**Name: Samarth Jain**

**USN: 4SU20CS081**

**Course: Cybersecurity**

**Trainer: Bharath Kumar**

**Date: 30/08/2023**

## Assignment Details

Assigned Date: 29/08/2023

Due Date: 30/08/2023

Topic: Capturing HTTP messages

## Introduction

Burp Suite is a powerful and widely used web vulnerability scanner and penetration testing tool. One of its key features is the ability to capture and analyze HTTP messages, which is essential for identifying and addressing potential security vulnerabilities in web applications. Capturing HTTP messages in Burp Suite is a fundamental step in the assessment of web applications' security posture.

To capture HTTP messages in Burp Suite, you first need to set up your proxy settings. You configure your web browser or application to route its traffic through Burp Suite's proxy server. This allows Burp Suite to intercept and record all HTTP requests and responses sent between your browser and the web server. Once the proxy is configured, Burp Suite acts as a man-in-the-middle, allowing you to inspect and manipulate the traffic.

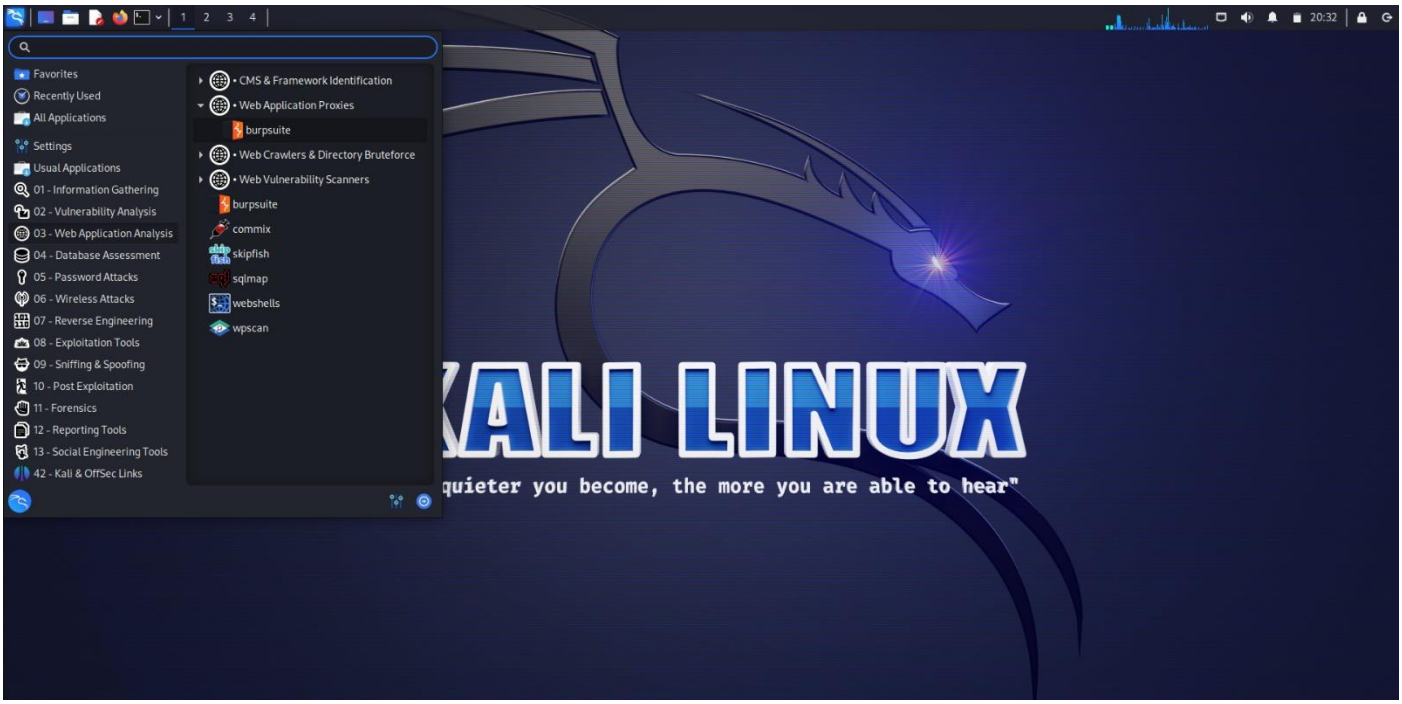
Once the proxy is configured, Burp Suite provides a user-friendly interface for viewing and analyzing captured HTTP messages. You can review the requests and responses in a structured manner, including headers, parameters, and payloads. This enables security professionals to identify potential security flaws such as injection vulnerabilities, cross-site scripting (XSS), and broken authentication.

Additionally, Burp Suite offers various tools for further analysis and exploitation of captured HTTP messages. Security researchers can use the Repeater tool to modify and resend requests, the Intruder tool for automated fuzzing, and the Scanner tool for vulnerability detection. Overall, capturing HTTP messages in Burp Suite is a crucial step in the process of identifying and mitigating security vulnerabilities in web applications, making it an invaluable tool for web security professionals.

