AI FOR CYBERSECURITY WITH IBM QRADAR

ASSIGNMENT – 4

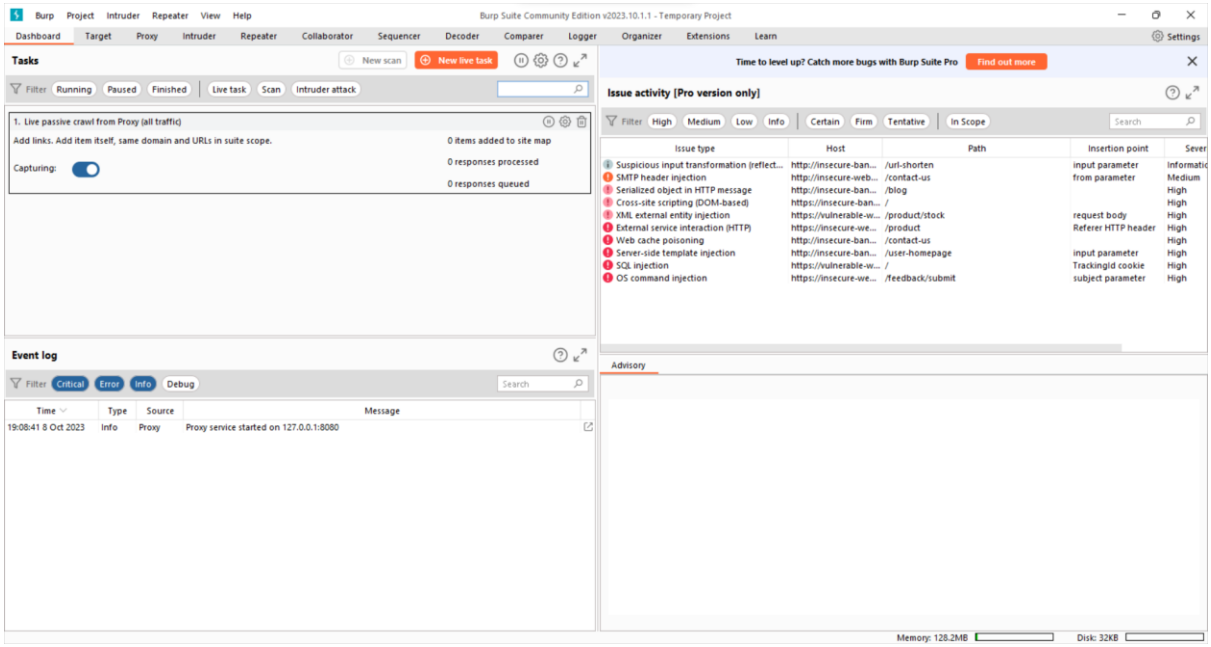
NAME: ORRA RAGHAVENDRA REDDY

BRANCH: CSE – INFORMATIION SECURITY

COLLEGE: VIT – VELLORE

Report on Burp Suite: Overview, Significance, Features, and Vulnerability Testing

BURP SUITE- COMMUNITY EDITION:



Introduction

Burp Suite is a comprehensive software toolkit primarily used for web application security testing and penetration testing. Developed by PortSwigger, it is widely recognized and employed by cybersecurity professionals and ethical hackers to assess the security posture of web applications. This report provides detailed information about Burp Suite, its significance, key features, and demonstrates a vulnerability assessment on the "testfire.net" web application.

What is Burp Suite?

Burp Suite is a suite of tools designed for web security testing. It offers various modules and features that aid in identifying and mitigating vulnerabilities in web applications. These tools assist security professionals in evaluating the security of web applications, APIs, and other web-based systems. Burp Suite is available in both free and paid versions, with the paid version (Burp Suite Professional) offering additional advanced features.

Why Burp Suite is Used and Its Significance

Purpose:

- Web Application Security Testing: Burp Suite is primarily used for assessing the security of web applications. It helps identify vulnerabilities, misconfigurations, and potential attack vectors that malicious actors could exploit.

Significance:

- Vulnerability Discovery: Burp Suite's automated and manual testing capabilities help discover a wide range of vulnerabilities, including SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and more.

- Penetration Testing: It is a vital tool for ethical hackers and penetration testers to evaluate an application's defenses, find weaknesses, and help organizations strengthen their security measures.

- Bug Bounty Hunting: Many security researchers and bug bounty hunters use Burp Suite to find security flaws in web applications and earn rewards for responsible disclosure.

- Web Application Developers: Developers can also benefit from Burp Suite to identify and fix security issues during the development and testing phases, thereby improving the overall security of their applications.

Key Features of Burp Suite

Burp Suite offers a wide range of features, including:

1. **Proxy**:

- **Explanation**: Burp Suite's Proxy feature acts as an intermediary between your web browser and the target web application. It captures and allows you to inspect HTTP requests and responses in real-time.

- **Use Case**: This is particularly useful for understanding how data is transmitted between the client and server, manipulating requests and responses, and identifying potential security issues.

