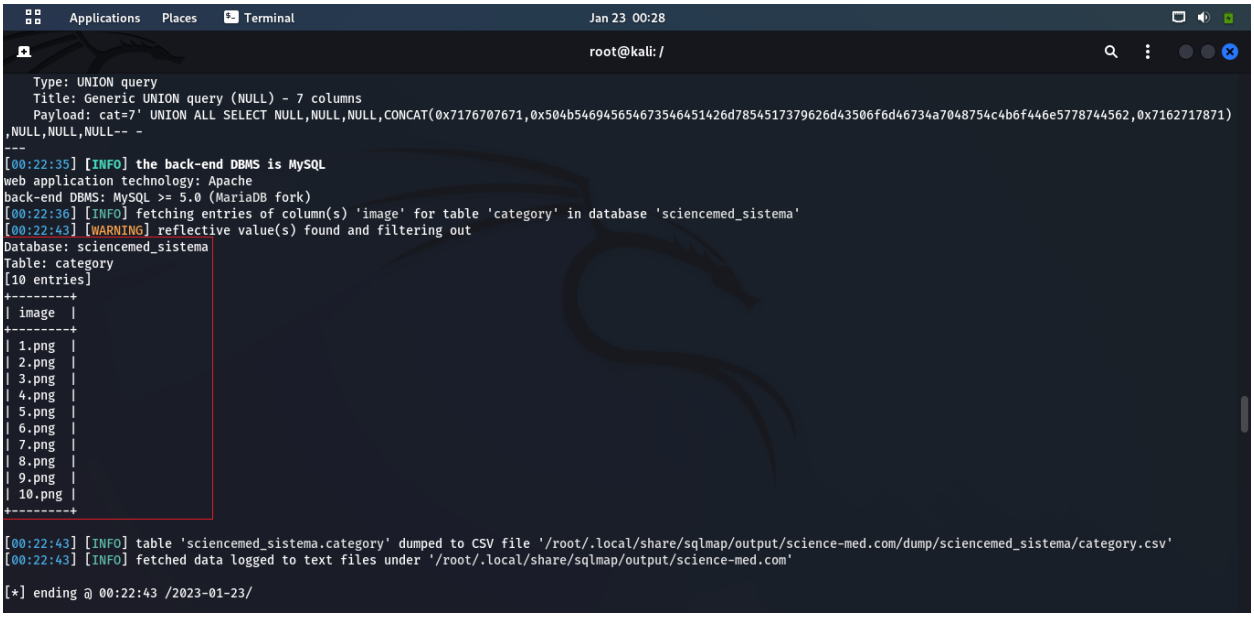
- Result: As a result of this injection, we found the data of those table.

  ✓ Id:

  ✓ Name:



✓ Image:

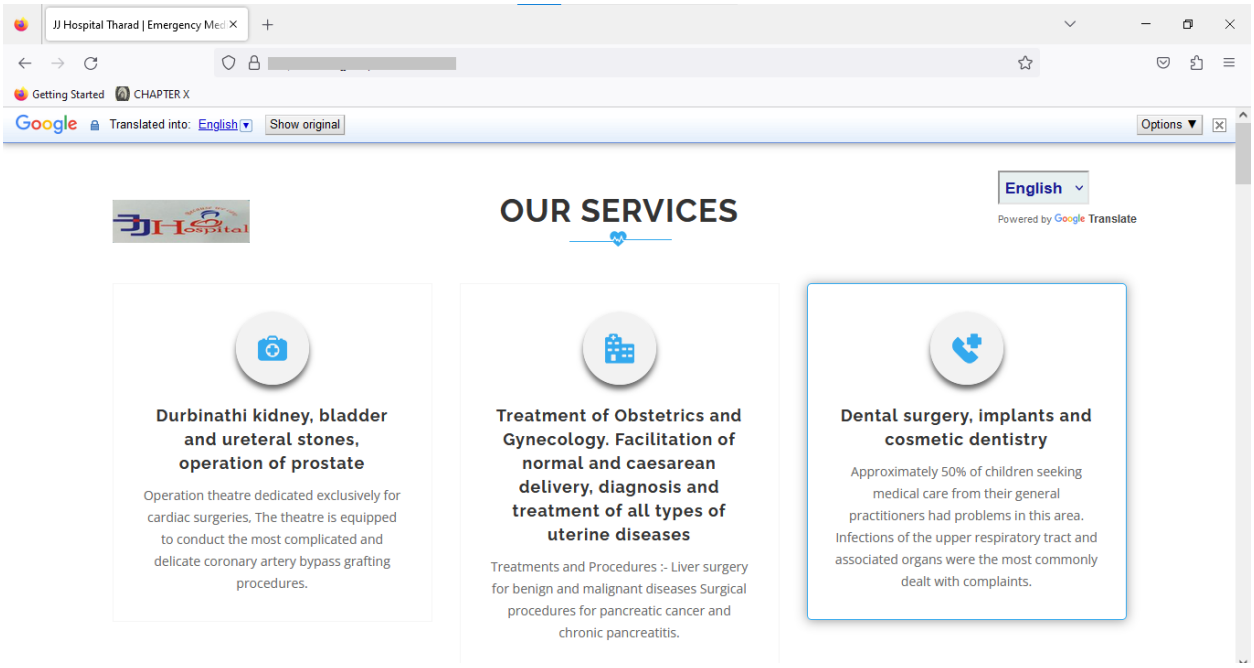


Observation

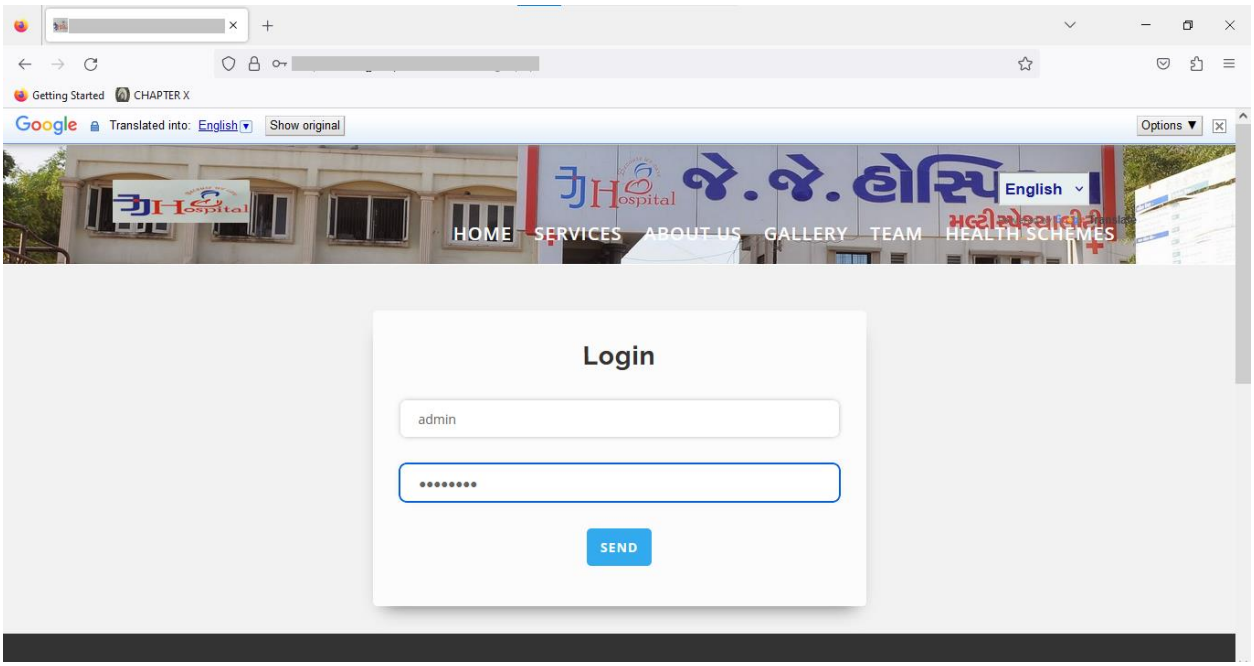
It was observed that a SQL injection attack consists of the insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration 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 effect the execution of predefined SQL commands. It is observed that the username attribute is vulnerable to SQL injection.

Sr. No. Title	
04	
Description	
Clear text Transmission of Sensitive Information	
Affected Resource / Parameter	**Severity**
https://www.jjhospitaltharad.com/login.php	**HIGH**
Impact / Consequences	
Once the attacker knows the credentials of the victim, an attacker can be able to access victim's 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	-
Proof of Vulnerability	

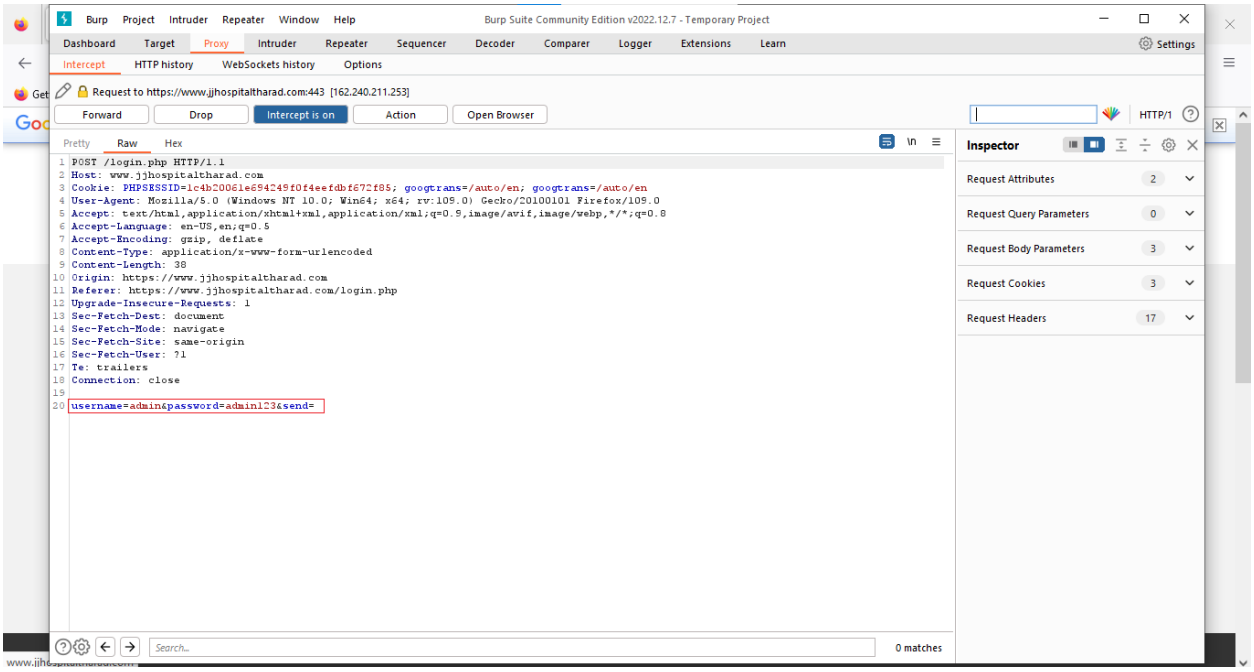
- Step 1: visit:



- Step 2: Enter Username and Password:



- Step – 3: Now using burp suite we can see the username and password clearly.