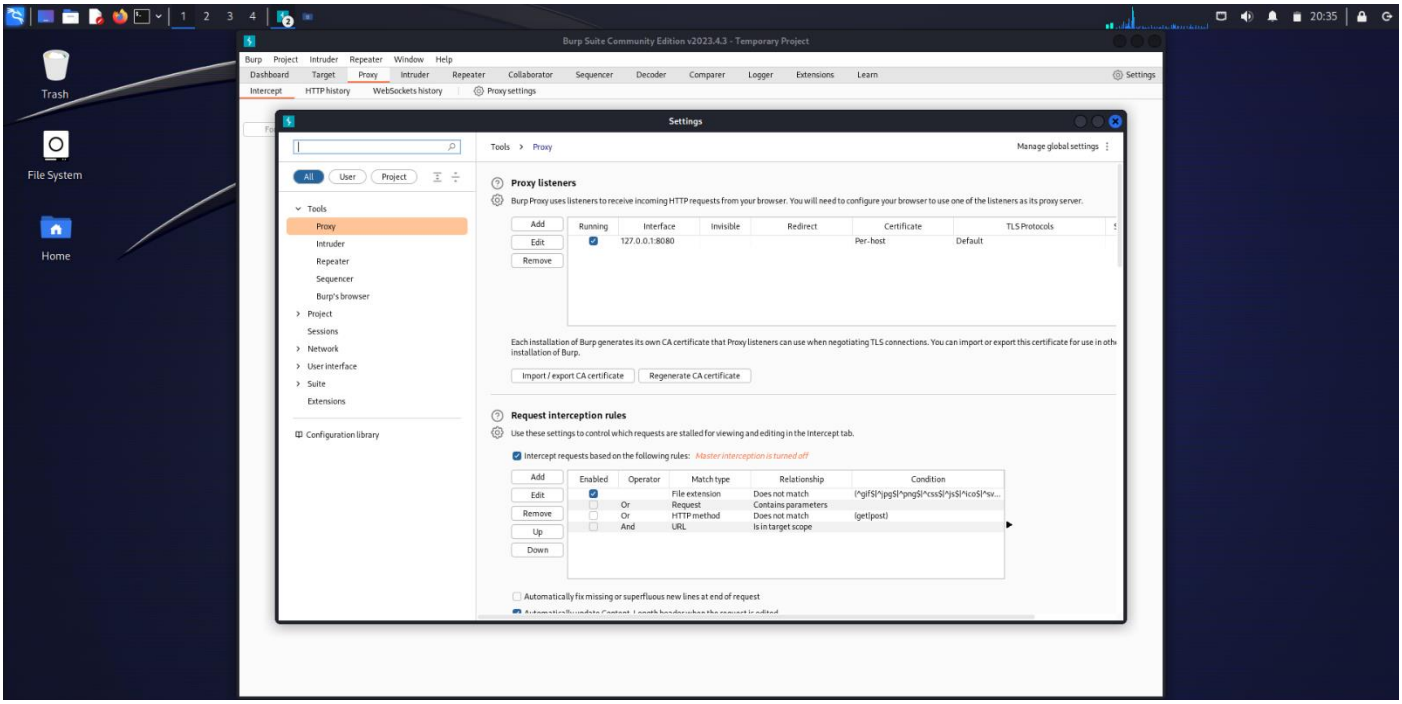
## Content

## Steps to Configure Burpsuite onto Firefox

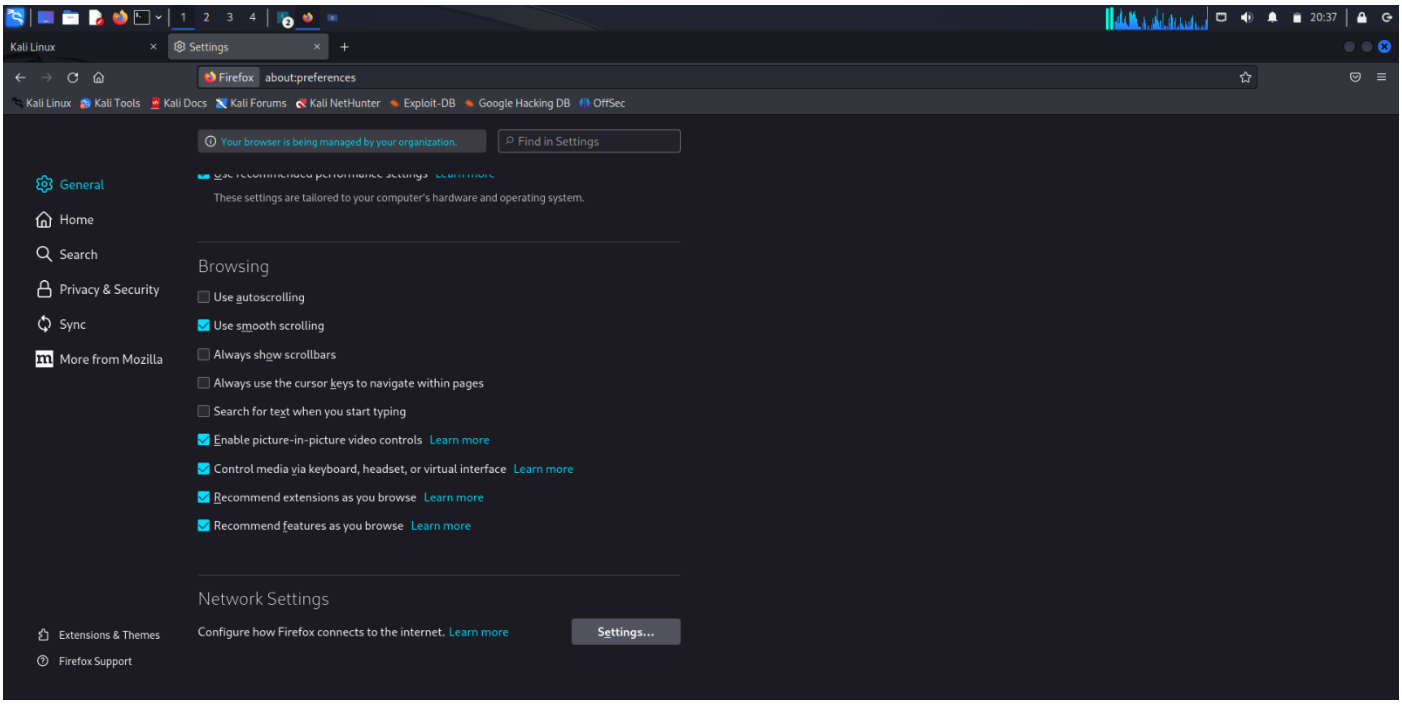
1. Locate Burpsuite
    - Click on Aplication on the top-left corner in Kali Linux
    - Select 03 – Web Application Analysis
    - Select Web Application Proxies
    - Click on Burpsuite



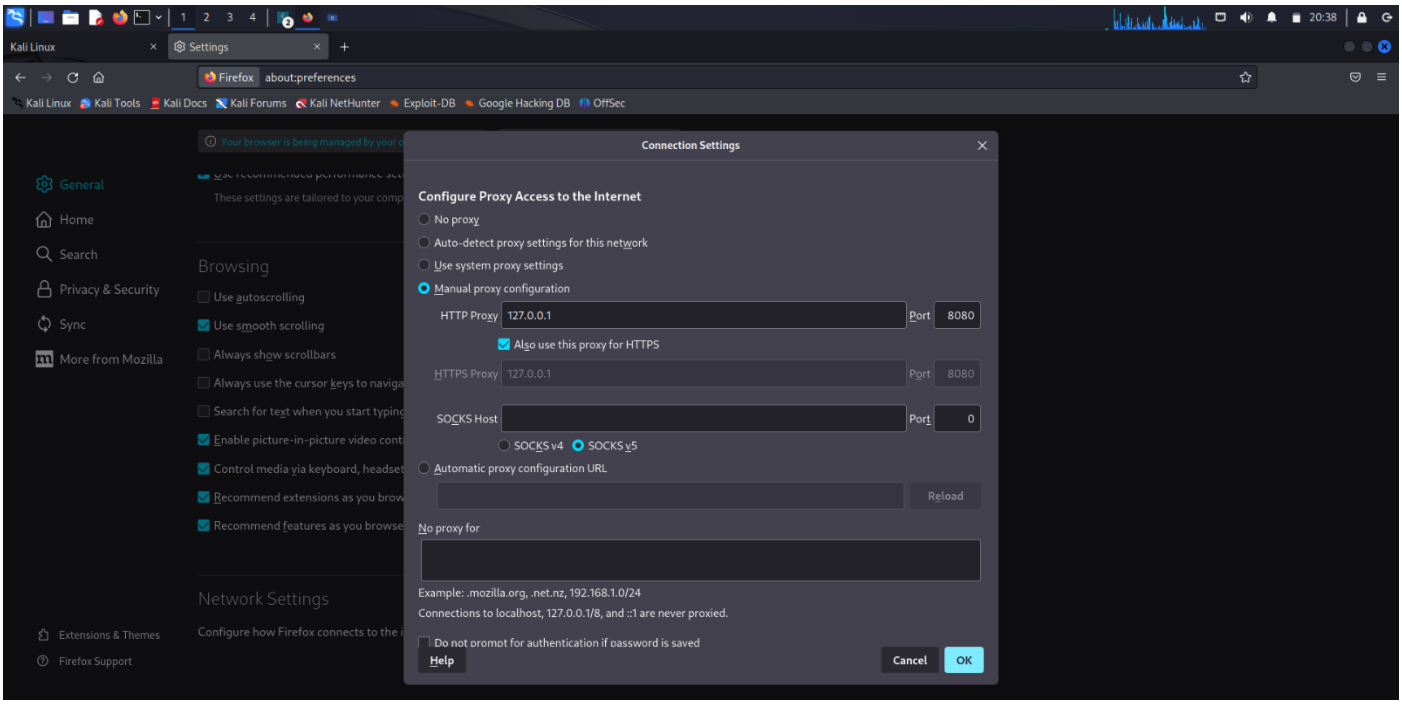

2. Ensure burpsuite is running on Localhost and Port 8080
    - Open Proxy tab
    - Click on Proxy Settings
    - Make sure it is running on Localhost(IP address: 127.0.0.1) and Port 8080



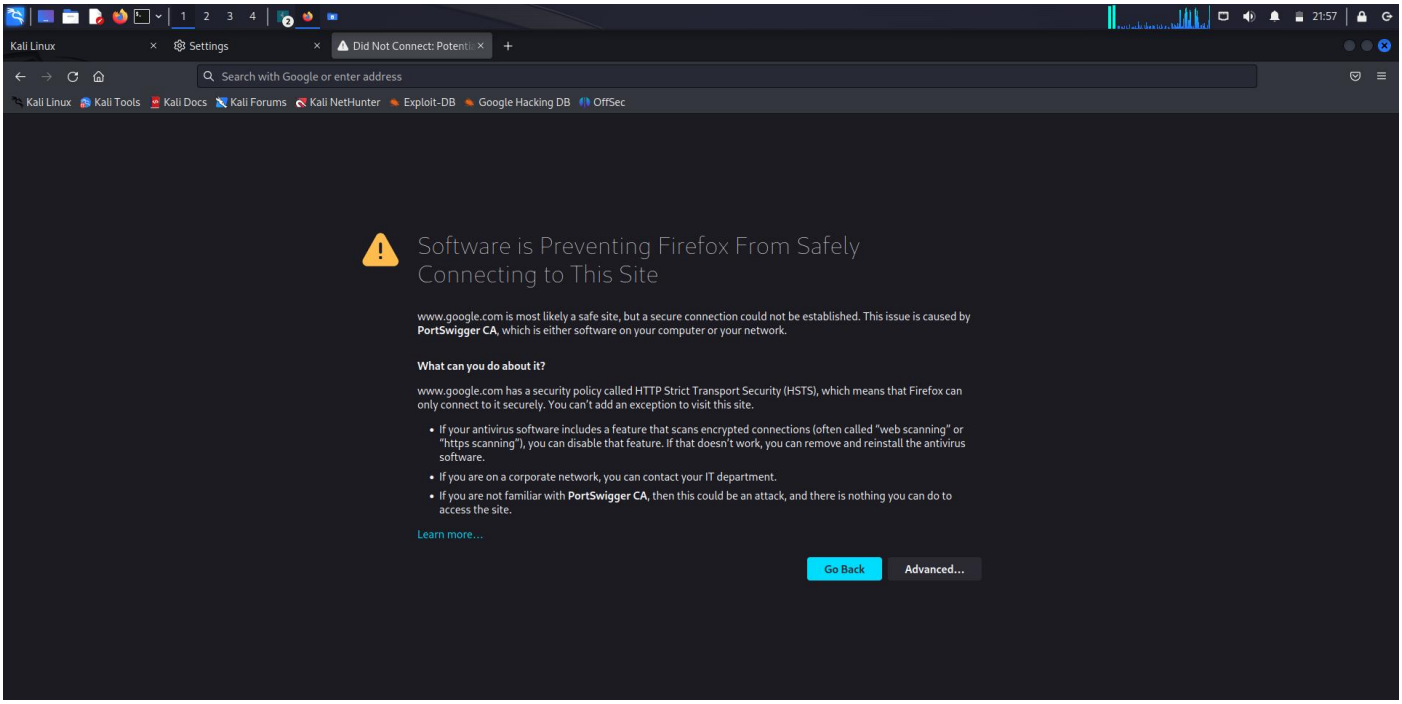
3. Open Firefox Browser settings
    - Open the Firefox Browser
    - Open the Settings
    - Scroll down to the bottom in the General section
    - Click on the Network Settings



