Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 29/08/2023

Assignment Details

Assigned Date: 28/08/2023

Due Date: 29/08/2023

Topic: Configuring Burpsuite

Introduction

In an increasingly interconnected digital landscape, web applications have become the cornerstone of modern business operations. These applications streamline processes, facilitate communication, and enable transactions on a global scale. However, with these benefits come inherent security risks that must be diligently addressed. To ensure the robustness of web applications against potential cyber threats, a comprehensive penetration testing approach is essential.

This report presents the findings and insights derived from a thorough penetration testing exercise conducted on a web application using the Burp Suite tool. Burp Suite, a renowned web vulnerability scanner and penetration testing framework, was employed to assess the security posture of the target application. The primary objective of this assessment was to identify and evaluate potential vulnerabilities, weaknesses, and security gaps that malicious actors could exploit to compromise the confidentiality, integrity, or availability of the application and its underlying data.

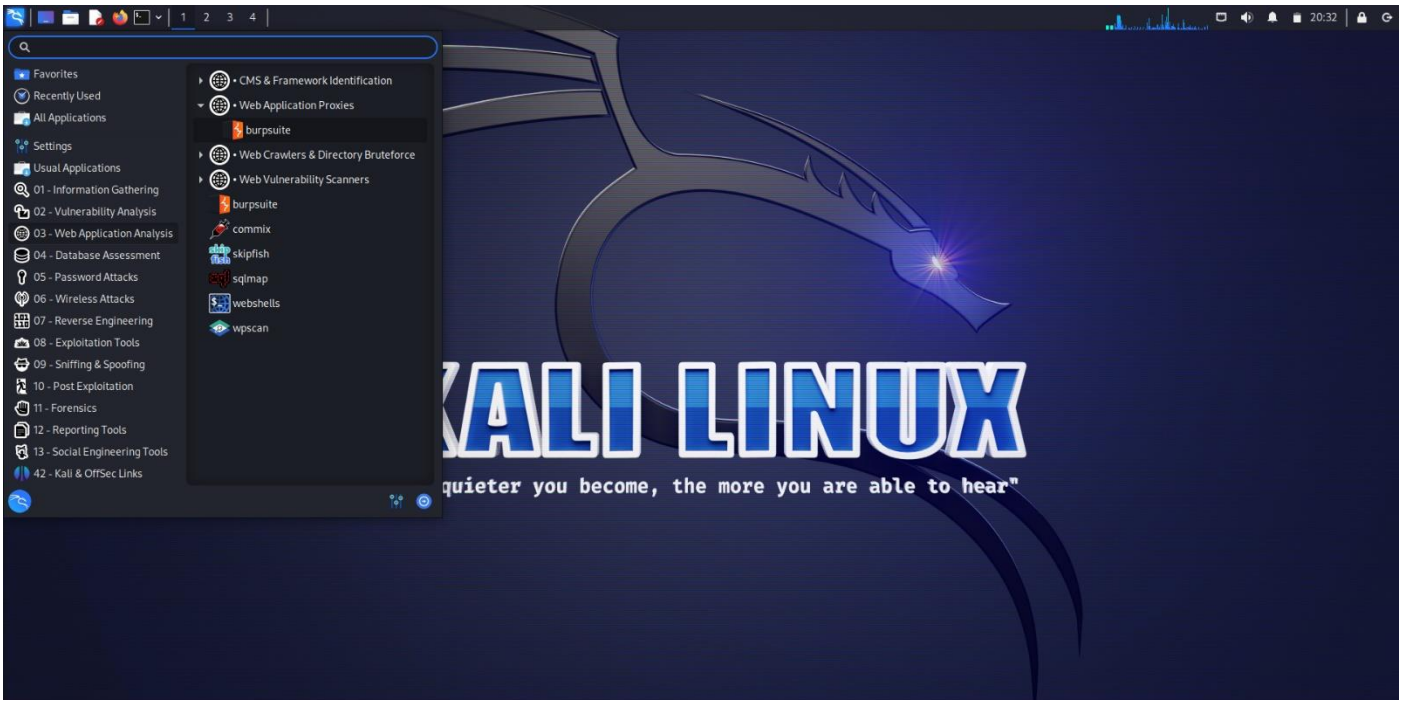
The scope of the penetration testing encompassed a systematic evaluation of the application's various components, including its front-end user interface, back-end functionality, authentication mechanisms, data handling processes, and communication channels. The testing process involved simulating real-world attack scenarios to ascertain the application's resilience against common threats, such as injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and more.

The subsequent sections of this report will provide a detailed analysis of the identified vulnerabilities, along with their potential impact on the application's security. Each vulnerability will be categorized based on its severity and accompanied by actionable recommendations for remediation. These recommendations are aimed at assisting the development and security teams in mitigating the identified risks and bolstering the application's overall security posture.