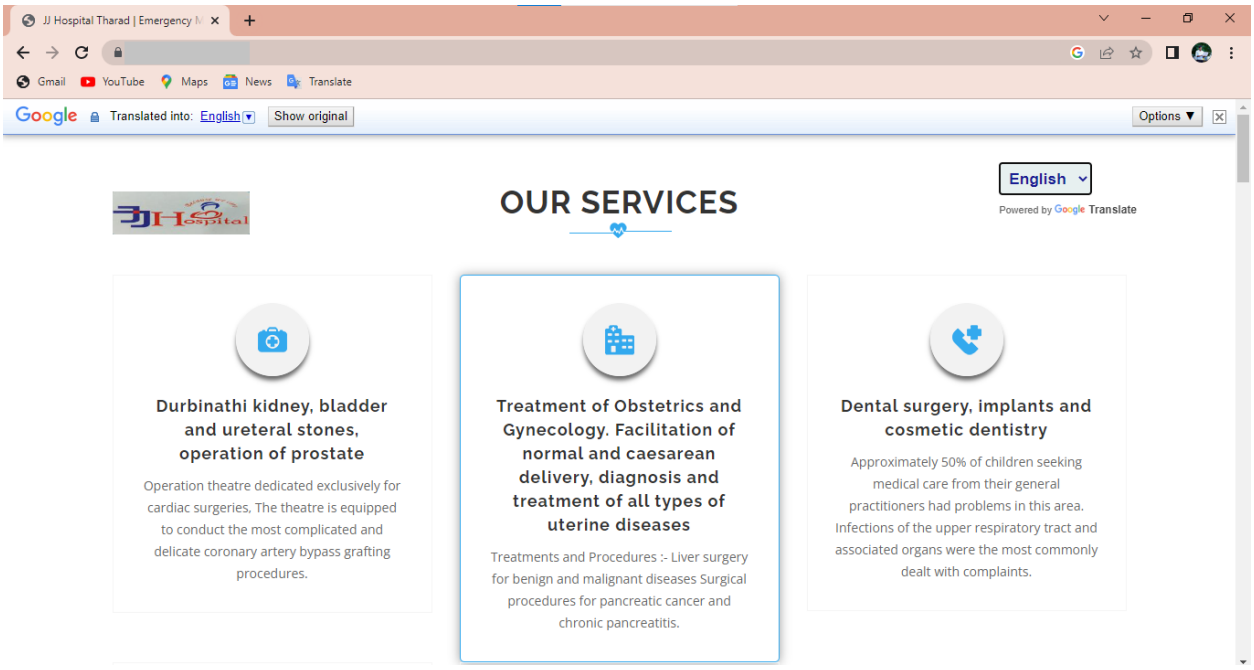


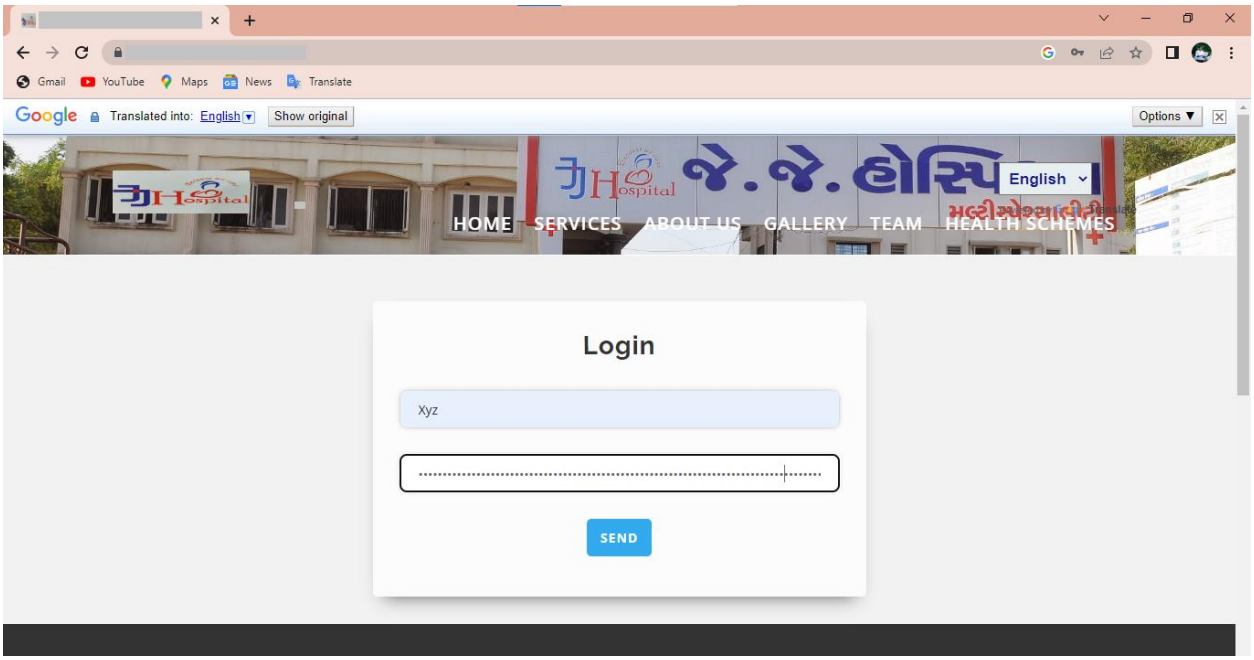
Observation

It was observed that application transmits sensitive or security-critical data in clear text 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. Common defences such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack.

Sr. No. Title	
05	
Description	
No Rate Limit on Current Password Field	
Affected Resource / Parameter	**Severity**
https://www.jjhospitaltharad.com/login.php	**HIGH**
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**
-	-
CWE	**OWASP Top 10**
307	-
Proof of Vulnerability	

- Step 1: visit:


JJ Hospital Tharad | Emergency
Gmail
YouTube
Maps
News
Translate
Google
Translated into: English
Show original
Options
English
Powered by Google Translate
OUR SERVICES
Durbinathi kidney, bladder and ureteral stones, operation of prostate
Operation theatre dedicated exclusively for cardiac surgeries, The theatre is equipped to conduct the most complicated and delicate coronary artery bypass grafting procedures.
Treatment of Obstetrics and Gynecology. Facilitation of normal and caesarean delivery, diagnosis and treatment of all types of uterine diseases
Treatments and Procedures :- Liver surgery for benign and malignant diseases Surgical procedures for pancreatic cancer and chronic pancreatitis.
Dental surgery, implants and cosmetic dentistry
Approximately 50% of children seeking medical care from their general practitioners had problems in this area. Infections of the upper respiratory tract and associated organs were the most commonly dealt with complaints.


Gmail
YouTube
Maps
News
Translate
Google
Translated into: English
Show original
Options
English
HOME
SERVICES
ABOUT US
GALLERY
TEAM
HEALTH SCHEMES
Login
Xyz
SEND

Observation
They protect your electronic accounts and devices from unauthorized access, keeping your sensitive personal information safe. The more complex the password, the more protected your information will be from cyber threats and hackers.

Sr. No. Title	
06	
Description	
Html Injection	
Affected Resource / Parameter	**Severity**
https://kubbair.com/blog_details.php?blog_id=9	**MEDIUM**

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.

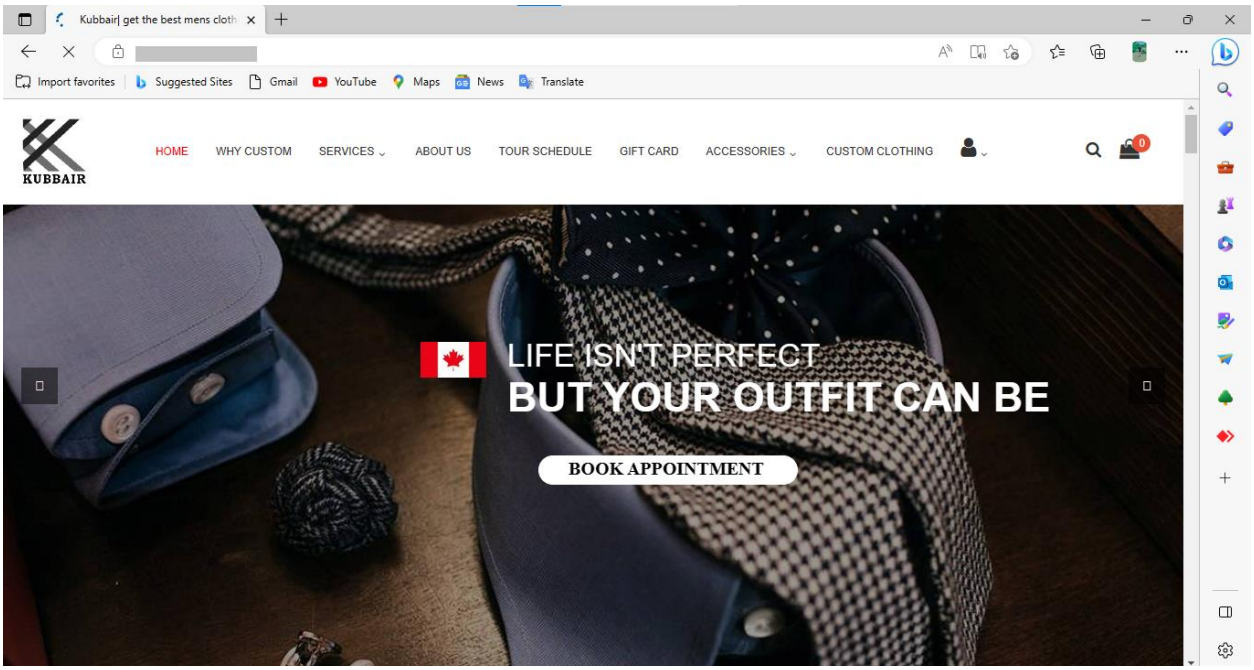
•Use the proper sanitizer the input fields.

Ex. You can use mysqli_real_escape_string function at database side.

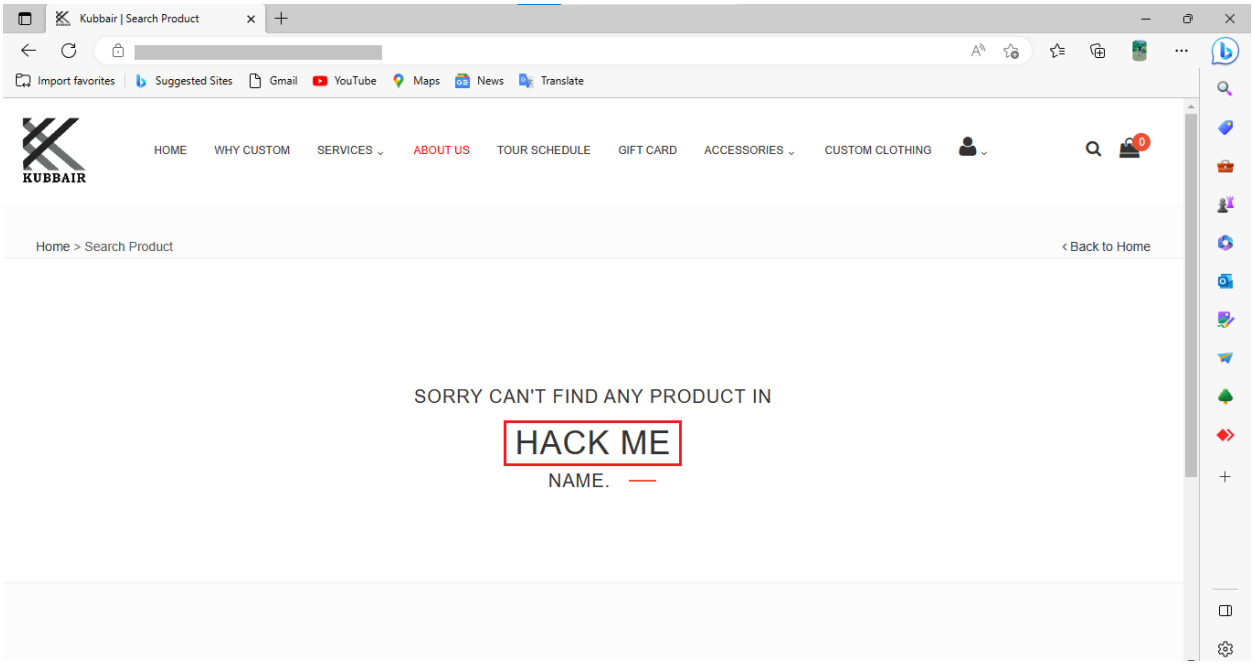
Tools Used	References
-	-
CWE	**OWASP Top 10**
644	WSTG-INPV-17

Proof of Vulnerability

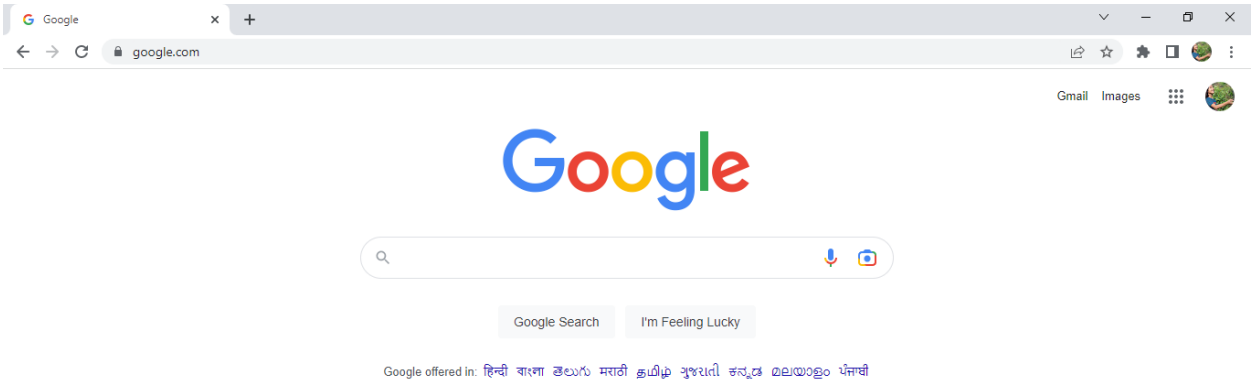
- Step – 1: Visit:



- Step – 2: Try To inject HTML code in to the id parameter. Here we use <a> tag for referring an URL .
- Step – 3: Here whenever anyone click on the HACK ME, he will be redirect to the google.com Because In code we injectHACK ME



- Result: As a result, when anyone click on this HACK ME He will be redirect to the google.com.



- If attacker provide the URL of his own site and he can steal the data of users who fill those form.

Observation
Many application developers did not realize that the HTTP host header is accessible and controllable by all users. In an application security perspective, the input given by the user is always deceivable, and it is unsafe to trust.

