**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:**

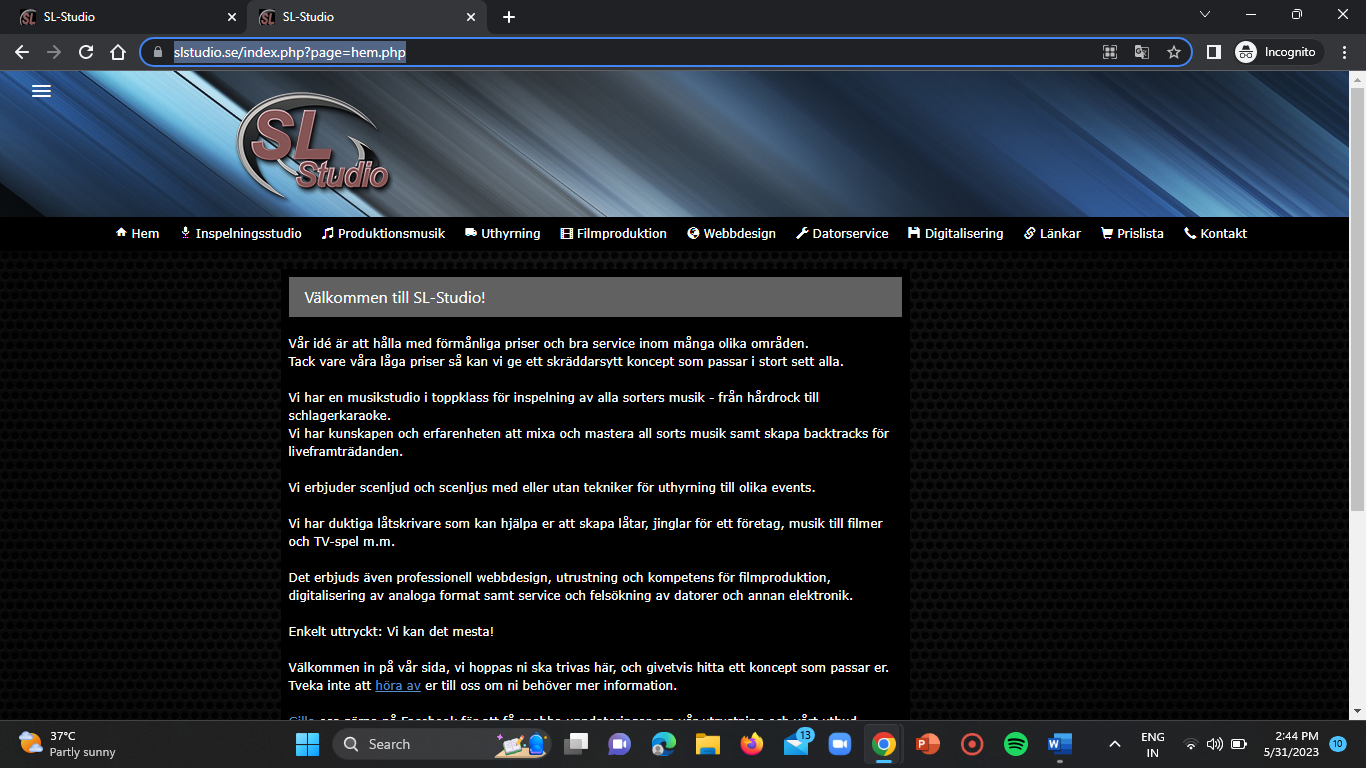
**Directory transversal/ Path transversal vulnerable websites:**

**WEBSITE-1:** <https://www.slstudio.se/>

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

**Step-1:**

Open the URL in the browser.



**Step-2:**

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

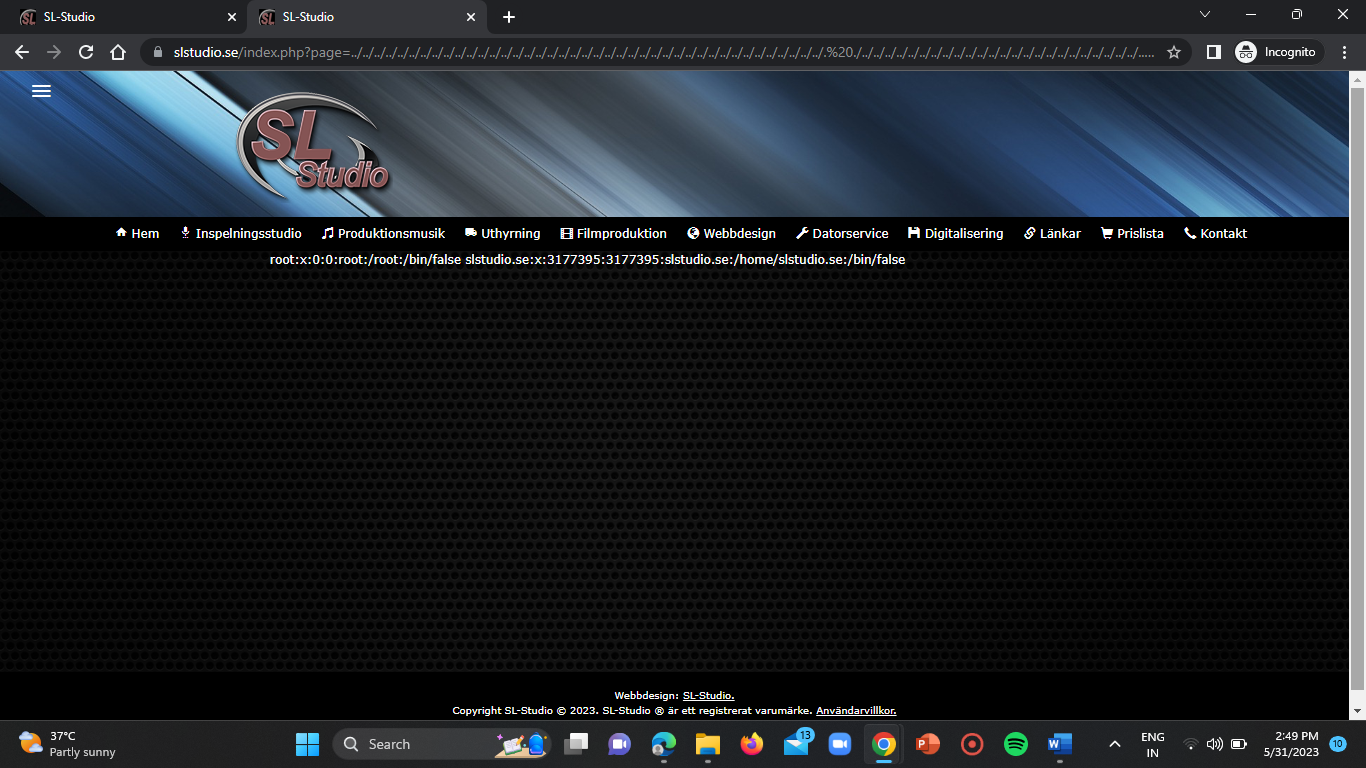
**Payload:**

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



**Step-3:**

Now click on enter.