2. **Scanner**:

- **Explanation**: The Scanner feature automates the process of finding security vulnerabilities in web applications. It analyzes the application for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and more.

- **Use Case:** Testers use Scanner to quickly identify and report potential vulnerabilities, saving time compared to manual testing.

3. **Repeater**:

- **Explanation**: Repeater allows testers to manually manipulate and send HTTP requests to the target application. It is useful for testing different payloads, modifying request parameters, and observing the application's responses.

- **Use Case**: Testers can fine-tune attacks, validate vulnerabilities, and explore the application's behavior under various conditions.

4. **Intruder**:

- **Explanation**: Intruder is designed for automated attacks on web applications. Testers can define attack scenarios, customize payloads, and specify attack parameters to test for issues such as brute force attacks or input validation problems.

- **Use Case**: Intruder is used to automate and scale security testing, especially when dealing with complex attack patterns.

5. **Spider**:

- **Explanation**: The Spider tool crawls the target application, mapping its content and structure. It helps testers identify all accessible pages, endpoints, and APIs within the application.

- **Use Case**: Spider is valuable for creating a comprehensive view of the application's attack surface and discovering hidden or undocumented features.

6. **Sequencer**:

- **Explanation**: Sequencer assesses the quality of randomness in tokens, session identifiers, and other data generated by the application. It helps identify vulnerabilities related to weak session management or session fixation.

- **Use Case**: Security testers use Sequencer to analyze the predictability of application-generated data, which can be critical in protecting session-related security mechanisms.

7. **Decoder**:

- **Explanation**: The Decoder tool assists in encoding and decoding various data formats, such as URL encoding, Base64 encoding, and more. It is used to manipulate and understand data sent to or received from the application.

- **Use Case**: Testers use Decoder to craft specific payloads, bypass input validation, or investigate how data is handled by the application.

8. **Comparer**:

- **Explanation**: Comparer allows testers to compare two HTTP requests or responses side by side, highlighting any differences. This is helpful for identifying variations in behavior or responses under different input conditions.

- **Use Case**: Testers use Comparer to spot discrepancies or changes in the application's responses during security testing.

9. **Extensibility**:

- **Explanation**: Burp Suite is highly extensible through its Extender API. Users can develop custom plugins and scripts to automate tasks or create tailored testing workflows.

- **Use Case**: Security professionals and developers use Extensibility to customize Burp Suite to their specific needs and integrate it into their existing security testing processes.

10. **Collaborator**:

- **Explanation**: The Collaborator tool helps identify out-of-band vulnerabilities by generating unique DNS and HTTP interactions. It can detect when the application makes external requests based on user input.

- **Use Case**: Collaborator is used to discover hidden vulnerabilities that may not be apparent through traditional testing methods, such as blind SSRF (Server-Side Request Forgery) or DNS data exfiltration attacks.

These features collectively make Burp Suite a versatile and powerful tool for identifying and addressing security vulnerabilities in web applications, enhancing the overall security posture of web-based systems.

Vulnerability Testing on "testfire.net"

Methodology:

1**. Proxy Configuration**: Configure Burp Suite's proxy to intercept and log HTTP traffic between the user and the target application.

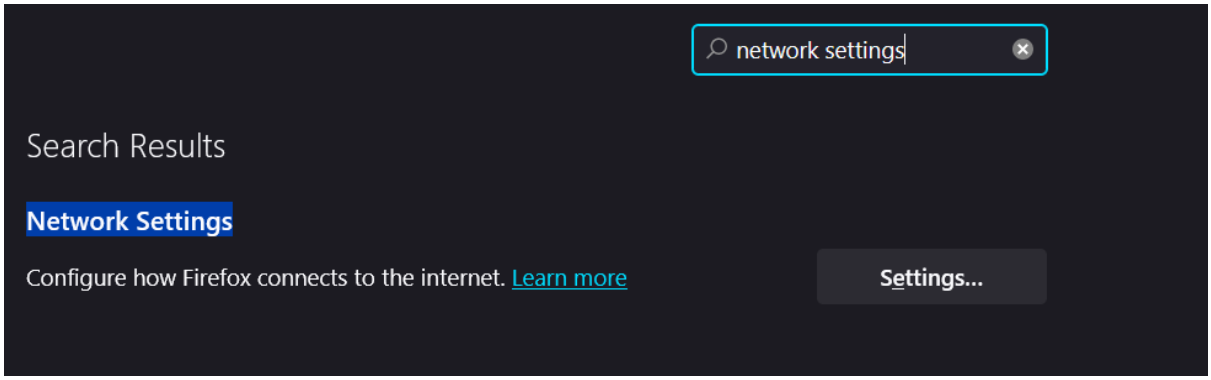
2. **Spidering**: Use the Spider tool to crawl the "testfire.net" website, mapping its content and identifying potential entry points for further testing.

3. **Scanner**: Run the automated scanner to detect common vulnerabilities such as SQL injection, XSS, and more.

