## **School of Computer Science**

## **UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

## **DEHRADUN-248007**

## **SEMESTER- 4**

## **AUG-DEC 2023**

## **LAB FILE**

## **SUBMITTED BY : ARUSH DUBEY**

## **SAP ID : 500106703**

## **BATCH 1**

A web server creates cookies, which are little data files that are transmitted to a web browser.

They assist the website in remembering details about your visit, including your login credentials, shopping cart contents, and preferences.

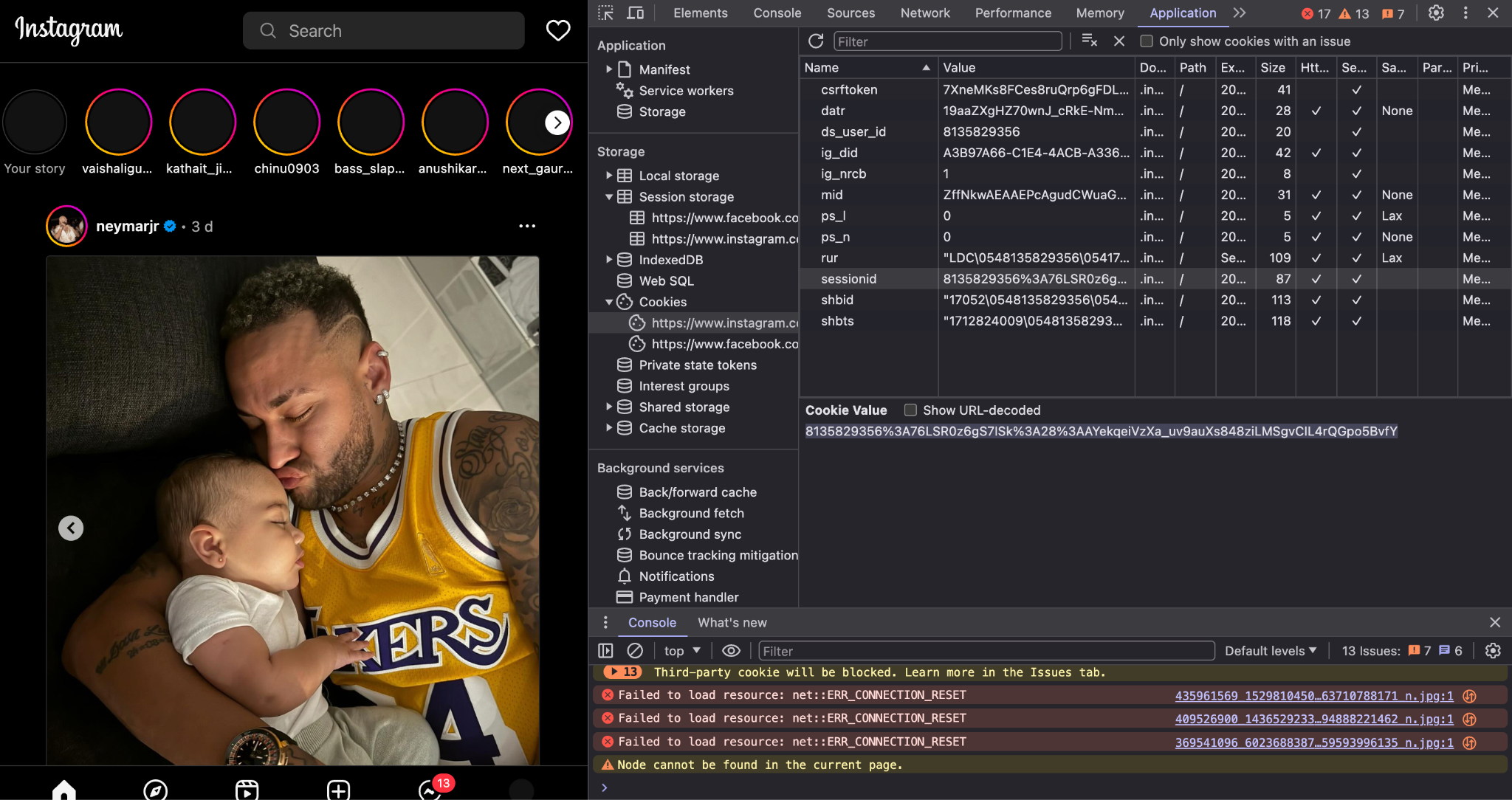
For a set amount of time, or the duration of a user's session on a website, web browsers retain the cookies they receive.