Sr. No. Title	
07	
Description	
XSS (CROSS-SITE SCRIPTING)	
Affected Resource / Parameter	**Severity**
https://www.webloadmpstore.com/	**MEDIUM**

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.
- ✓ XSS can also impact a business's reputation. An attacker can deface a corporate website by altering its content, thereby damaging the company's image, or spreading misinformation

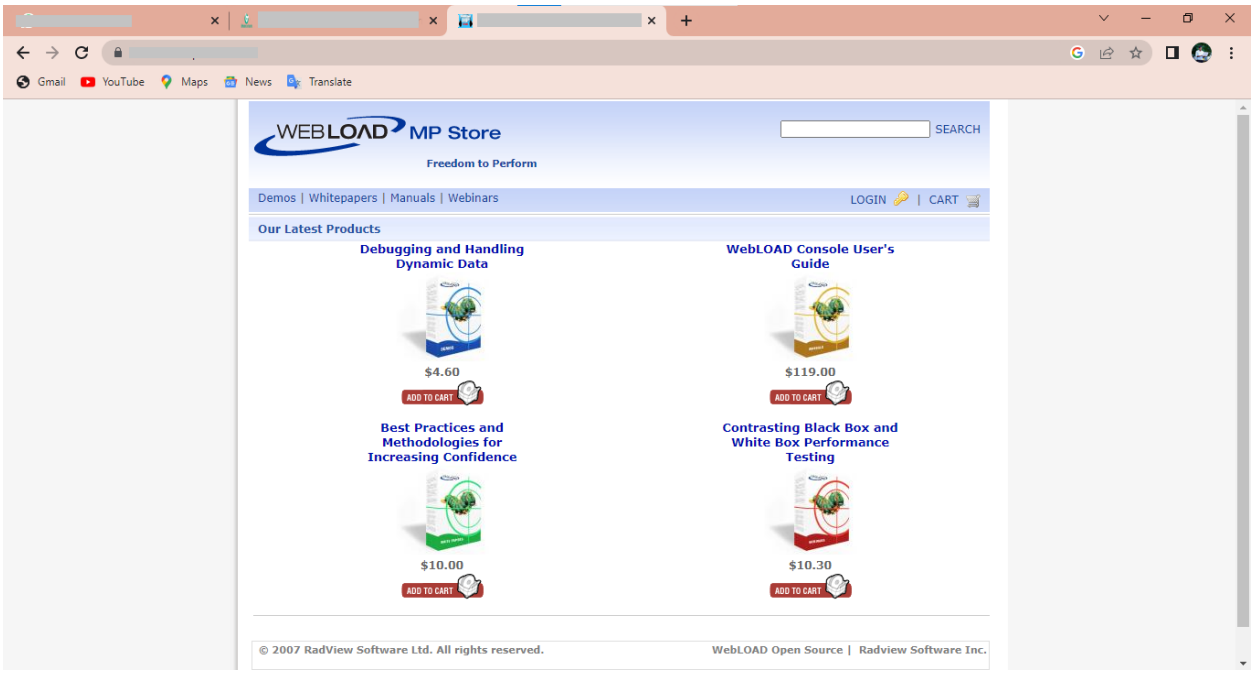
Recommendations

- ✓ 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.
- ✓ Use appropriate response headers. To prevent XSS in HTTP responses that are not intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
- ✓ Content Security Policy. As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

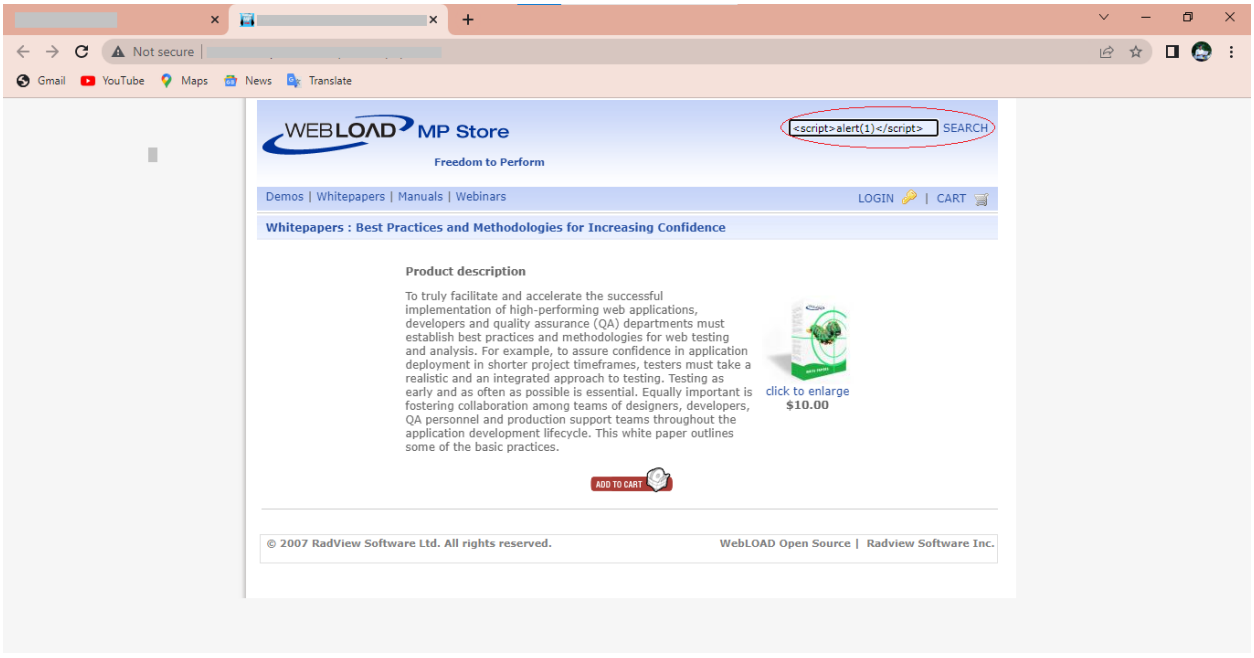
Tools Used	References
-	-
CWE	**OWASP Top 10**
79	WSTG-INPV-01

Proof of Vulnerability

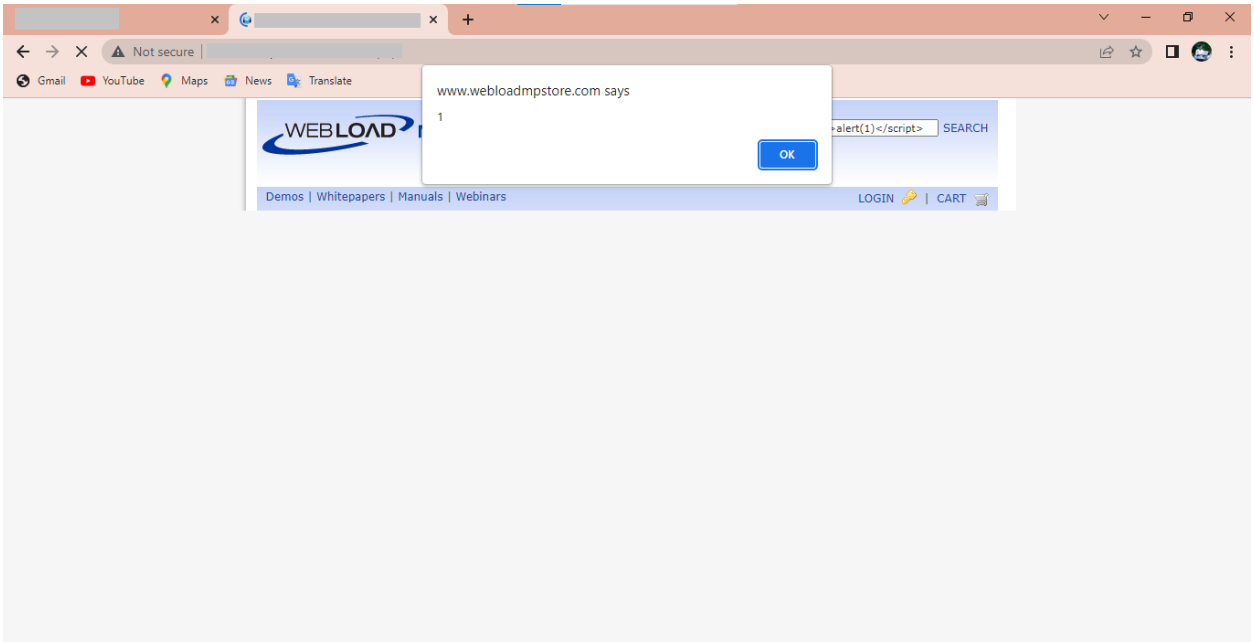
- Step – 1: Visit:



- Step – 2 :- Try To inject JavaScript in this URL in the id parameter like <script>alert(1)</script>



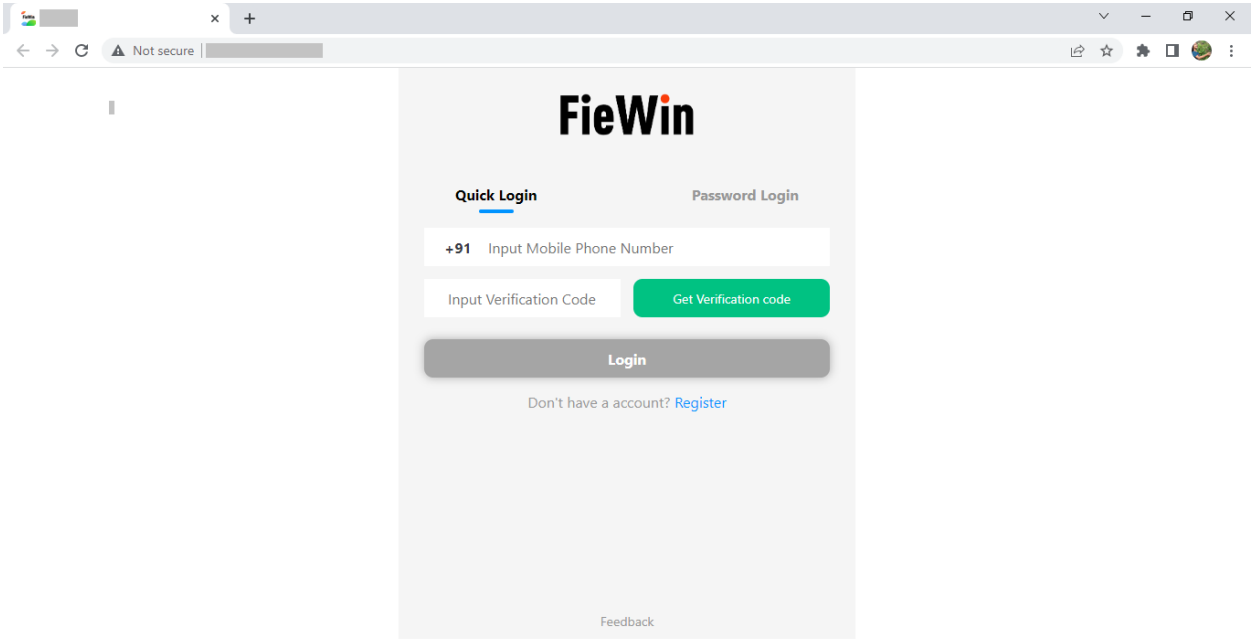
- Step – 3: - Result: After this we get a pop up and with the content is (1) Which one I injected in the parameter. here we can also modify and use document. Cookie for etc. the cookie of the user, document. Location for getting location, etc.



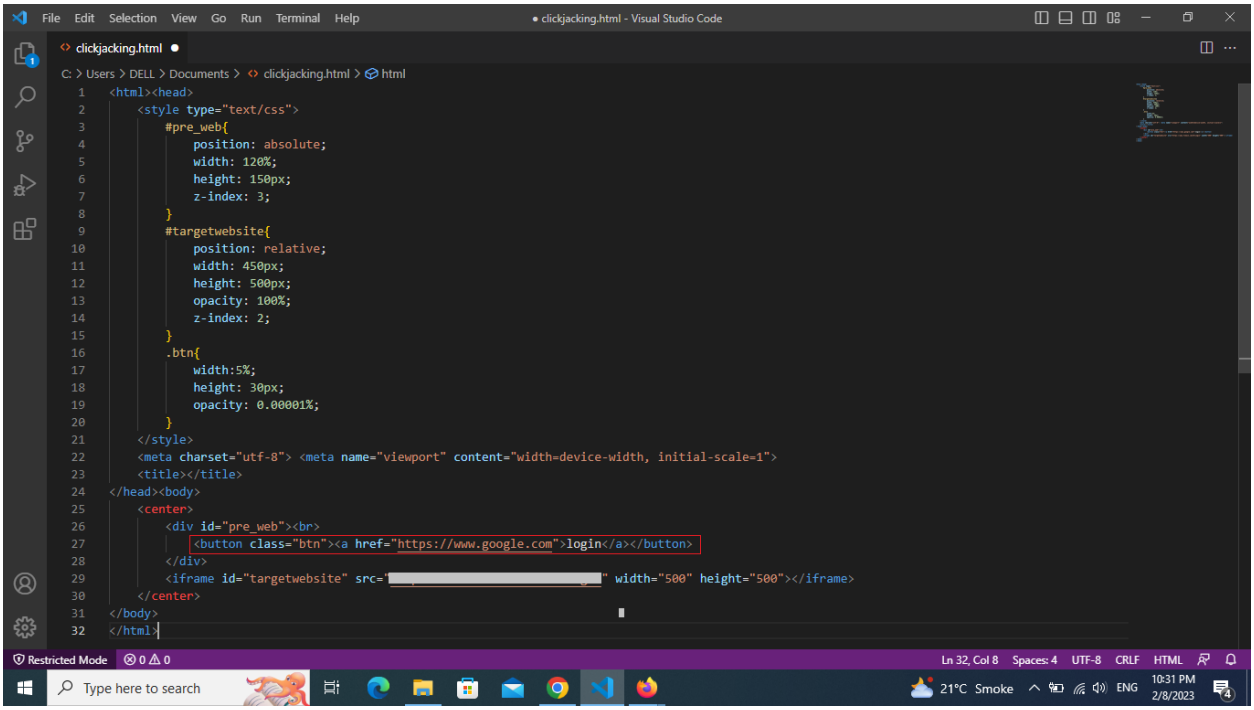
Observation
It was observed that the website is missing X-XSS-Protection which means that the website may be at risk of Cross-site Scripting (XSS) attacks. The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.