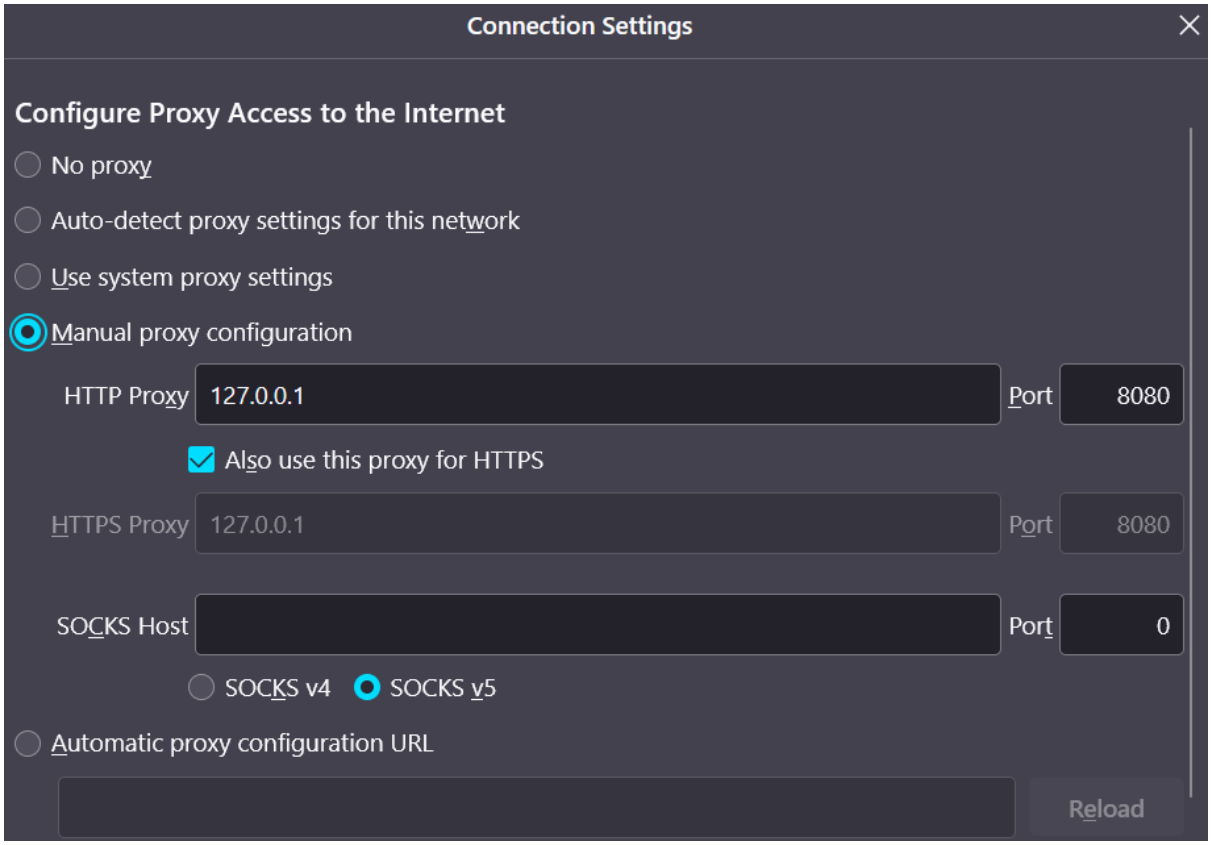
4. **Manual Testing**: Utilize the Repeater and Intruder tools for manual testing, targeting specific parameters or pages to identify vulnerabilities.

5. **Report Generation**: After testing, generate a comprehensive report detailing the identified vulnerabilities, their severity, and recommendations for mitigation.