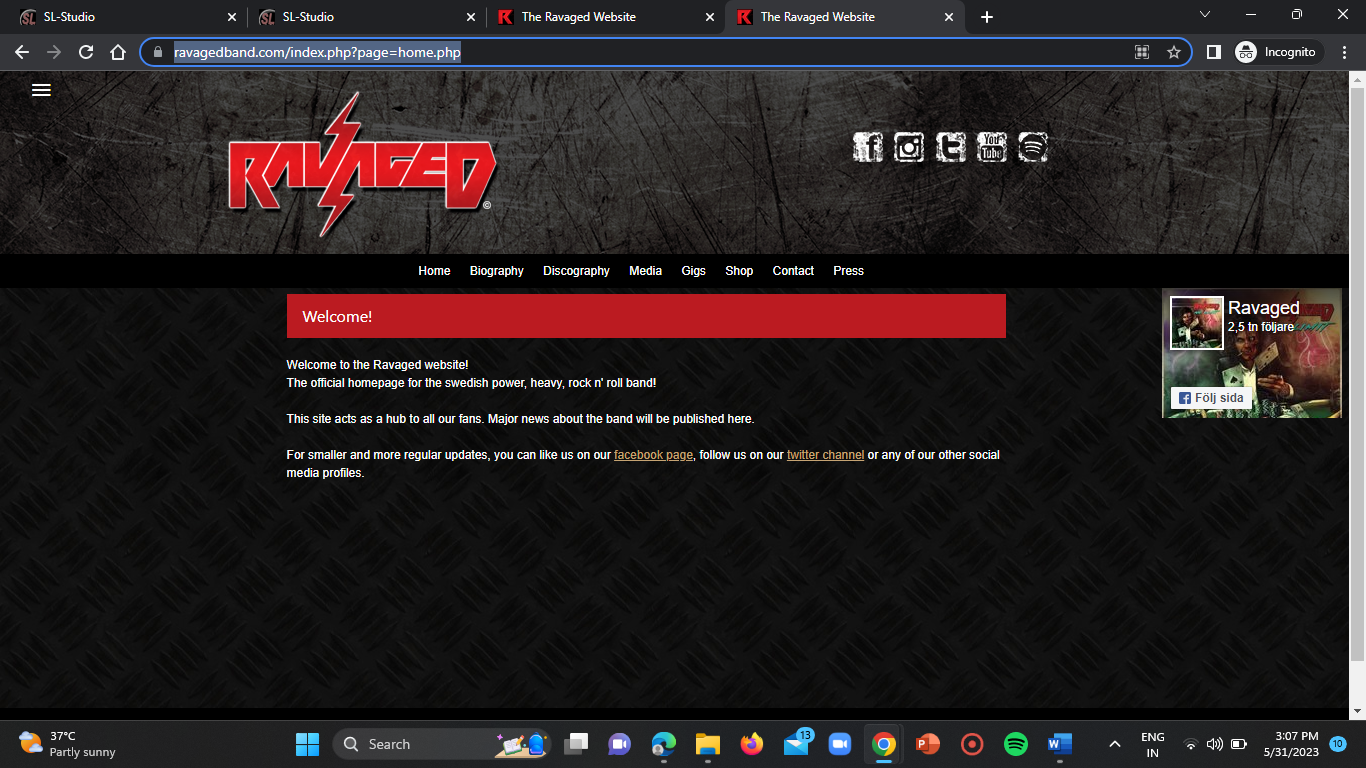
Here we are able to view the path location of the user information. Hence, the website is vulnerable.

**WEBSITE-2:** <https://www.ravagedband.com/>

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

Now repeat the above steps once again.

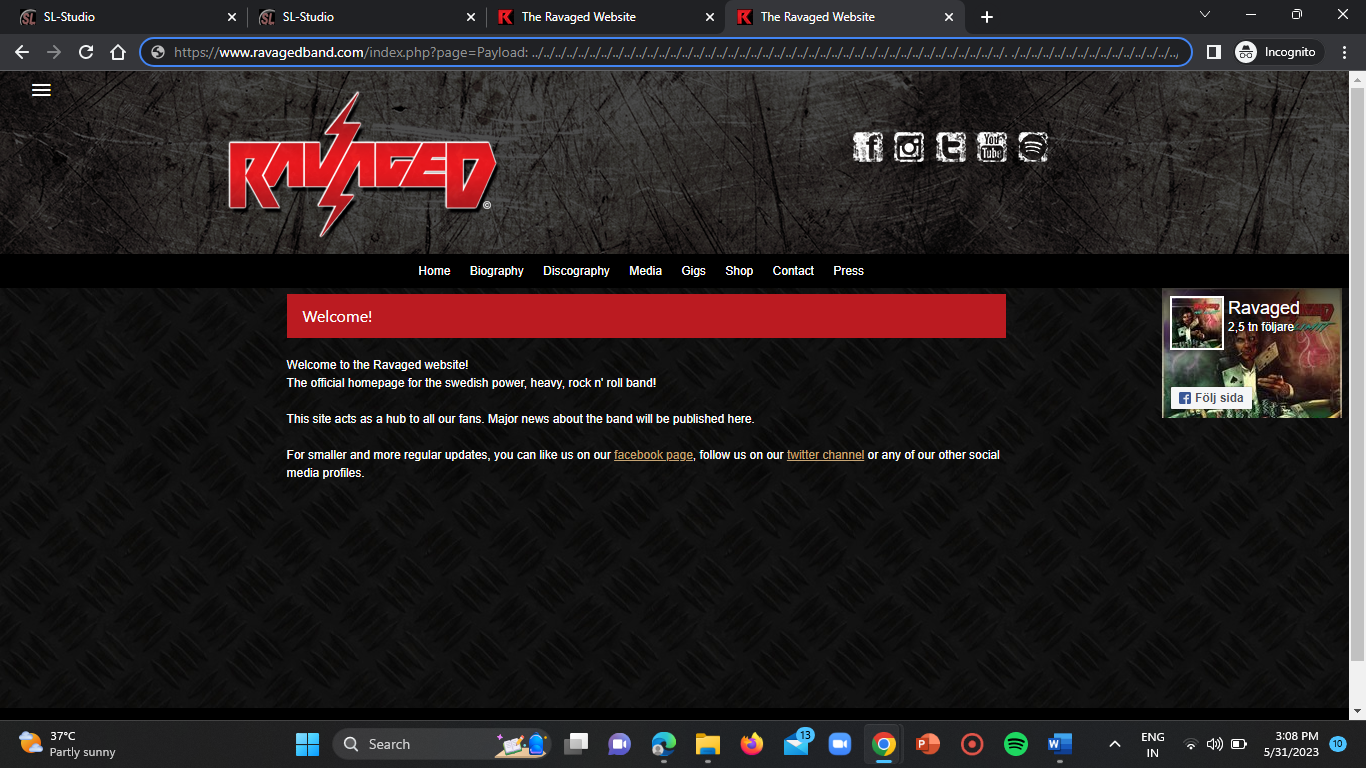
Firstly, open the URL in your browser.