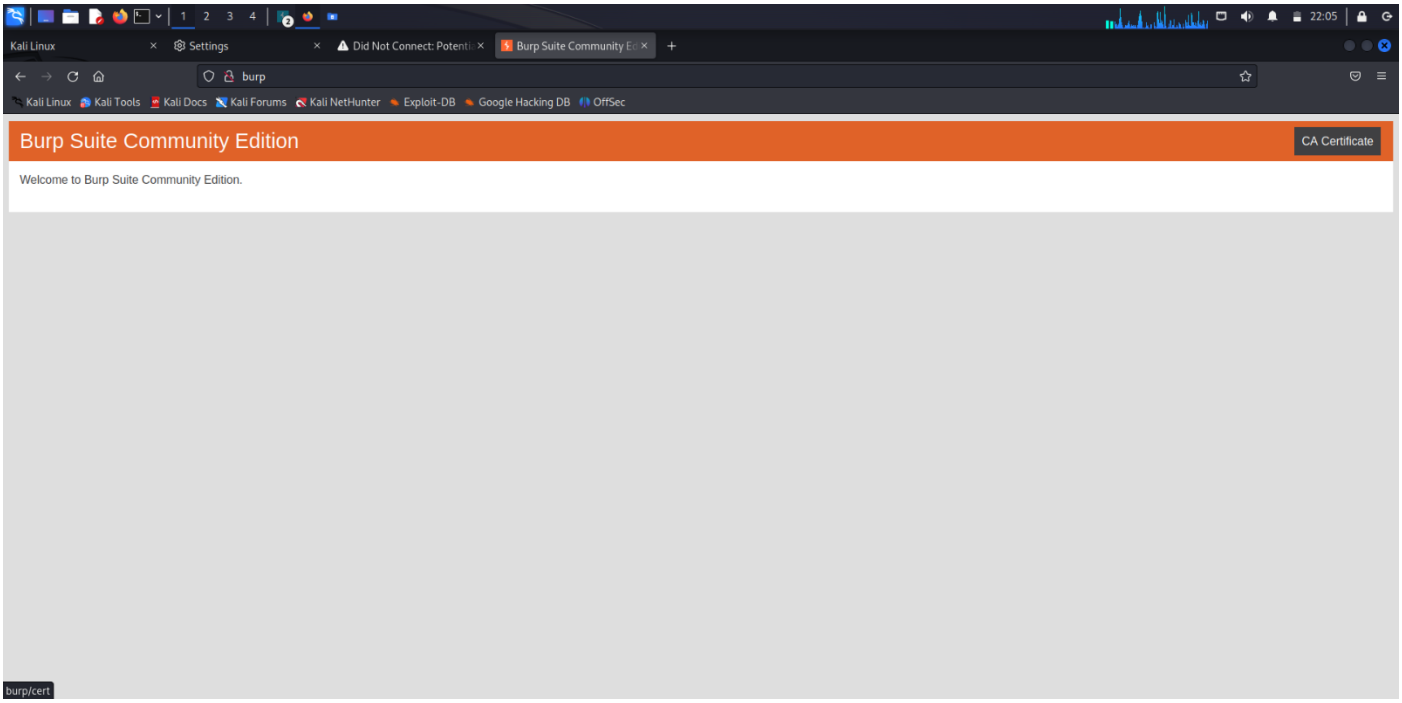

4. Configure the Firefox Settings
    - Select the radio button saying Manual Proxy Configuration
    - Set, HTTP Proxy: 127.0.0.1; Port: 8080
    - Check the box saying “Also use this proxy for HTTPS”



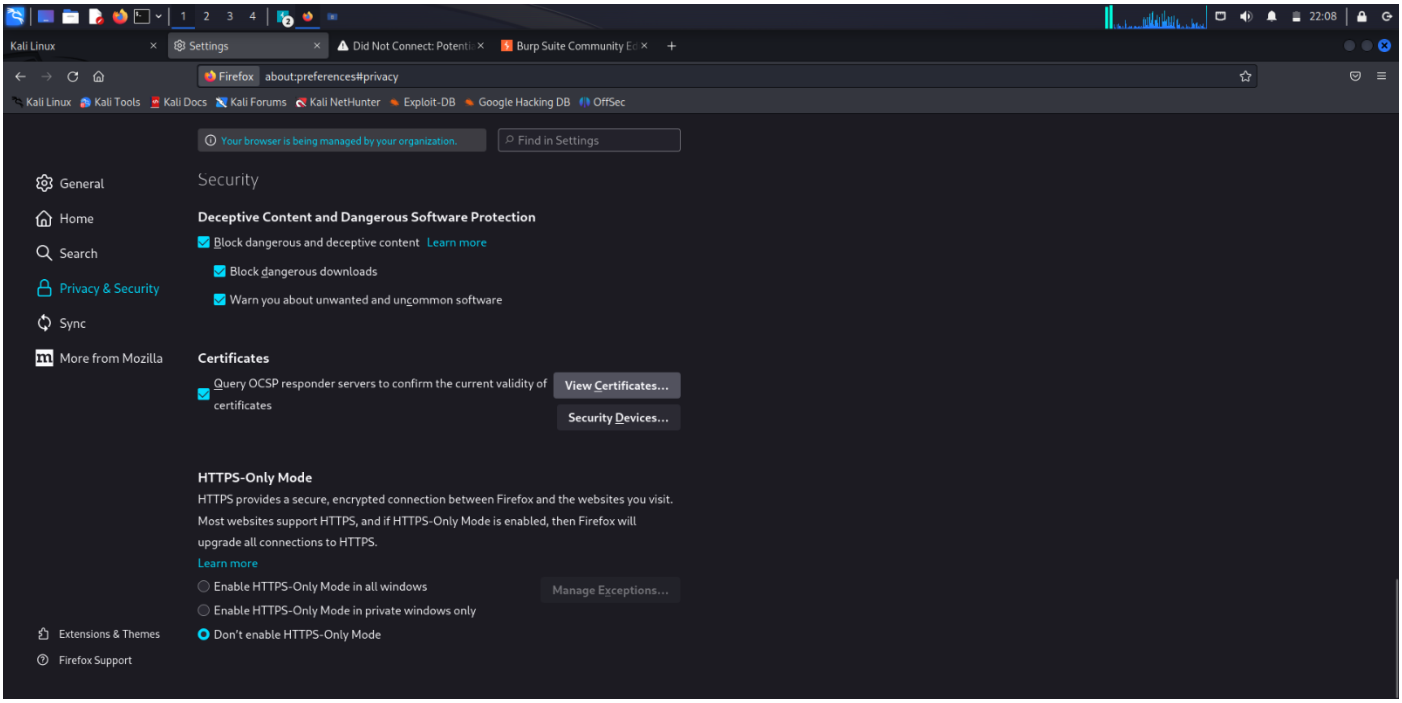
5. Check whether you can connect to a website
    - Open the browser and browse for any website
    - We're unable to create a connection
    - A CA certificate, also known as a Certificate Authority certificate, is a digital certificate issued by a trusted entity known as a Certificate Authority (CA). It is a critical component of the public key infrastructure (PKI) and plays a crucial role in ensuring the security and integrity of digital communications, particularly over the internet.



