**Task – 5 (web app sec)**

**TARGET:**

**1)** Find 3 websites vulnerable to CLICKJACKING/ UI REDRESS vulnerability.

**2)** Find 2 websites vulnerable to NO RATE LIMITING vulnerability in login pages, usernames finder/ email enumeration pages.

**3)** Find 1 website with NO RATE LIMITING vulnerability in categories.

**1.** Forgot password or Password reset pages.

**2.** Comment pages

**3.** Review pages

**4.** Get Quote Pages

**SYNOPSIS:**

**CLICKJACKING/ UI REDNESS Vulnerability:**

It is a type of web security vulnerability where an attacker tricks a user into clicking on a hidden or disguised element on a webpage without their knowledge. This technique allows the attacker to hijack the user’s clicks and perform unintended actions, potentially leading to a unauthorised access, data theft or other malicious activities.

**NO RATE LIMITING Vulnerability:**

Rate limiting is an important security measure used to protect web applications from abuse, brute-force attacks, and unauthorised access. It limits the number of requests an individual user or client can make within a specific timeframe. However, a rate limiting vulnerability refers to a weakness in the rate limiting implementation that can be exploited by an attacker.

**PROCEDURE:**

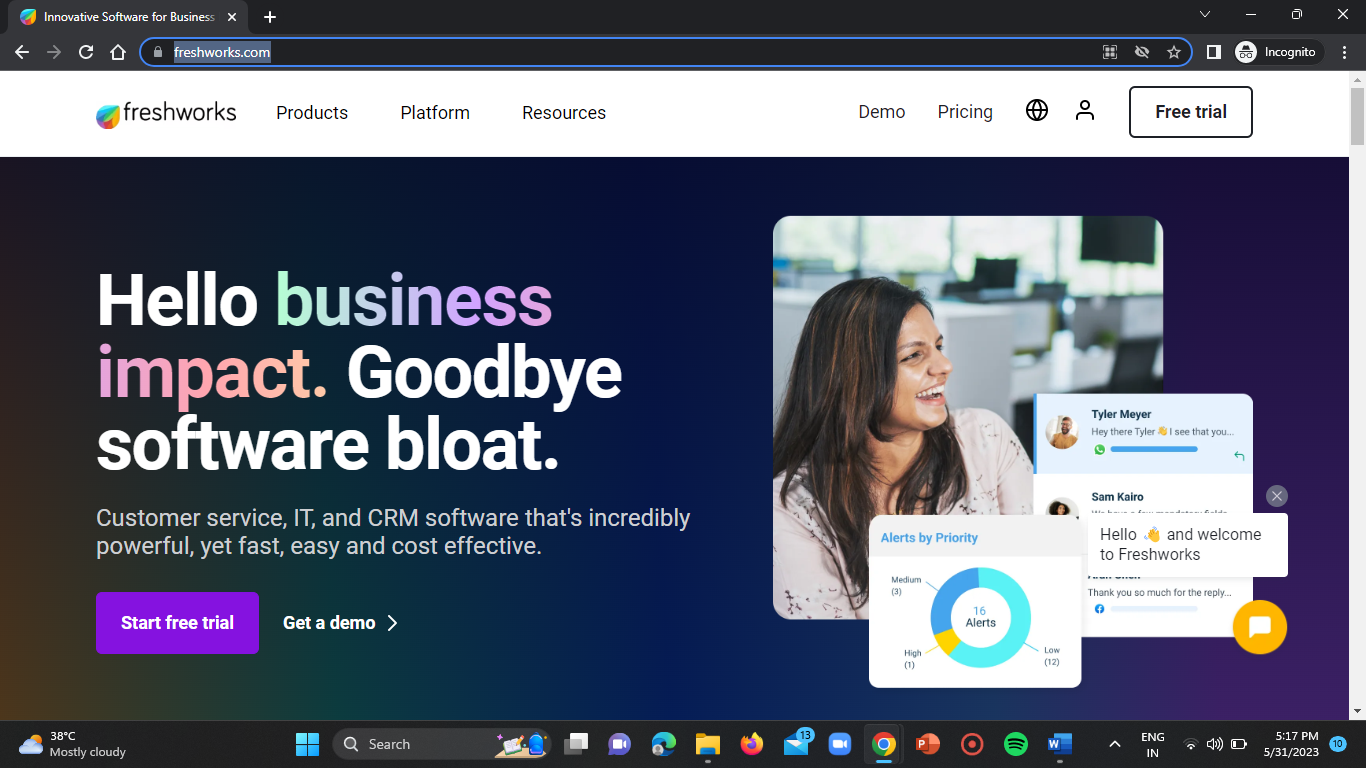
**Websites vulnerable to CLICKJACKING/ UI REDNESS vulnerability:**