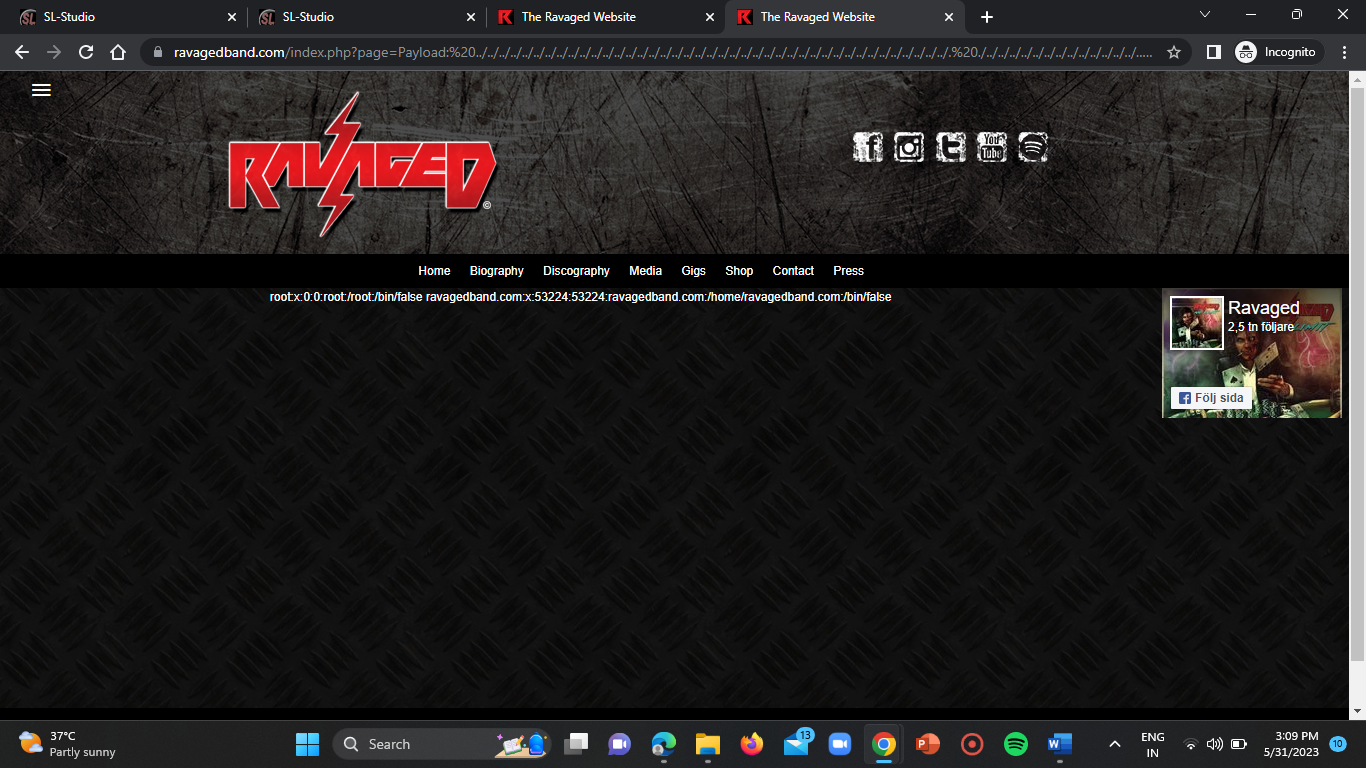
Then replace the home.php from the URL with the below mentioned payload.

**Payload:**

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



Now click on enter to view the result.



