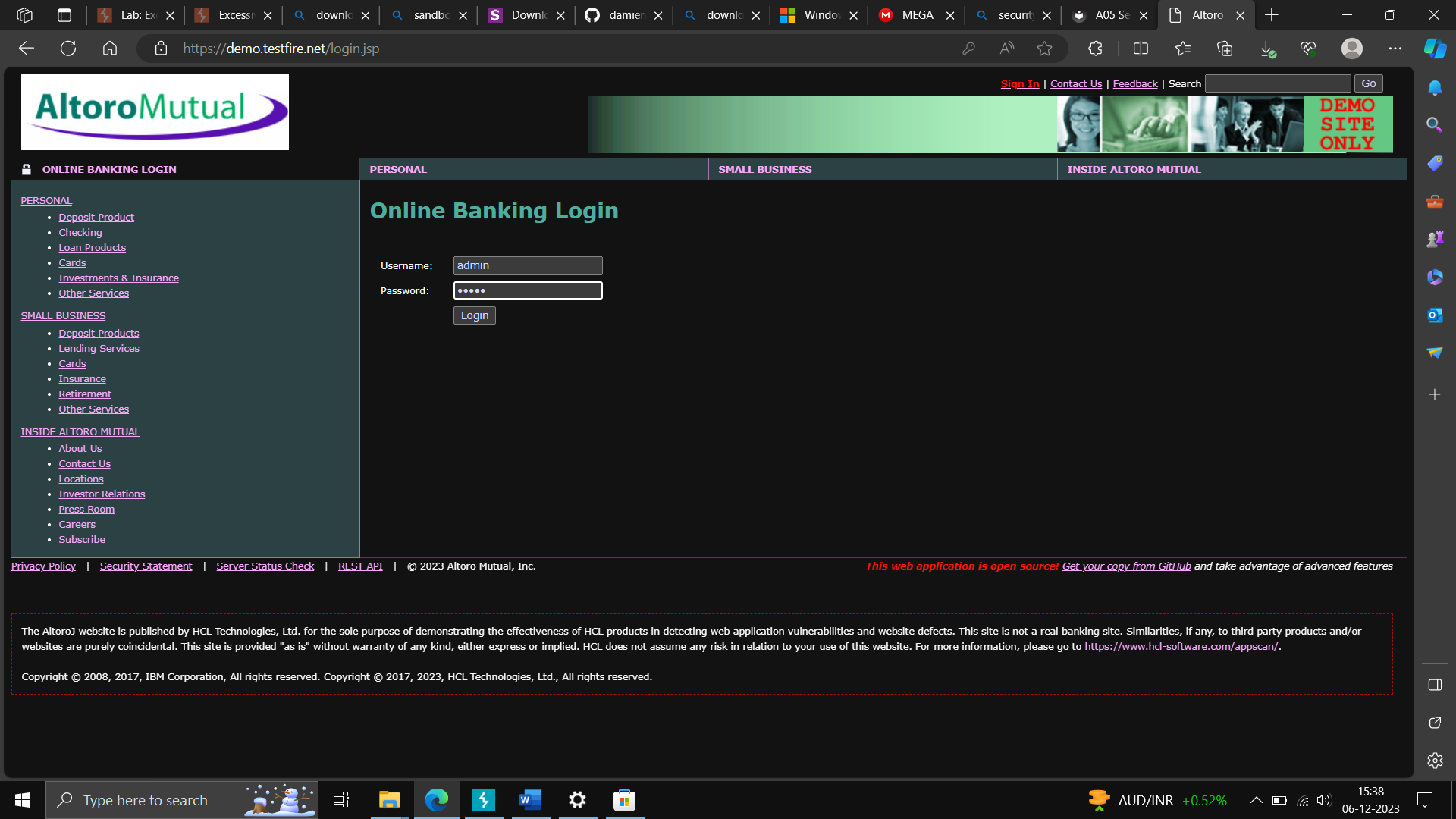