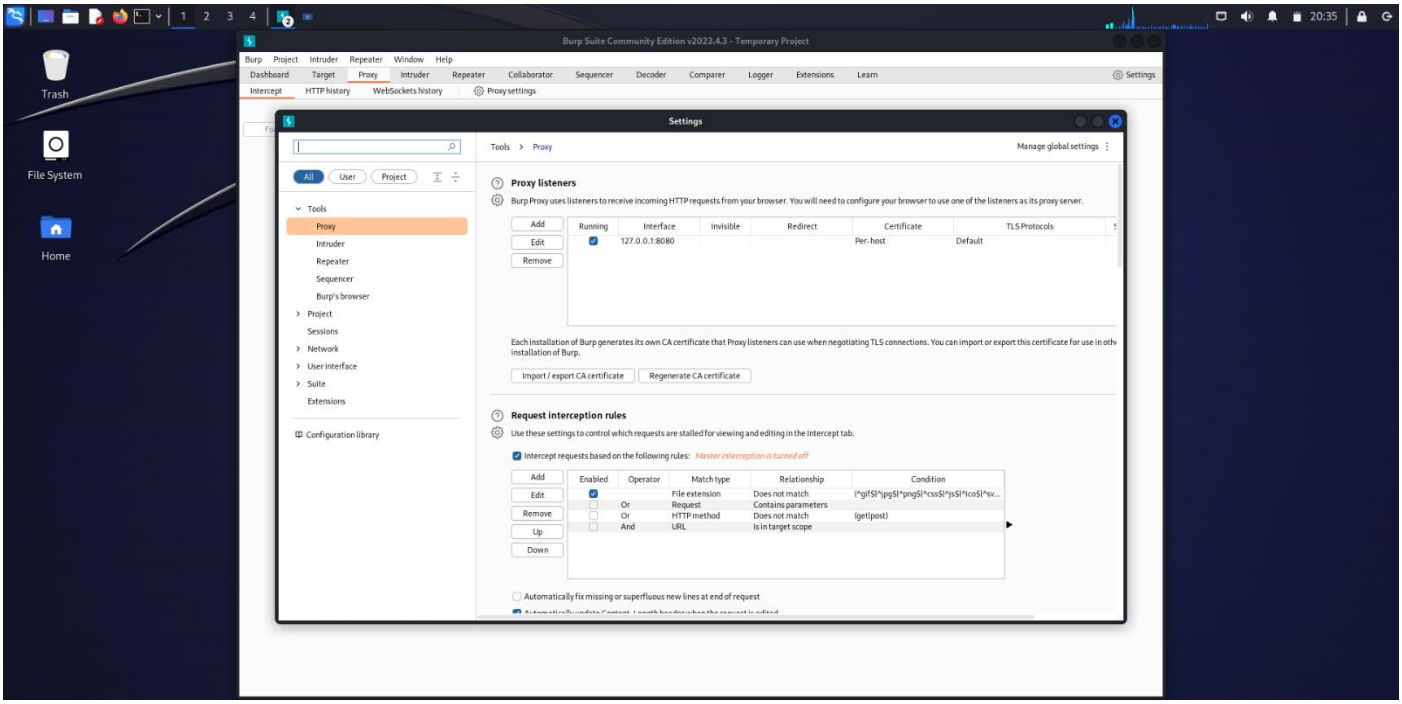
Content

Steps to Configure Burpsuite onto Firefox

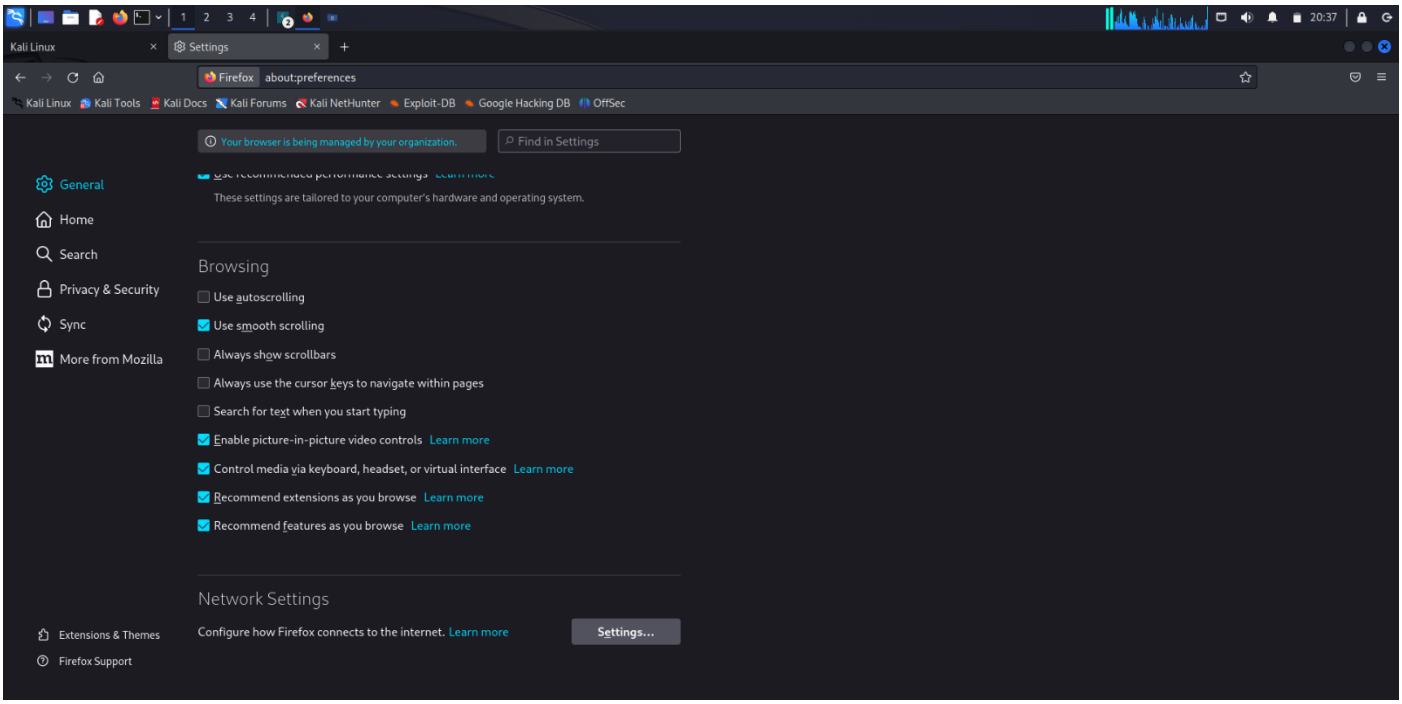
1. Locate Burpsuite
    - Click on Aplication on the top-left corner in Kali Linux
    - Select 03 – Web Application Analysis
    - Select Web Application Proxies
    - Click on Burpsuite



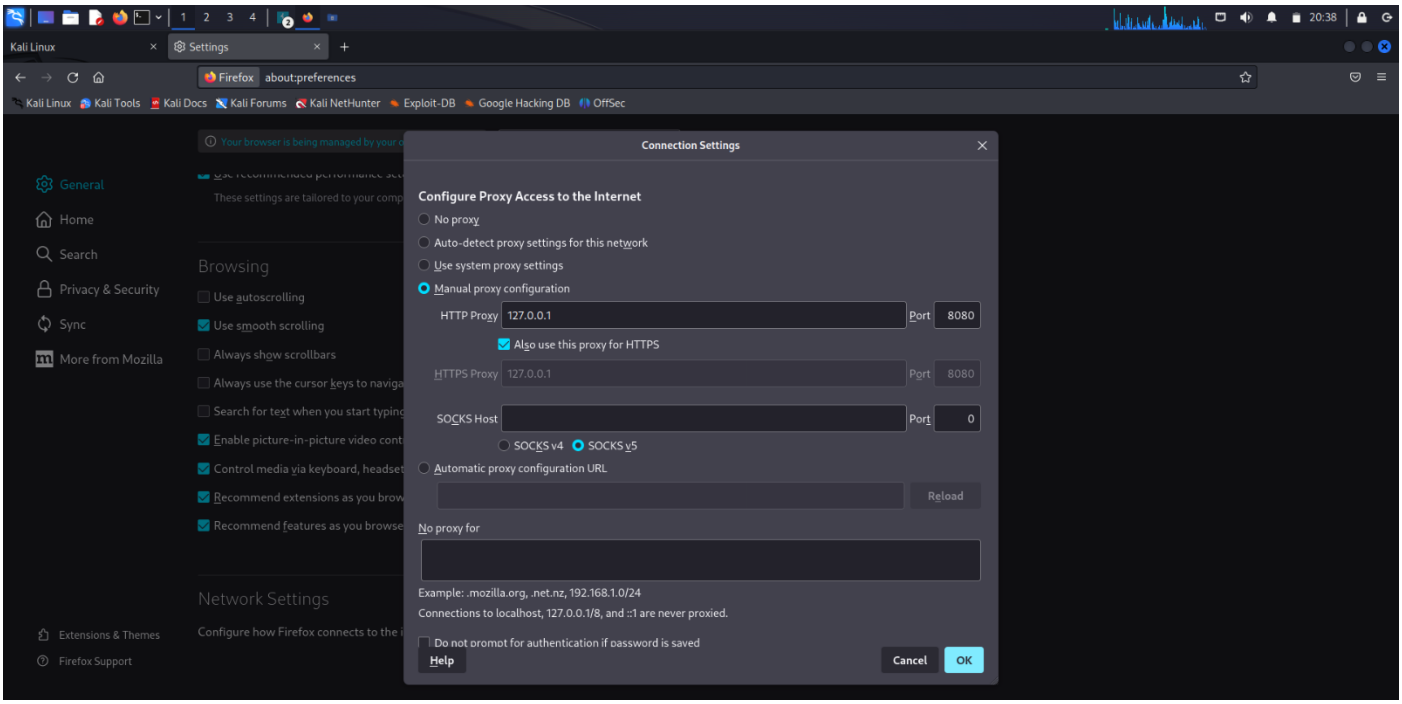
2. Ensure burpsuite is running on Localhost and Port 8080
    - Open Proxy tab
    - Click on Proxy Settings
    - Make sure it is running on Localhost(IP address: 127.0.0.1) and Port 8080