**WEBSITE-1:**

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

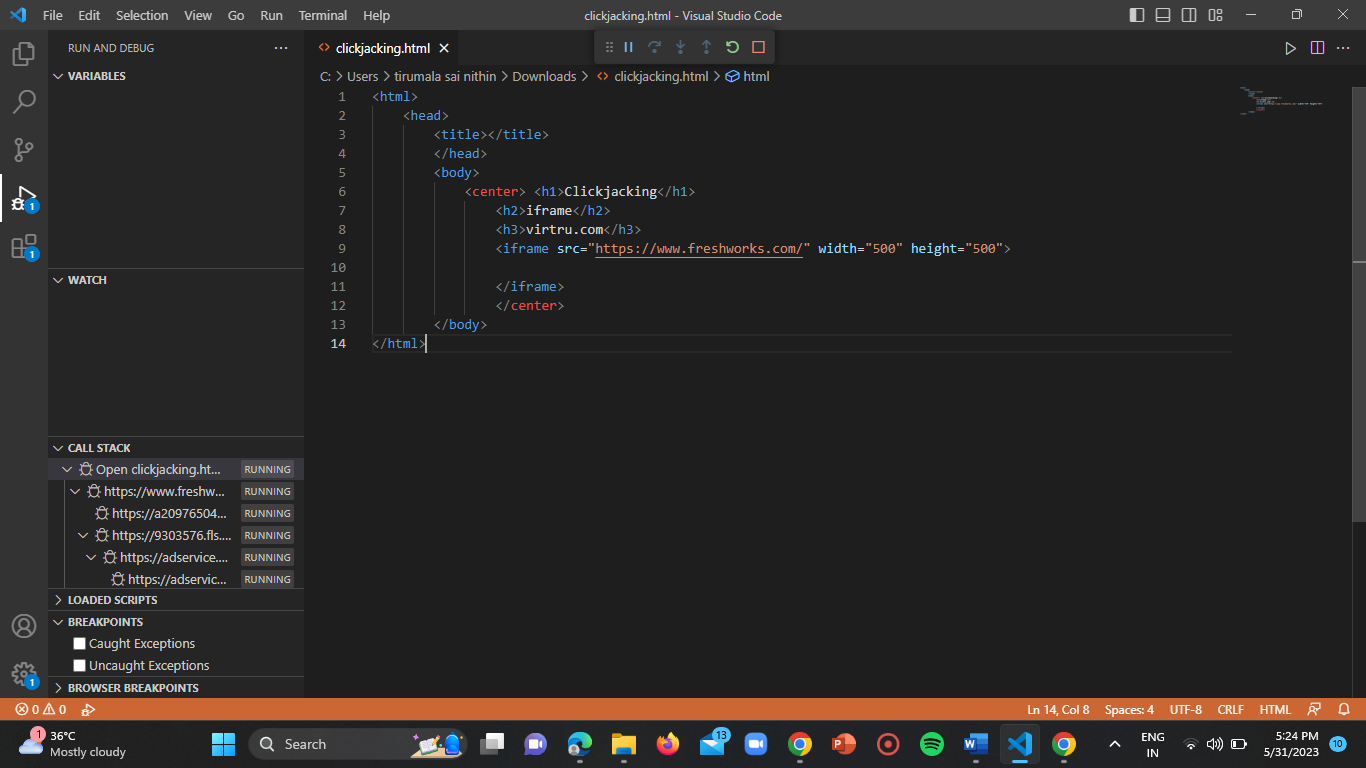
**Step-1:**

Open the above given URL in your browser.



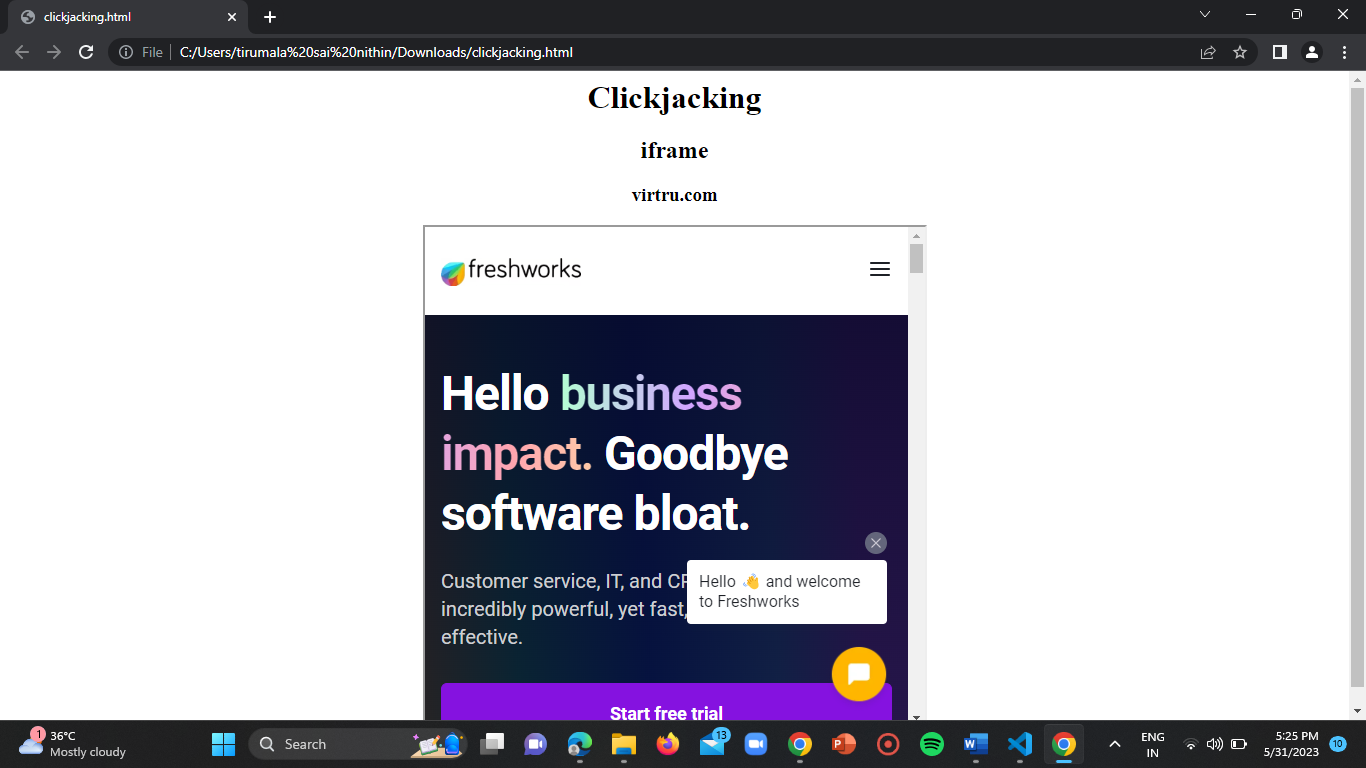
**Step-2:**

Now open the HTML file with the target URL in the browser.



**Step-3:**

The target website is embedded in the HTML page.



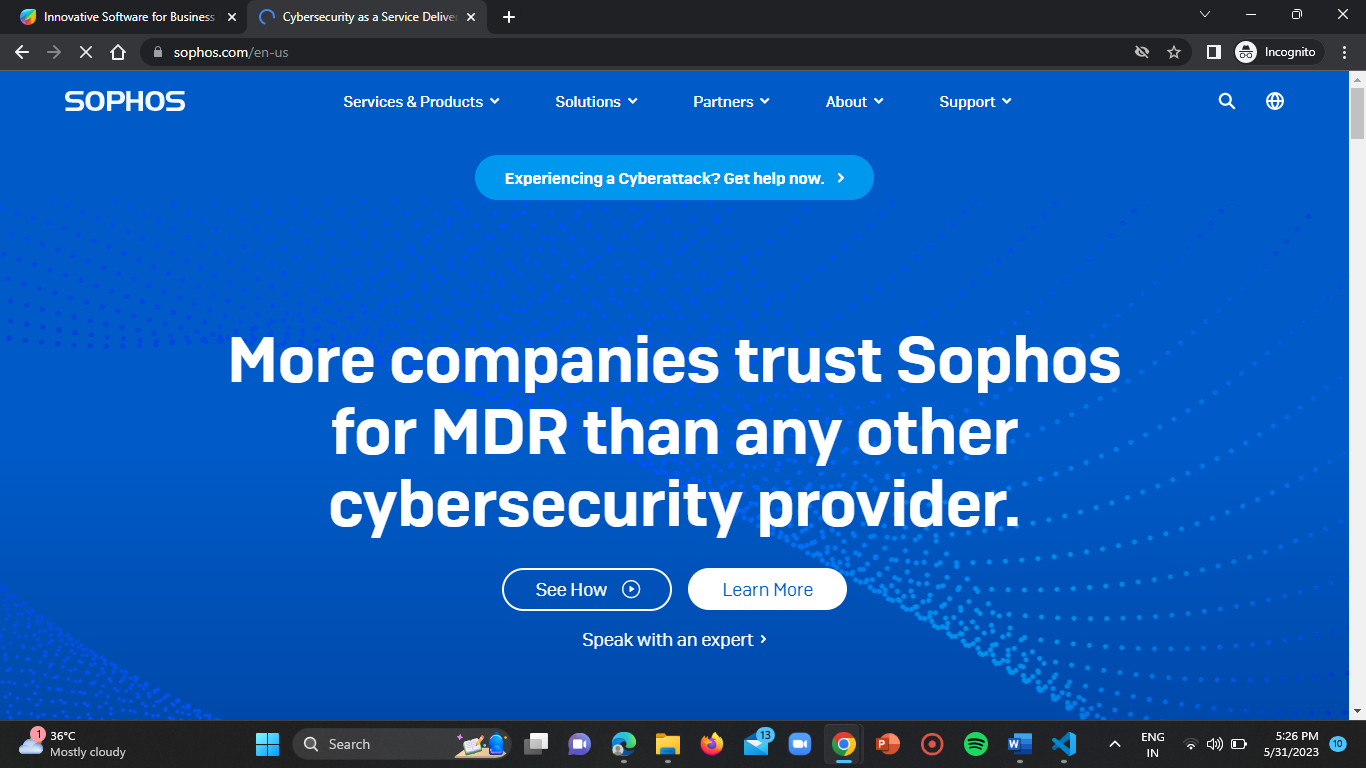
Hence the website is vulnerable.