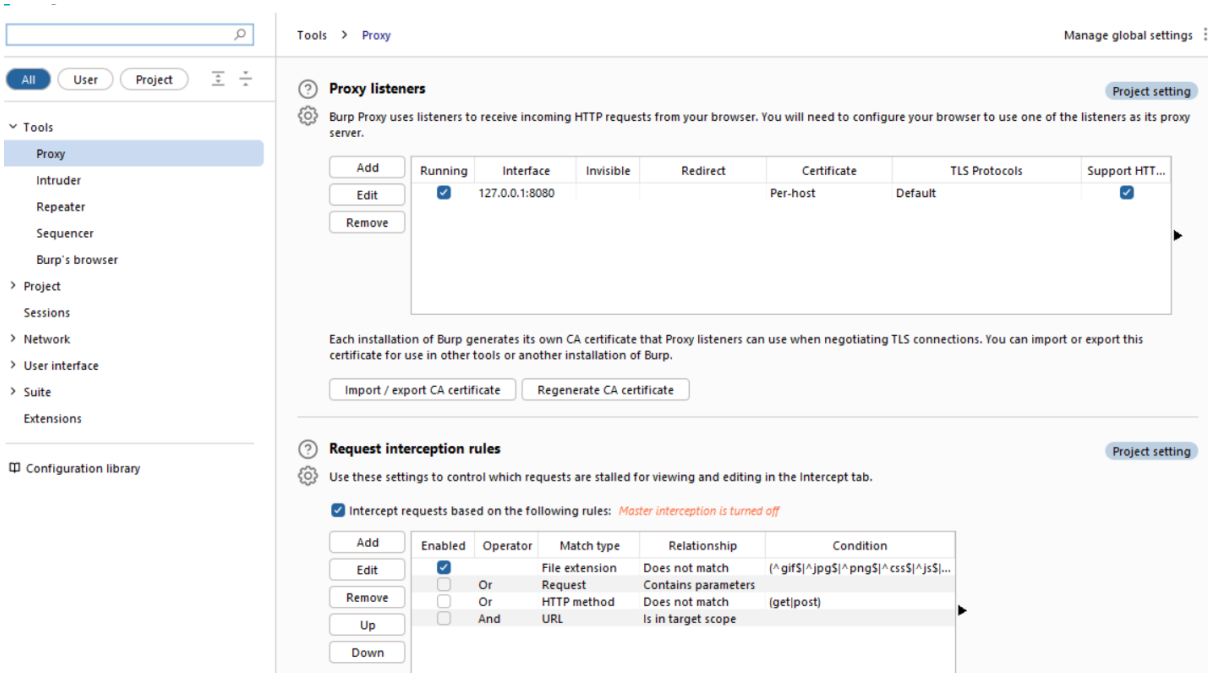
First we need to select a browser and then we need to configure the network settings



Then we need to create a new proxy manually for connecting the burp suite and the browser

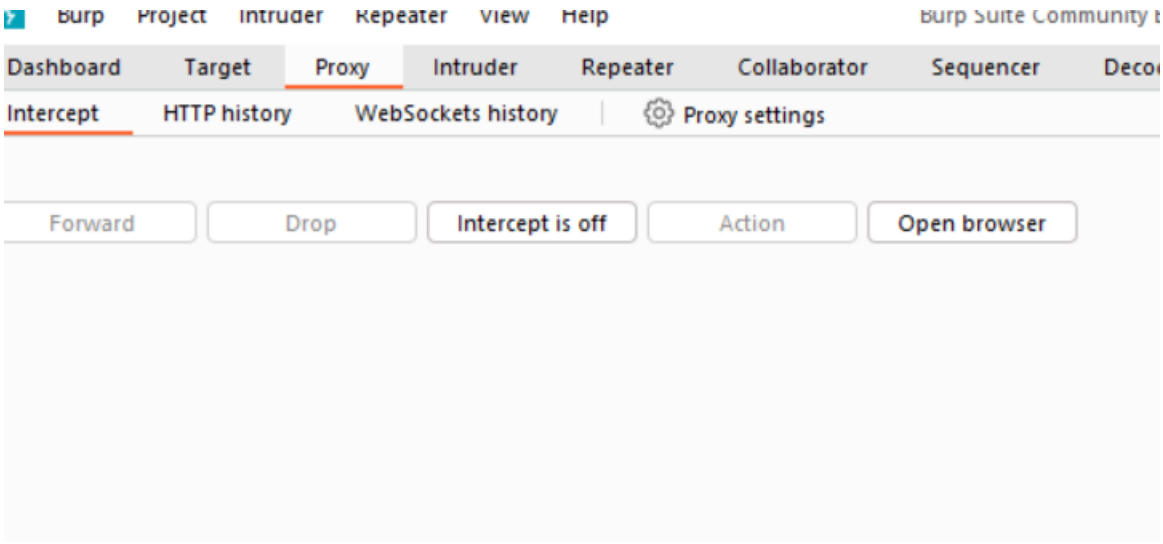


Here the http proxy is default for all the devices as it is the ip address of the burp suite and '8080' is the designated port number for the burp suite by default.