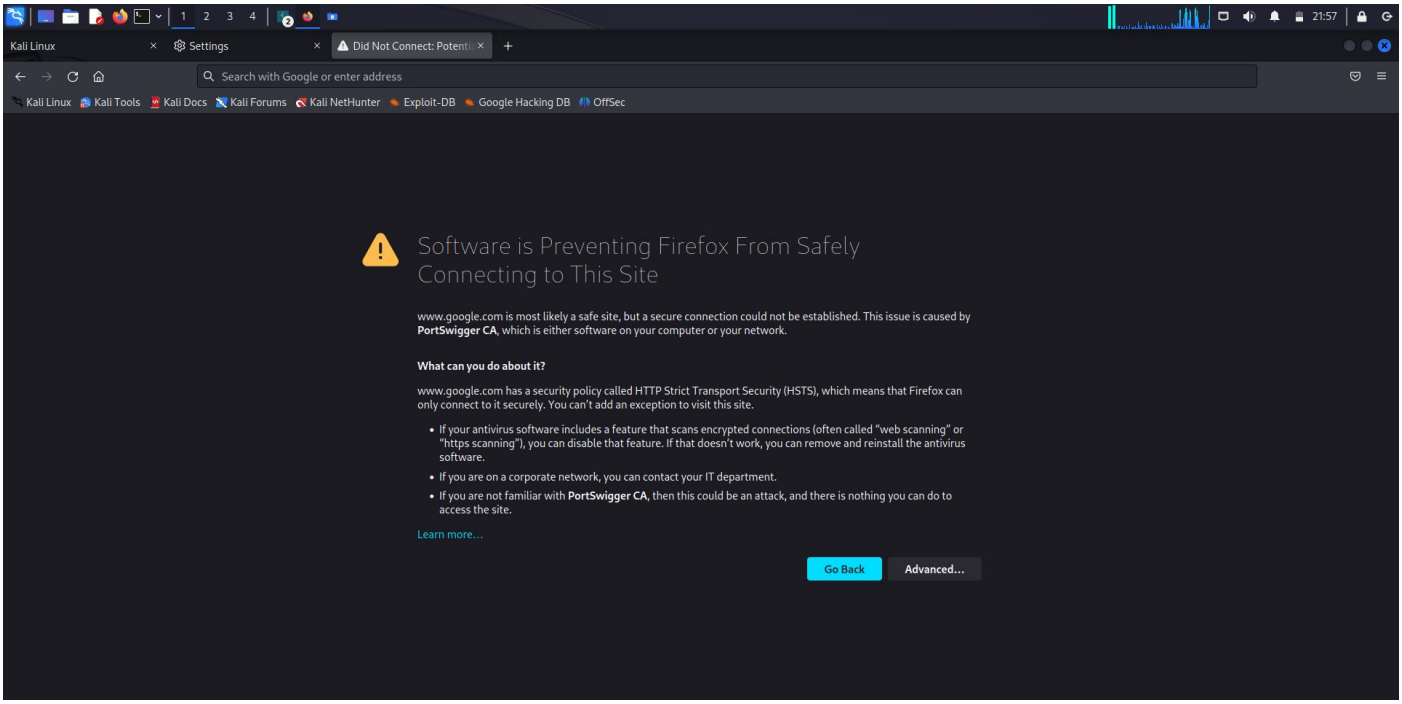
3. Open Firefox Browser settings
    - Open the Firefox Browser
    - Open the Settings
    - Scroll down to the bottom in the General section
    - Click on the Network Settings



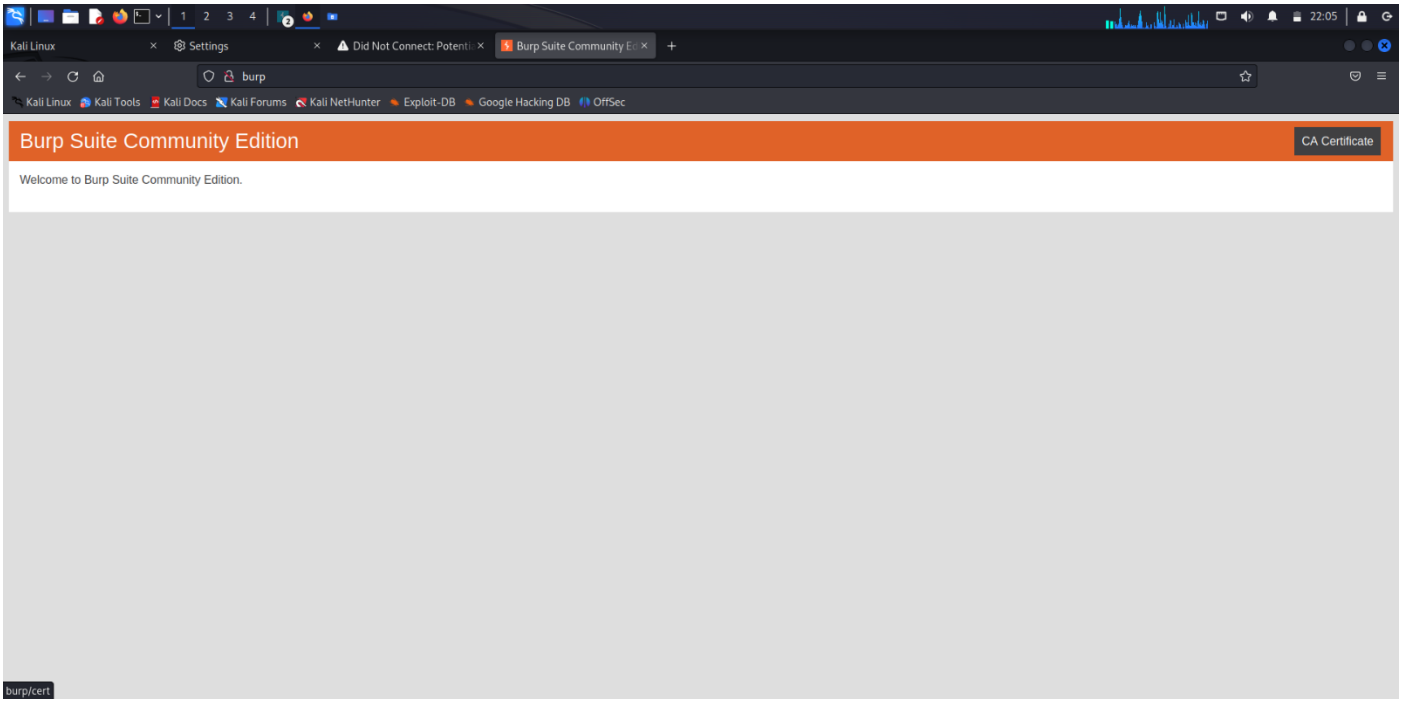
4. Configure the Firefox Settings
    - Select the radio button saying Manual Proxy Configuration
    - Set, HTTP Proxy: 127.0.0.1; Port: 8080
    - Check the box saying “Also use this proxy for HTTPS”