## What is cookie stealing?

A cyberattack described as "cookie stealing" happens if someone steals cookies from a user's computer in order to access their data or login credentials,if a malicious actor gains access to a user’s cookies, they can use that information to hijack their session and access sensitive data

**How Cookie Stealing happens**

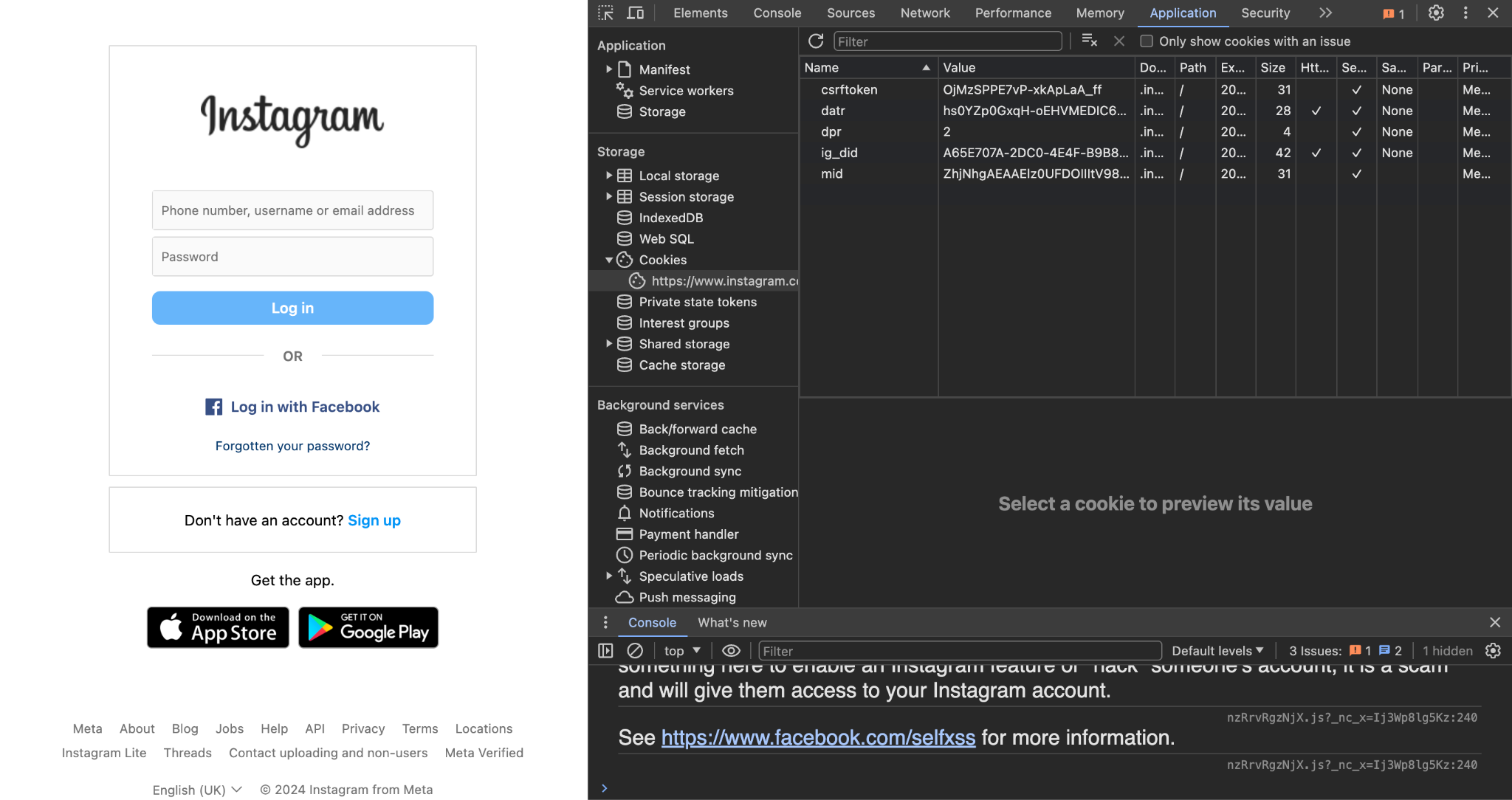
1. Open any site in a browser and login
2. Go to inspect, Click on application
3. Copy value [ eg – sessionid ]