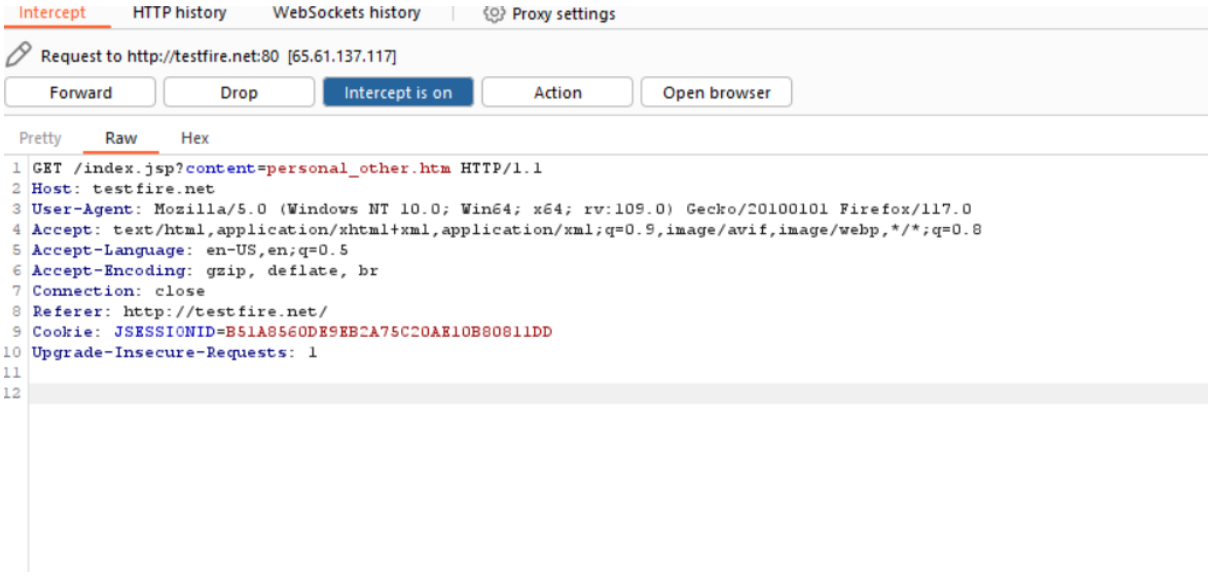


We can see the details of the burp suite in the proxy settings. We can even change it if we want for now we will keep it as it is and use default settings for our browser.

We need a CA certificate for burp suite in order to access the webpages while connecting the burp suite with the browser and keeping the intercept on.

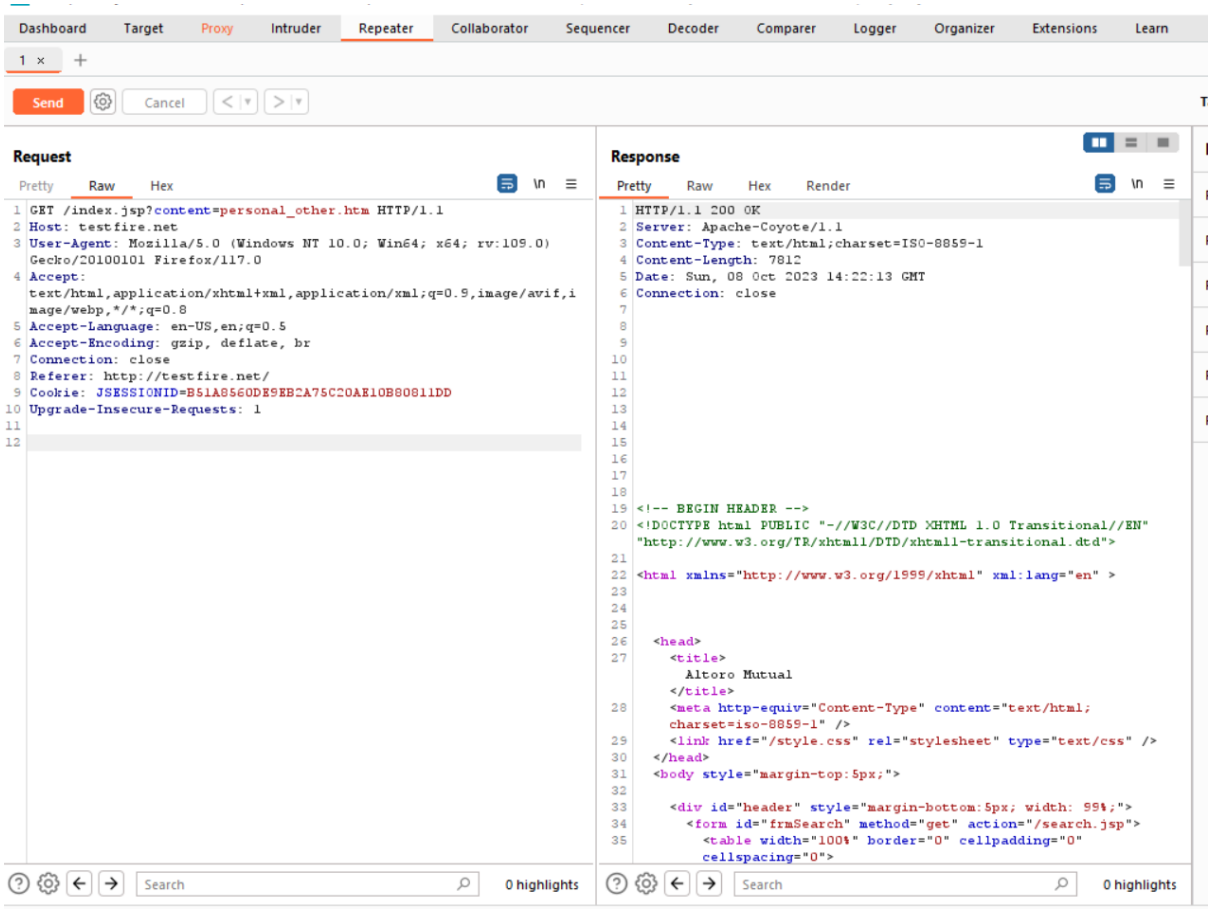


When the intercept is on we connect to the burp suite we will get info of the particular page we have connected to in the proxy