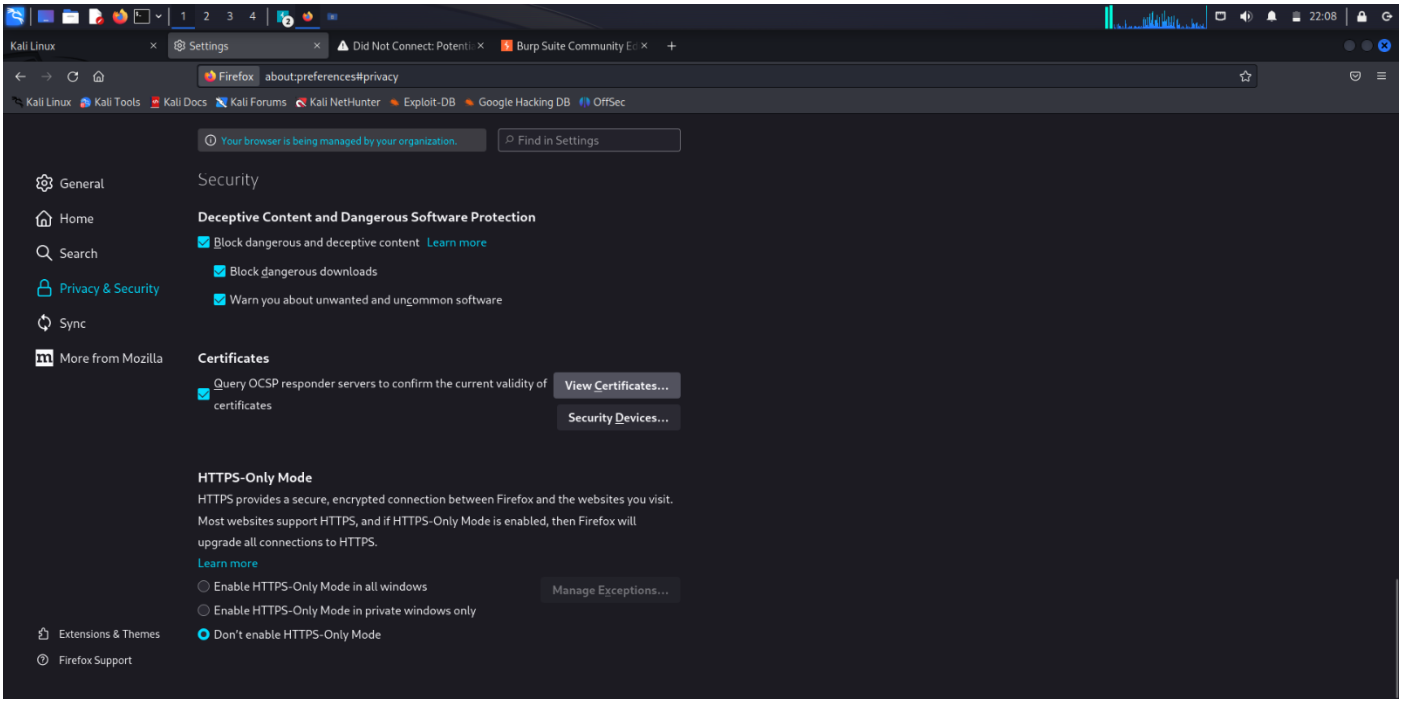
5. Check whether you can connect to a website
    - Open the browser and browse for any website
    - We're unable to create a connection
    - A CA certificate, also known as a Certificate Authority certificate, is a digital certificate issued by a trusted entity known as a Certificate Authority (CA). 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.



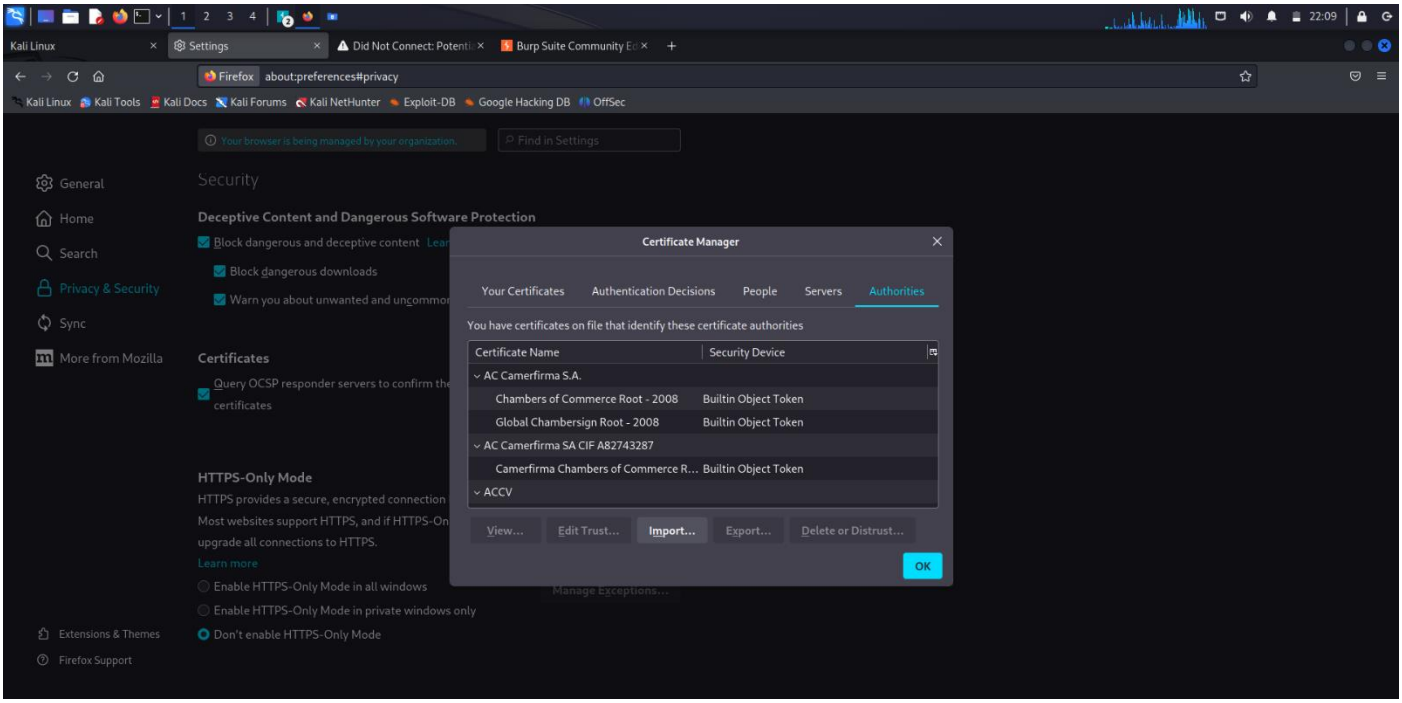
6. Download the CA certificate
    - Open a browser tab and enter the URL: http://burp.com
    - Click on the CA Certificate button on the top-right corner of the page