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

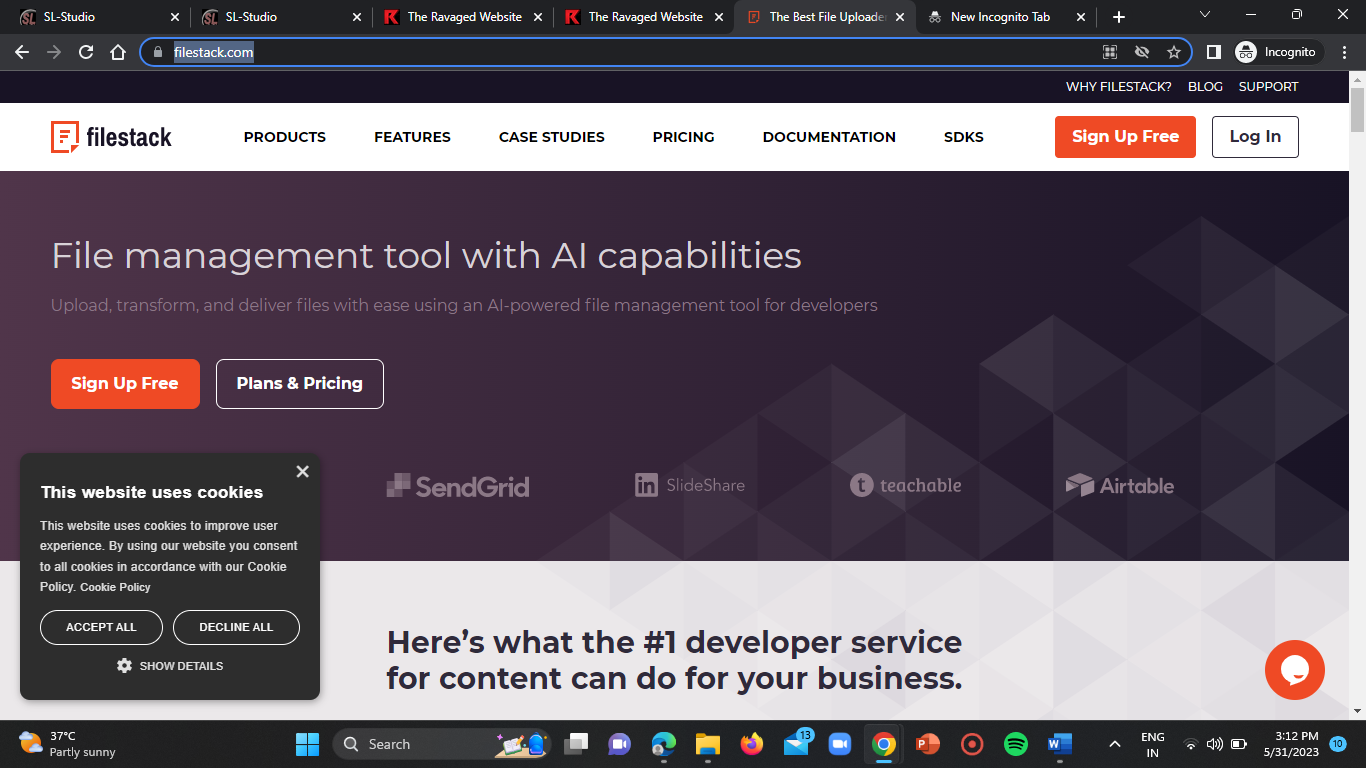
**Websites vulnerable to File Upload Vulnerability:**

**WEBSITE-1:**

**URL =** <https://www.filestack.com/>

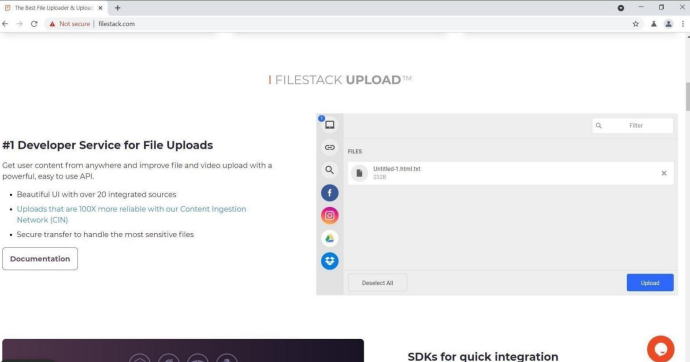
**Step-1:**

Open the URL in your browser.



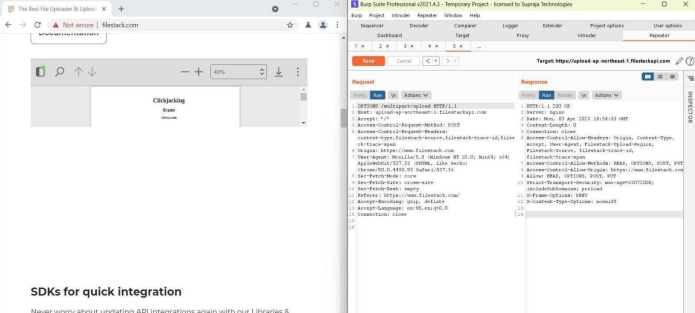
**Step-2:**

Upload a .html file that you already downloaded.



**Step-3:**

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



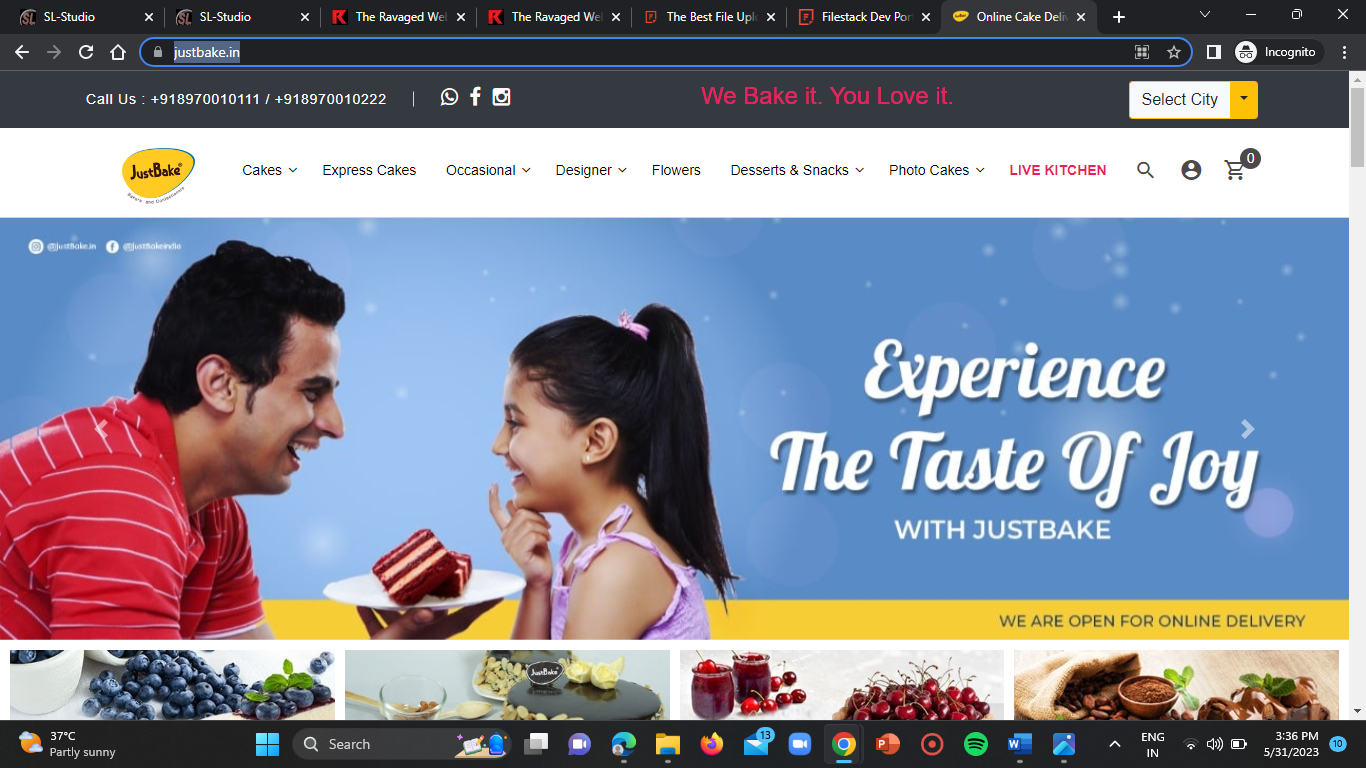
**Websites vulnerable to Parameter Tampering:**