Sr. No. Title	
08	
Description	
CLICK JACKING	
Affected Resource / Parameter	**Severity**
http://fiewin.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**
-	-
CWE	**OWASP Top 10**
1021	WSTG-CLNT-09
Proof of Vulnerability	

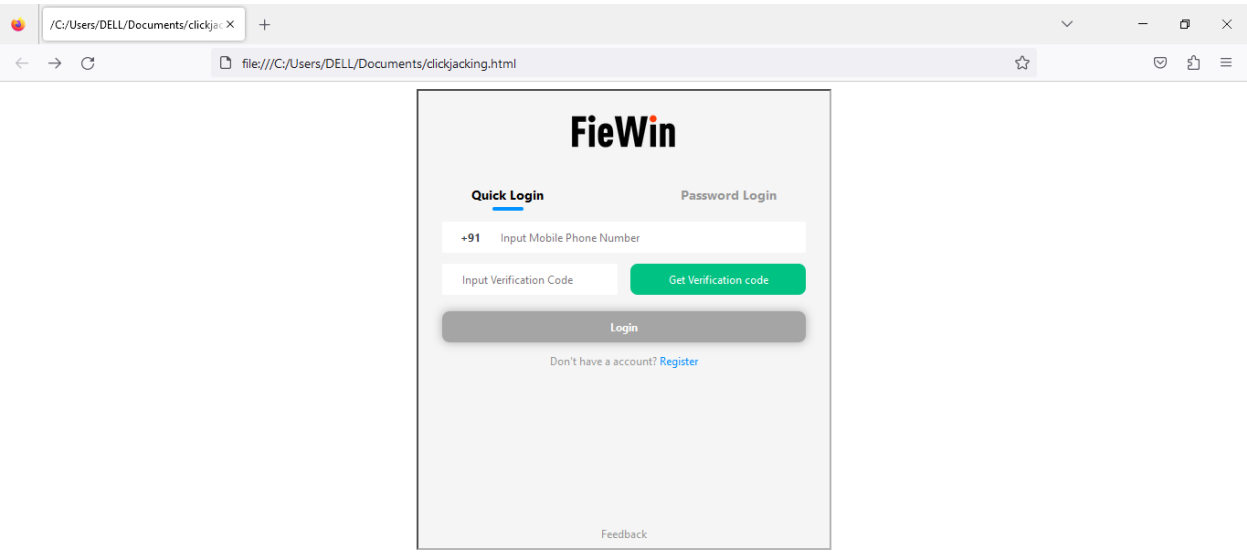
- Step – 1: Visit:



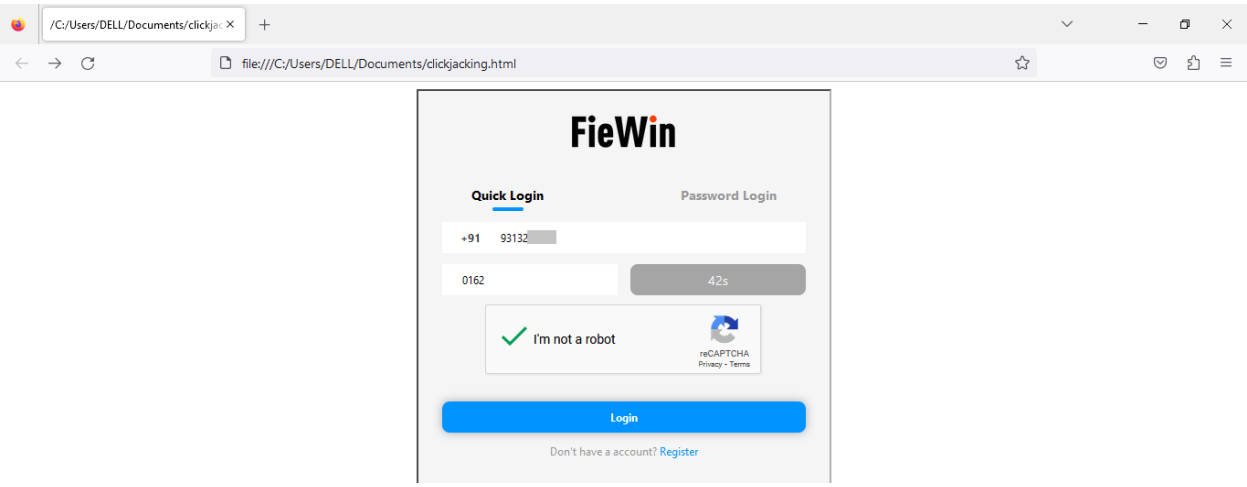
- Step – 2: Here enter the script like this



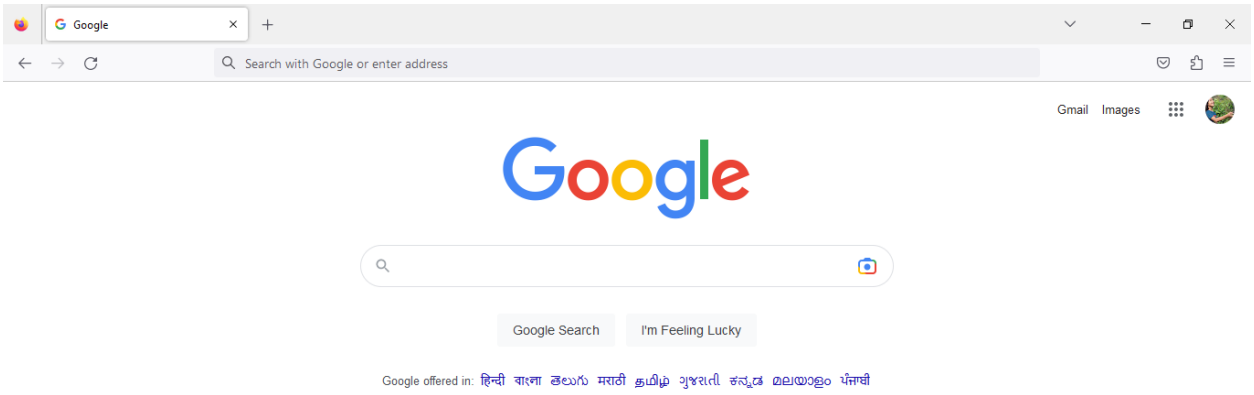
- Step – 3: after This script run it its looks like this because it is i-frame



- Step – 4: Here I click on Login after fill the form...



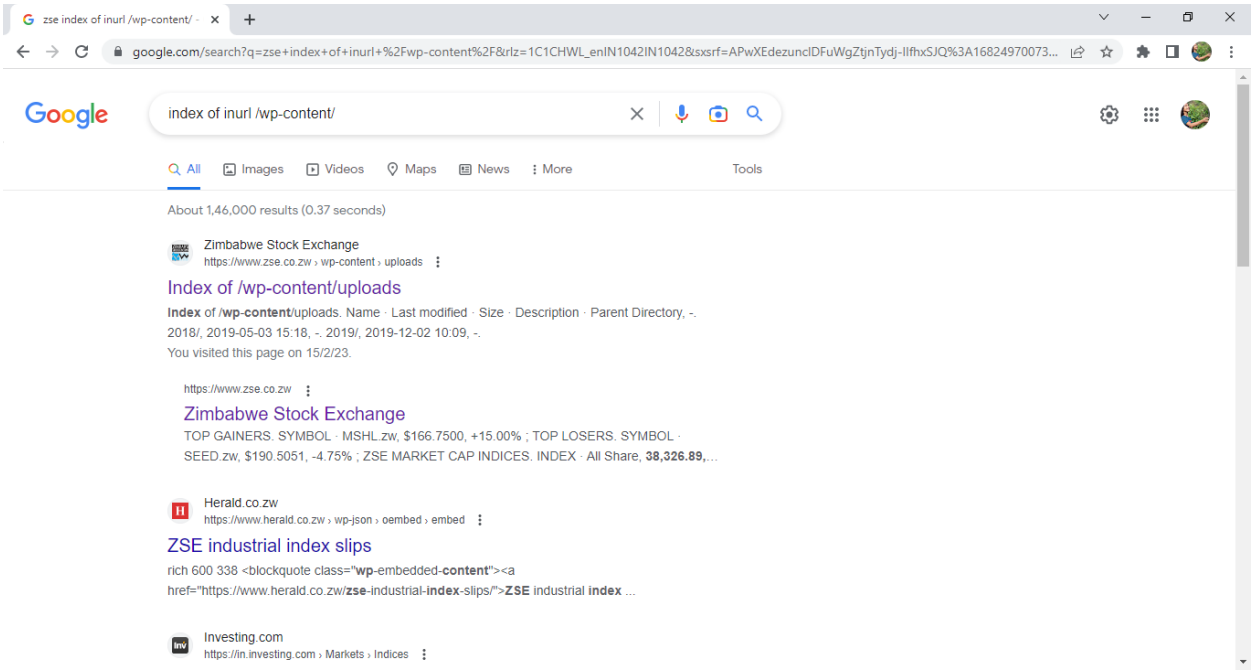
- Step – 5: after clicking on login, it will be redirect to the google because I written this in this script.



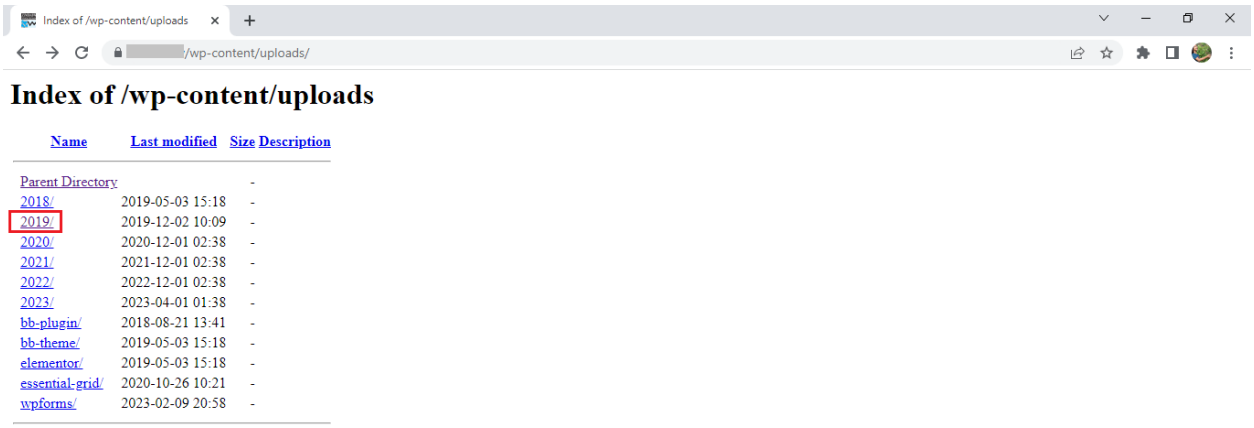
Observation
It was observed that the server didn't return an `X-Frame-Options` header which means that this website could be at risk of a click jacking attack. click jacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking 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. The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or I frame. Sites can use this to avoid click jacking attacks, by ensuring that their content is not embedded into other sites

Sr. No. Title	
09	
Description	
DIRECTORY TRAVERSAL	
Affected Resource / Parameter	**Severity**
https://www.zse.co.zw/	**MEDIUM**
Impact / Consequences	
An attacker can leverage a directory traversal vulnerability in the system to step out of the root directory, allowing them to access other parts of the file system to view restricted files and gather more information required to further compromise the system.	
Recommendations	
✓ The most effective way to prevent file path traversal vulnerabilities is to avoid passing user-supplied input to file system APIs altogether. Many application functions that do this can be rewritten to deliver the same behavior in a safer way. ✓ If it is considered unavoidable to pass user-supplied input to file system APIs, then two layers of defense should be used together to prevent attacks: ✓ The application should validate the user input before processing it. Ideally, the validation should compare against a whitelist of permitted values. If that is not possible for the required functionality, then the validation should verify that the input contains only permitted content, such as purely alphanumeric characters. After validating the supplied input, the application should append the input to the base directory and use a platform file system API to cannibalize the path. It should verify that the cannibalized path starts with the expected base directory.	
Tools Used	**References**
-	-
CWE	**OWASP Top 10**
22	WSTG-ATHZ-01
Proof of Vulnerability	