**WEBSITE-2:**

**URL =** <https://www.sophos.com/en-us>

**Step-1:**

Open the URL in the browser.



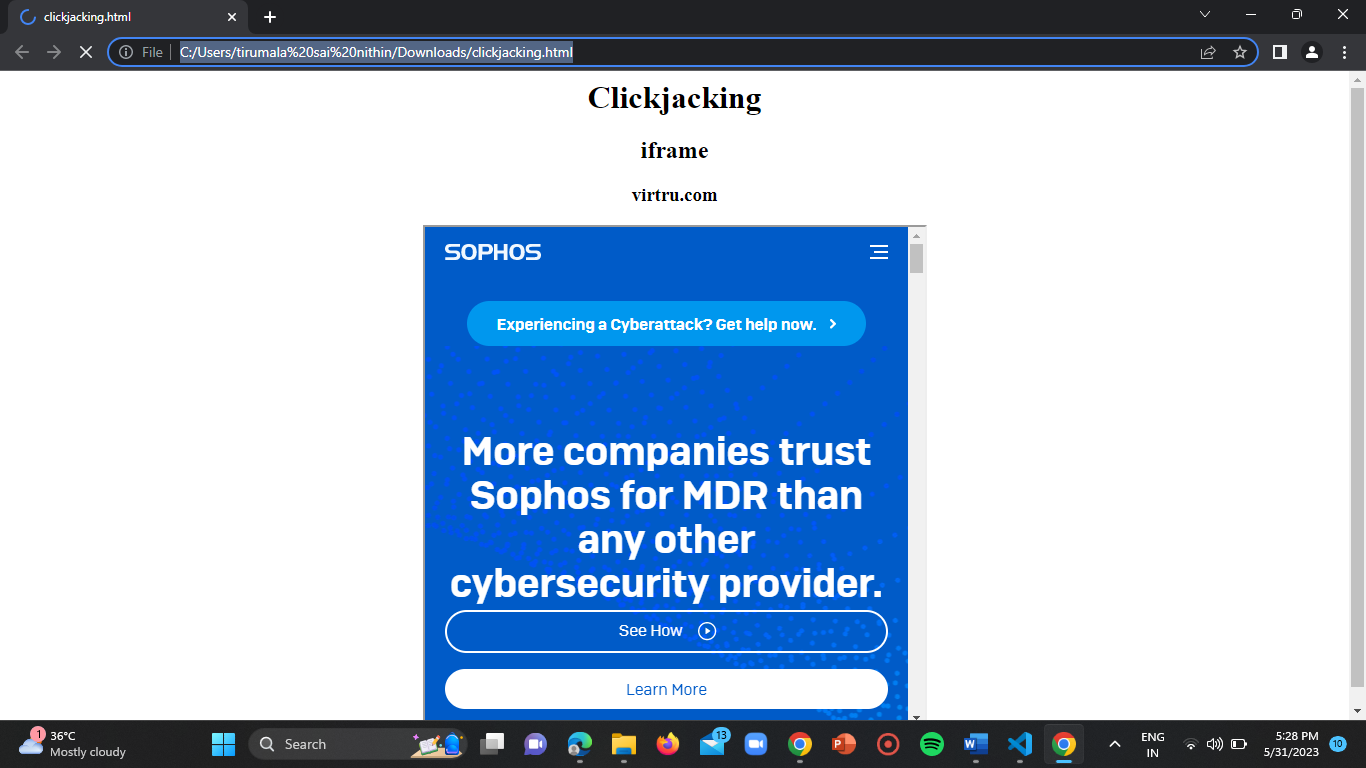
**Step-2:**

Follow the steps similarly to that of website-1.

HTML file:

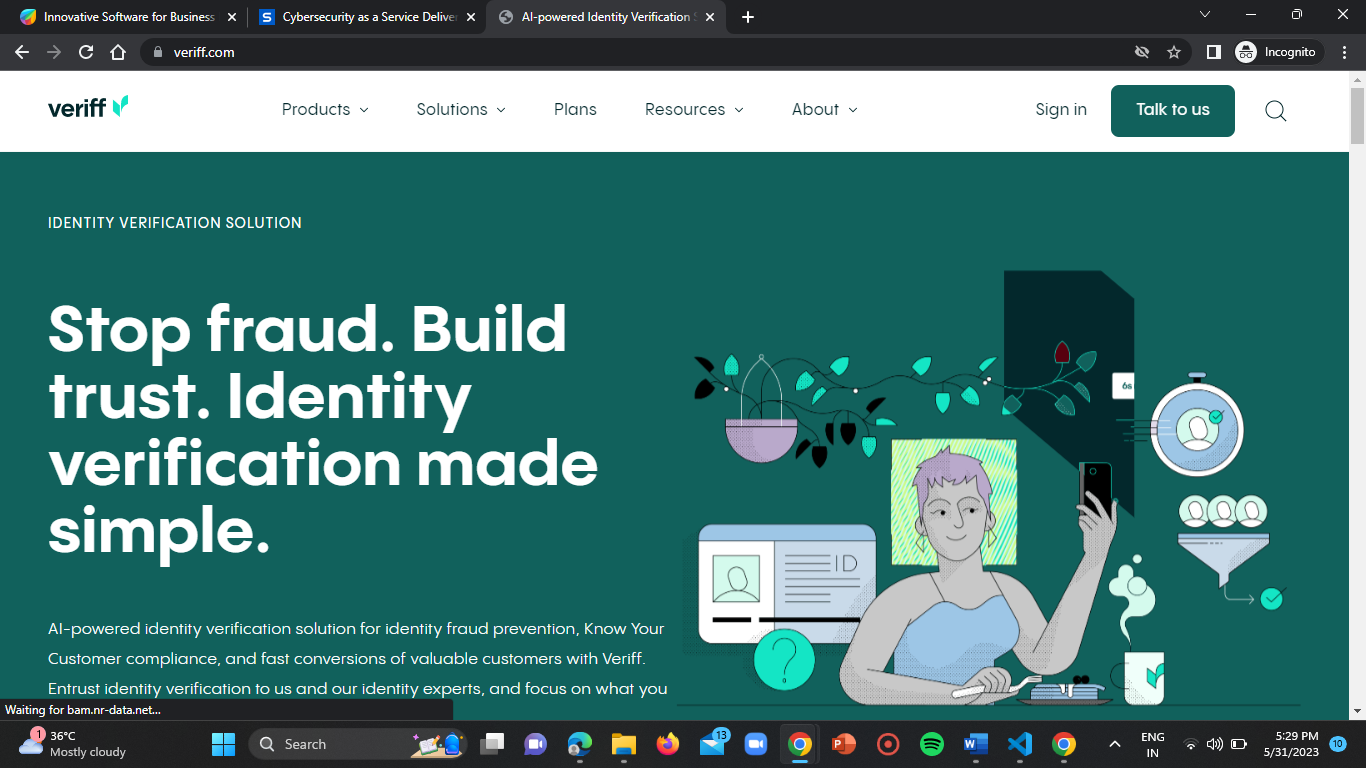


Result:

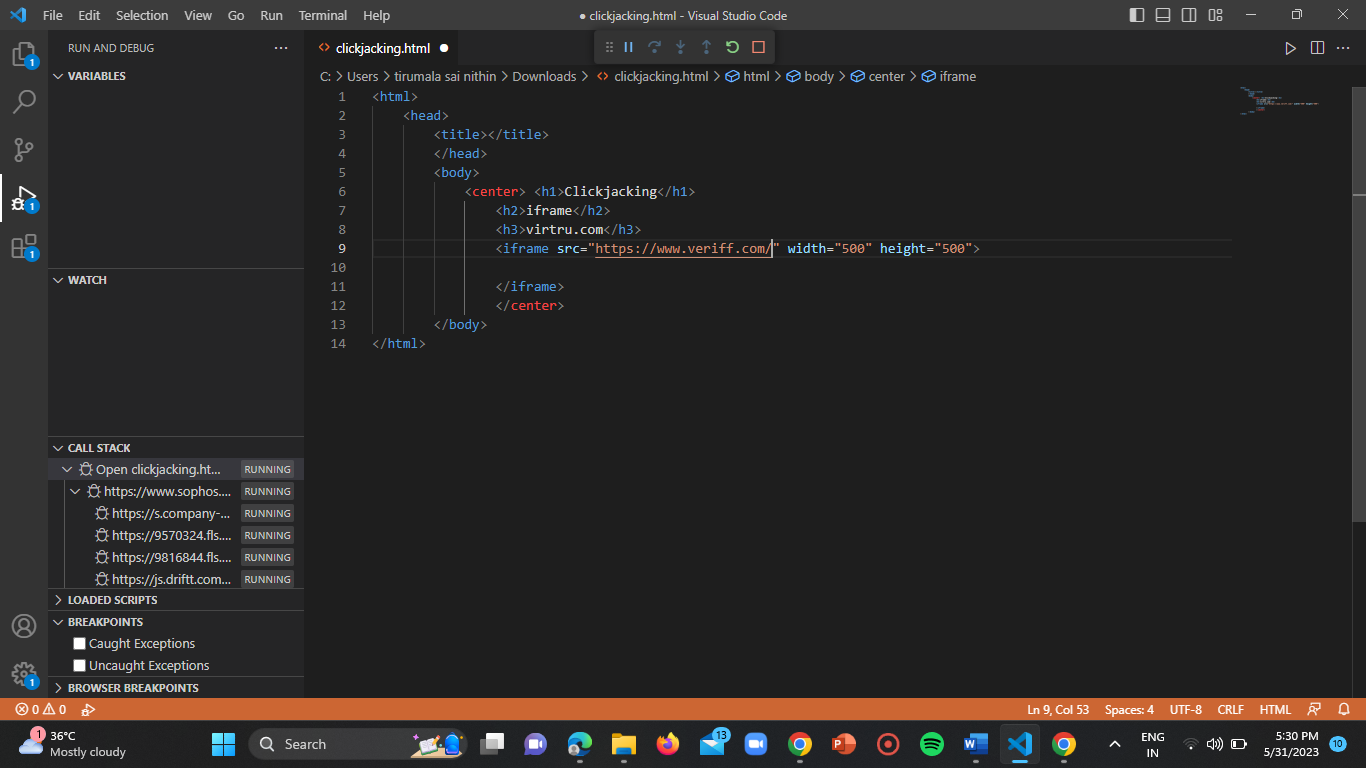


**WEBSITE-3:**

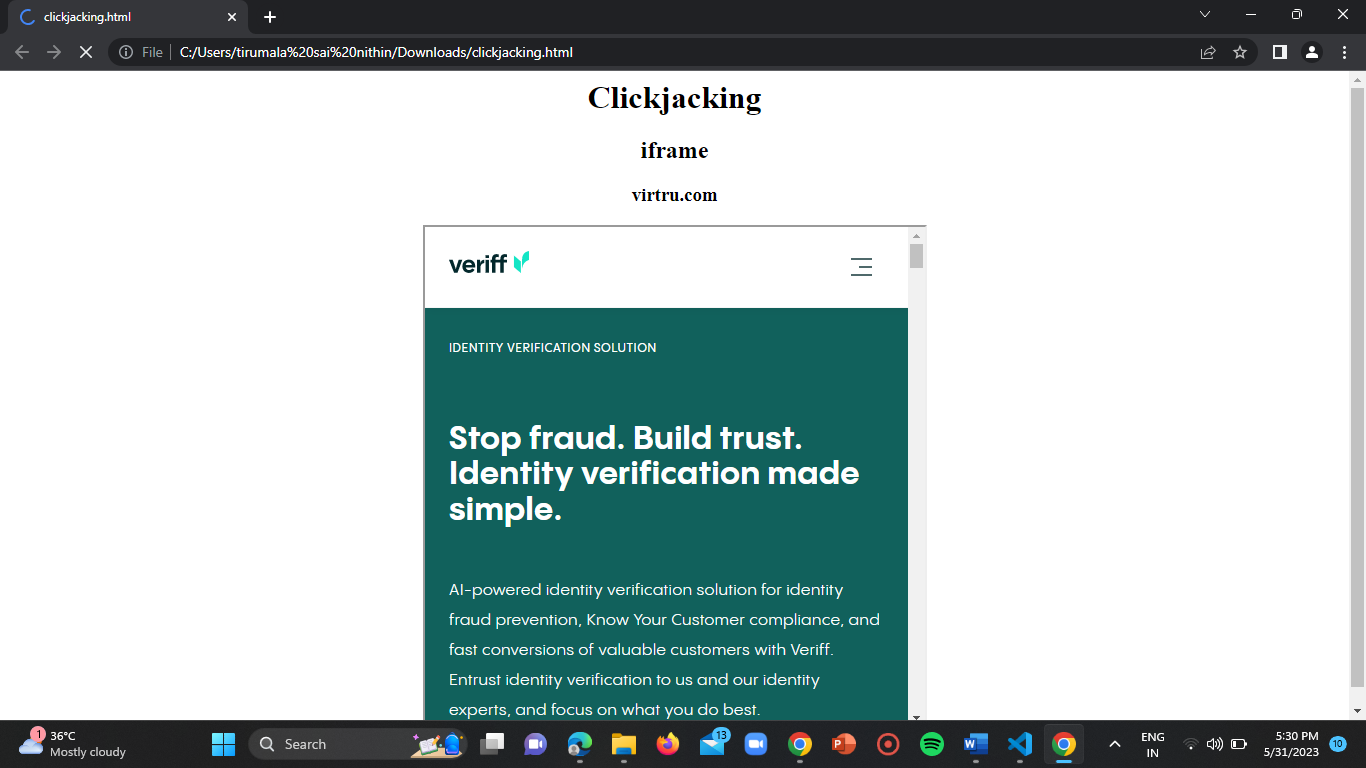
**URL =** <https://www.veriff.com/>



HTML page:



Result:



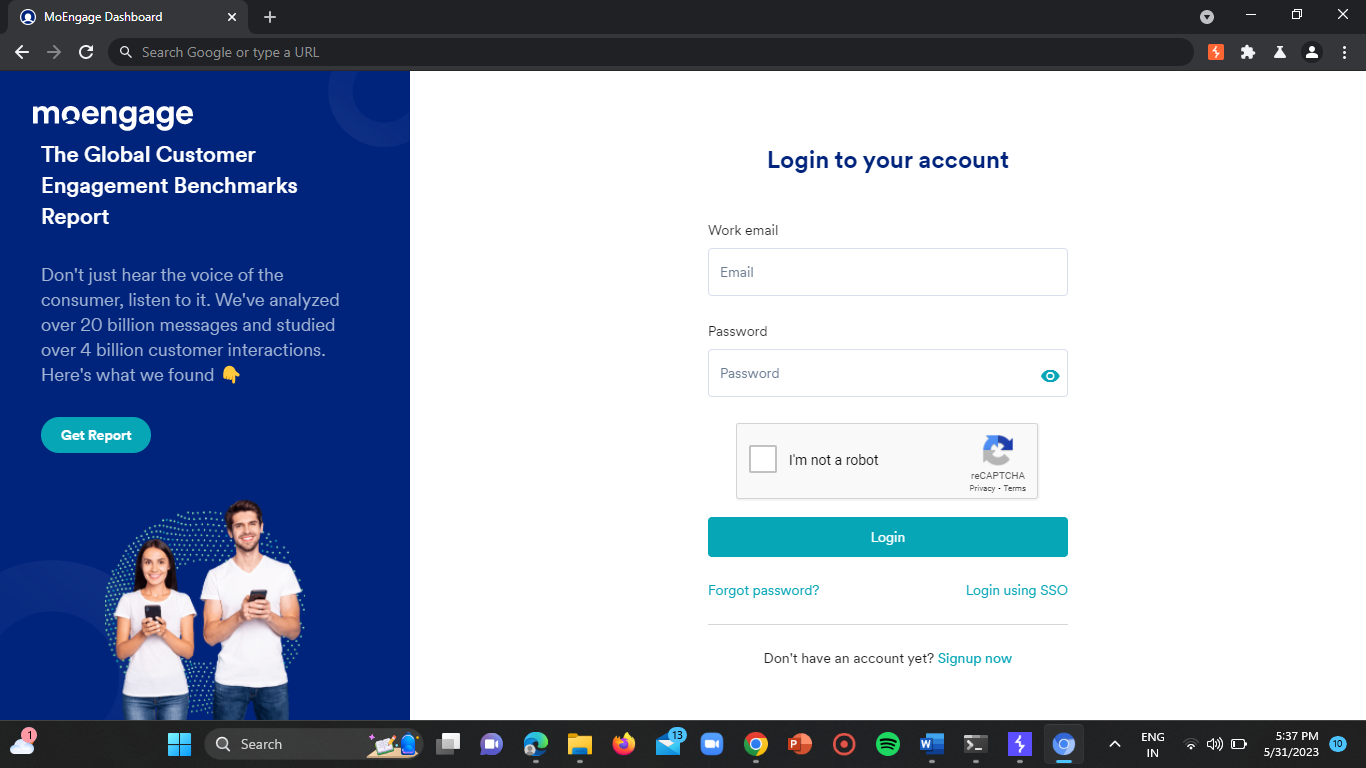
**Websites vulnerable to NO RATE LIMITING Vulnerability in login pages, usernames finder/ email enumeration pages:**

**WEBSITE-1:** <http://www.app.moengage.com/>

**URL =** <https://dashboard-01.moengage.com/v4/%23/auth>

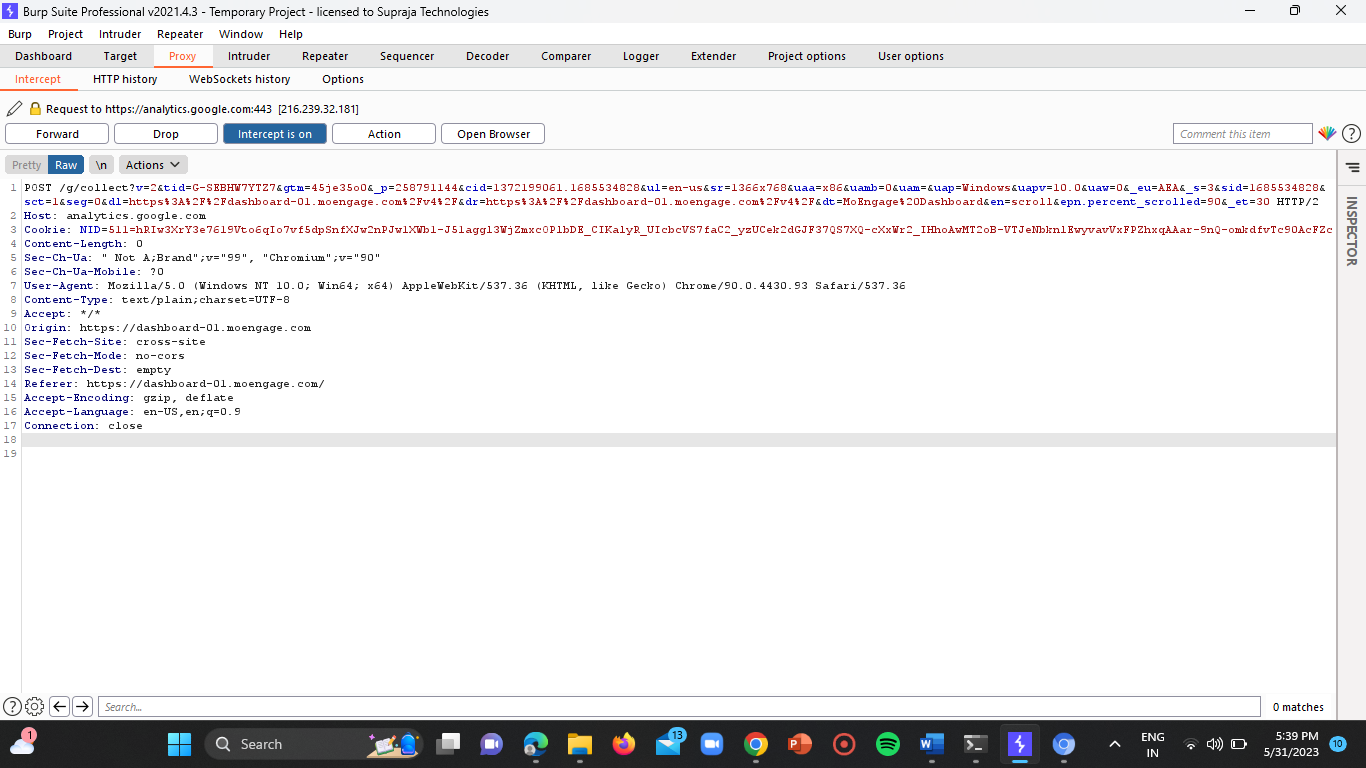
**Step-1:**

Open the URL in the browser.