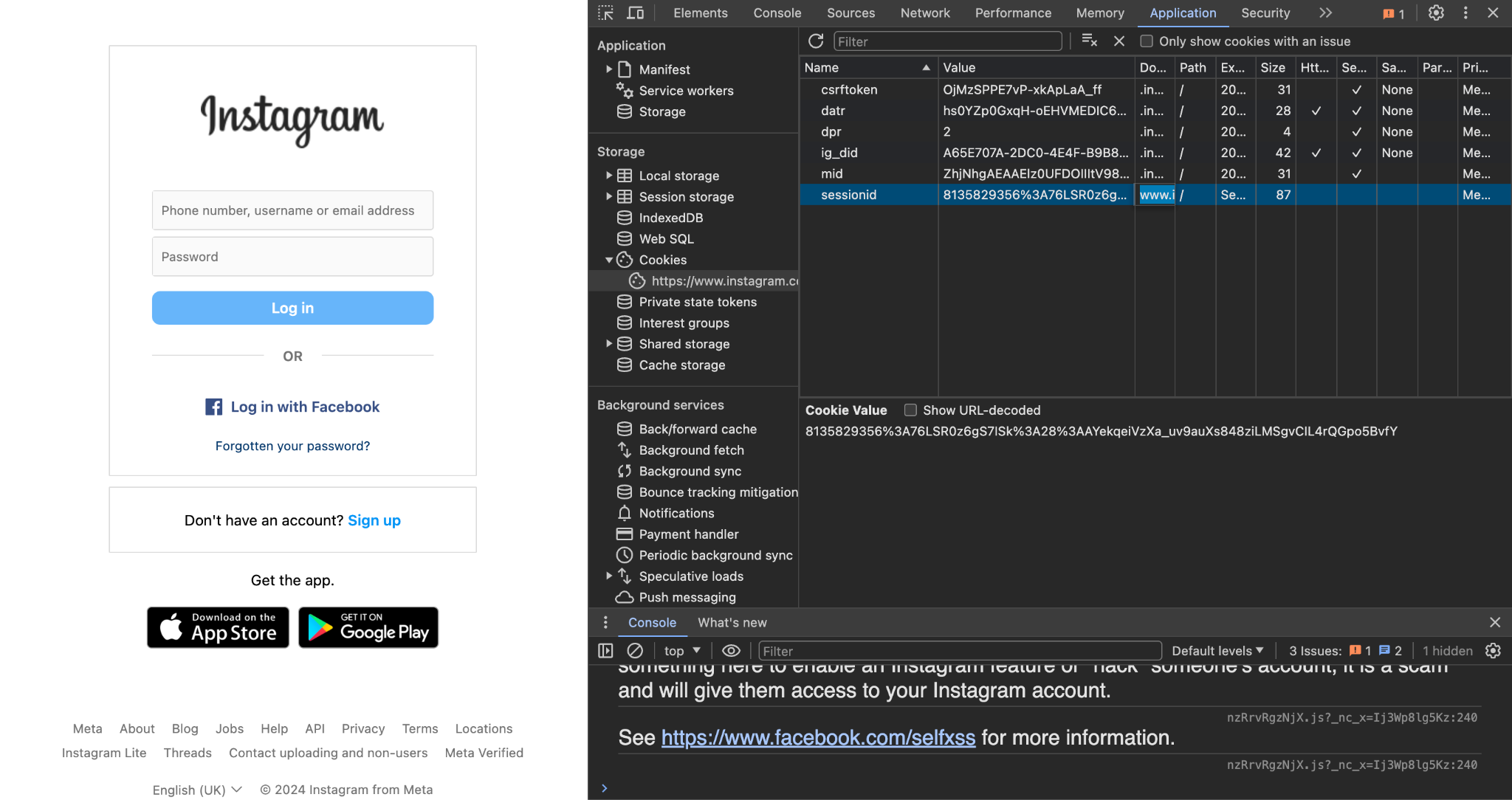
4.Open another brower where the site is not login