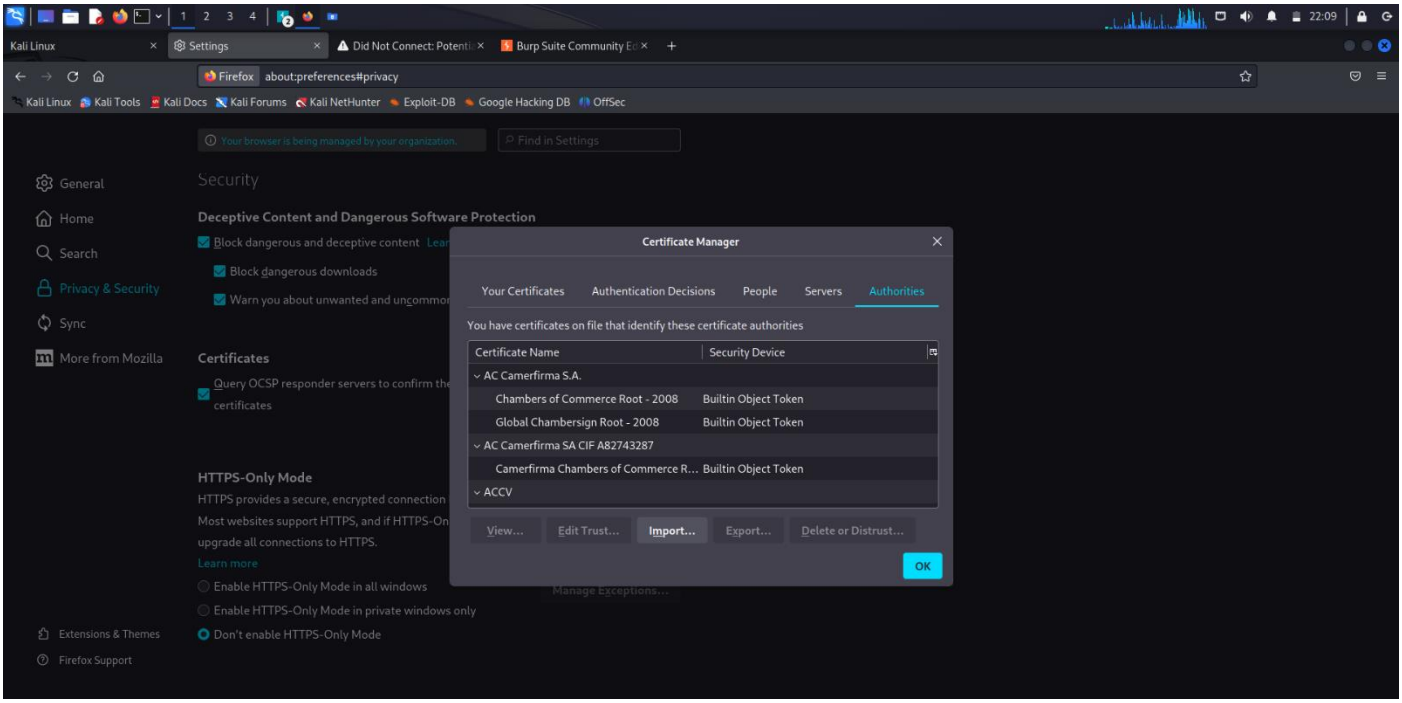

6. Download the CA certificate
    - Open a browser tab and enter the URL: http://burp.com
    - Click on the CA Certificate button on the top-right corner of the page



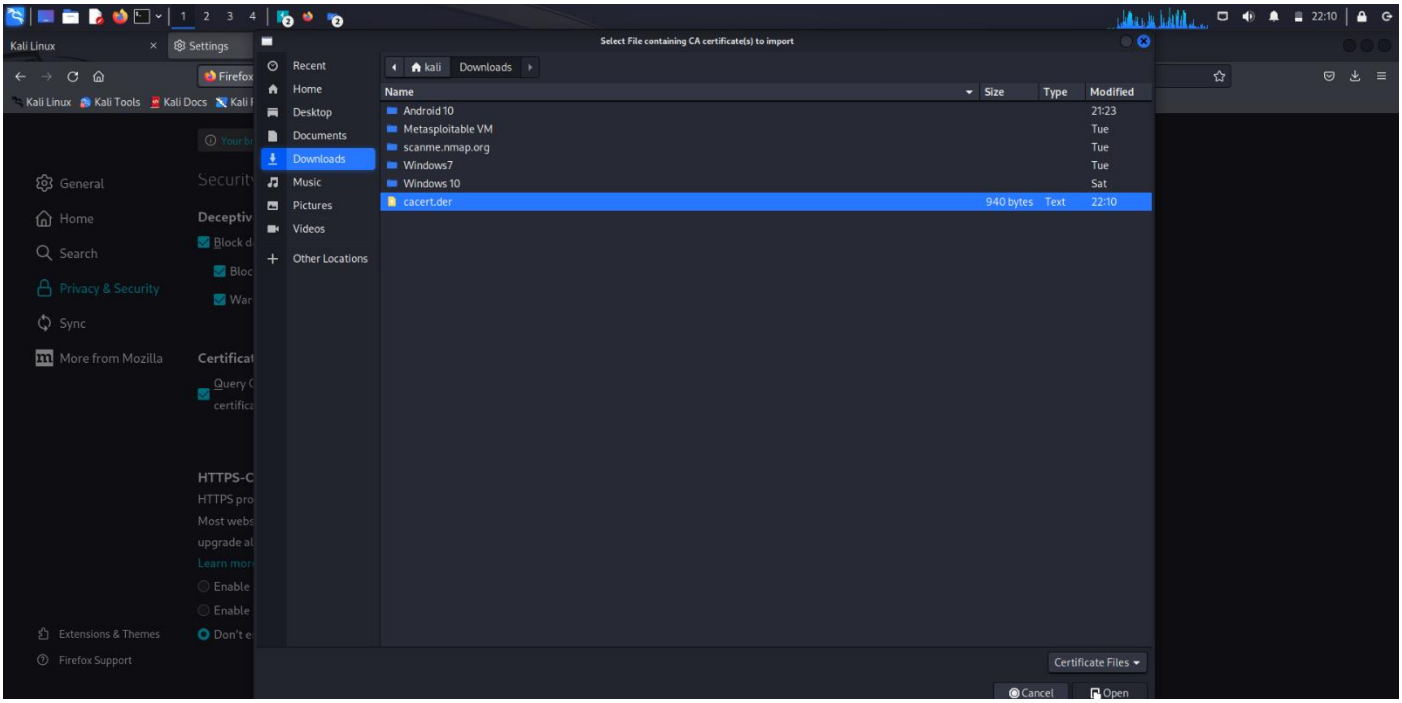
7. Import the CA certificate onto the Firefox Browser
    - Enter the browser settings
    - Enter the Privacy and Security section
    - Click on View Certificates