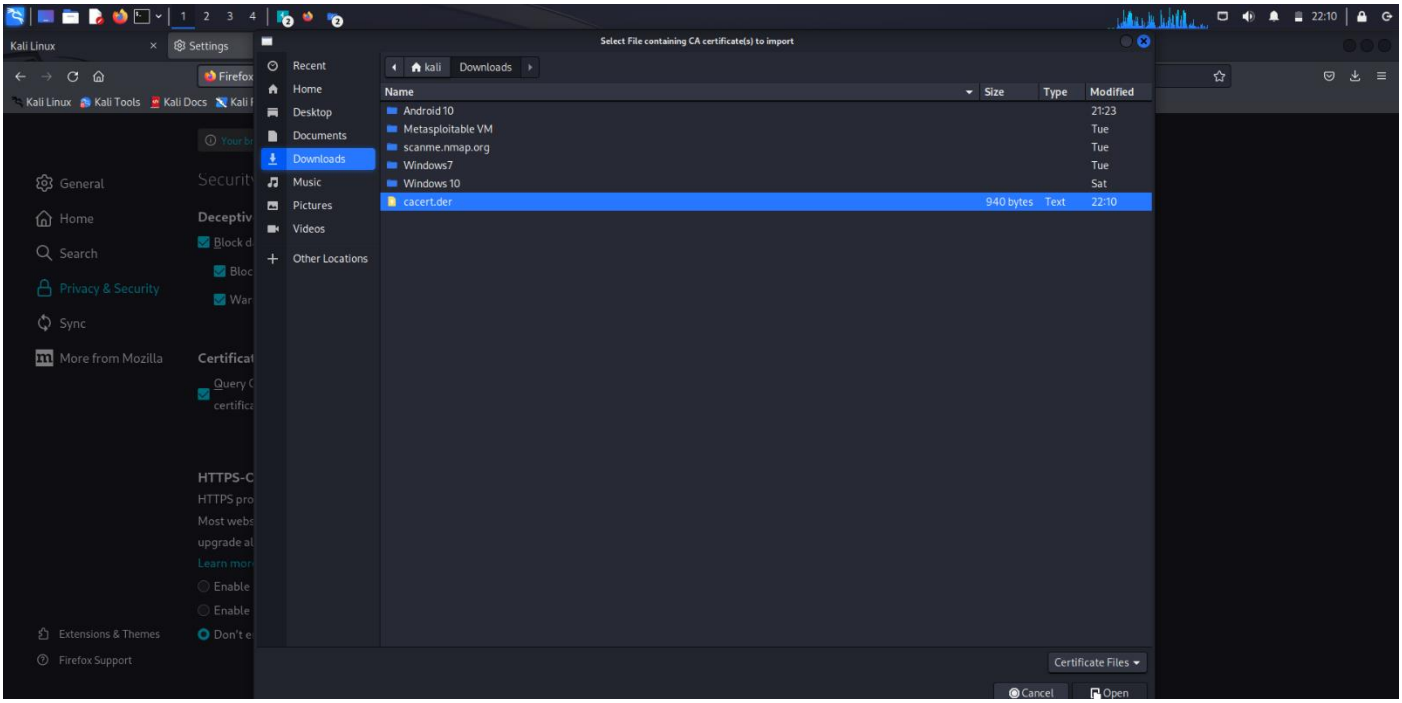
7. Import the CA certificate onto the Firefox Browser
    - Enter the browser settings
    - Enter the Privacy and Security section
    - Click on View Certificates



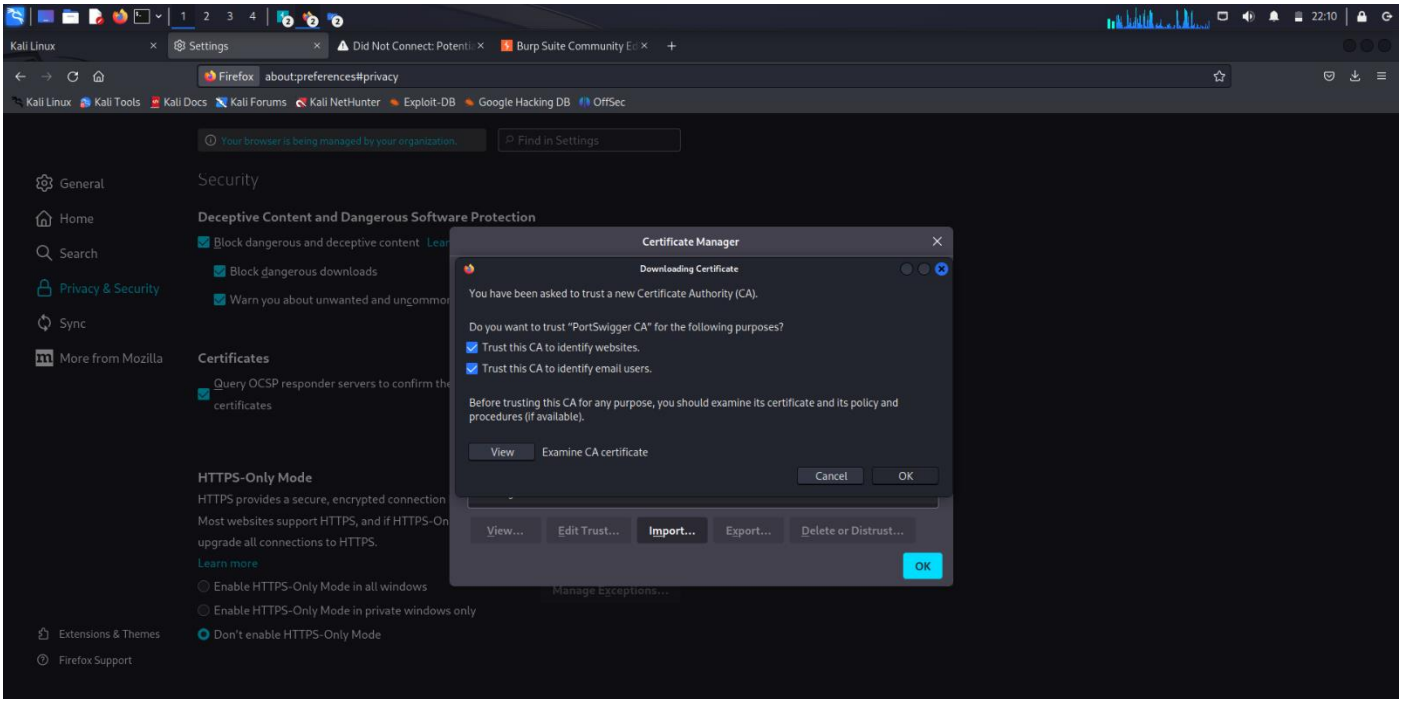
- Certificate Manager is opened
- Click on Import