5.Again go to inspect and then to application

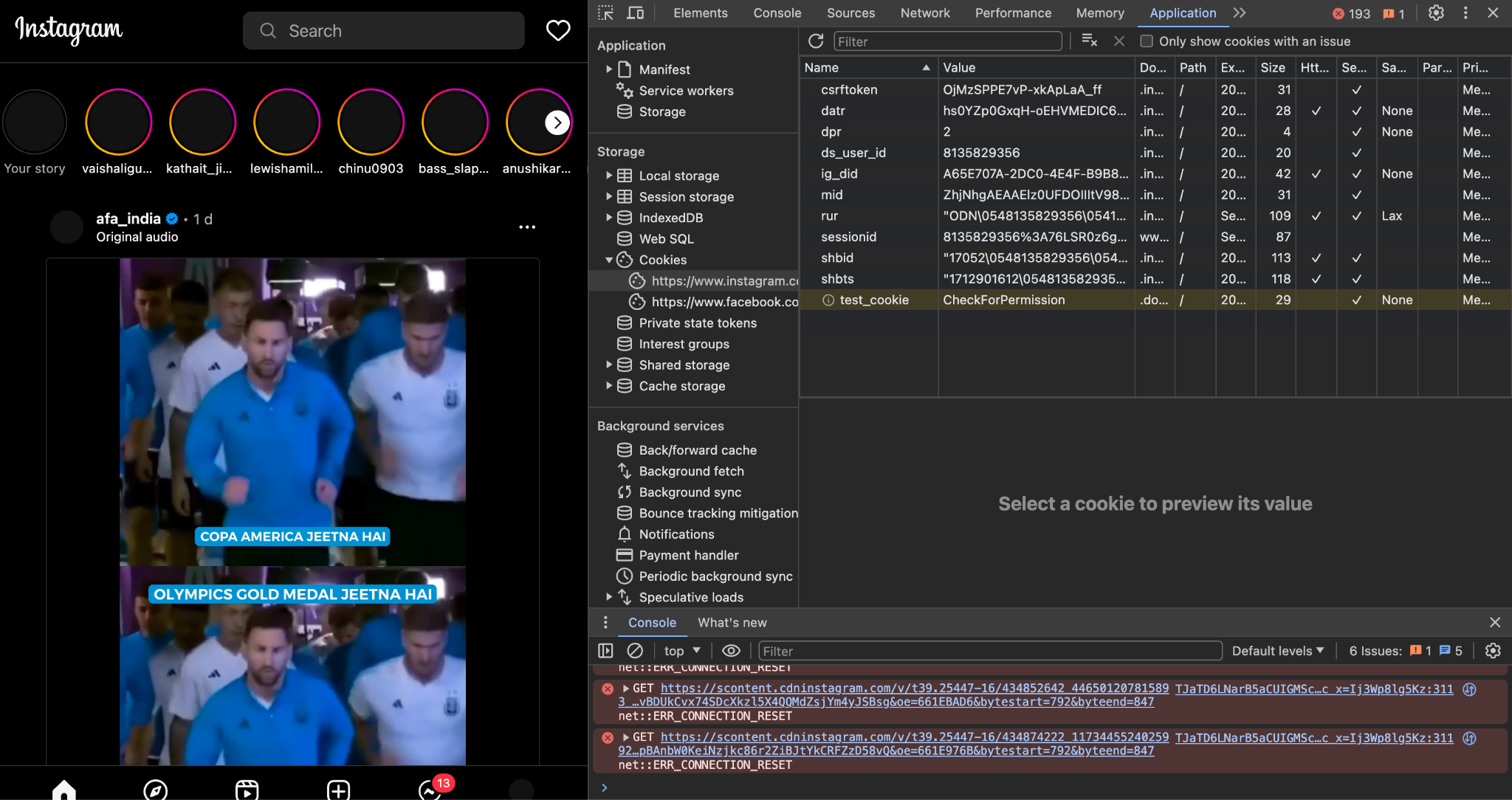
6.Now paste the copied value there



Now pasting the cookie with name as session id



And now we refresh the website



Now trying with [Demo.testfire](https://demo.testfire.net/bank/main.jsp):