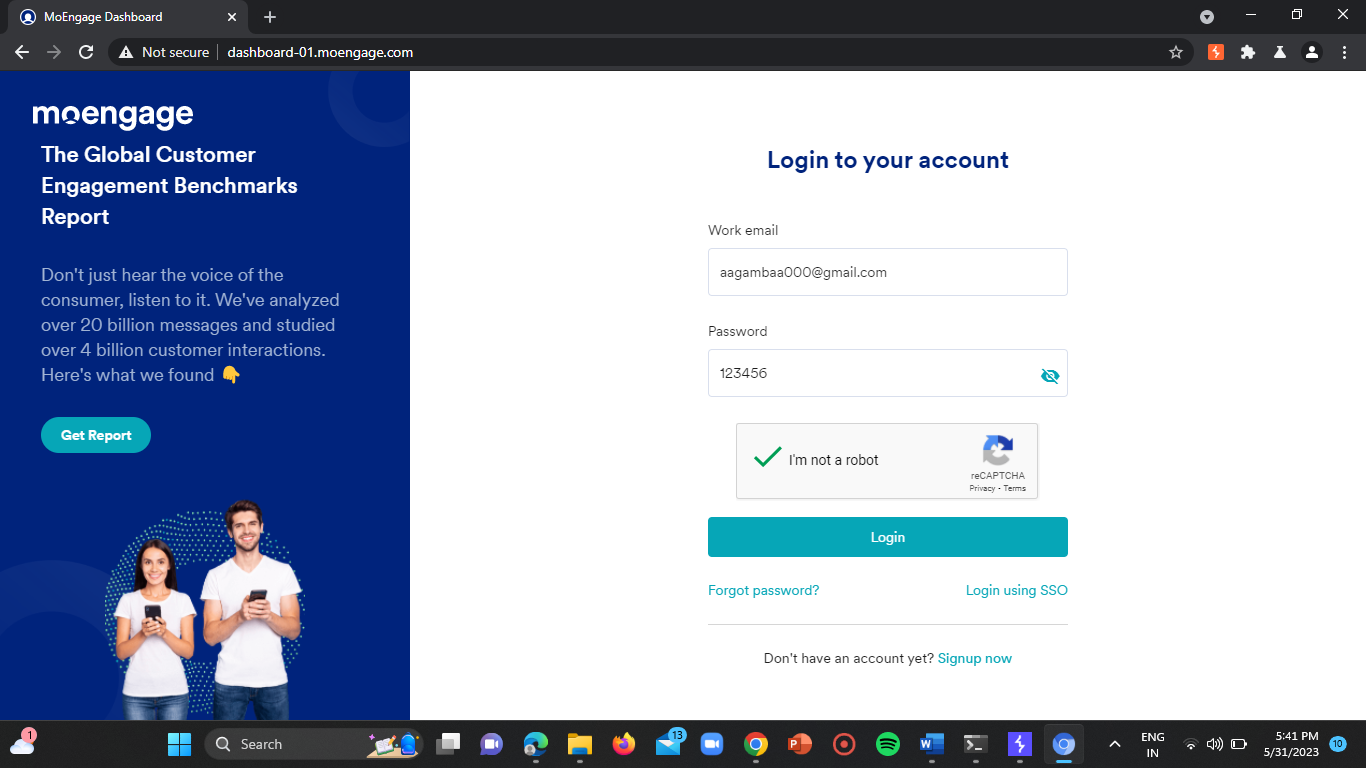
**Step-2:**

Turn on the intercept proxy in the burp suite.



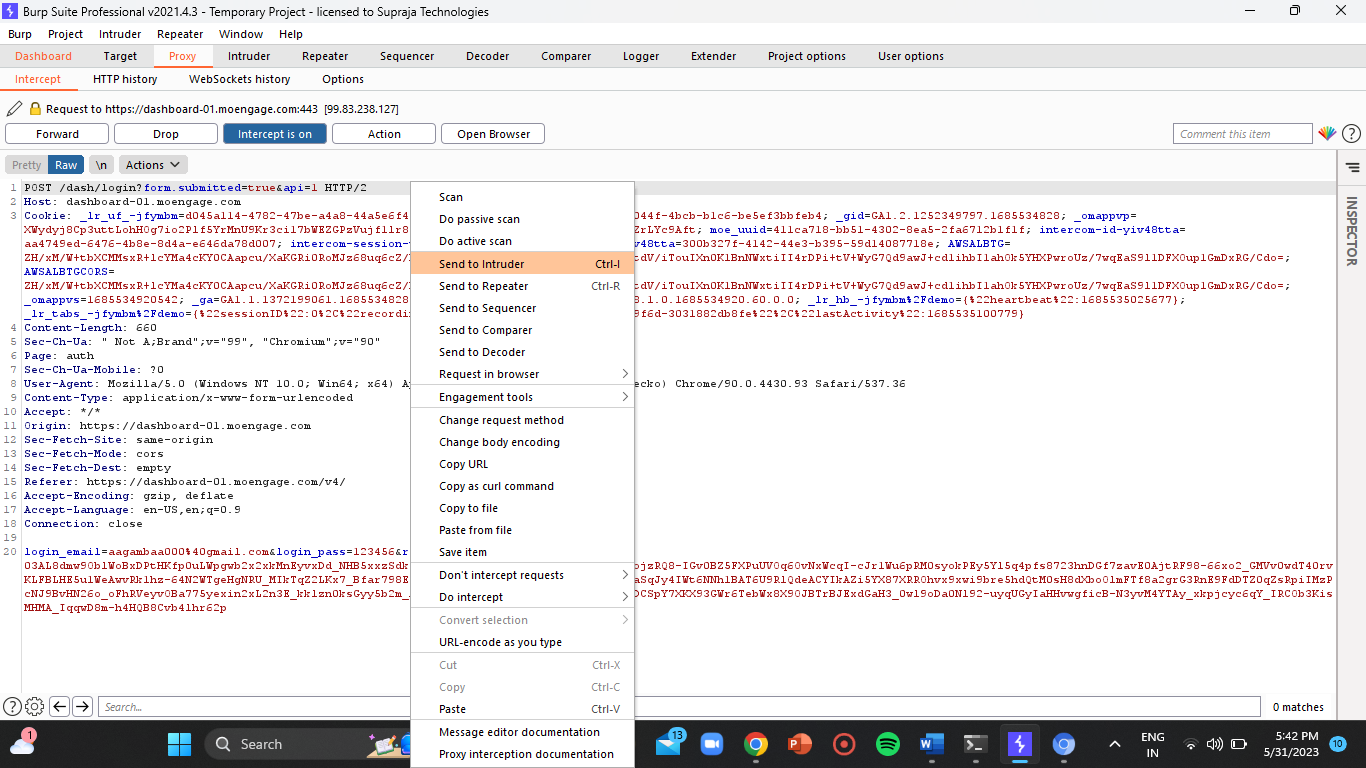
**Step-3:**

Then enter the username and password in their respective input fields and click on enter.



