Saumyaa Prajapat
21BCI0265

ASSIGNMENT 4

Understanding Burp Suite

What is burp suite?

Burp Suite software is the best toolkit for web security testing. During web security testing, intrusion also protects the grace of engineers. Used to find and exploit search vulnerabilities. Therefore, Burp Suite is designed for point-and-click use. Understanding how systems are attacked is essential for anyone working in security, whether they are a developer or a security professional. Burp Suite is a platform and graphical tool that work together to perform security testing on online applications.

Why burp suite?

Burp Suite is a proxy program that allows us to monitor, review and modify requests made by our browser before they are transmitted to a remote server. It is the leading web application security solution. It gives us the ability to manually check for vulnerabilities, intercept HTTP messages, and modify message content and headers.
Comprehensive framework that can be used to perform a number of activities, including:

- Collect information on the web.
- Test web applications, manually and automatically. Web application analysis.
- Detect vulnerabilities
- BurpSuite also has the advantage of being integrated into the Chrome browser.

What are the features of burp suite?

- Intercept everything your browser sees

Burp Suite's built-in browser works right out of the box - enabling you to modify every HTTP message that passes through it.

- Quickly assess your target

Determine the size of your target application. Auto-enumeration of static and dynamic URLs, and URL parameters.

- Speed up granular workflows

Modify and reissue individual HTTP and WebSocket messages, and analyze the response - within a single window.

- Manage recon data

All target data is aggregated and stored in a target site map - with filtering and annotation functions.
Exposing hidden attack surfaces
Find hidden target functionality with advanced auto-detection for “hidden” content.

- Working with HTTP/2

Burp Suite provides unprecedented support for HTTP/2-based testing, allowing you to work with HTTP/2 requests in ways other tools cannot.

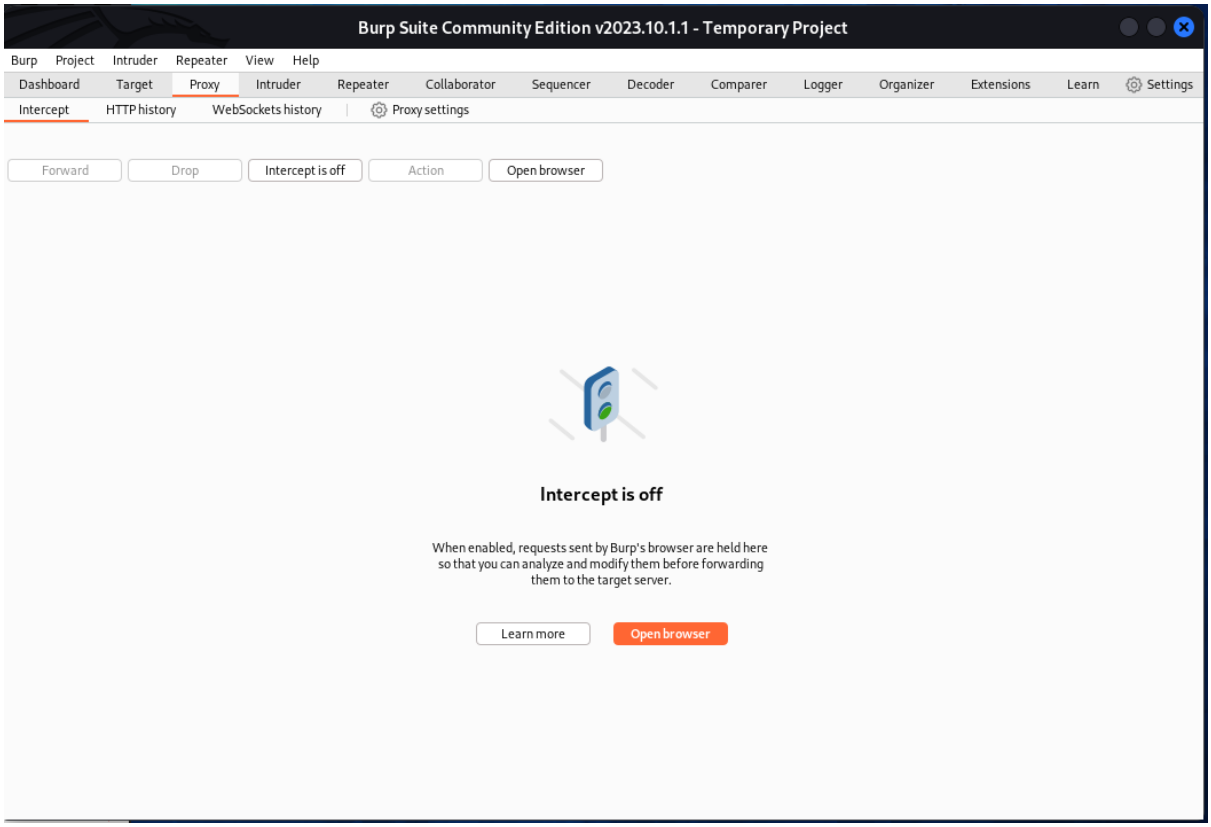
- Manually check for out-of-band vulnerabilities

Use a dedicated client to integrate Burp Suite's out-of-band (OAST) capabilities during manual testing. DOM invader
Use Burp Suite's built-in browser to check for DOM XSS vulnerabilities more easily - with DOM Invader.