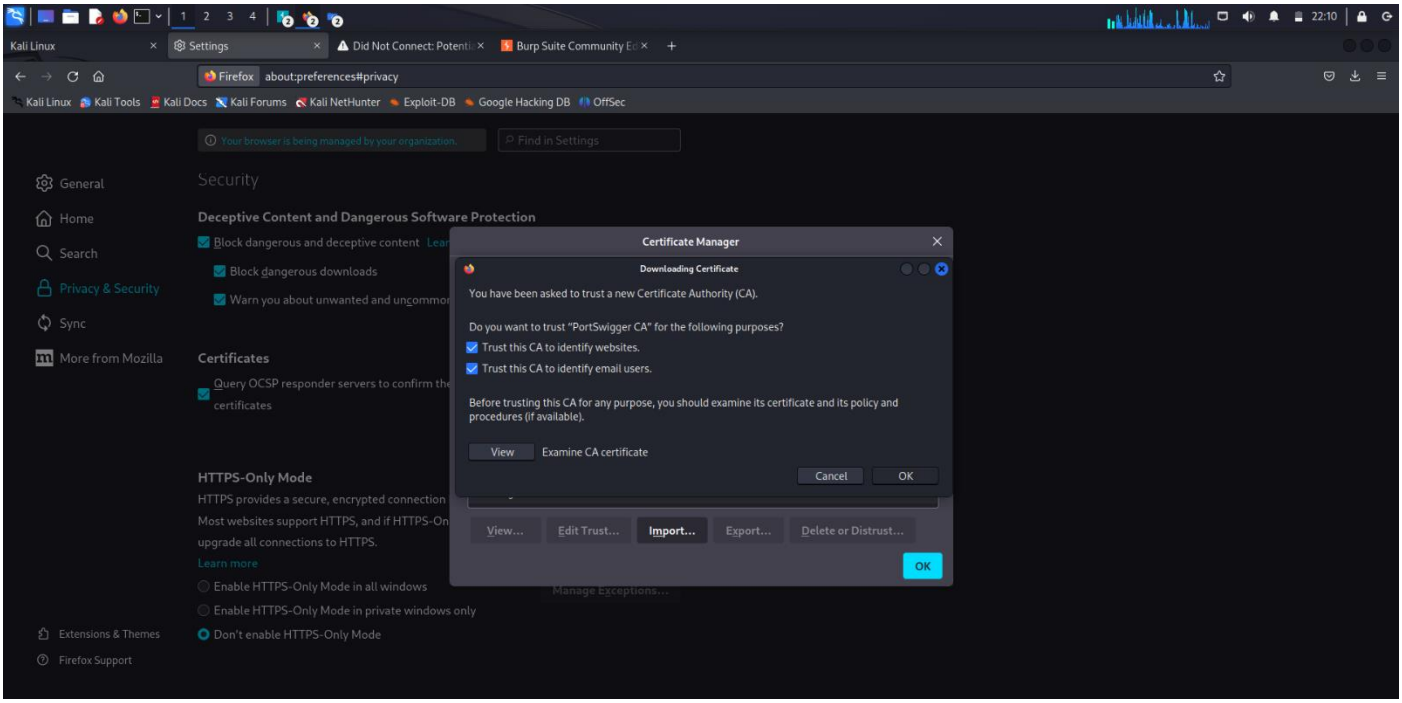

- Certificate Manager is opened
- Click on Import



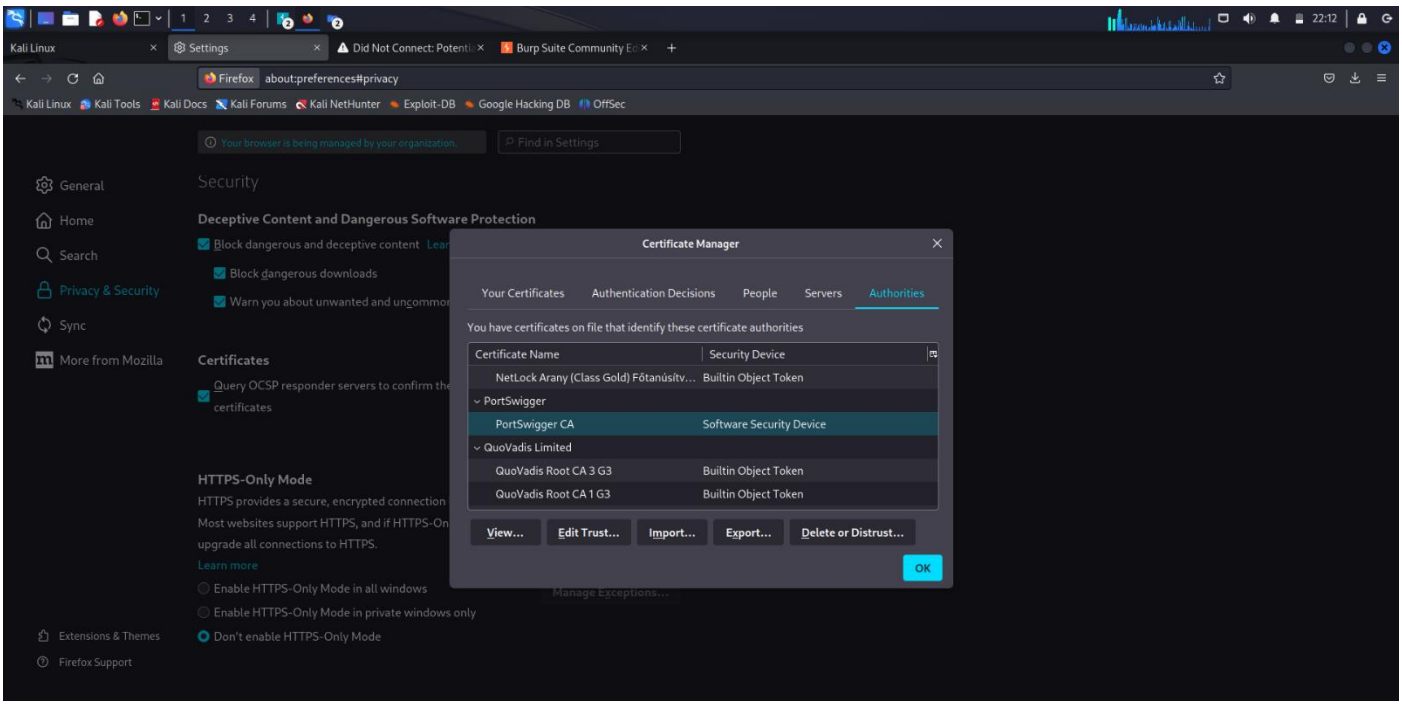
- Browse to the location of the certificate
- Click on the certificate file, it is saved as “cacert.der”

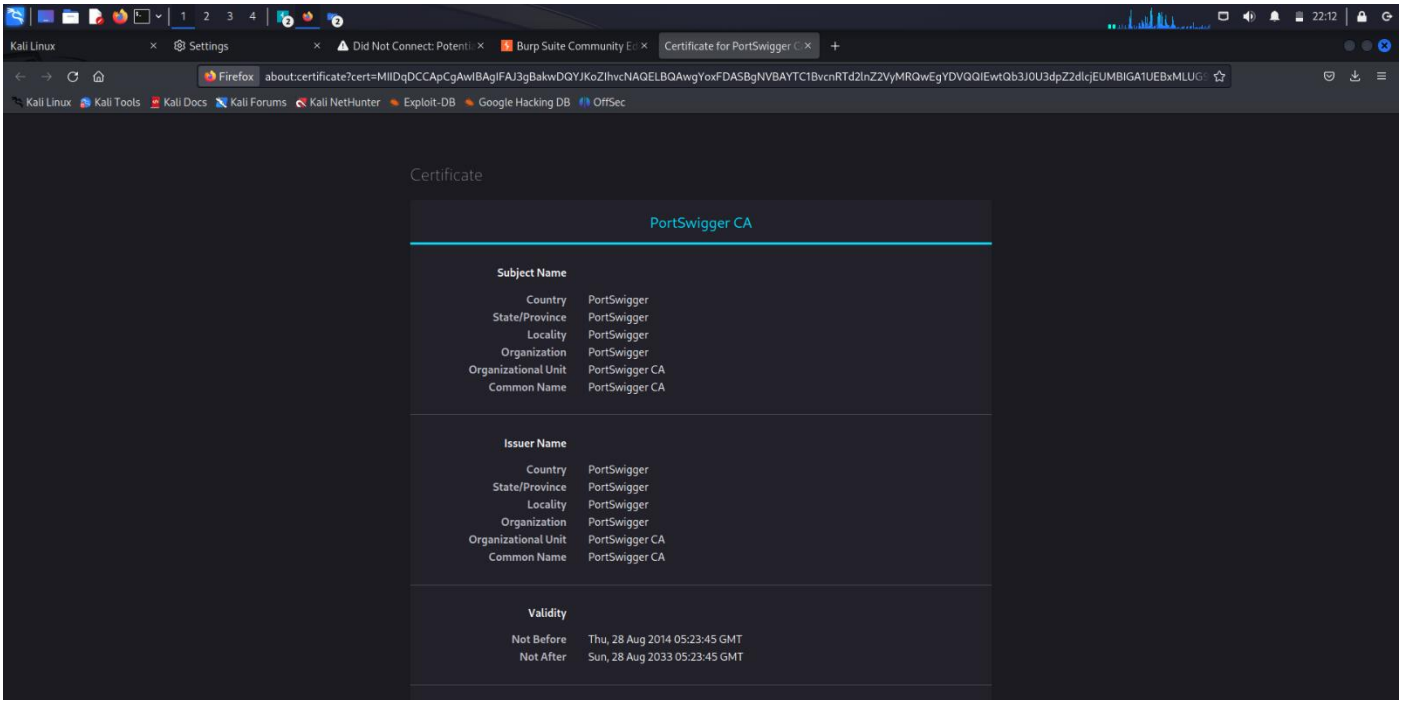



- Check the boxes saying
  - ✓ Trust this CA to identify websites.
  - Trust this CA to identify email users.
- Click on OK

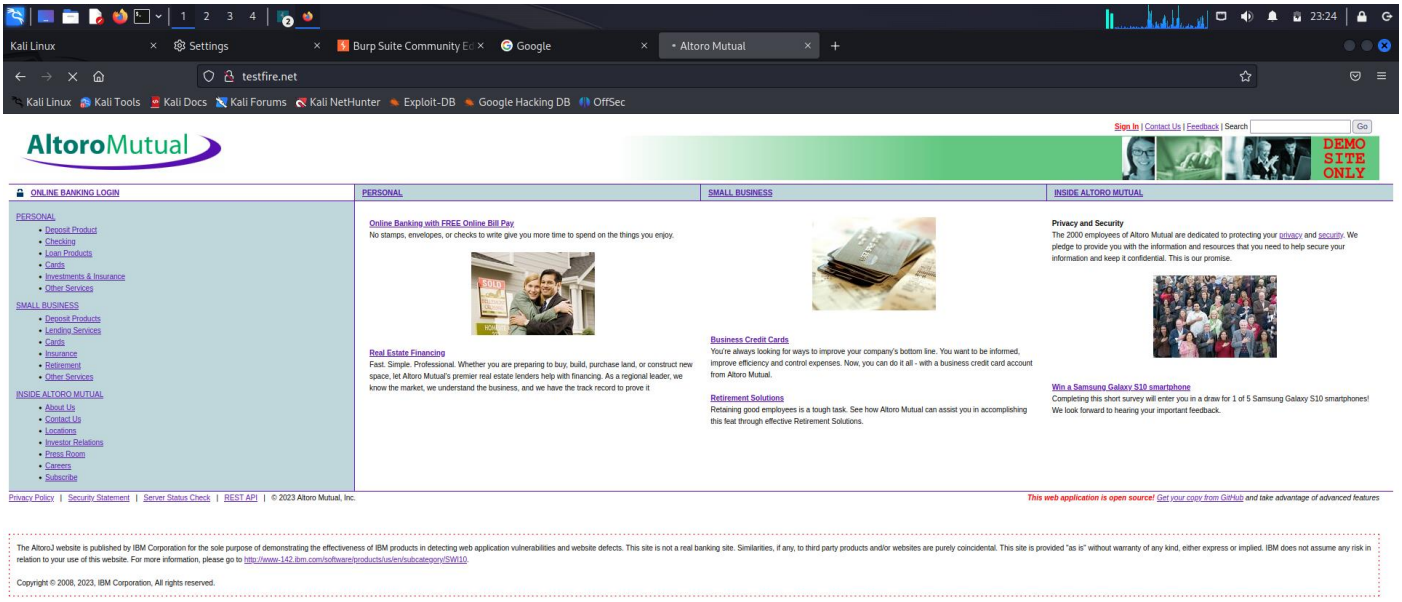


- Ensure that the CA certificate has been imported
- Search for Portswigger in Authorities, if it is present then the import has been successful