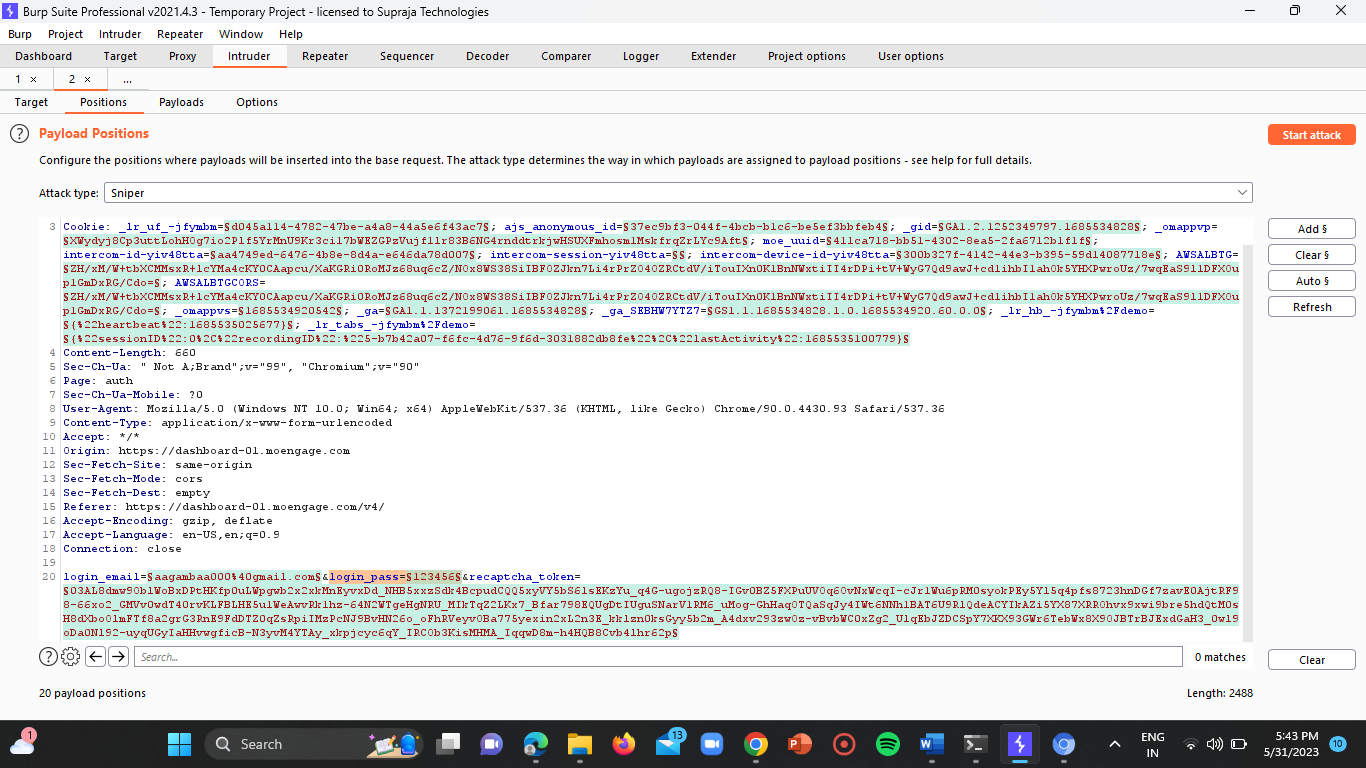
**Step-4:**

Forward the HTTP request to the intruder.



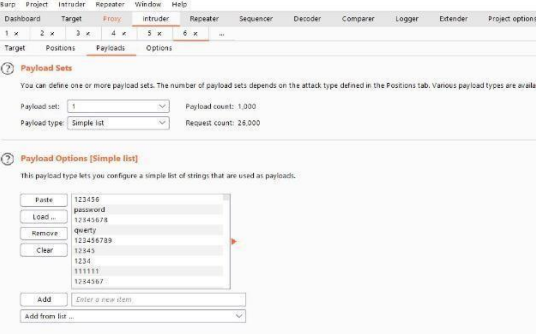
**Step-5:**

Now turn off the intercept and go to the intruder and select the password parameter.



**Step-6:**

Then click on the add button and load the password file from your internal storage.

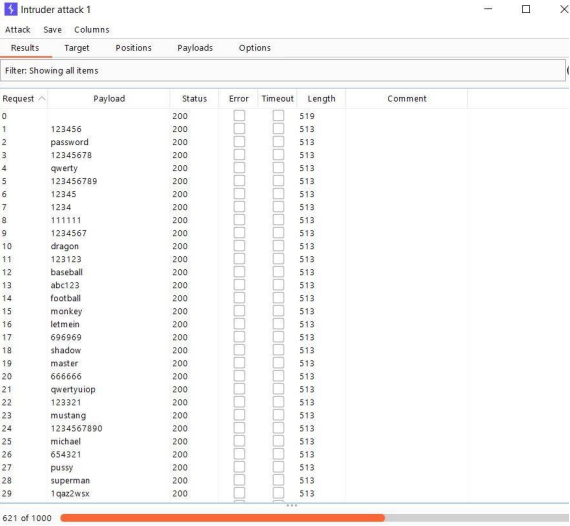


**Step-7:**

Start the attack and wait for some time.

You will be able to see 200 OK requests for 200 times.

If there are more than 200 OK responses within seconds, then the website is vulnerable.



**Websites vulnerable to NO RATE LIMITING vulnerability in categories.**

**1) forgot password or password reset pages**

**2) comment pages**

**3) review pages**

**4) get quote pages**

**WEBSITE-1:** <http://www.app.moengage.com/>

**URL =** <https://dashboard-01.moengage.com/v4/#/auth>

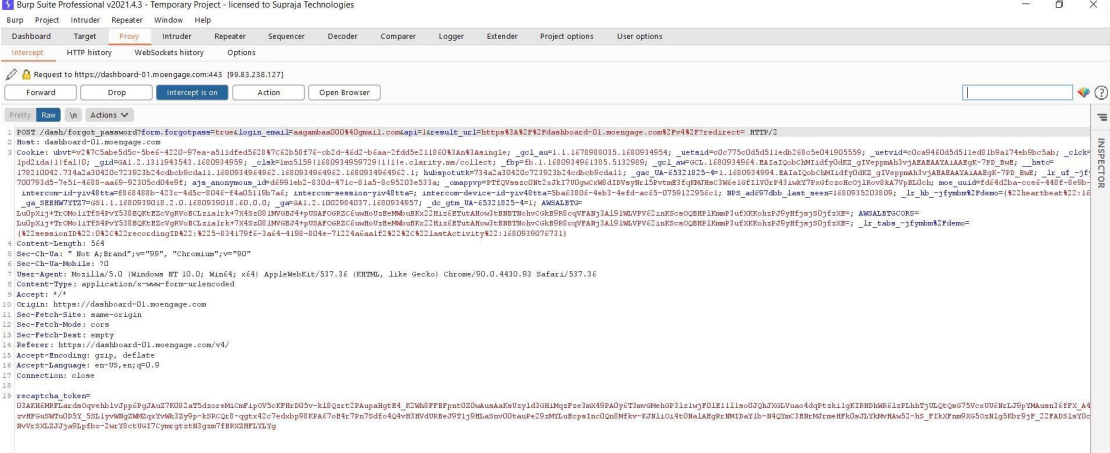
**Step-1:**

Open the above URL.