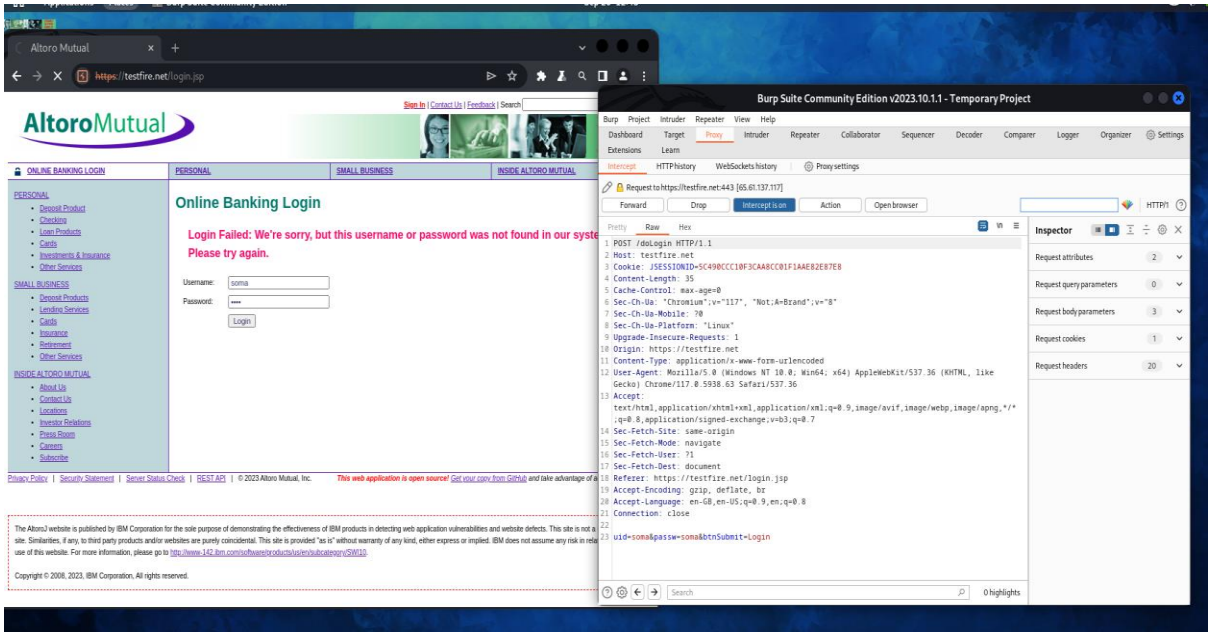
Saumyaa Prajapat
21BCI0265

Test the vulnerabilities of testfire.net :- http://testfire.net

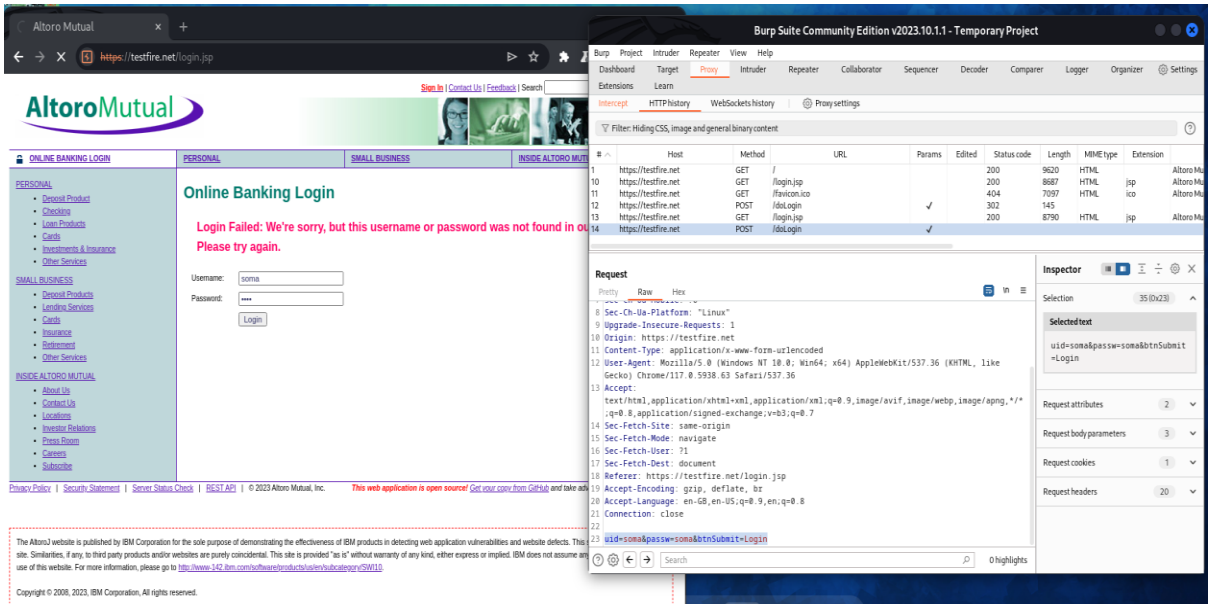
Step 1:
Open Burp Suite go to proxy and open the browser.



Step 2:
In browser search for the link and try to login with intercept on in burp suite.



Saumyaa Prajapat
21BCI0265



Result:

The given website is vulnerable as the passwords can be extracted using Burp Suite.