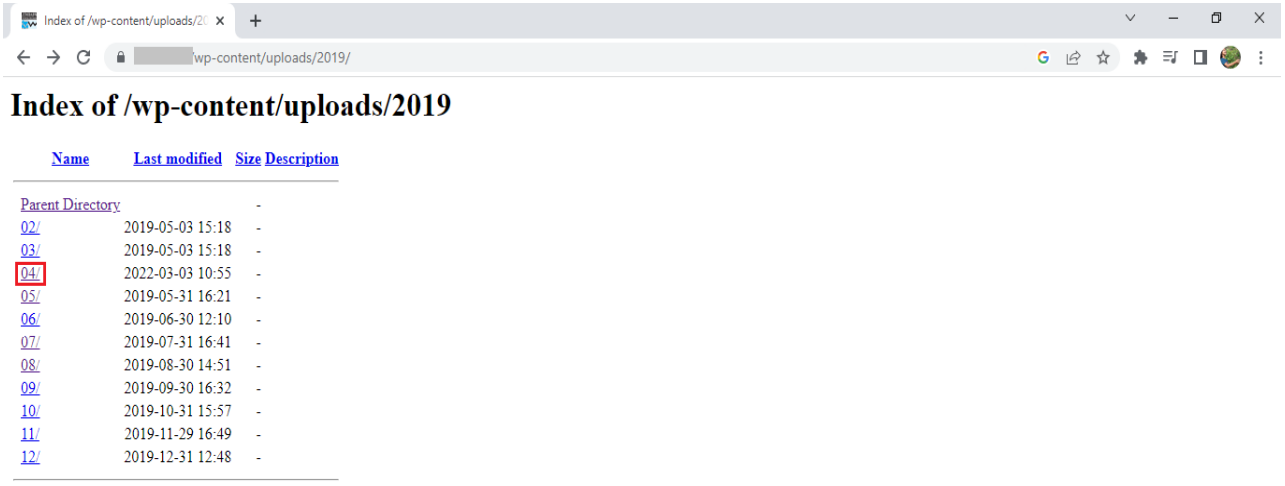
- Step 1: visit:



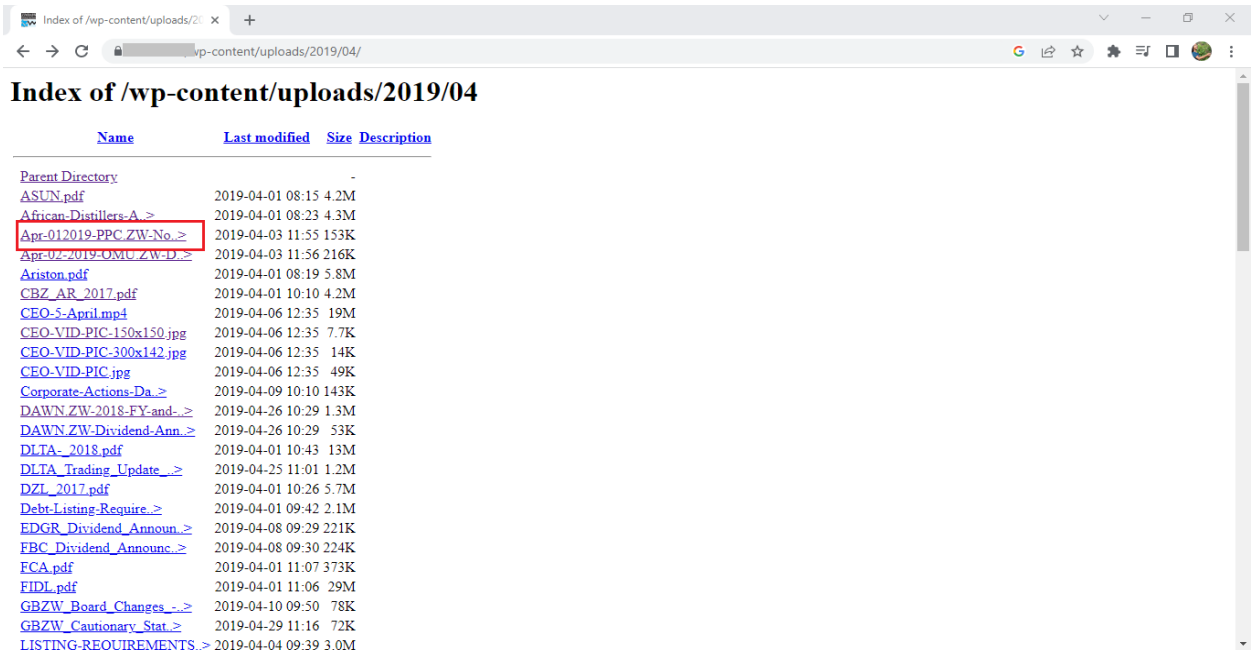
- Step 2 : Click any one directory. On clicking we can access all sub-directories of about directories.



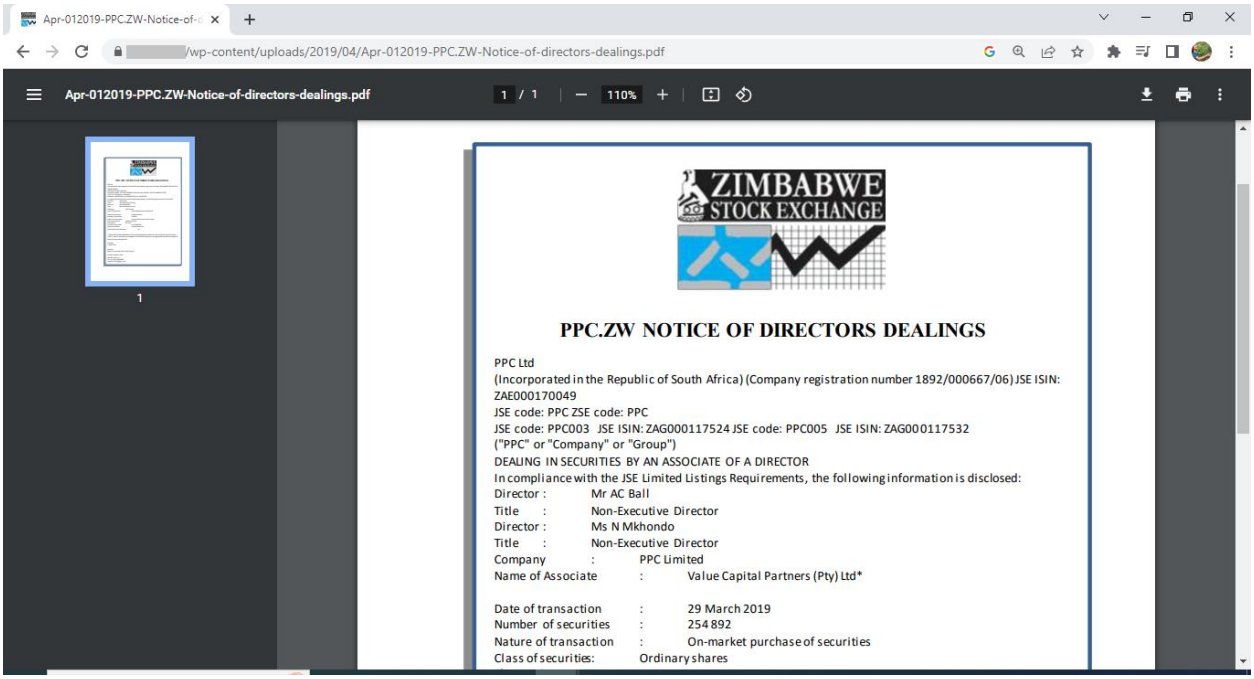
- Step 3: Here you can see the sub directories of about directory. You can select any one directory from the following. Here we have selected 04 directory.



- Step 4: Here you can see the all files like pdf or images which are in the 04 directory. You can open any of the given file. We have clicked on 2019-04-apr-012019-PPC.ZW-Notice-of-directors-dealings.pdf.



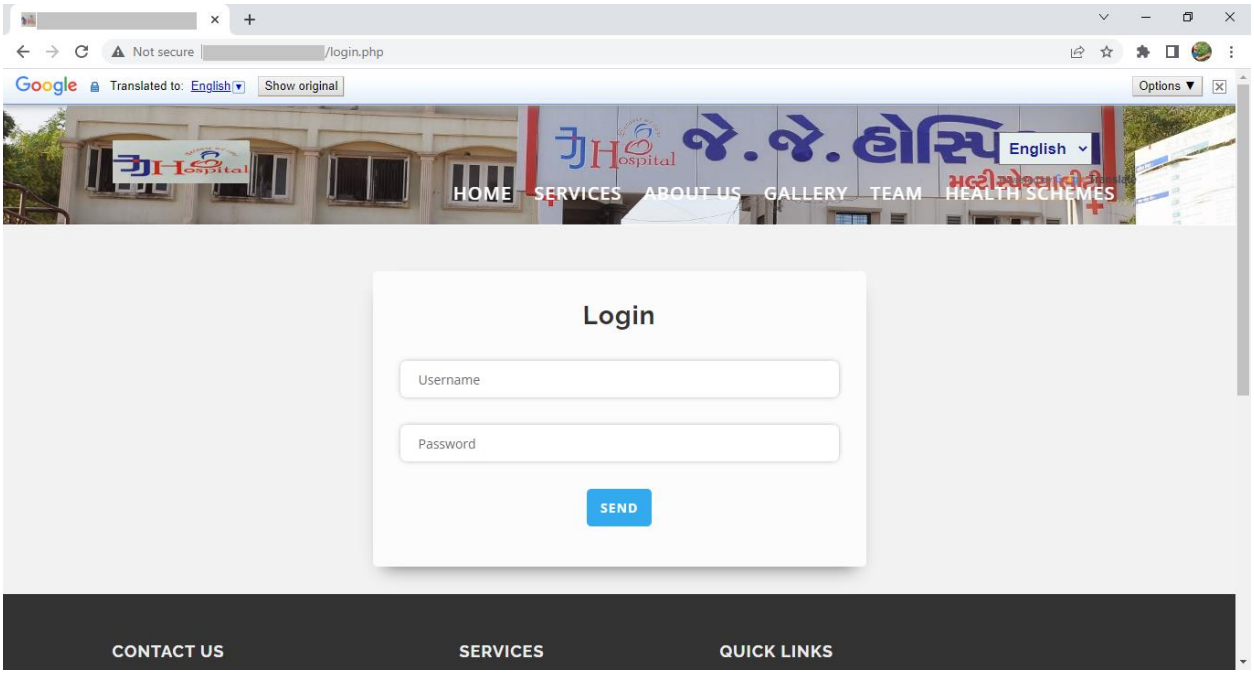
- Step 5: As a result, we can see the pdf.



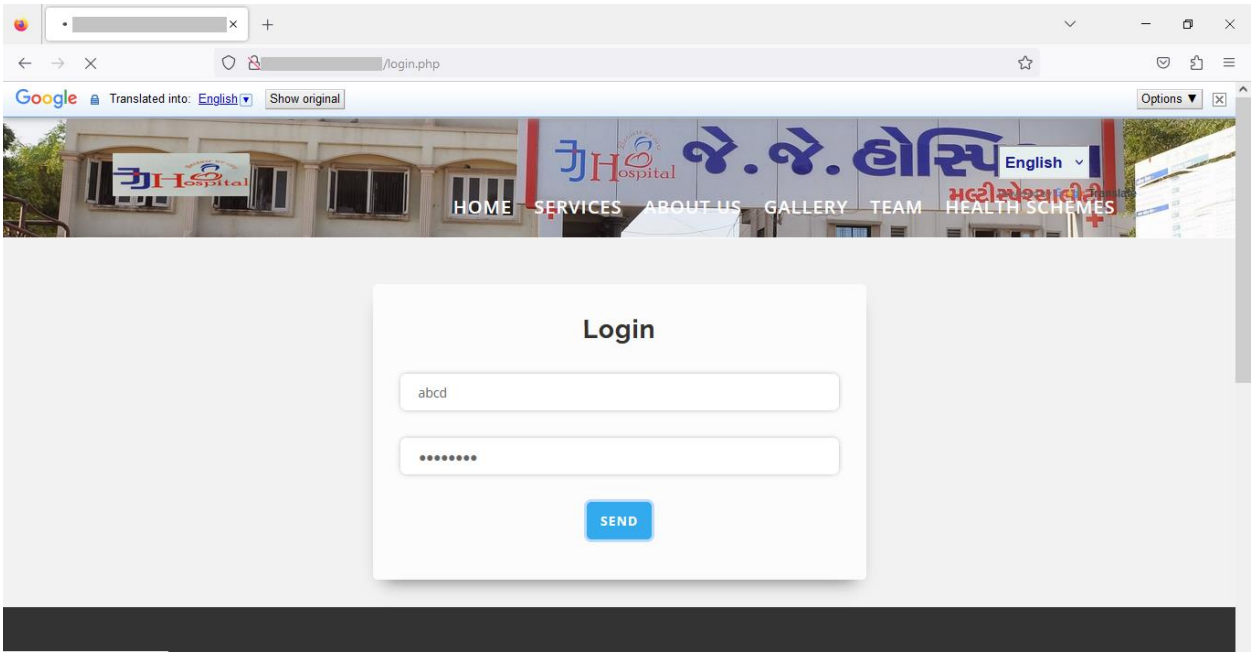
Observation
It was observed that the Web server is permitting directory listing which is used for sharing files. Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information and page disclosure. Web servers can be configured to automatically list the contents of directories that do not have an index page present. This can aid an attacker by enabling them to quickly identify the resources at a given path and proceed directly to analyzing and attacking those resources. It particularly increases the exposure of sensitive files within the directory that are not intended to be accessible to users, such as temporary files and crash dumps. Scanner discovered that the affected page permits directory listing