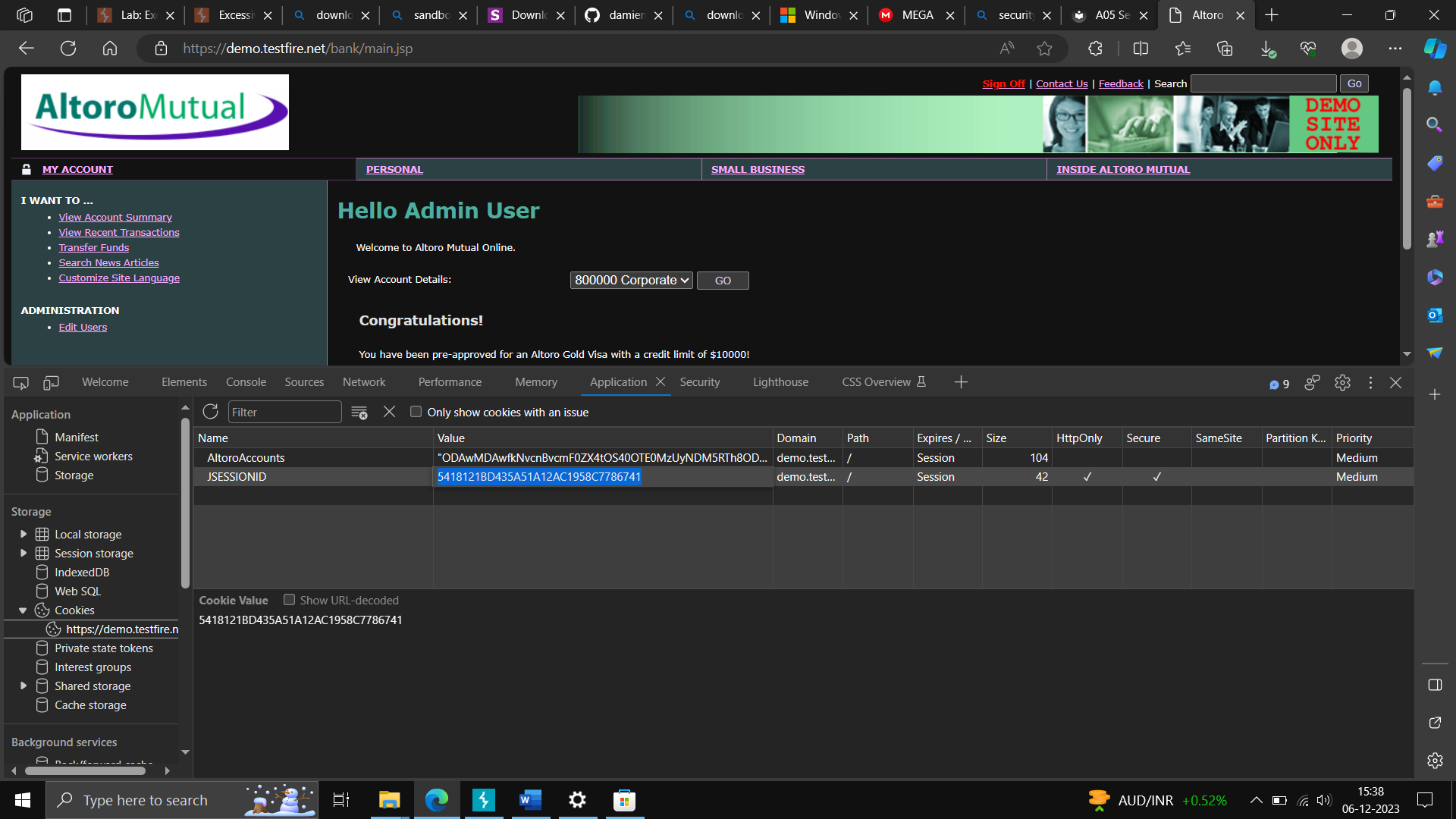
**BROKEN AUTHETICATION**