**WEBSITE-1:**

**URL =** <https://www.justbake.in/>

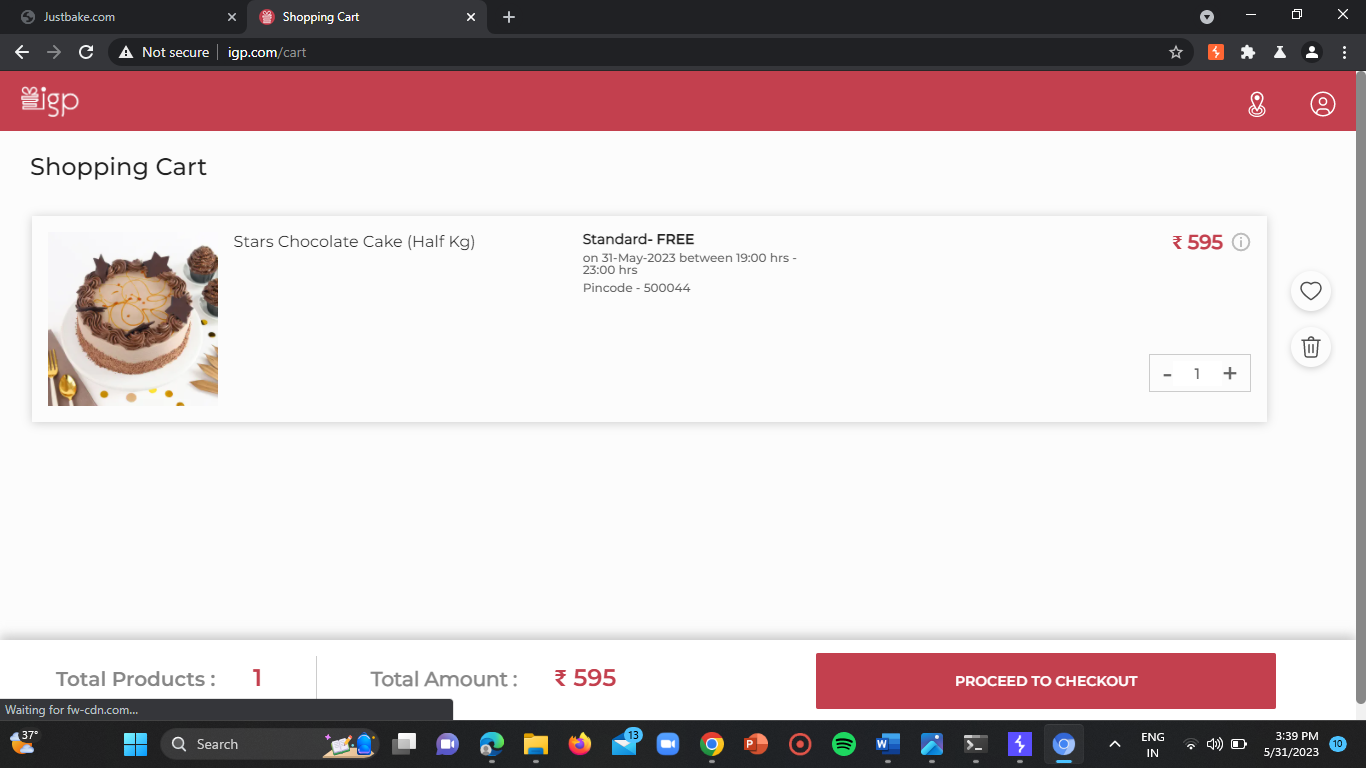
**Step-1:**

Open the vulnerable website in your browser.