Sr. No. Title	
10	
Description	
NO RATE LIMITING ON ADMIN LOGIN PAGE	
Affected Resource / Parameter	**Severity**
https://www.jjhospitaltharad.com/login.php	**MEDIUM**
Impact / Consequences	
The impact of this vulnerability is high; A malicious minded user can continually try to brute force an account password. If user forget to logout account in some public computer, then attacker is able to know the correct password, and also able to change the password to new one by inputting large number of payloads.	
Recommendations	
It is recommended to limit the rate for current password field. Add A ReCAPTCHA & Sort of Something Which Requires Manual Human Interaction to Proceed Like You Can Add Captcha Like 2+2=___ so that it cannot be brute forced and you also can have a limit at the backend for particular number up to 5 times a day user can request Forget Password Email or Link something like that will prevent you from someone exploiting this vulnerability.	
Tools Used	**References**
Burp-Suite	https://portswigger.net/burp
CWE	**OWASP Top 10**
307	-
Proof of Vulnerability	

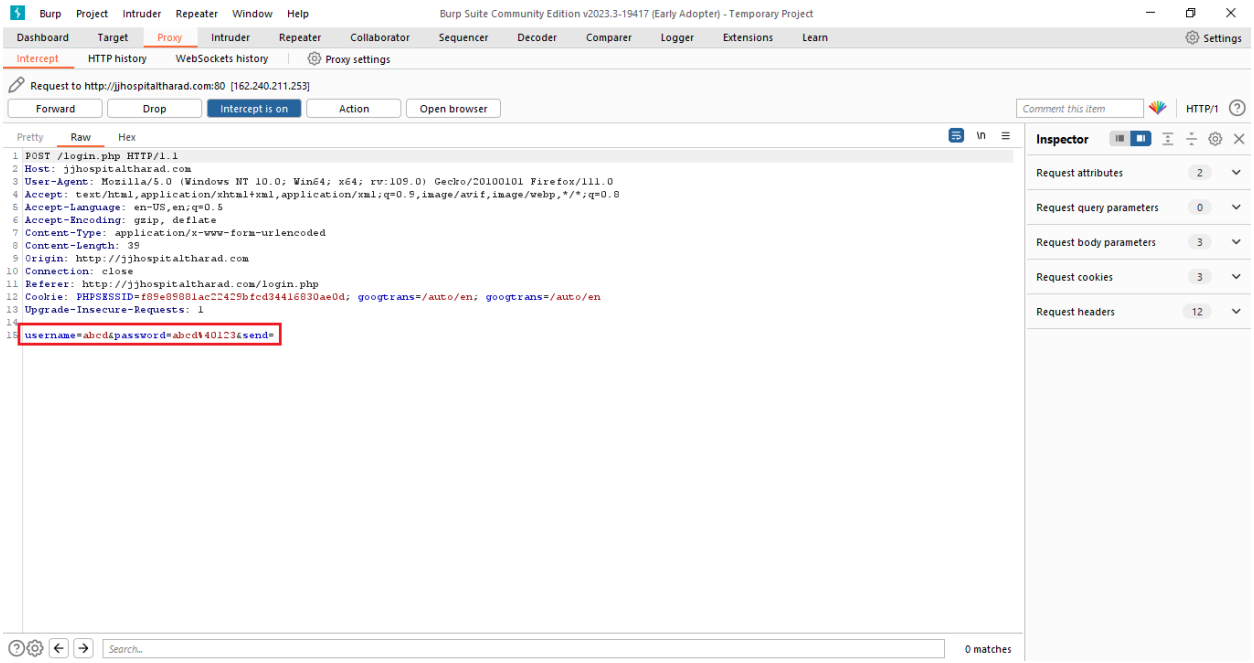
- Step 1: visit



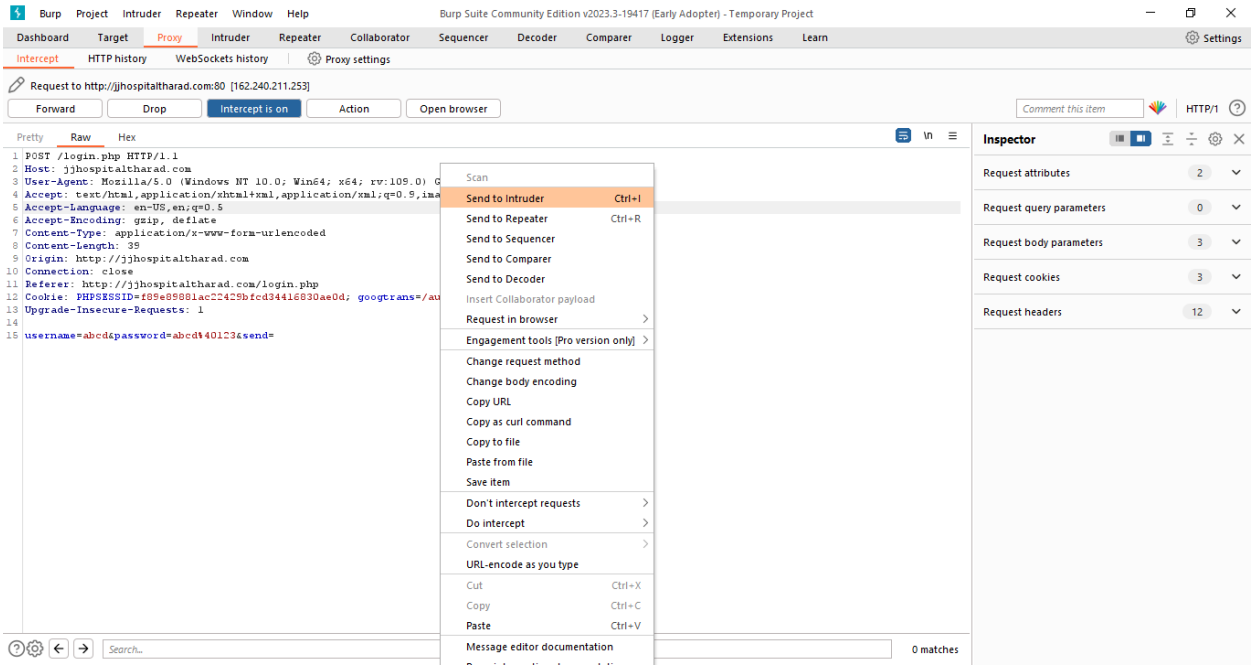
- Step 2 : Here, we have write username and password and send.



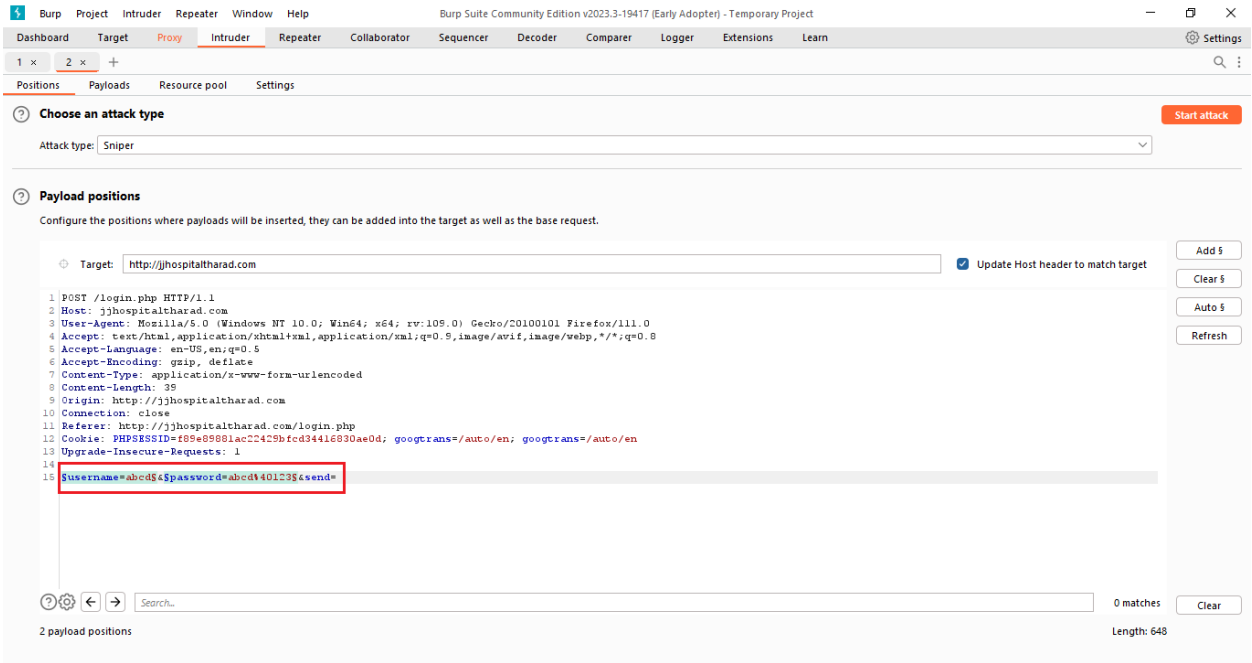
- Step 3 : In the burp suite , we can see username and password of whatever we can send.



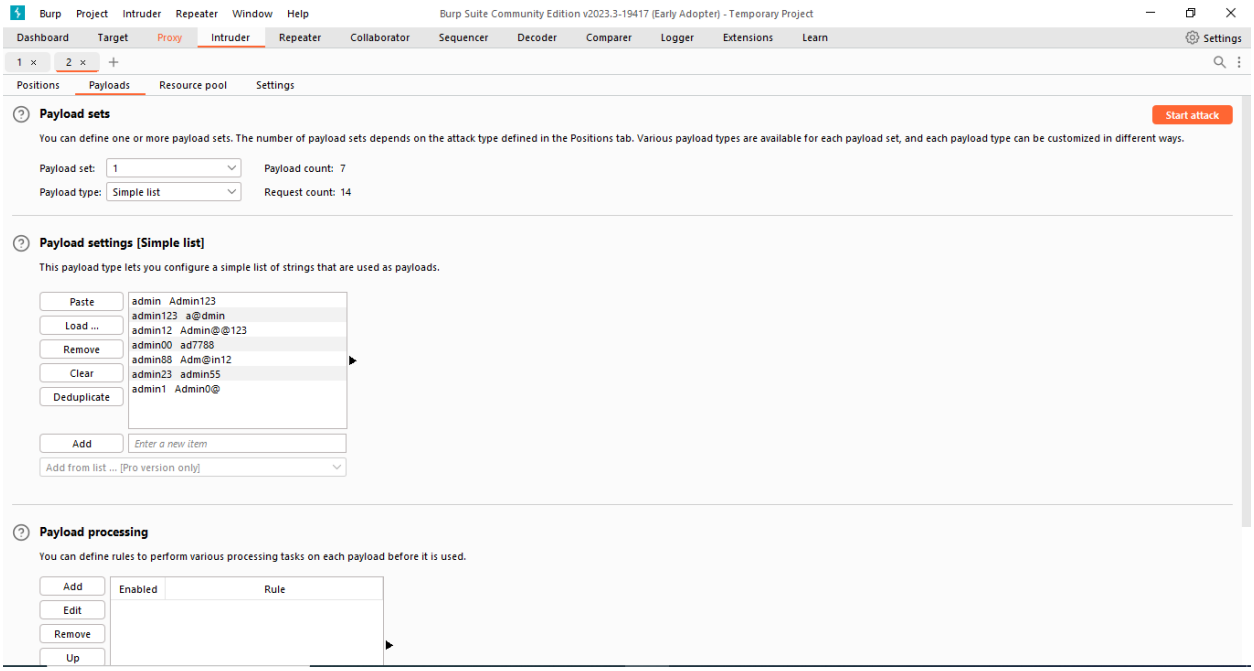
- Step 4 : Now , here we click on right and send to intruder.