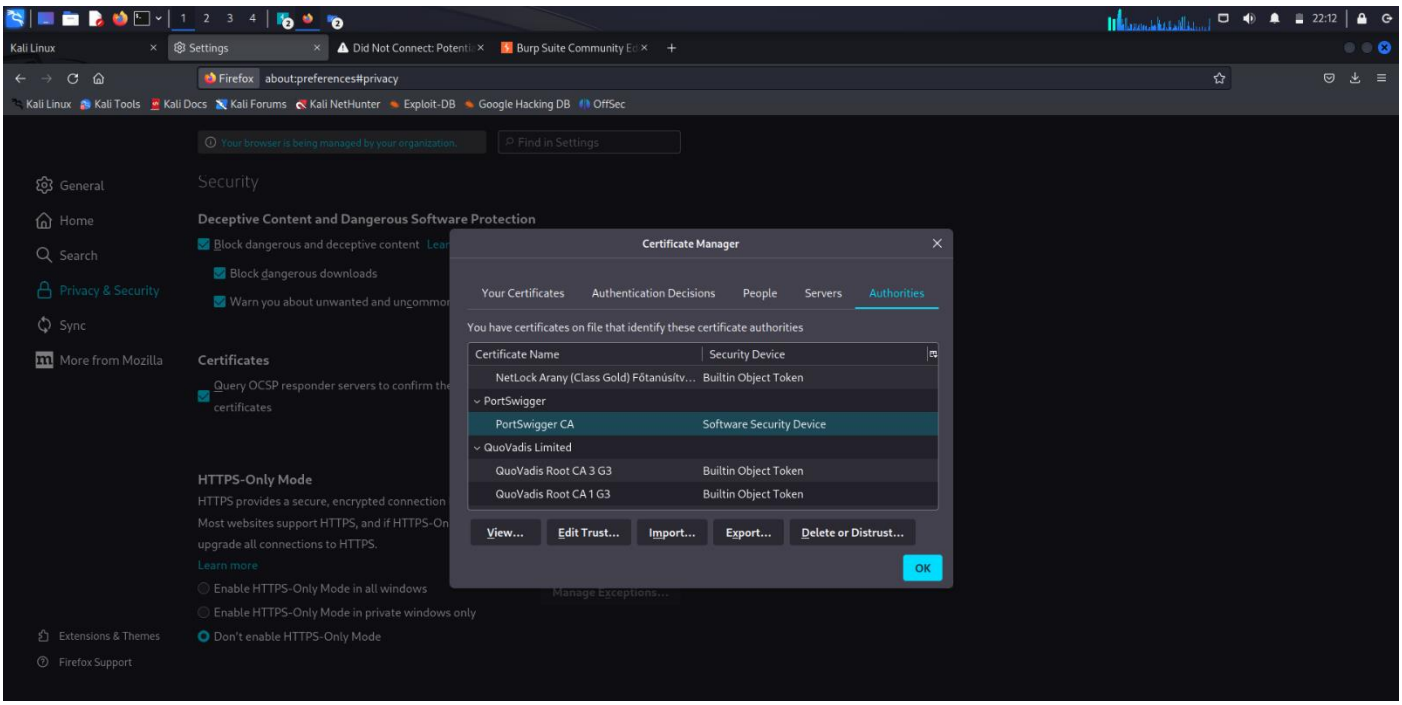
- Browse to the location of the certificate
- Click on the certificate file, it is saved as “cacert.der”