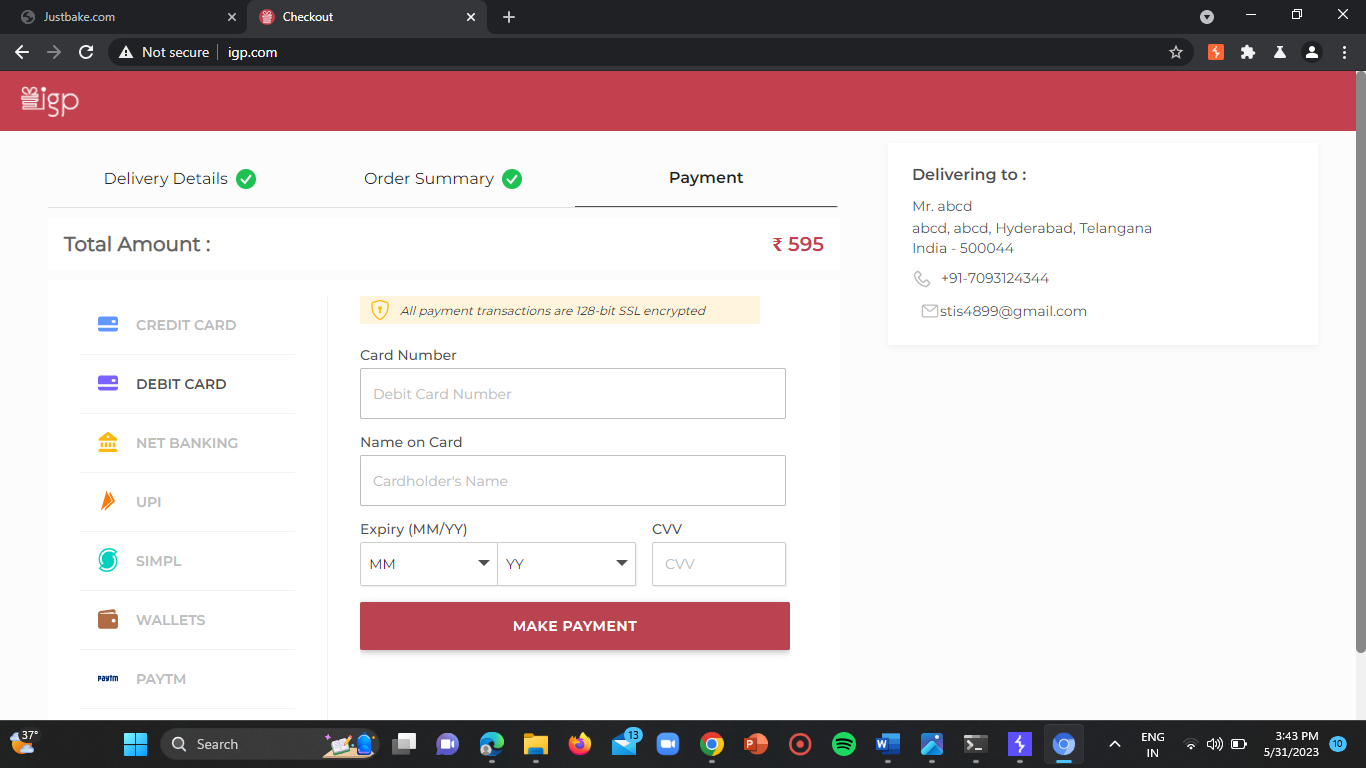
**Step-2:**

Login to your account and try to place an order.



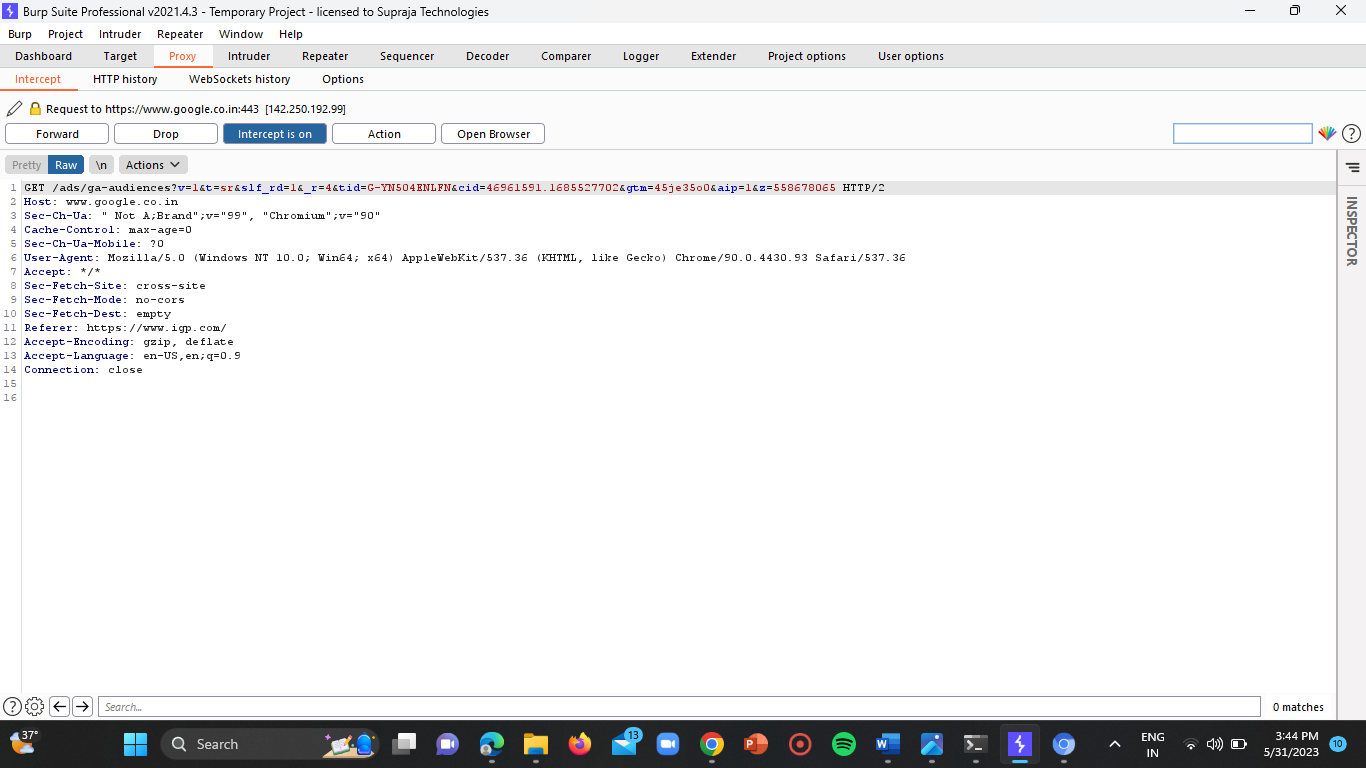
**Step-3:**

Proceed to checkout and select your desired payment gateway option.