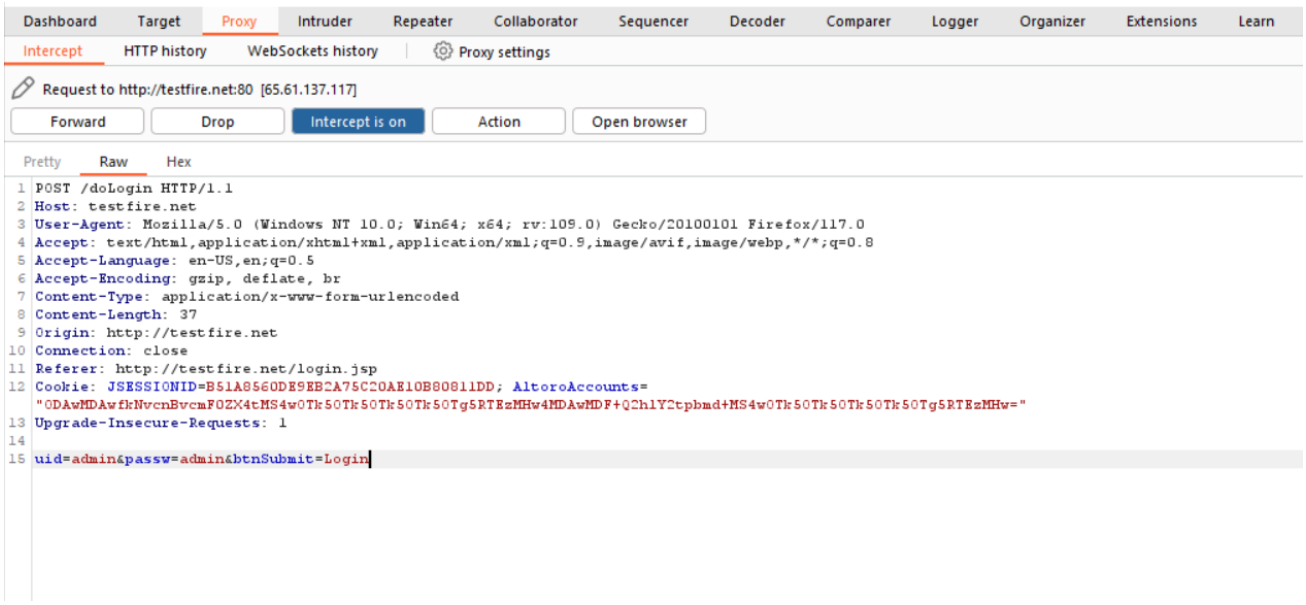
We can send this information to the repeater/ intruder to any type of attacks we need.

First we will send this information to the repeater by right-clicking on the proxy page and selecting send to repeater

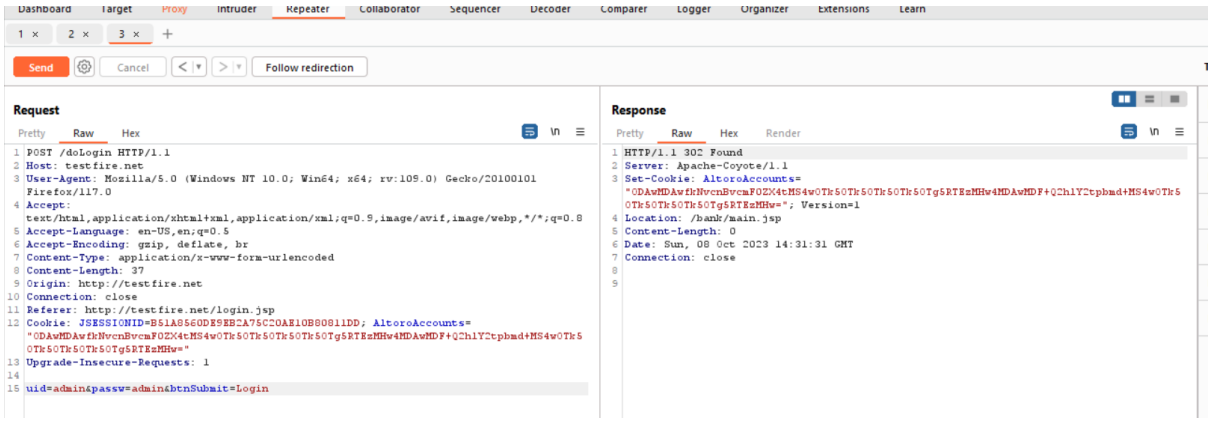


Here we can see the repeater page and when we click on send button we receive a response. In the response we can see a lot of info like what type of server it is and all the source code of the webpage as well.