POC

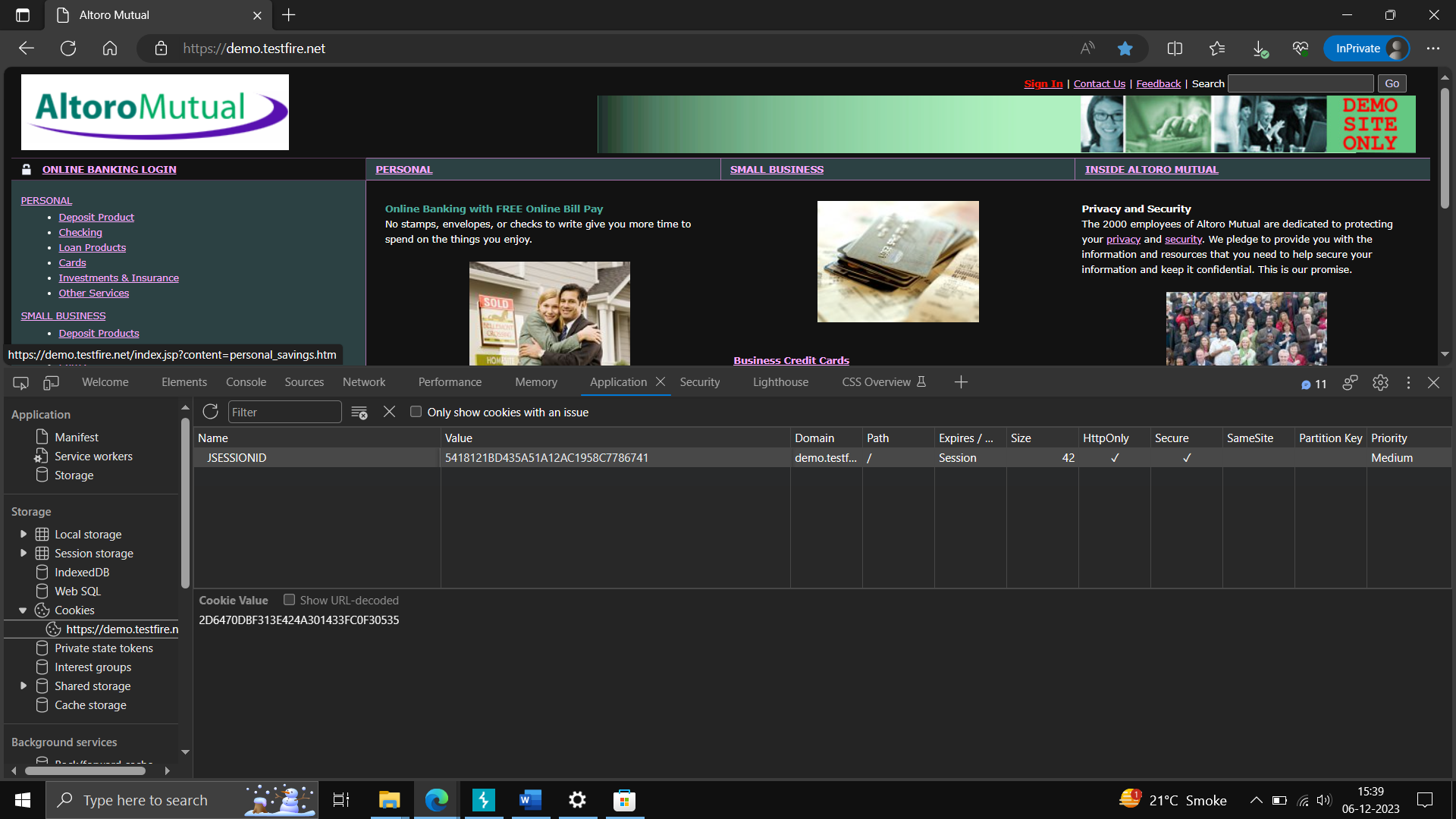
Step1-) open demo.testfire.net-> login as user name admin, password admin -> click on login ->



Step2) On the dashboard, right click inspect -> Storage/Application -> go on cookies -> view the site->copy the session -> paste in notepad ->



Step3)-go on any another browser like chrome, open the same website in browser-> right click on the screen, go on inspect element-> go on application->check the cookies and edit it with the cookies paste in notepad.



This attack is also called as Session Hijacking.