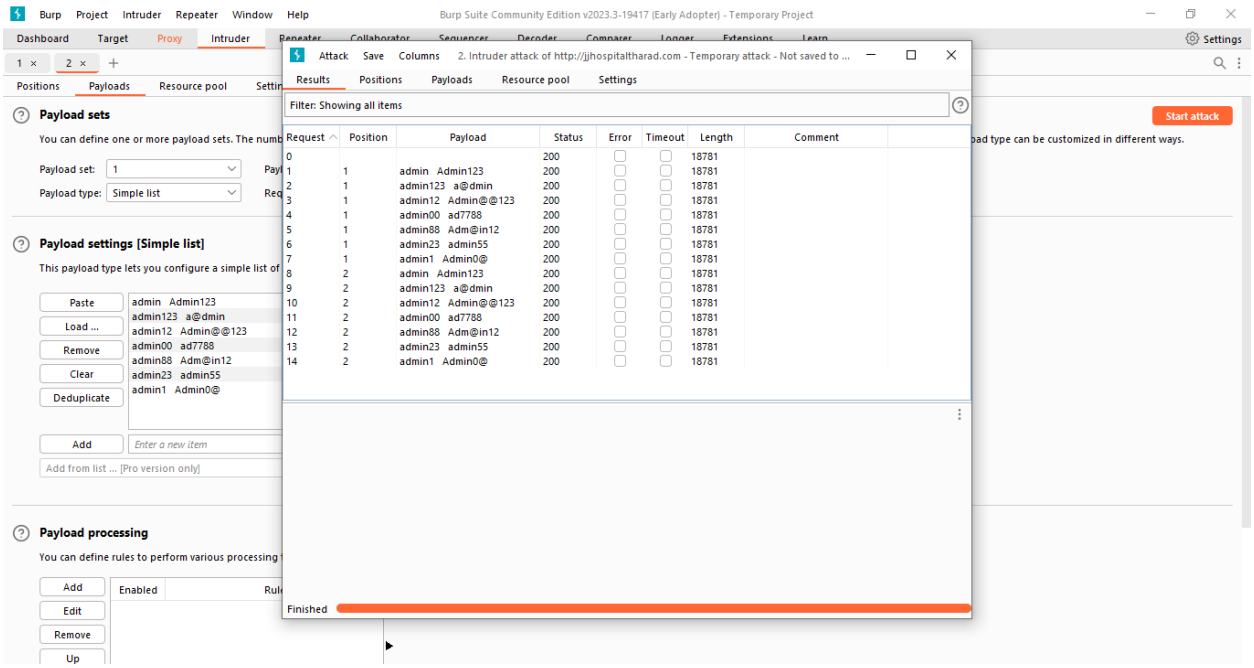
- Step 5 : Here, firstly we have to clear and add the username and password and go to the payloads.



- Step 6 : Here, we add some username and password and click on start attack.



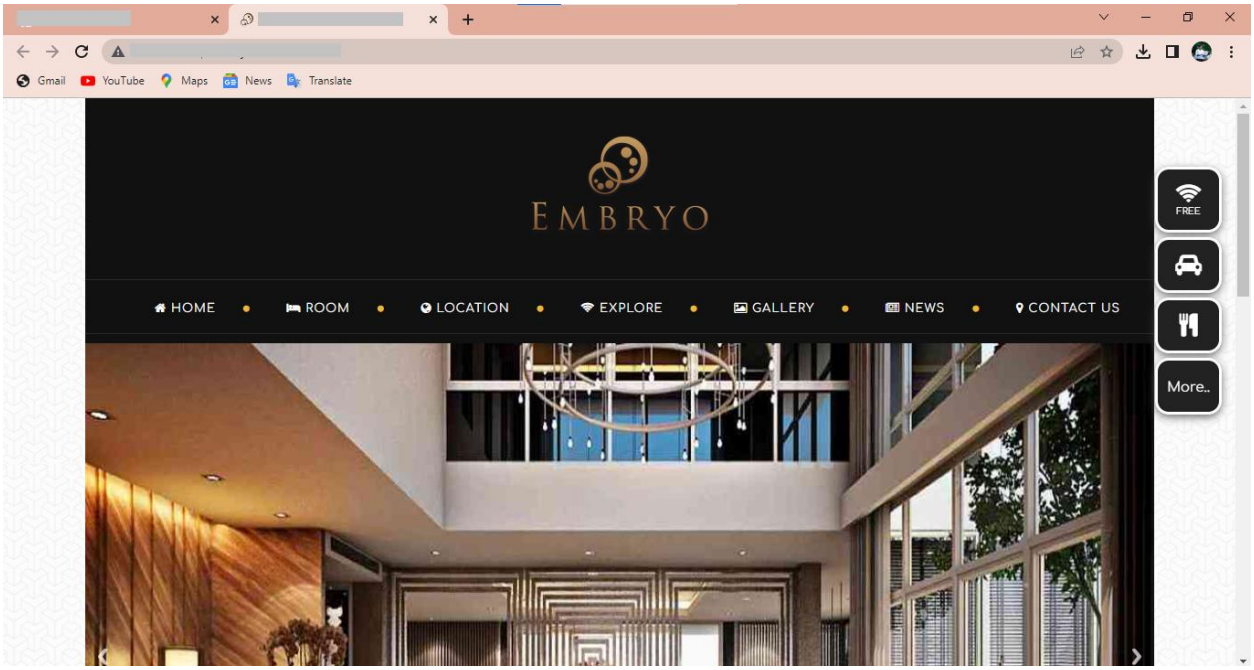
- Result :



Observation
They protect your electronic accounts and devices from unauthorized access, keeping your sensitive personal information safe. The more complex the password, the more protected your information will be from cyber threats and hackers.

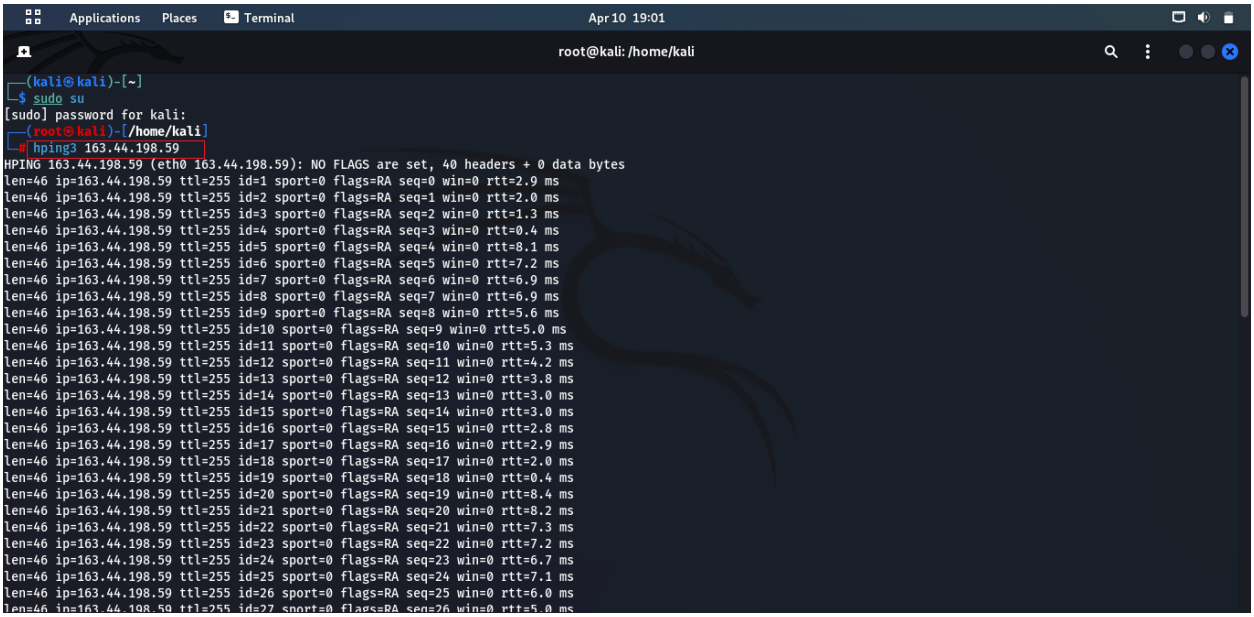
Sr. No. Title	
11	
Description	
DOS ATTACK	
Affected Resource / Parameter	**Severity**
http://www.embryohotel.com/	**MEDIUM**
Impact / Consequences	
Genuine users are not able to access resources, so may not be able to find the information or carry out the actions they need. Businesses may not be able to carry out time critical actions. They may suffer reputational damage. Customers may choose to use a competitor.	
Recommendations	
Perform a network vulnerability audit. In order to properly defend your network, you have to understand its weaknesses. ✓ Secure your infrastructure. ✓ Reduce the attack surface. ✓ Create a DoS response plan. ✓ Know the warning signs.	
Tools Used	**References**
hping3	https://hping.apponic.com/
CWE	**OWASP Top 10**
400	OAT-015
Proof of Vulnerability	

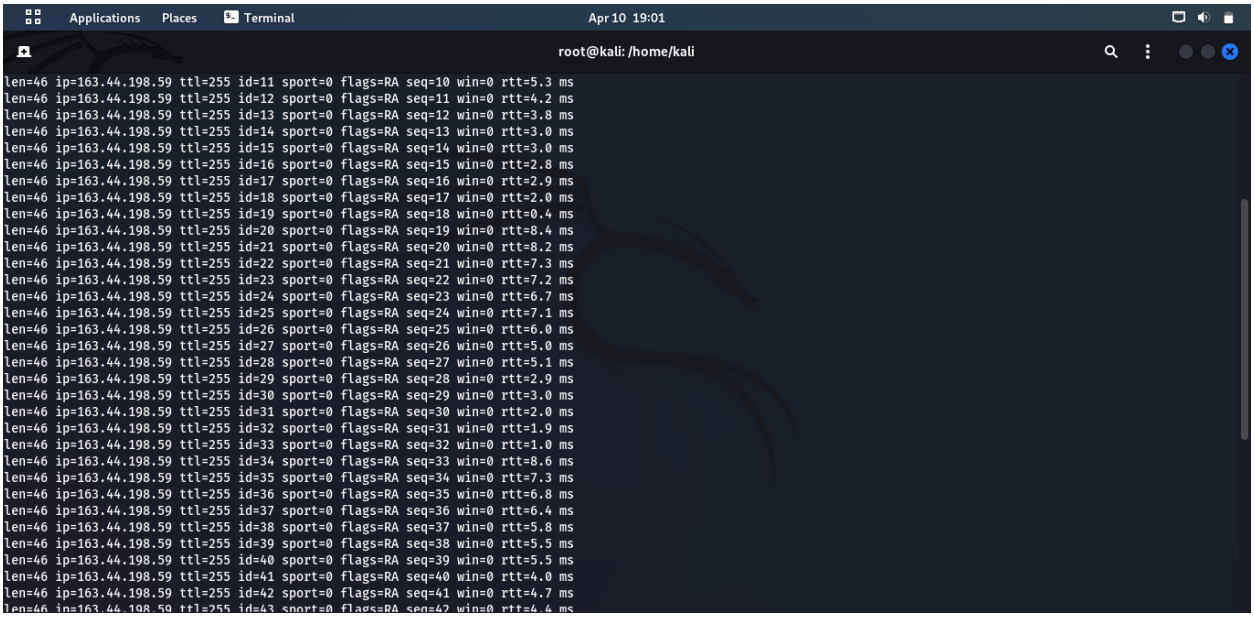
- Step 1: Visit:



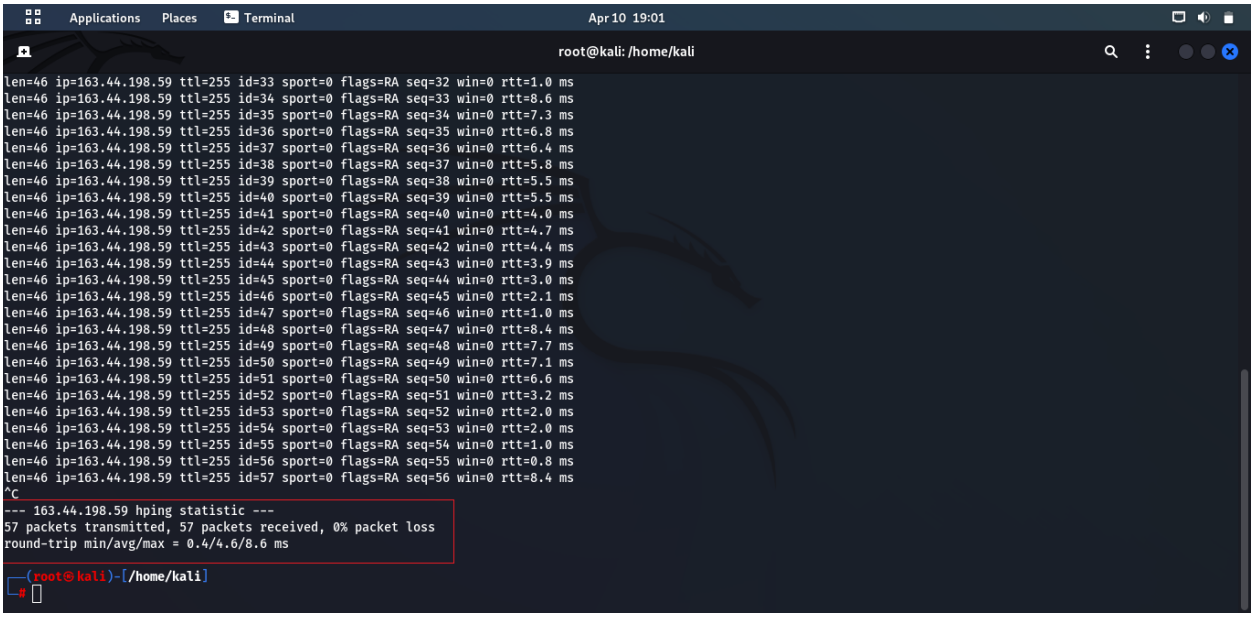
- Step 2: Here, we used command prompt and pinging the website and we found IP of the website

- Step 3: Here, we used kali Linux and install tool that is hping3 tool for dos(denial of service) attack.