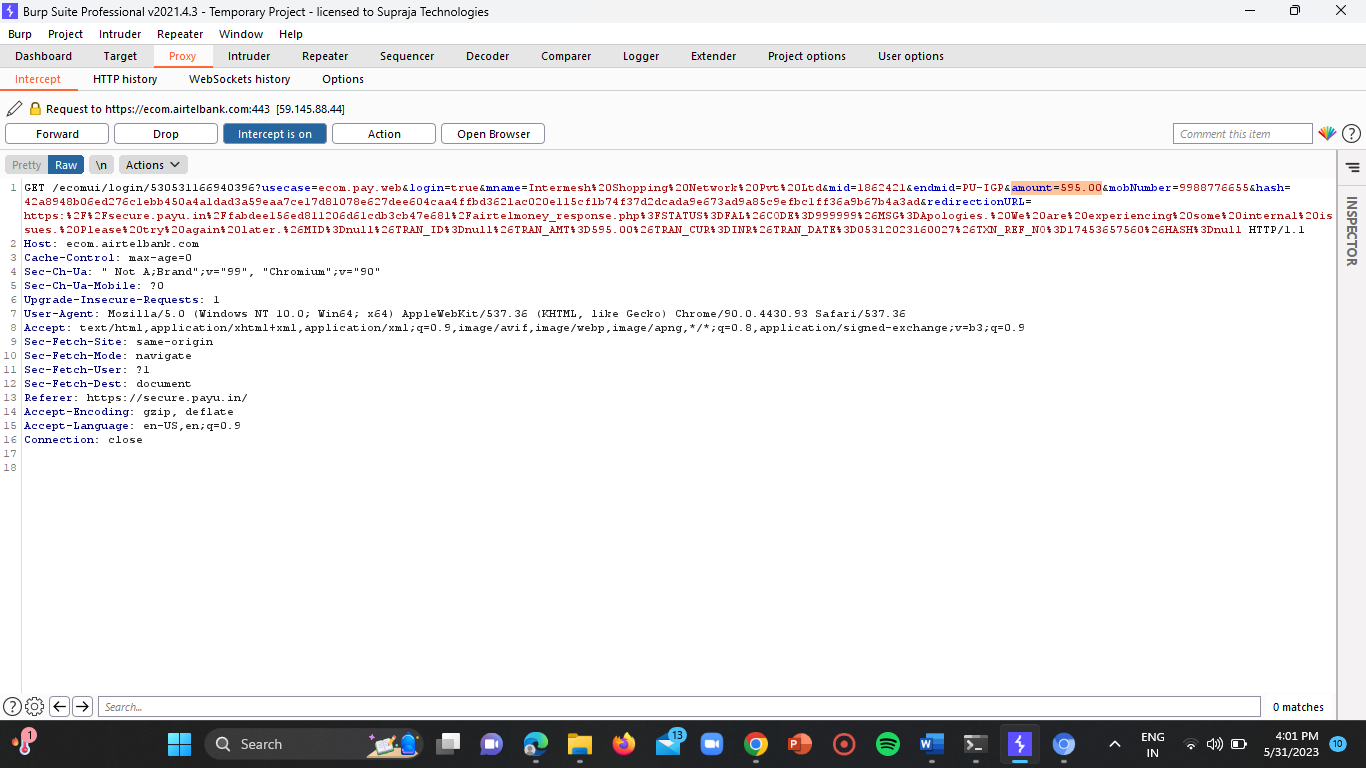
**Step-4:**

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



**Step-5:**

Now select the amount parameter in the HTTP request field.

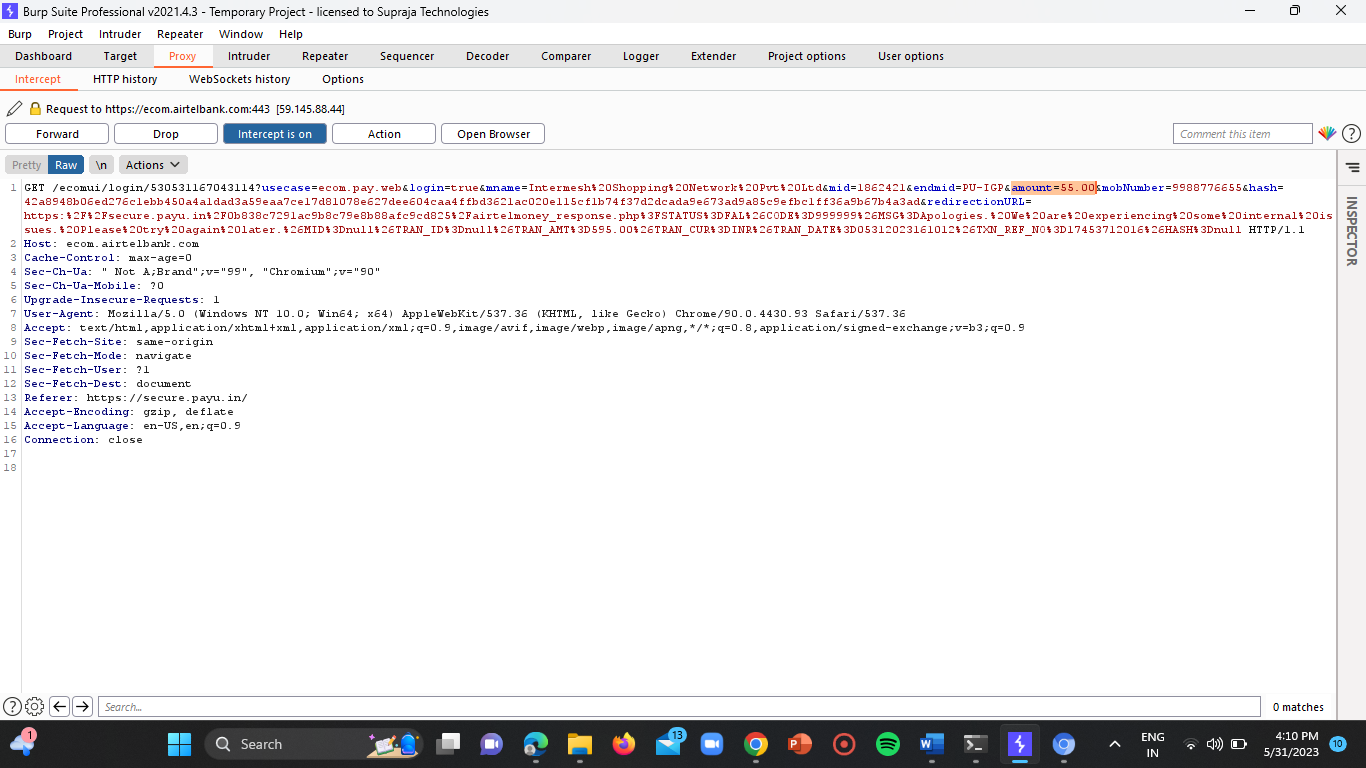


**Step-6:**

Then modify the amount field as rupees 5.