**LFI or RFI**

**POC-**

Step 1-

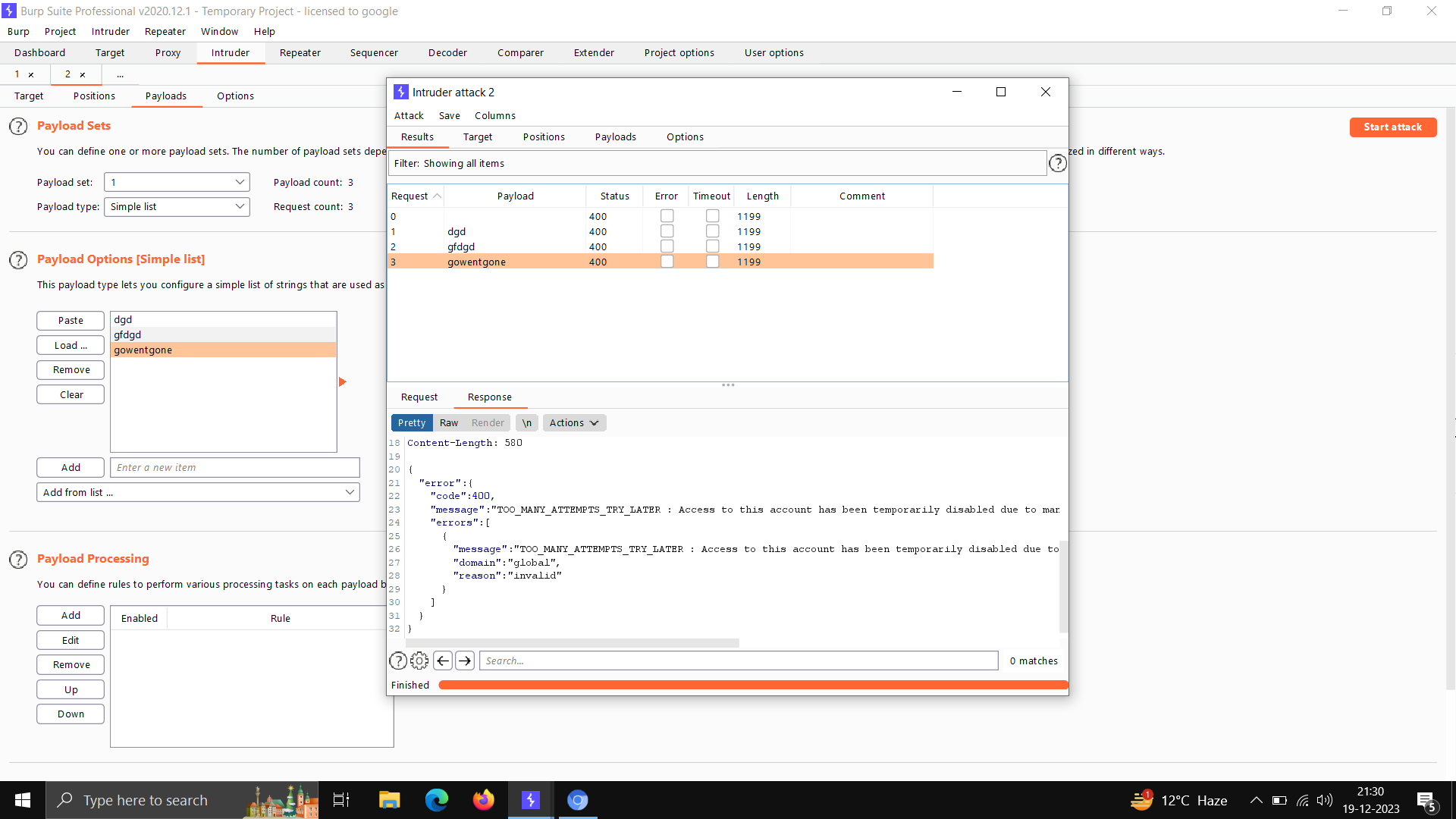
# Access the lab - Lab: [File path traversal](https://portswigger.net/web-security/file-path-traversal), simple case