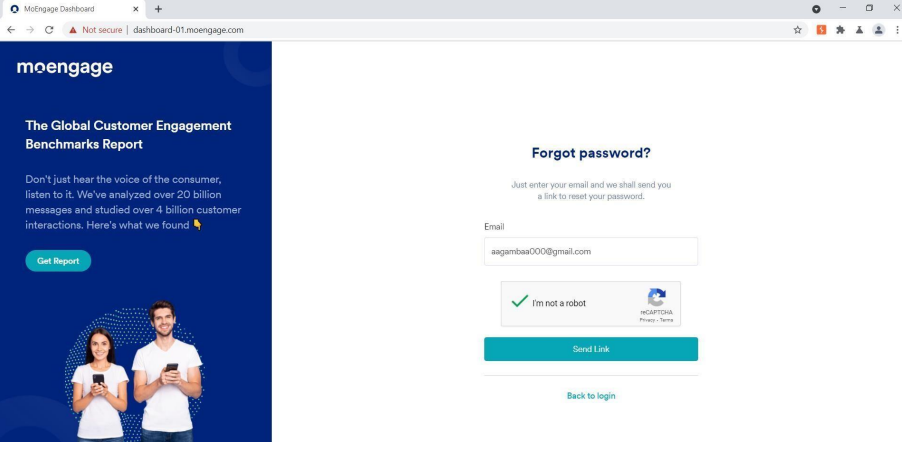
**Step-2:**

Turn on the intercept in the burp suite proxy.



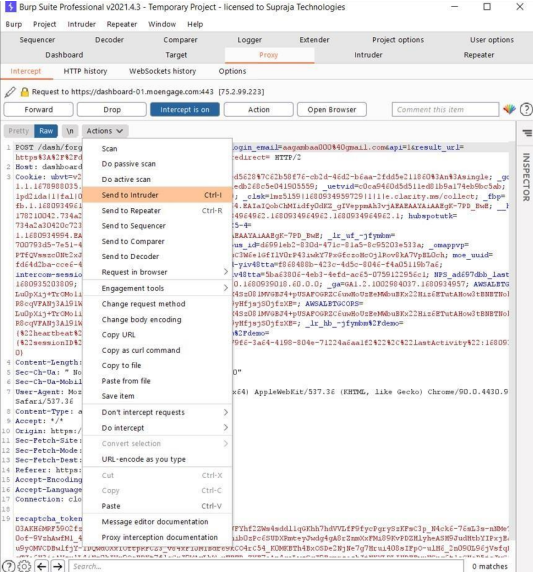
**Step-3:**

Enter the username and password in their respective input fields and clik on enter.



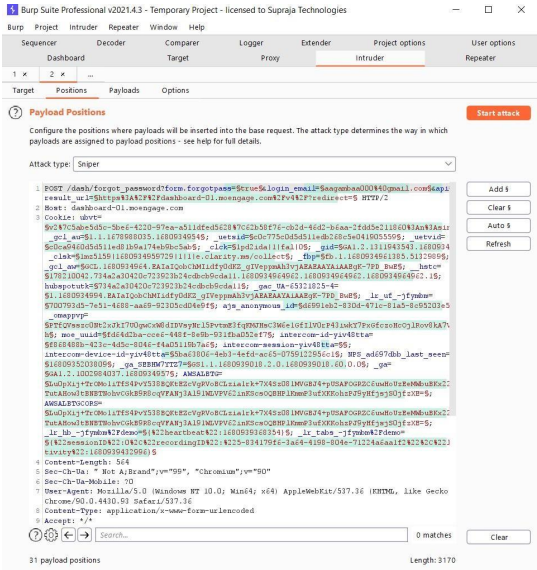
**Step-4:**

Forward the HTTP request to the intruder.



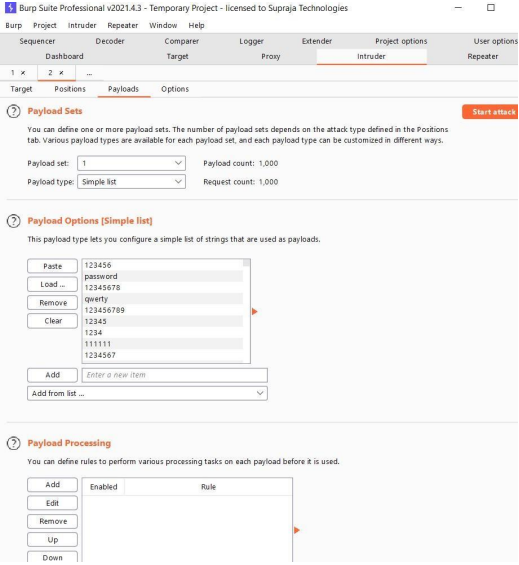
**Step-5:**

Turn off the intercept and go to the intruder and click on the clear button in the position tab.



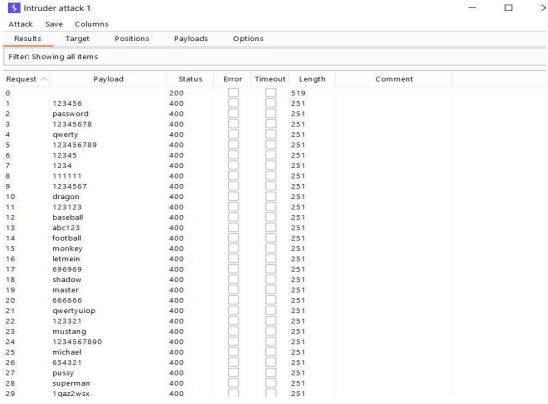
**Step-6:**

Select the email/username parameter value and click on add button and load the password file.



**Step-7:**

Start the attack and wait for more than one minute.



**Step-8:**

If there exist more than 200 requests stating that 200 OK responses within a few seconds then the domain is vulnerable.

**CONCLUSION:**

By performing this task we learnt about how an attacker utilises the CLICKJACKING and NO RATE LIMITING vulnerabilities in a web application to gain unauthorised access to the sensitive data. Also we got to know the importance of fixing up such bugs in the web applications which provides gateway to the attackers to perform such attacks.