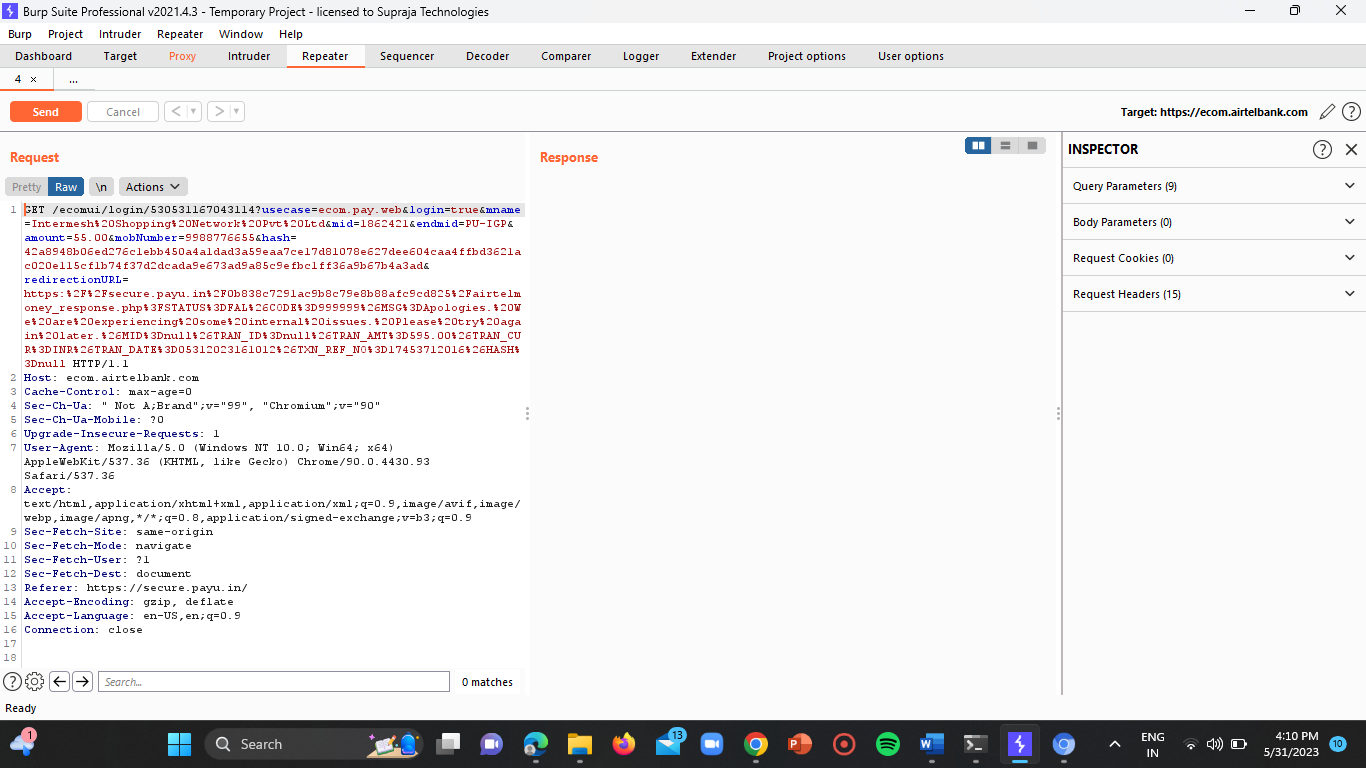
Use the below payload.

**Payload:** amount=55.00

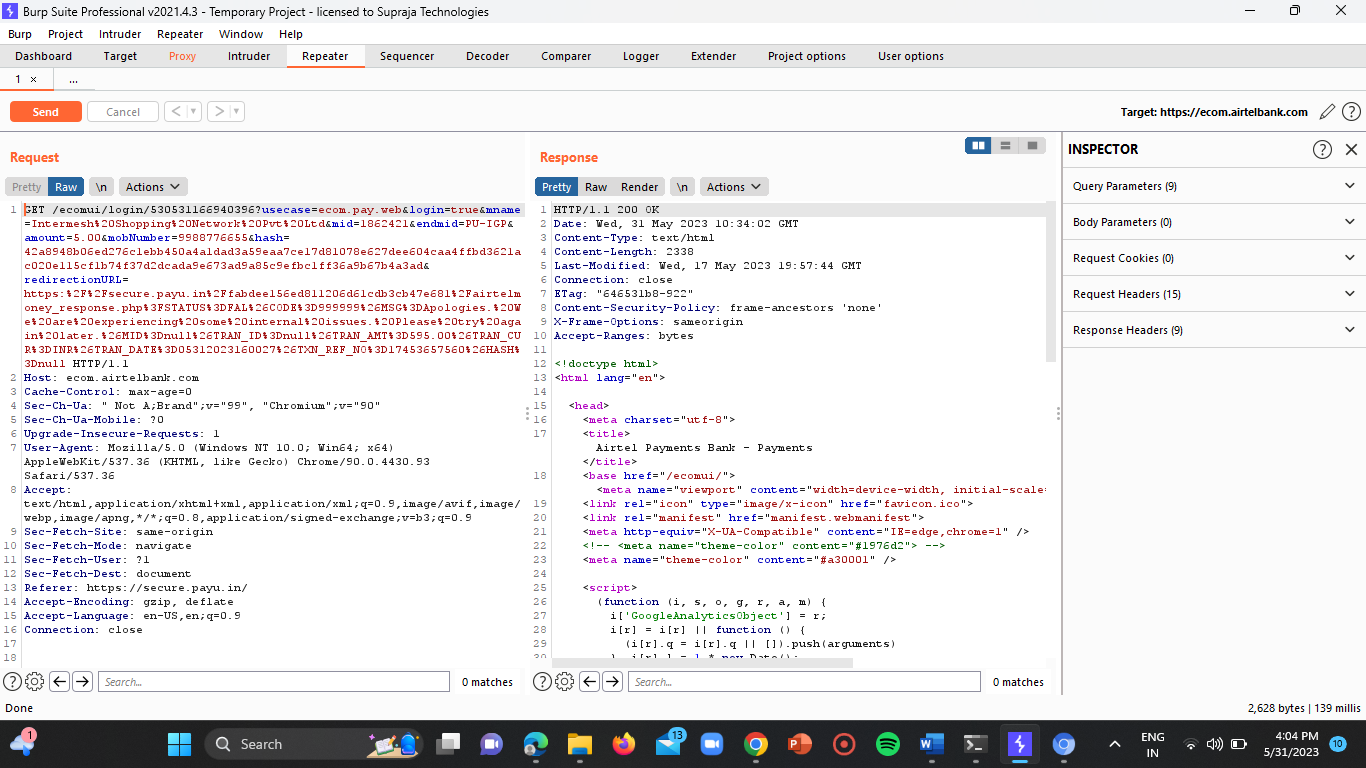


**Step-7:**

Now forward the request to the repeater.



Then click on send.





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.