# Try opening the image in new tab and check the parameter in burpsuite and use brute force for changing the directory

# 

# 

**USERNAME ENUMERATION –**

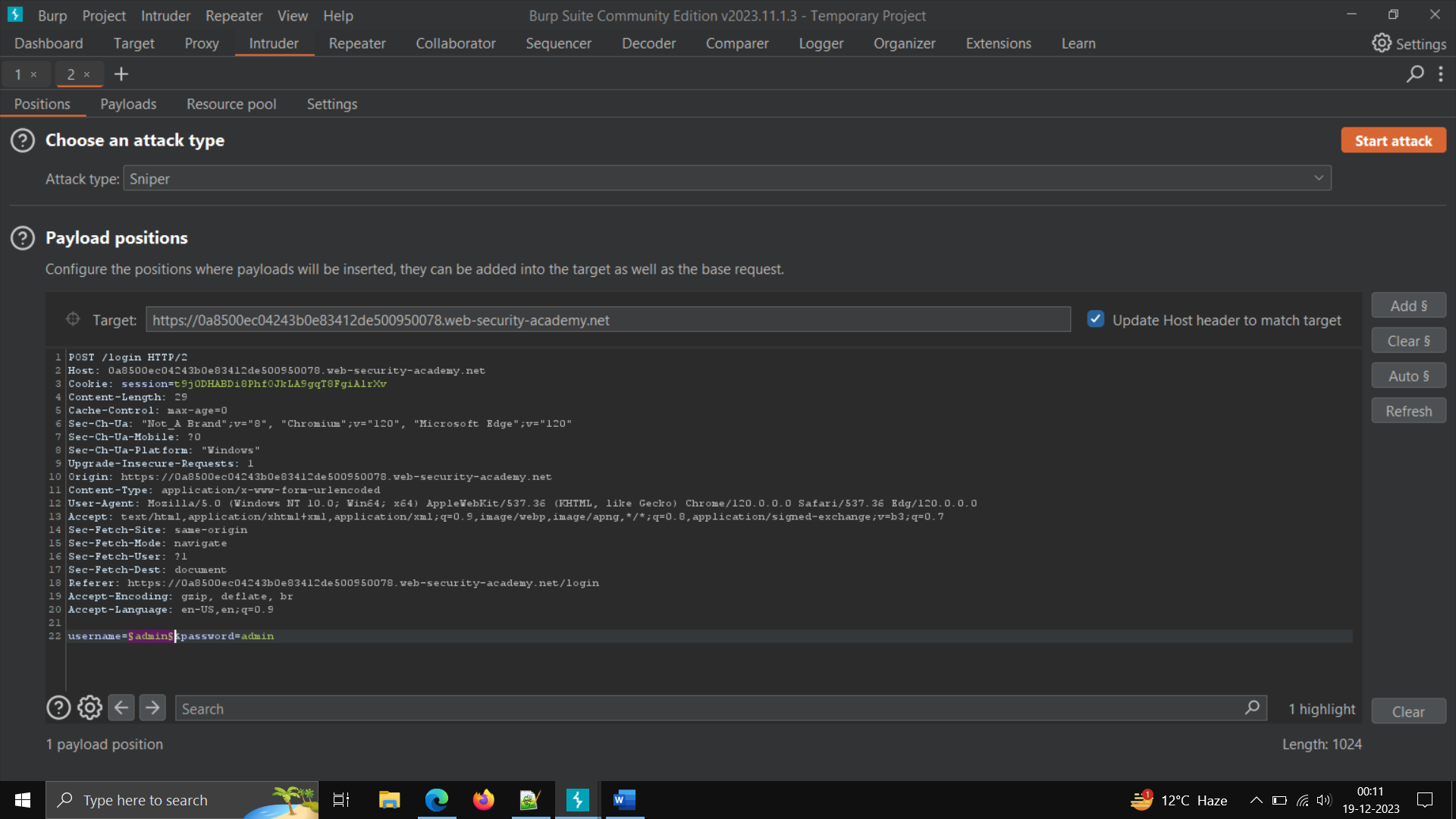


**POC –**

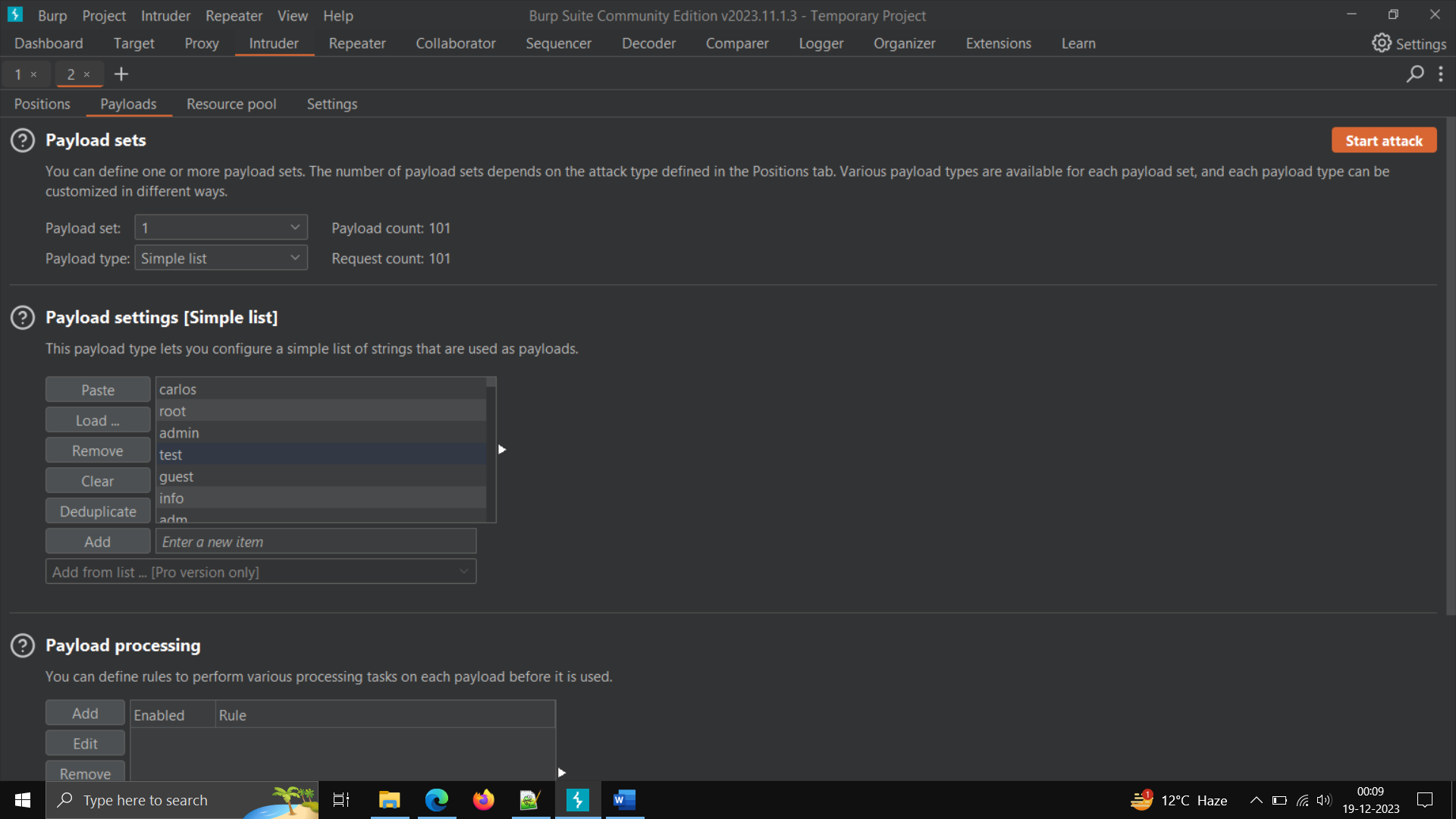
# Step 1 – access the lab - Username enumeration via different responses

# 

**Step 2 – copy the request to Intruder and set the payload at username = value – like this $ value$**



**Step3 – copy the list from the lab and set it as simple test in attack**



**Step4 -start attack – in valid input you will find the session ID.**