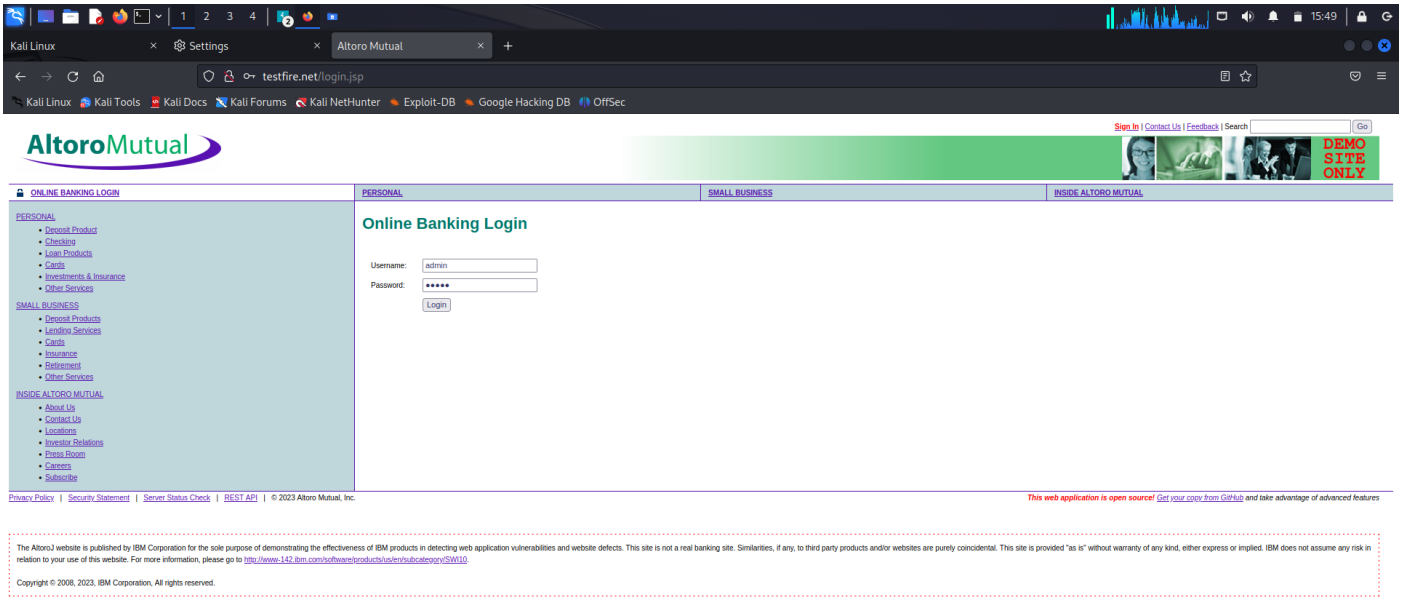



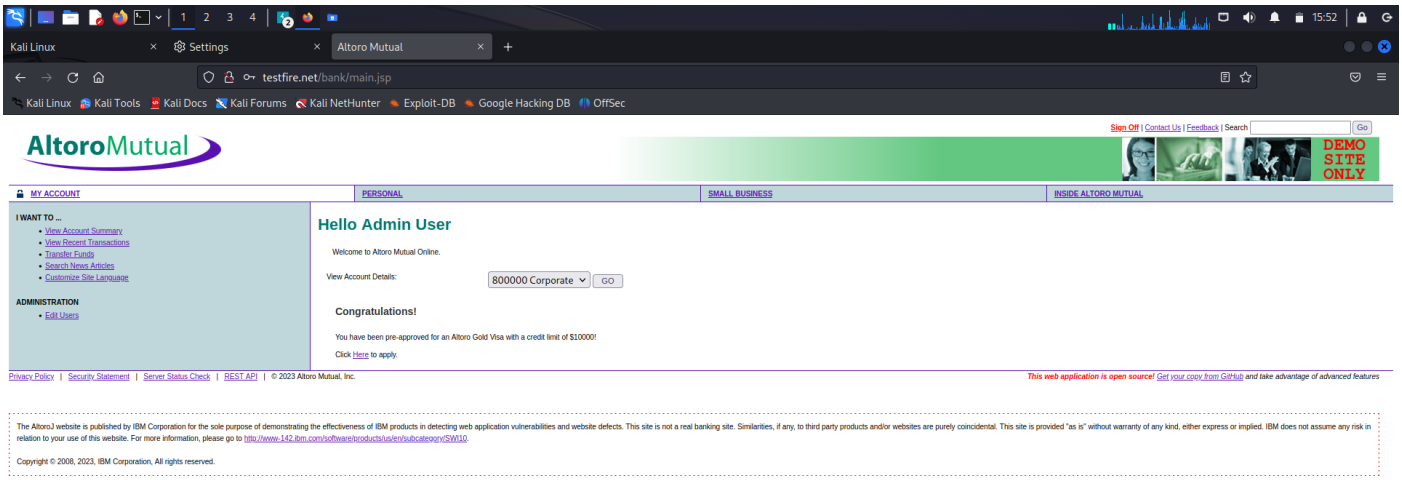
8. Open a HTTP website
    - Open any HTTP website(In this case, it is [http://testfire.net](http://testfire.net))
    - The connection has been established between the browser and the website successfully after importing the CA certificate.



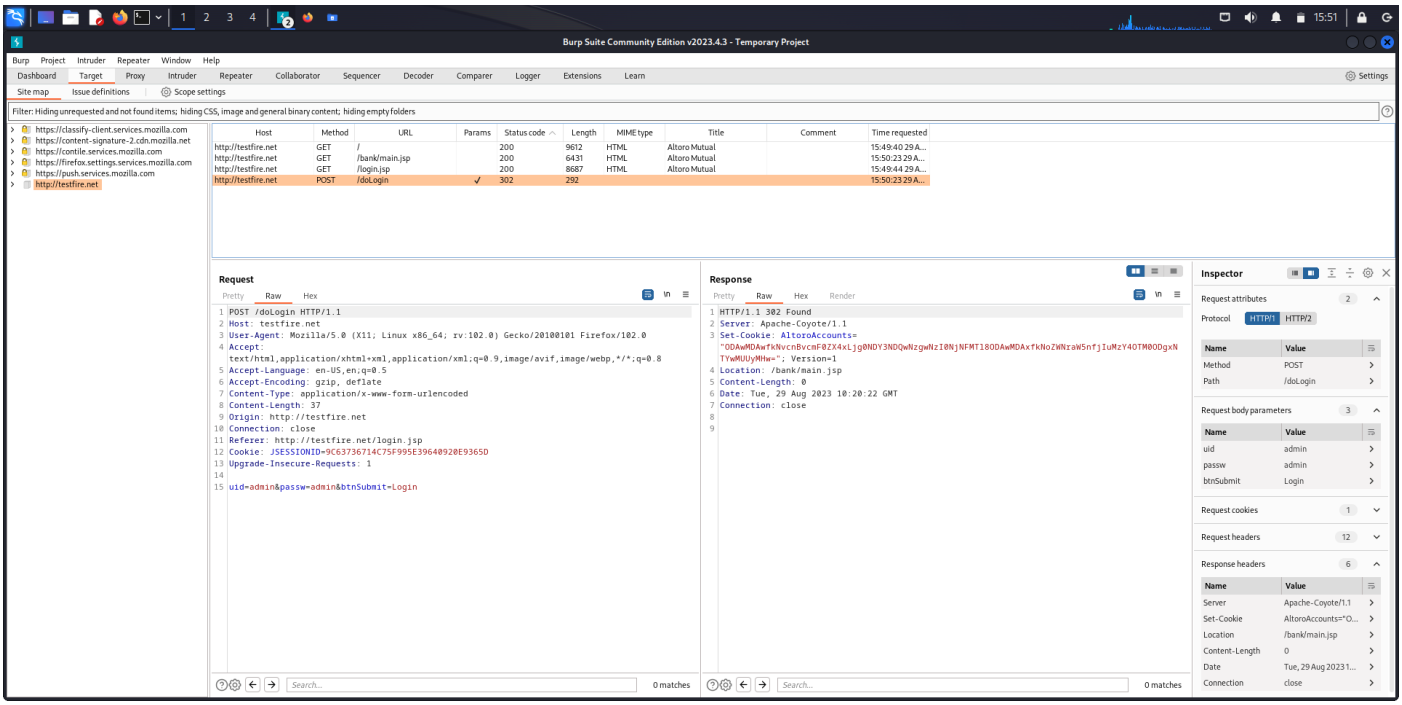


9. Open the Login page
    - Open the Login page of the site
    - Log in to using your credentials
      Username: admin, Password: admin
    - Click on Login

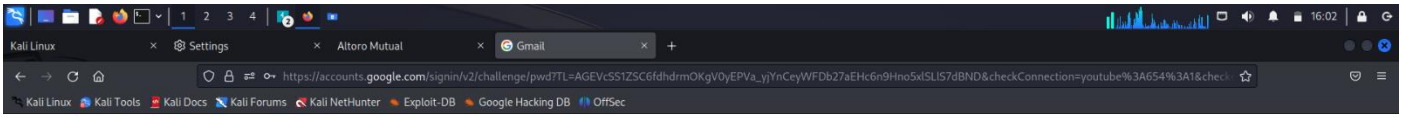


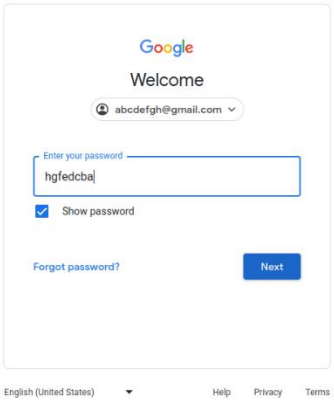



10. Ensure that the data is captured on Burpsuite
    - Open the Target tab
    - Filter the tab according to your preferences
    - Click on the URL of the website visited(In this case: http://testfire.net)
    - Click on the POST method in the list
    - As we can see, the information has been captured.