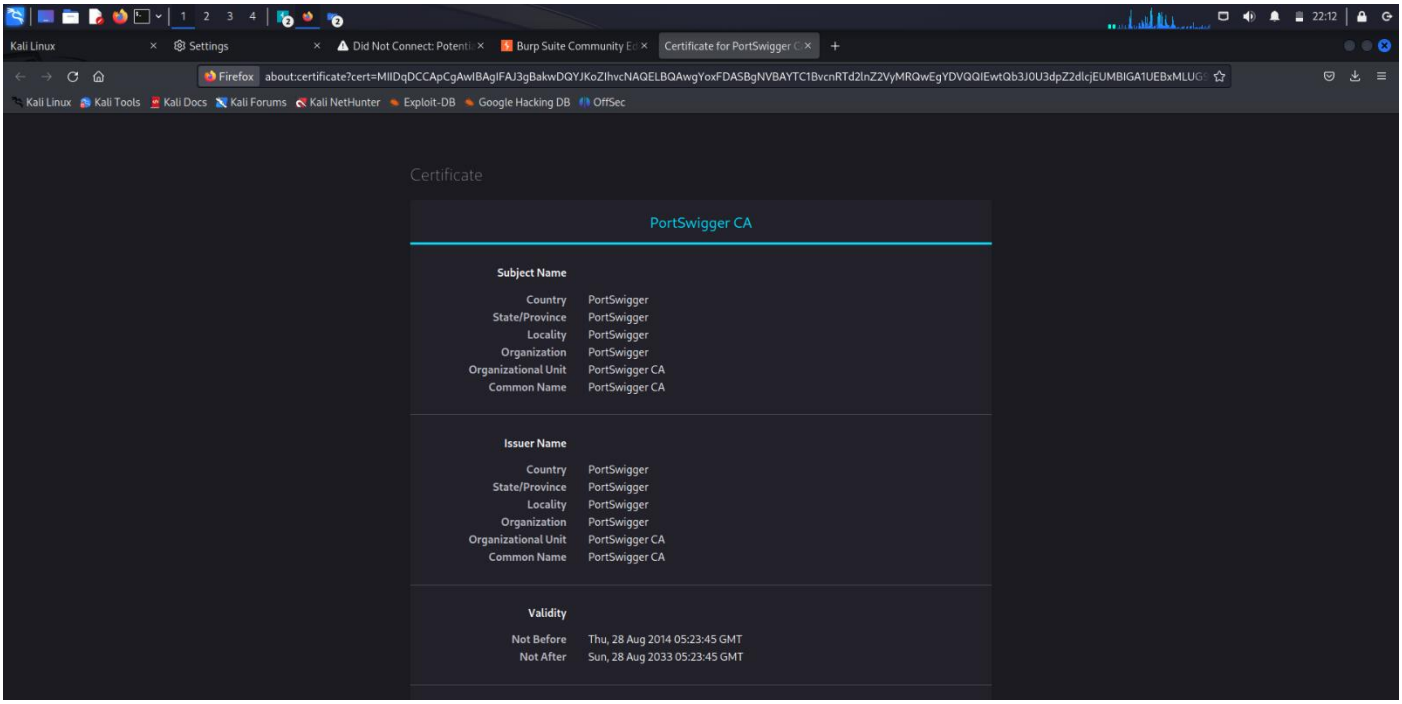


- Check the boxes saying
  - ✓ Trust this CA to identify websites.
  - Trust this CA to identify email users.
- Click on OK

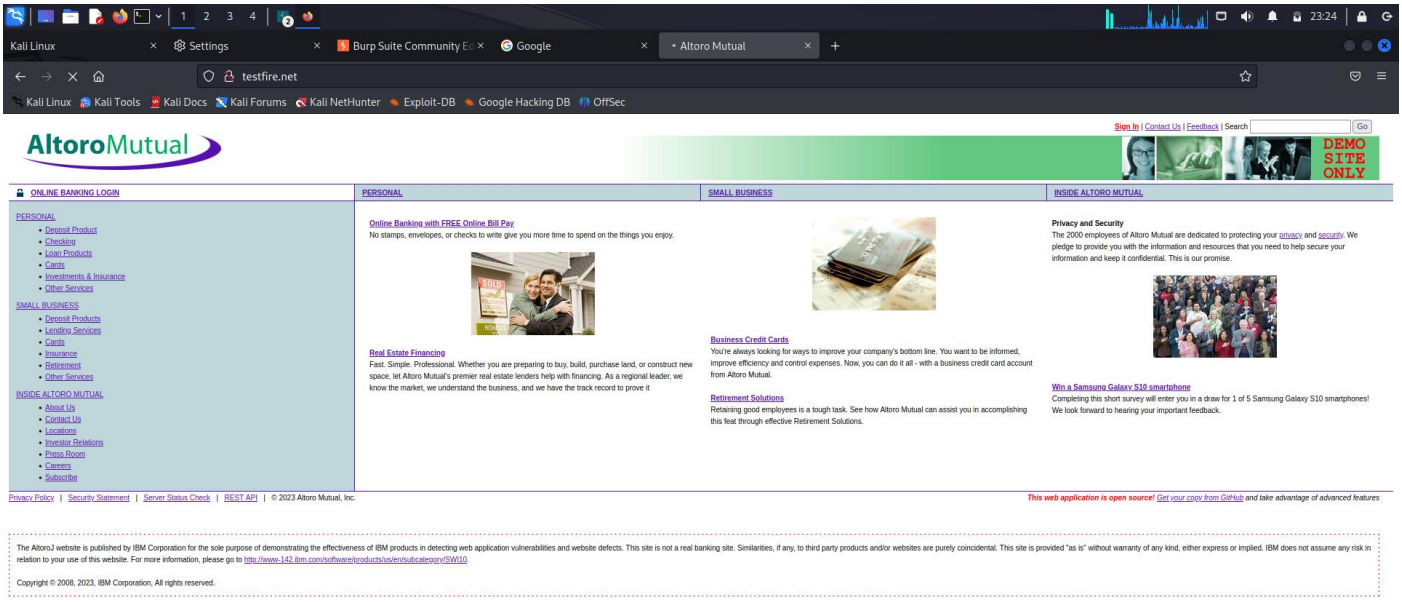


- Ensure that the CA certificate has been imported
- Search for Portswigger in Authorities, if it is present then the import has been successful