When the intercept is on and someone signs into the webpage we can see the login details as well

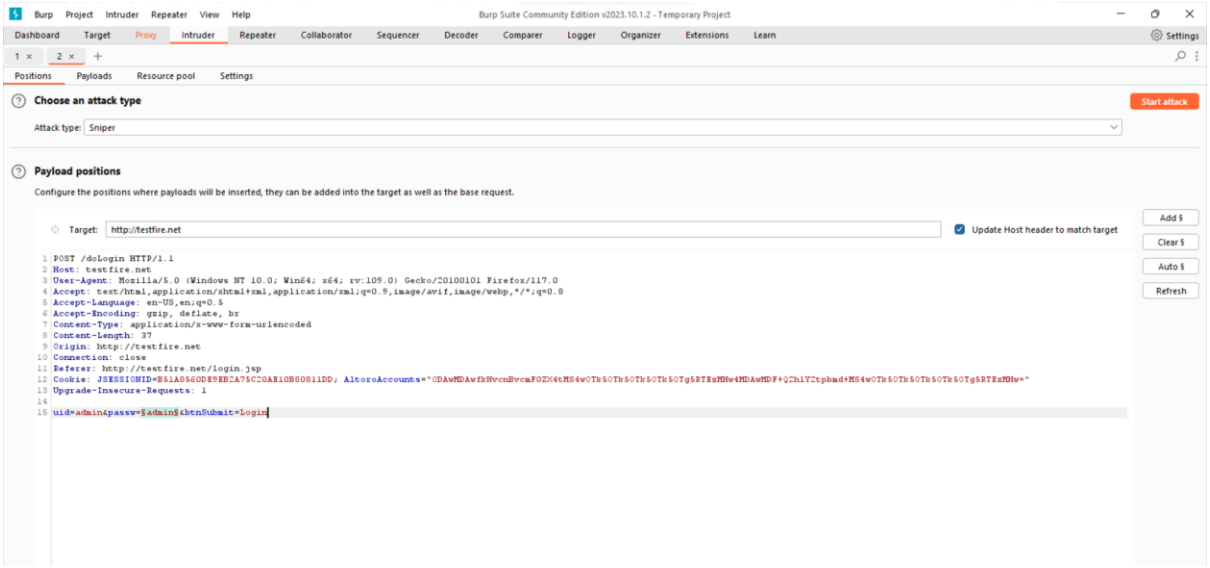


And when we send this login details to the repeater and get a response we can see this

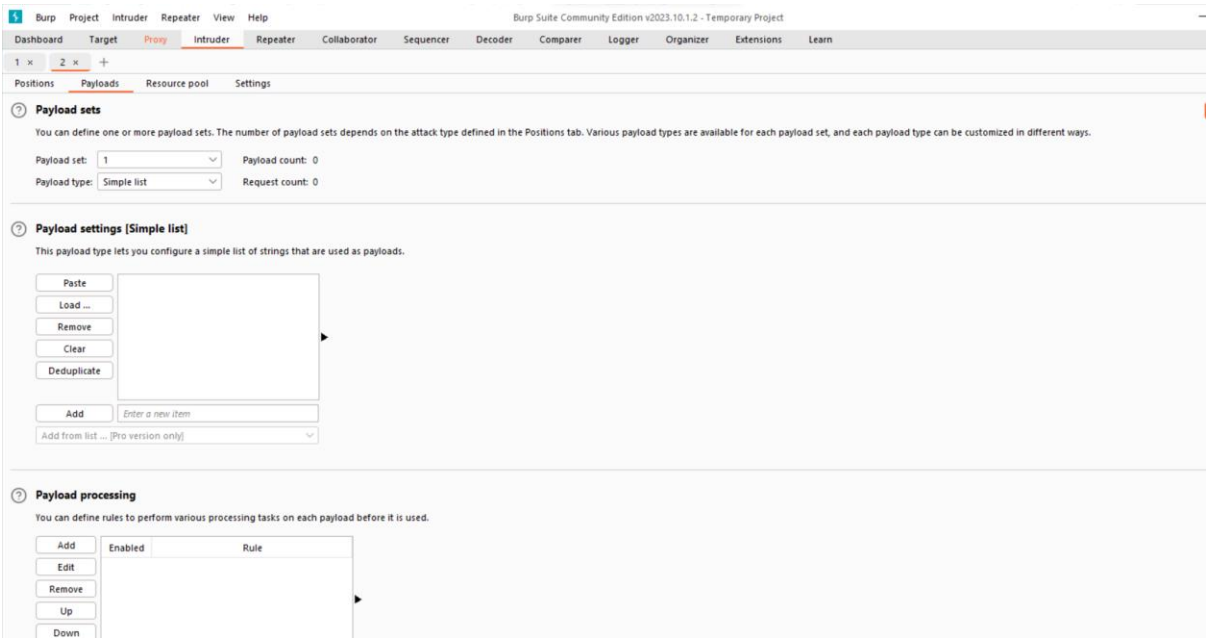


We can also see the hidden cookies in the response side.