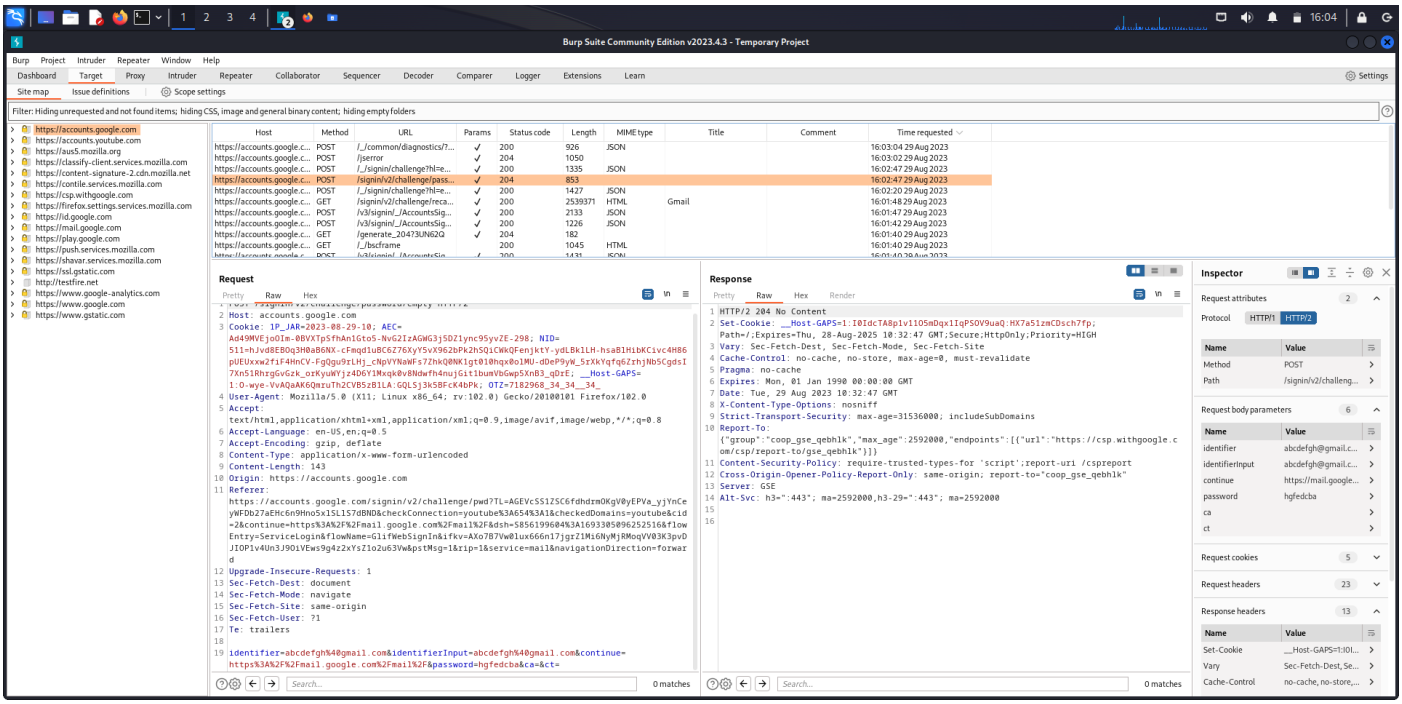


11. Capturing Gmail credentials during Login
    - Open the Gmail login page
    - Login using your credentials
    - Click on Next