Login with

User : Admin

Password : Admin

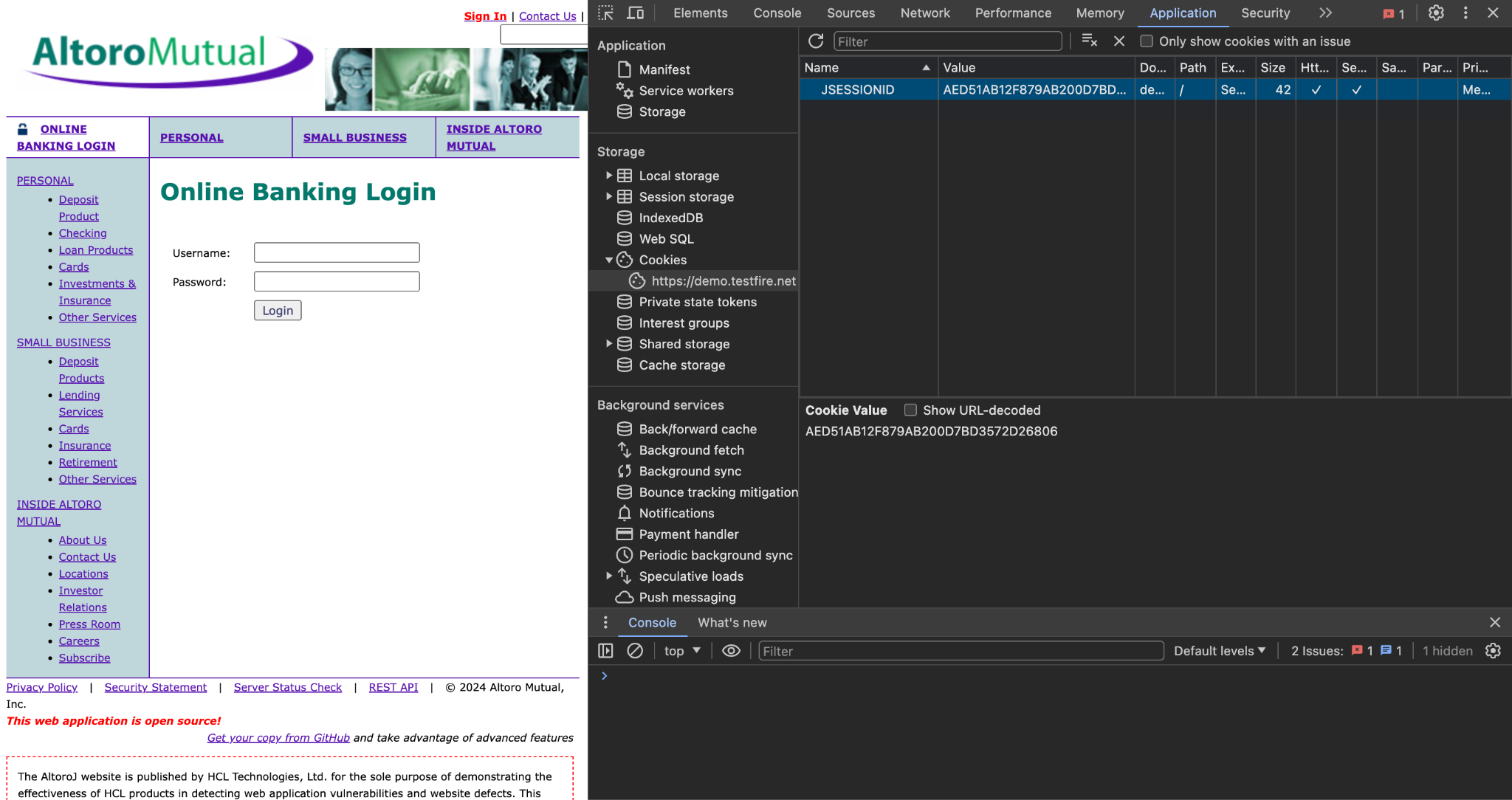


Then we copy the Session id

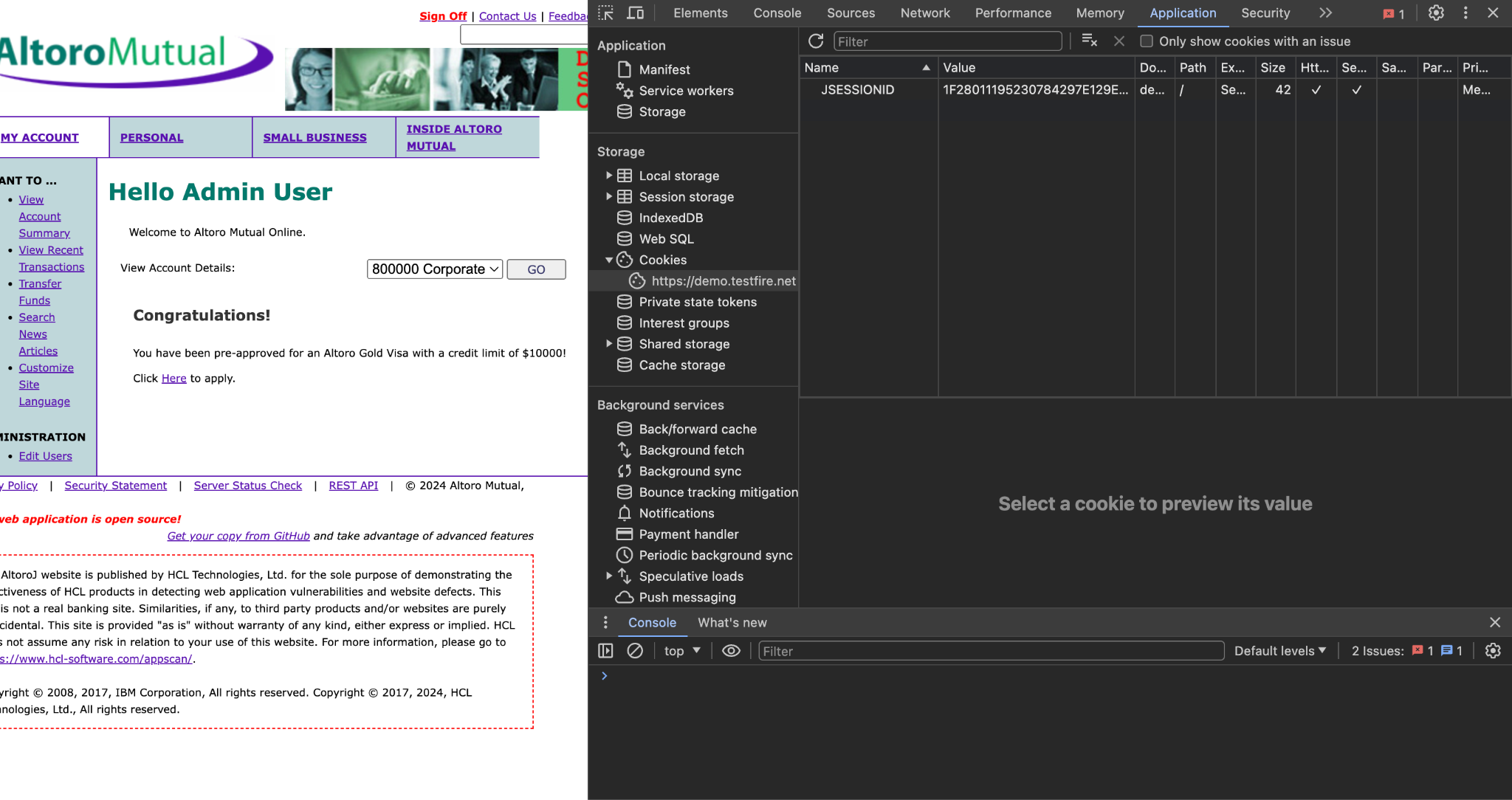
Next we go to a new browser and open the website



Now we inspect in the new browser



And now we paste the cookie from the other browser(sessionid) and then we reload



We can now clearly see that we have hijacked the session

## How to recover from a cookie stealing attack?

* **Scan for malware:**
* **Clean malware:**
* **Force logout of all sessions:**
* **Change passwords:**
* **Update** [**plugins**](https://blogvault.net/update-wordpress-plugins/) **and** [**themes**](https://blogvault.net/how-to-update-wordpress-theme/)**:**

## How to prevent cookie hijacking?

* **Install a firewal**l:
* **Use SSL:**
* **Use two-factor authentication:**
* **Implement strong password policies:**