Now we send this to the intruder to attack

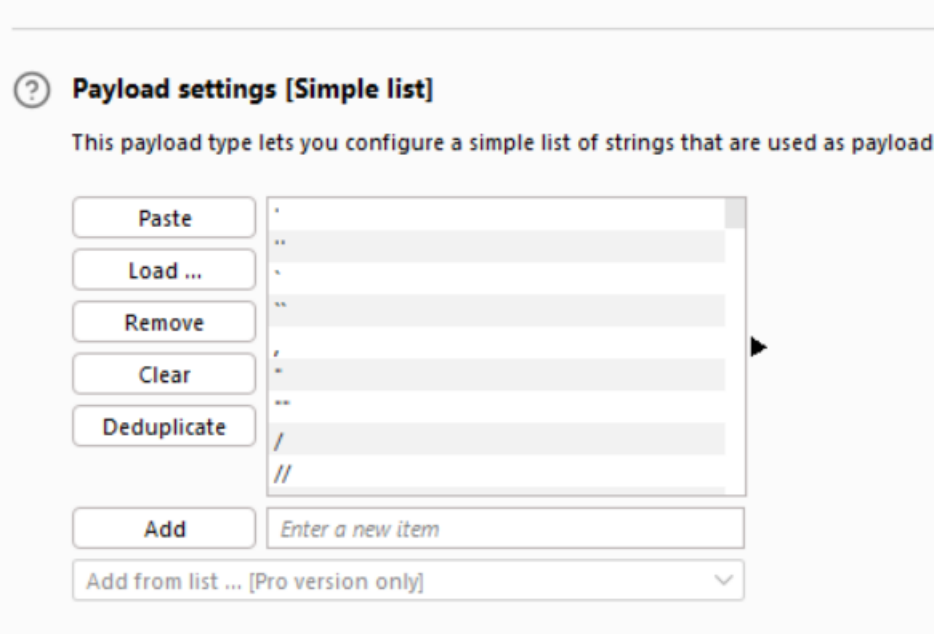


And we click on add$ button to the password and start the attack but in order to start the attack we need to input payloads to it

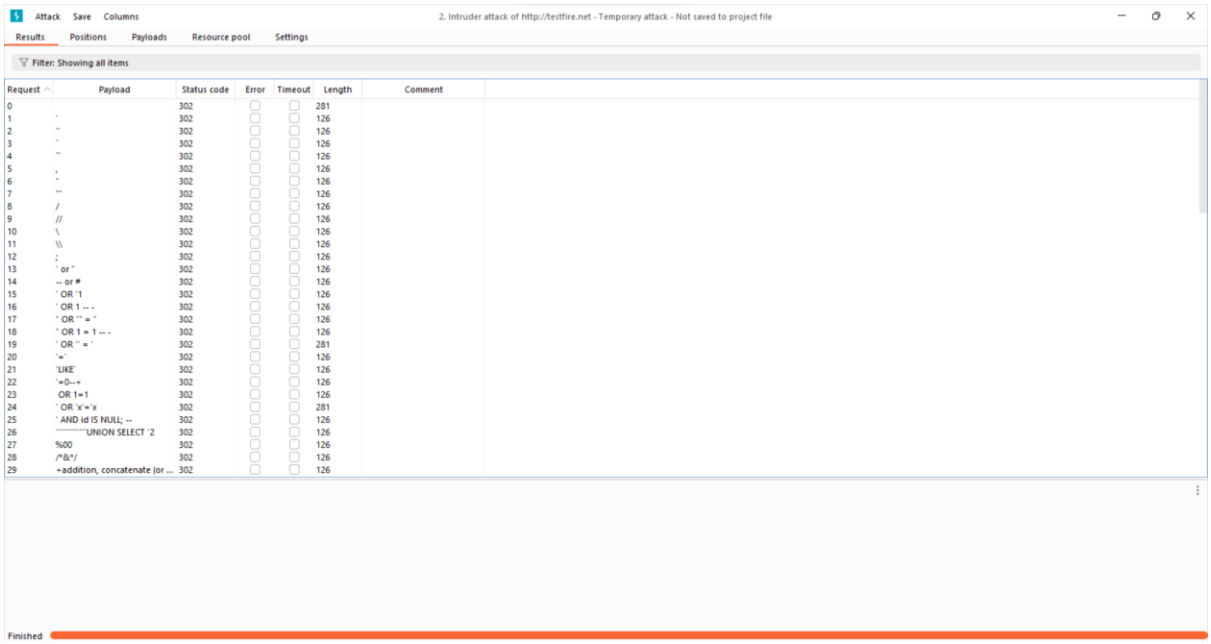


In this page we have to insert the payloads. So we search for the payloads on other browser as the current one is linked to the burp suite.

We can find the payloads on github copy it and paste it here



Now we need to start the attack. After starting the attack we will get a new popup and it shows us the status of the payload being inserted and the status code as well.



We have successfully injection sql code to the login page and got the result.

Conclusion:

Burp Suite is a powerful and widely-used tool for web application security testing and penetration testing. Its range of features, including proxying, scanning, and manual testing, make it an invaluable asset for security professionals and ethical hackers. By effectively assessing the security of web applications like "testfire.net," organizations can take proactive steps to enhance their security posture and protect against potential threats.