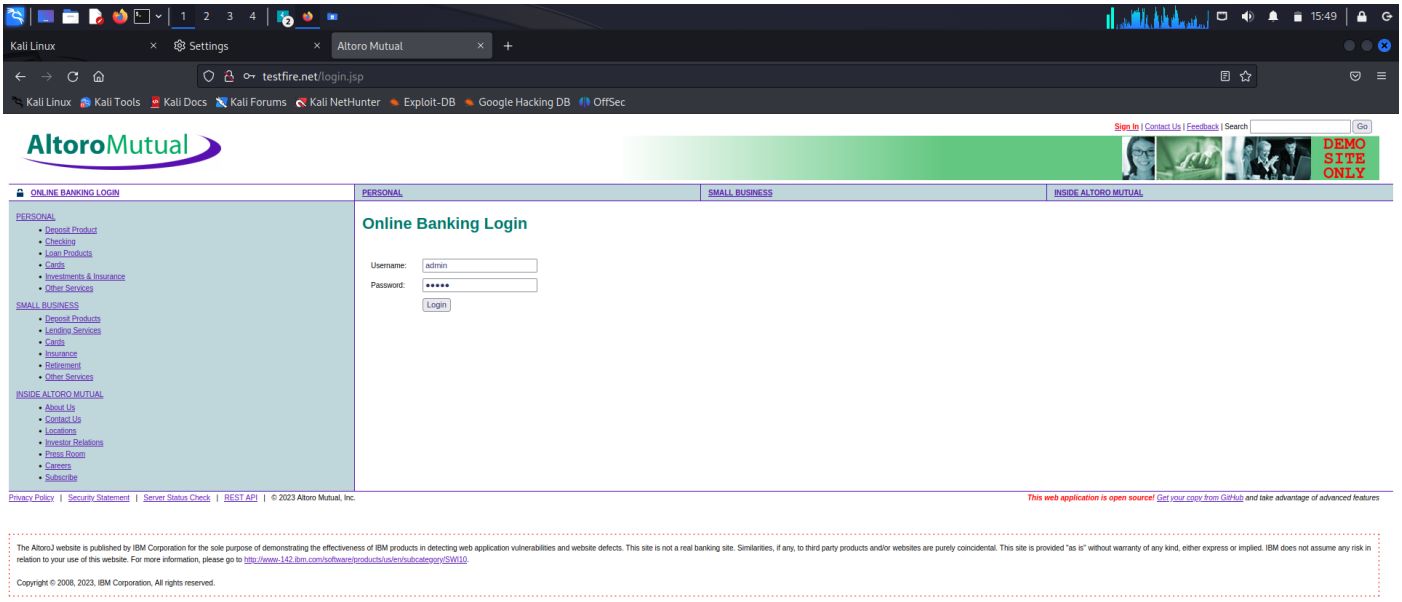


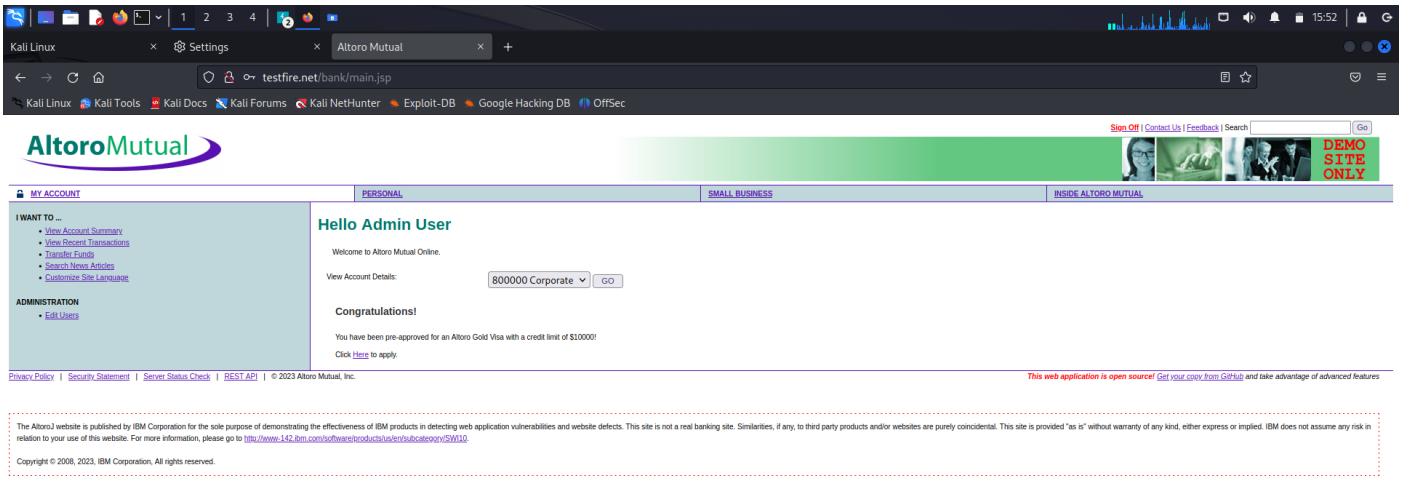


8. Open a HTTP website
    - Open any HTTP website(In this case, it is http://testfire.net)
    - The connection has been established between the browser and the website successfully after importing the CA certificate.

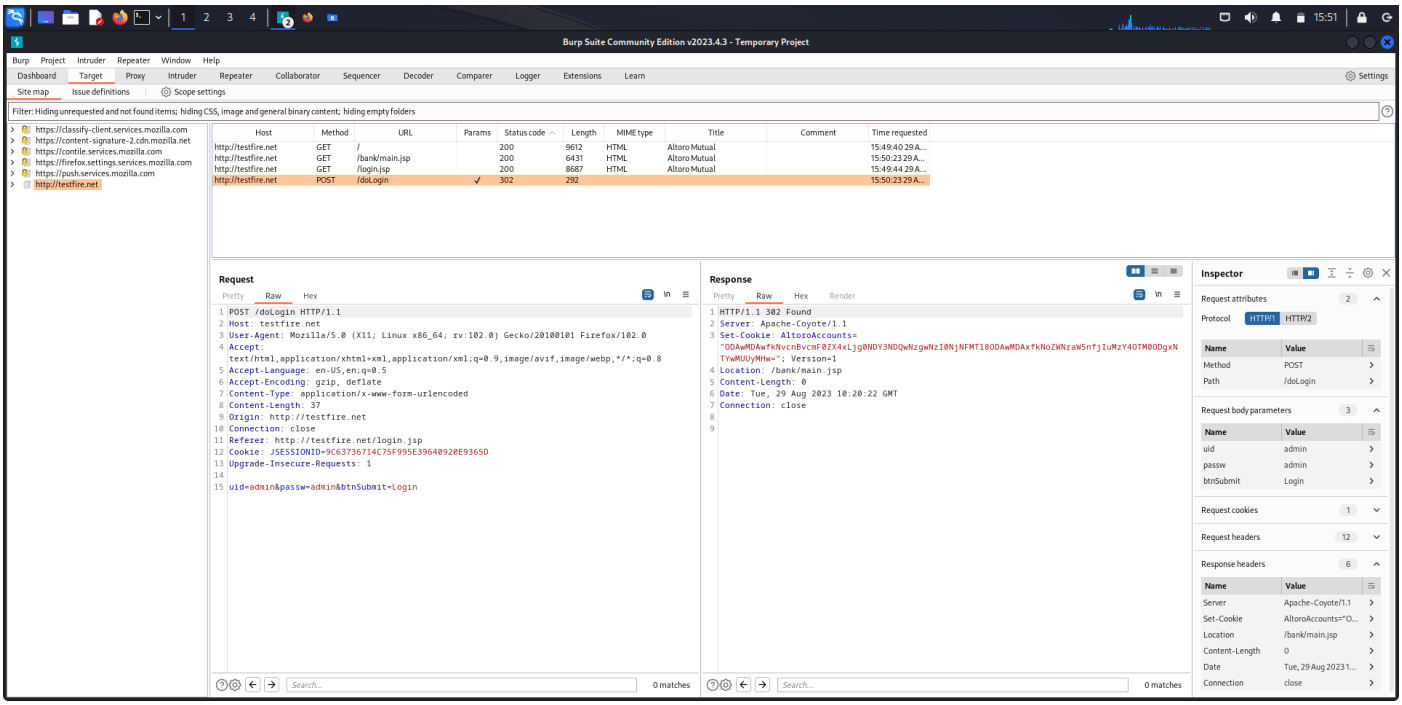


9. Open the Login page
    - Open the Login page of the site
    - Log in to using your credentials
      Username: admin, Password: admin
    - Click on Login





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.



Analysis

The analysis of the penetration testing results reveals a series of critical vulnerabilities that demand immediate attention. The application exhibited susceptibility to SQL injection attacks in its user authentication module, potentially granting unauthorized access to sensitive data. Additionally, multiple instances of cross-site scripting (XSS) were detected in user-input fields, posing a threat of client-side script execution. The absence of proper session management controls was observed, enabling potential session fixation attacks that could compromise user accounts.

Conclusion

In conclusion, the penetration testing process conducted on the web application using Burp Suite has unveiled substantial security concerns that need urgent resolution. The identified vulnerabilities, ranging from SQL injection and cross-site scripting to session management flaws, underscore the pressing need for comprehensive security measures. Addressing these issues promptly is paramount to safeguarding user data, maintaining business reputation, and ensuring regulatory compliance. By embracing the recommended remediation steps and fostering a proactive security mindset, the application can be fortified against potential threats and its overall security posture significantly improved.