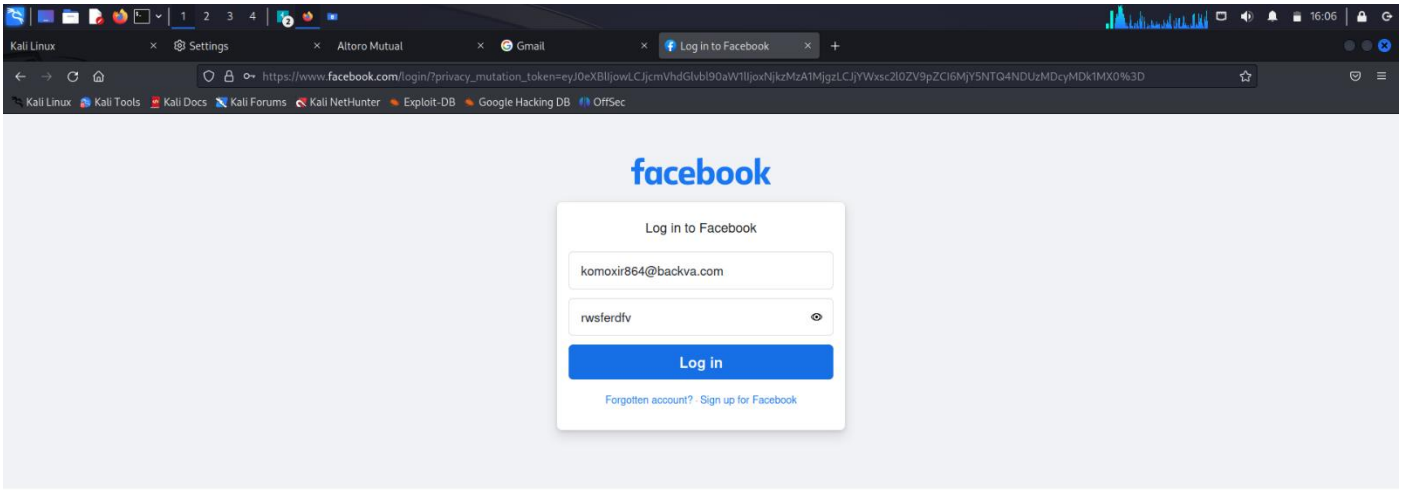


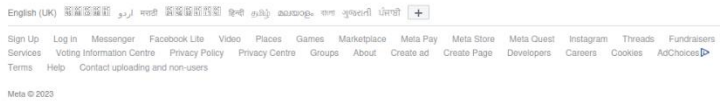




- Ensure that the details has been captured on Burpsuite

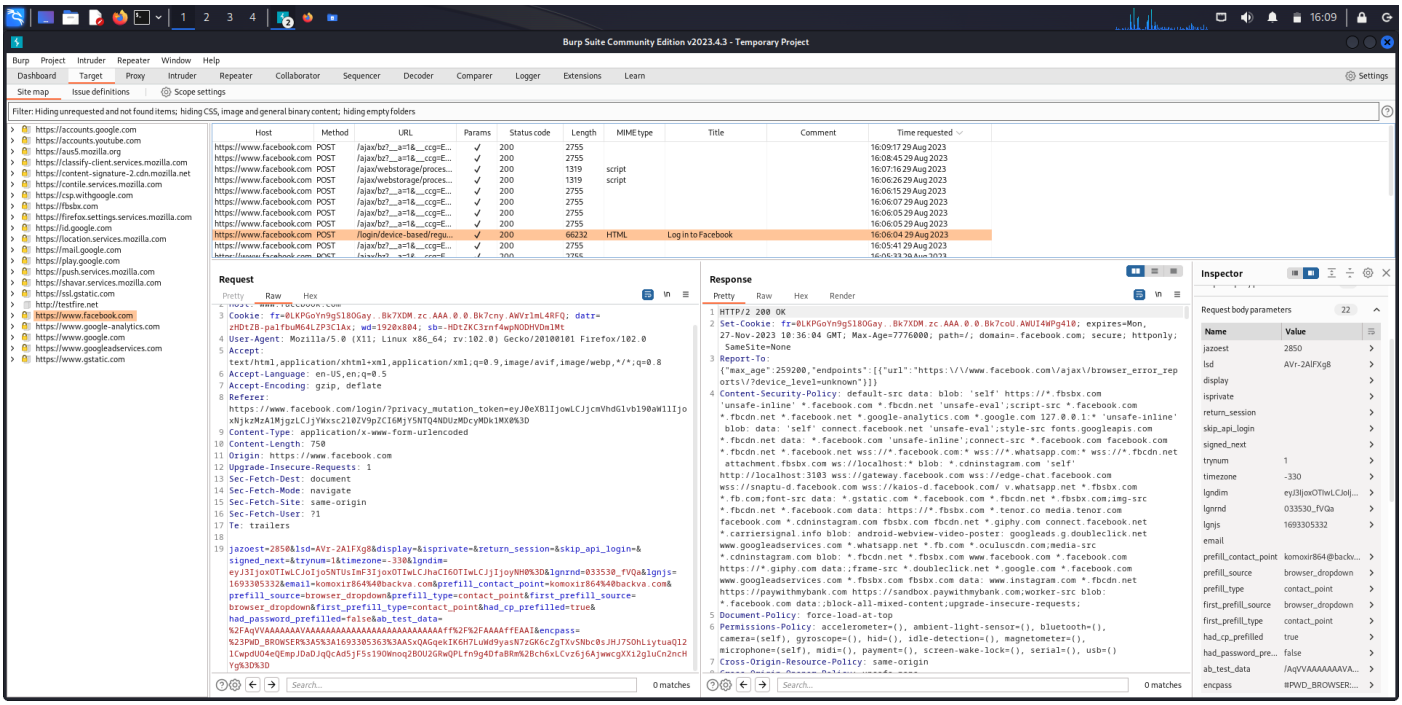


12. Capturing Facebook credentials during Login
    - Open the Facebook login page
    - Login using your credentials
    - Click on Log in

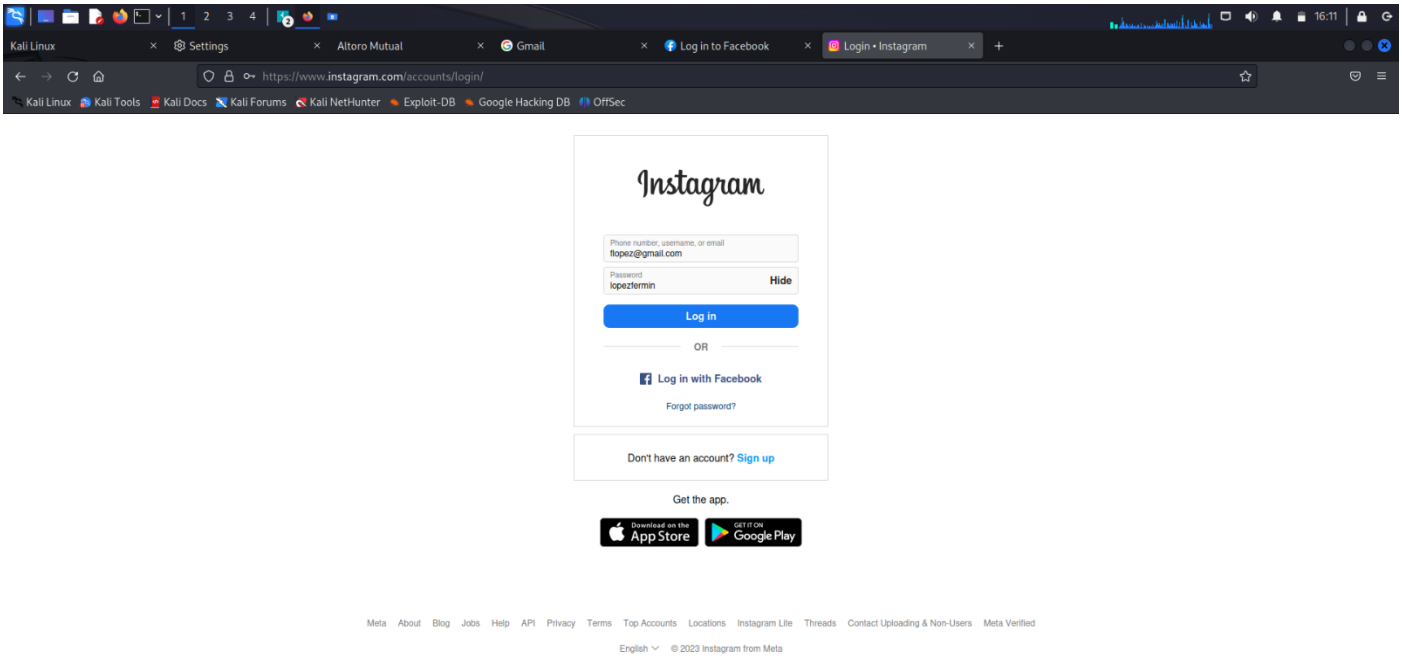


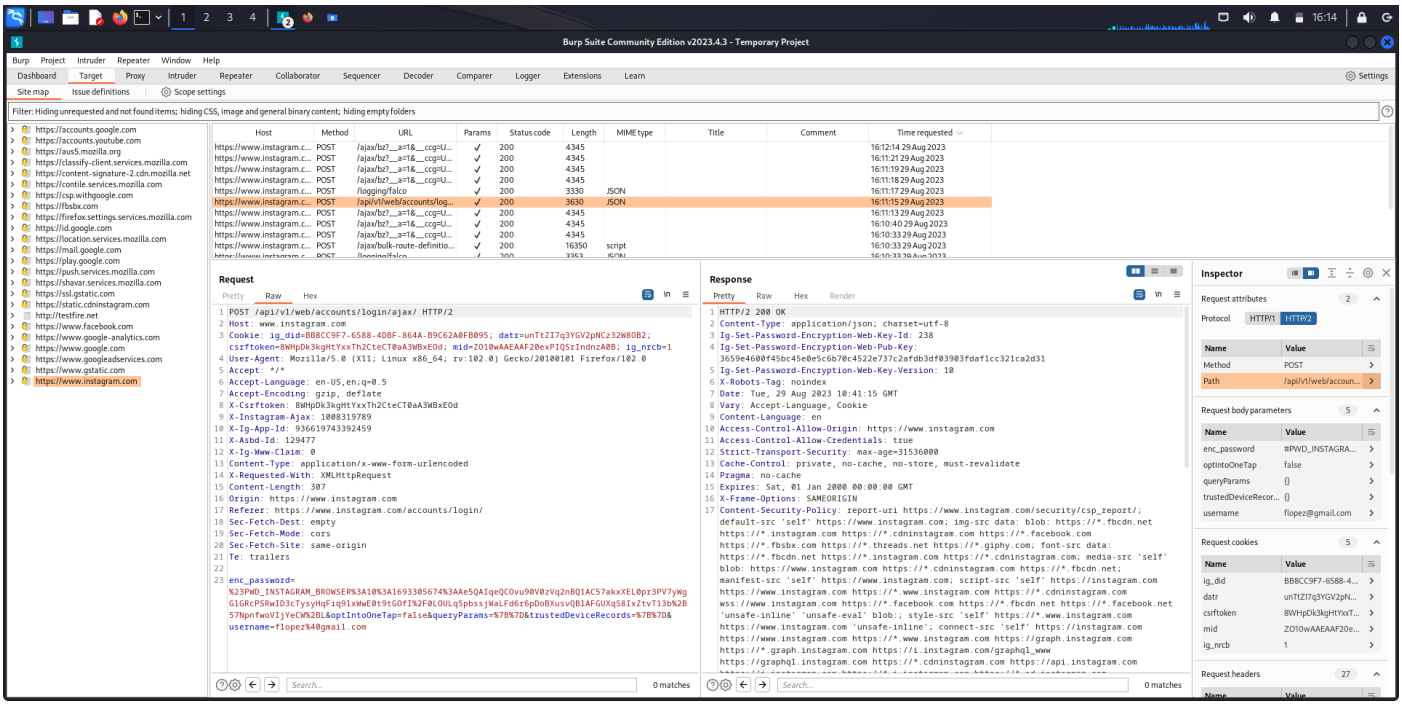

- Ensure that the details has been captured on Burpsuite



13. Capturing Instagram credentials during Login
    - Open the Instagram login page
    - Login using your credentials
    - Click on Log in




- Ensure that the details has been captured on Burpsuite



## Analysis

The analysis of capturing HTTP messages in Burp Suite underscores its significance in web application security assessments. By intercepting and analyzing traffic between a browser and web server, Burp Suite offers a robust means to identify and rectify potential vulnerabilities. This feature enhances the tool's utility for security professionals and penetration testers, allowing for the discovery of issues like injection vulnerabilities and cross-site scripting. Furthermore, the ability to utilize additional tools within Burp Suite, such as Repeater, Intruder, and Scanner, further streamlines the process of vulnerability detection and exploitation.

## Conclusion

In conclusion, the ability to capture and analyze HTTP messages using Burp Suite is an essential component of any comprehensive web application security assessment. Through the configuration of Burp Suite's proxy settings, security professionals gain unparalleled visibility into the interactions between web clients and servers, enabling them to identify and address potential vulnerabilities effectively. The user-friendly interface and accompanying tools provided by Burp Suite streamline the process of inspecting and manipulating HTTP traffic, making it an indispensable resource for security researchers and penetration testers. Overall, mastering the art of capturing and analyzing HTTP messages in Burp Suite equips organizations with the necessary tools to enhance the security of their web applications, fortify against potential threats, and ensure a safer online environment for users.