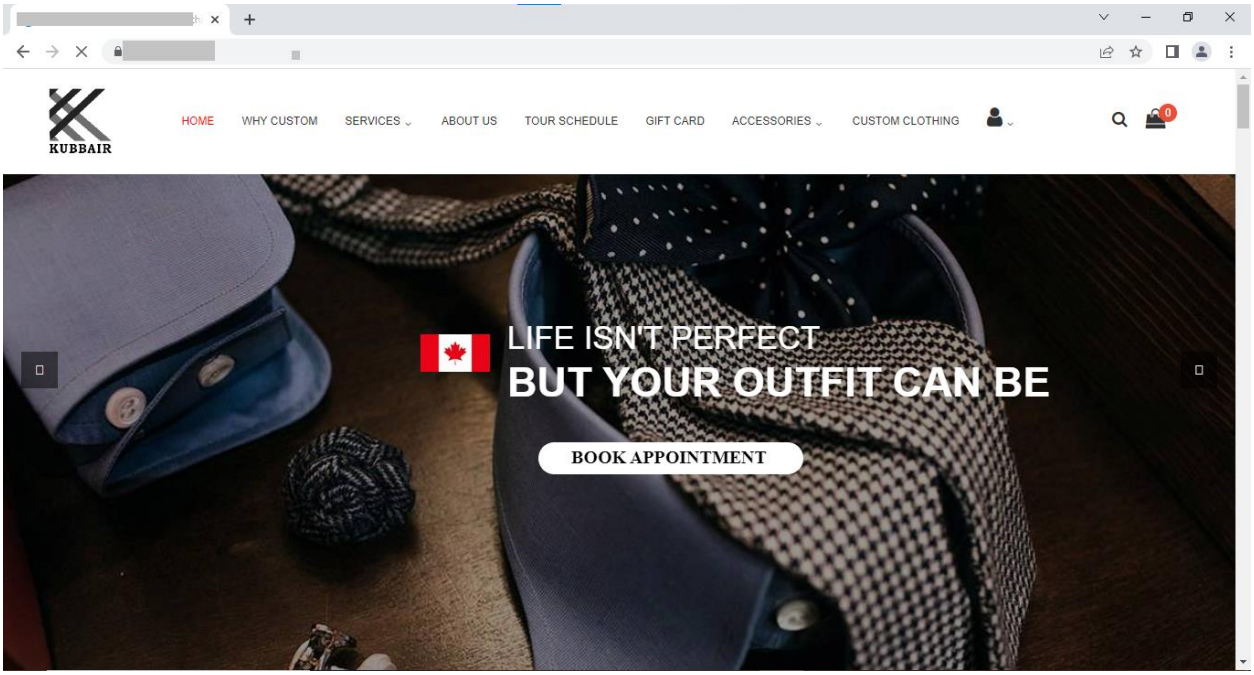
- Result:



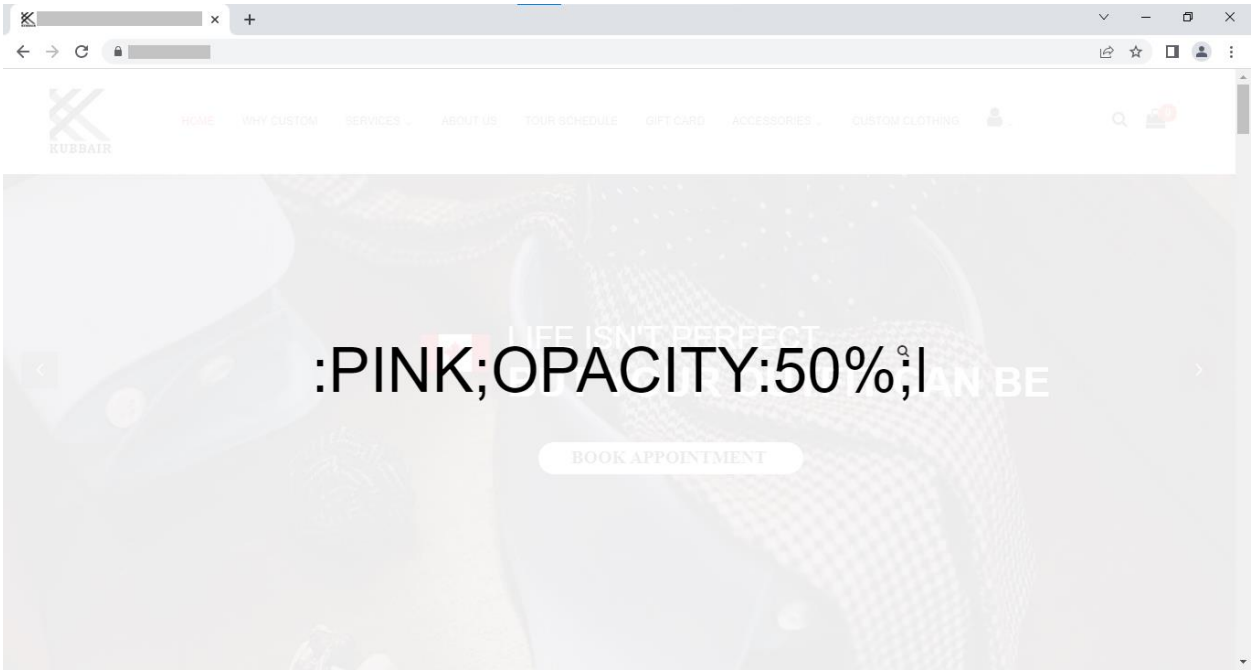
Observation
DoS attacks usually happen by generating mass bot traffic. Denial of Service attacks is usually generated for malicious intentions and, sometimes, they can happen unintentionally as well.

Sr. No. Title	
12	
Description	
CSS INJECTION	
Affected Resource / Parameter	**Severity**
https://kubbair.com/blog_details.php?blog_id=9	**LOW**
Impact / Consequences	
An attacker is able to execute arbitrary server-side code.	
Recommendations	
✓ Sanitization based on context ✓ Using a strong Content Security Policy ✓ Scanning your website using a vulnerability scanner	
Tools Used	**References**
-	-
CWE	**OWASP Top 10**
79	-
Proof of Vulnerability	

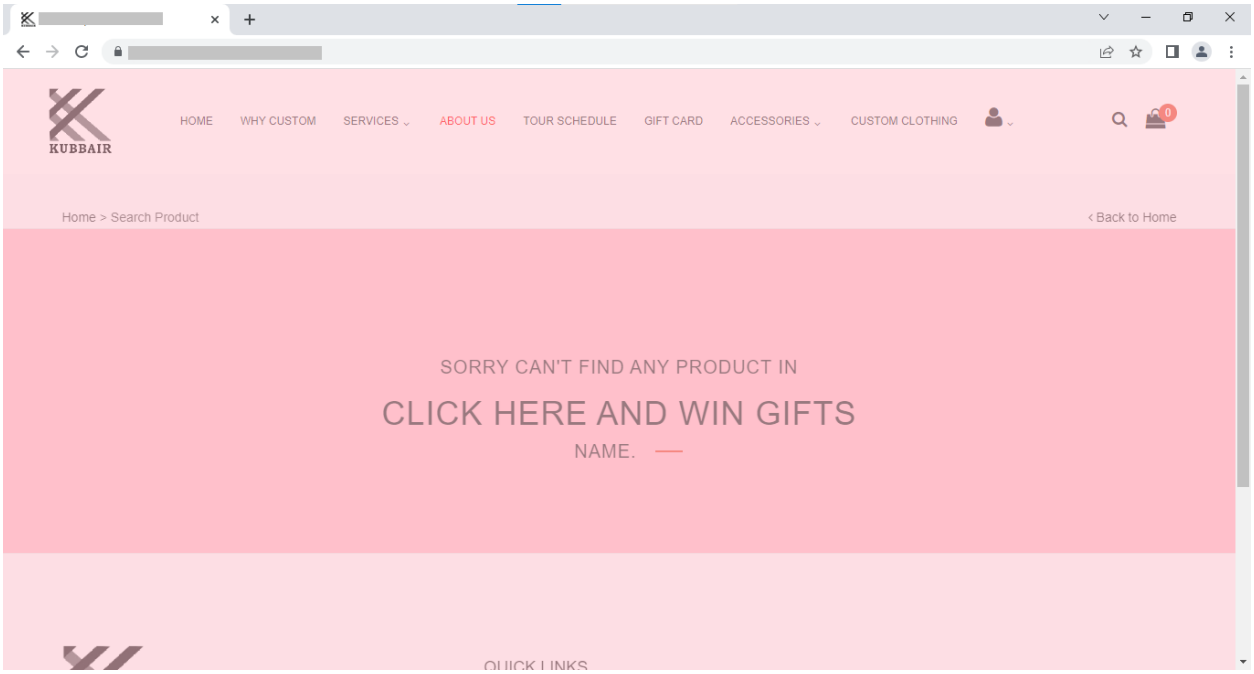
- Step - 1: Visit:



- Step - 2: Here we have injected a CSS code in this website.
  <body style="background-color: pink; opacity:50%; padding: top 50px;"></body>



- Step - 3: As we can see the color has been changed to blue same as the code we have entered.



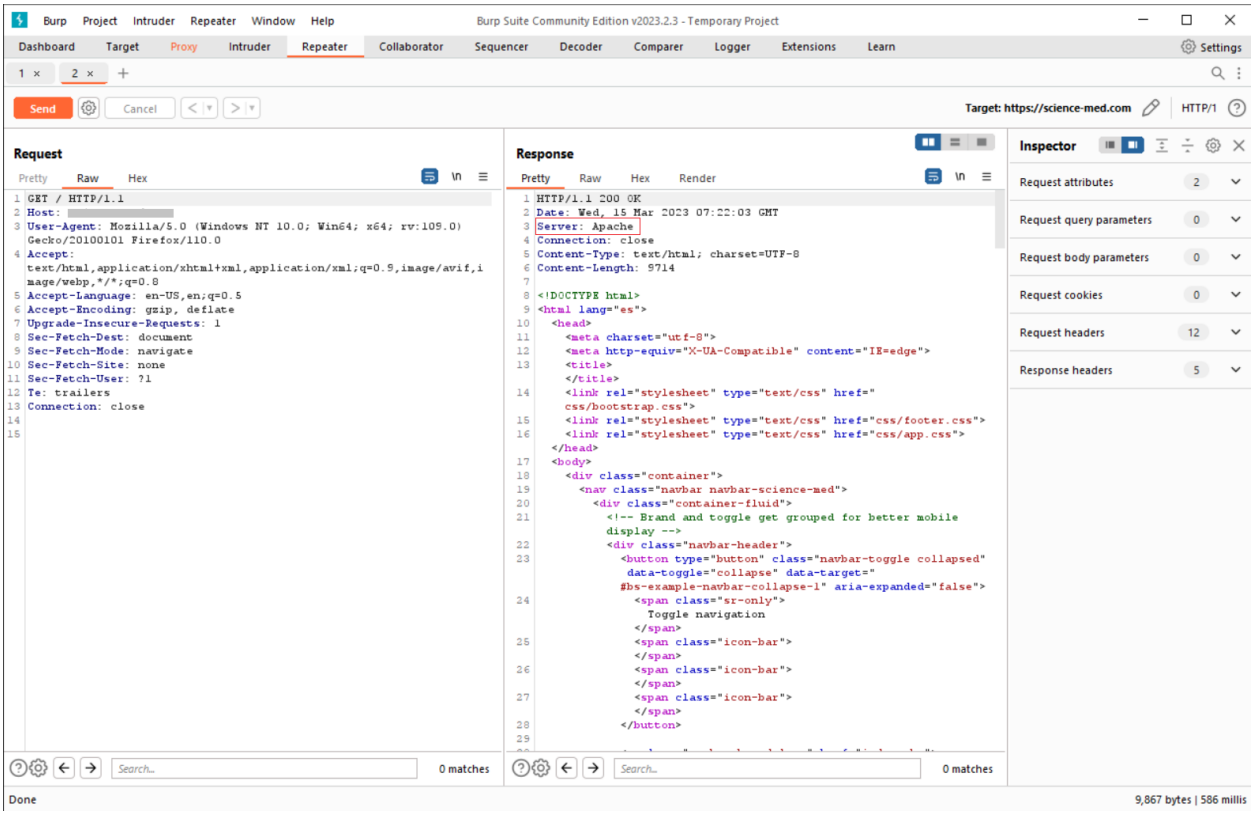
  - Result: Anyone can change any image or description etc.

Observation
CSS Injection vulnerability involves the ability to inject arbitrary CSS code in the context of a trusted web site which is rendered inside a victim's browser. The impact of this type of vulnerability varies based on the supplied CSS payload. It may lead to cross site scripting or data exfiltration.

Sr. No. Title	
13	
Description	
PHP VERSION DISCLOSURE	
Affected Resource / Parameter	**Severity**
https://science-med.com/	**Low**
Impact / Consequences	
An attacker can use the disclosed the 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	

- Step 1: visit:

- Below screenshot shows that PHP version.



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.

6. 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.

7. REFERENCE

- APKTool: http://ibotpeaches.github.io/APKTool
- Jd-Gui: http://java-decompiler.github.io/
- Burp-suite: https://portswigger.net/burp/communitydownload
- Owasp: https://owasp.org/
- google dork: https://www.exploit-db.com/google-hacking-database
- GitHub: https://github.com/

THANK YOU