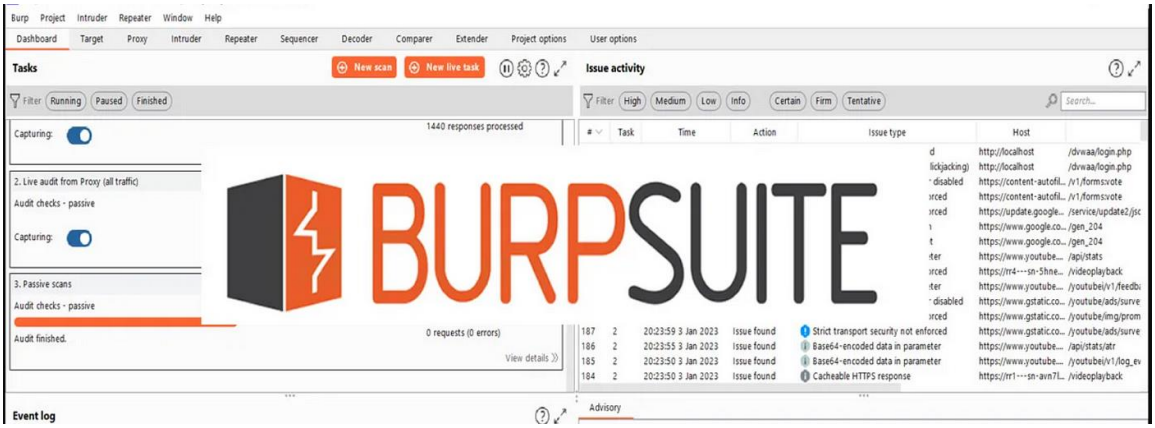
Run Your First Vulnerability Scanner Burp Suite Project

Table of Contents

Introduction

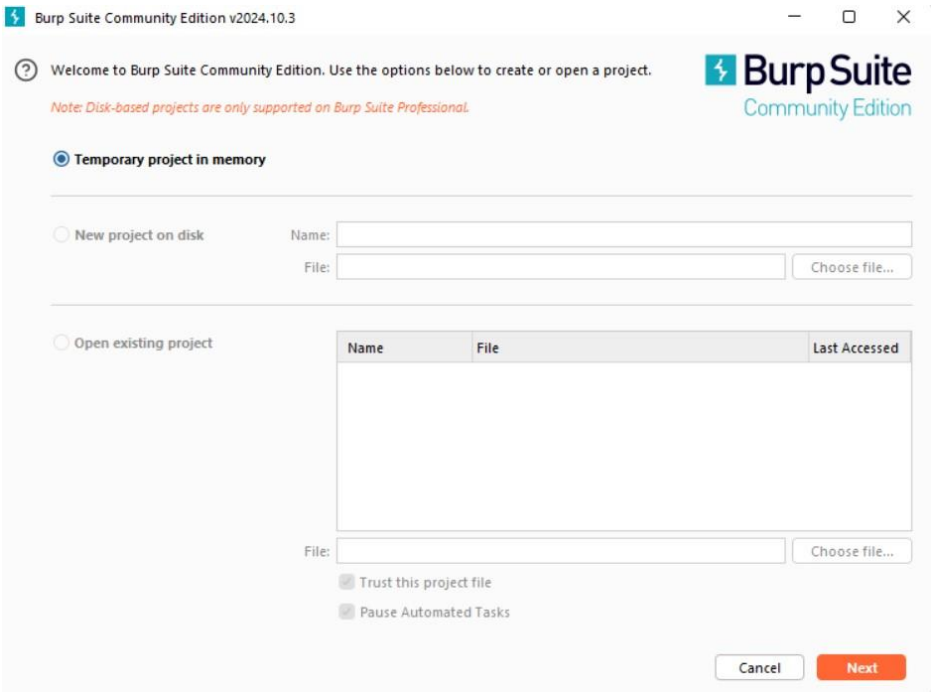
This project explores the use of **Burp Suite**, a powerful web vulnerability scanner and testing tool. Through this project, I gained practical experience in intercepting, modifying, and analyzing HTTP traffic. The project demonstrates Burp Suite's features, including Proxy, Repeater, and Scanner, and their role in identifying security vulnerabilities.



Objective

The primary goal was to familiarize myself with Burp Suite by:

1. Installing and setting up the tool.
2. Intercepting and modifying HTTP requests.
3. Analyzing traffic and identifying vulnerabilities on a deliberately vulnerable web application.



Project Setup

Tools Used

- **Burp Suite Community Edition**: Web vulnerability scanning and testing.
- **Web Security Academy**: A platform for practicing web security using intentionally vulnerable applications.

Environment

- A desktop computer with the Burp Suite Community Edition installed.
- Access to the Web Security Academy labs.

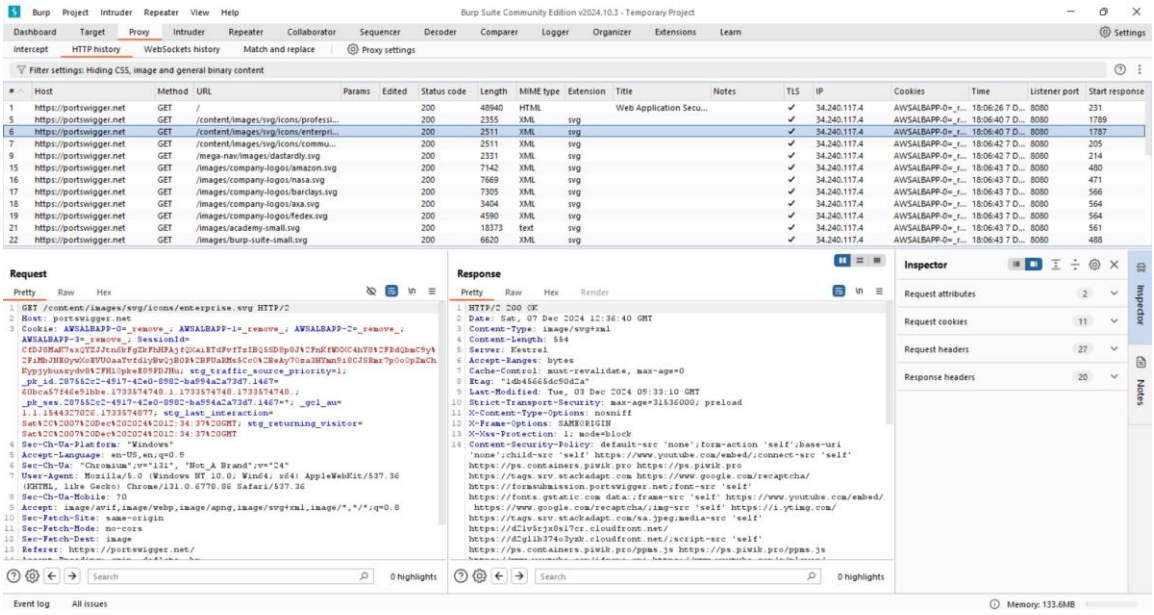
Steps to Set Up

1. **Download and Install**: Obtained the Burp Suite installer and followed the guided installation steps
2. **Launching Burp Suite**:
    - Selected the Community Edition project type.
    - Set up Burp Proxy to intercept HTTP traffic.
3. **Lab Environment**: Accessed the Web Security Academy for test scenarios.

Implementation

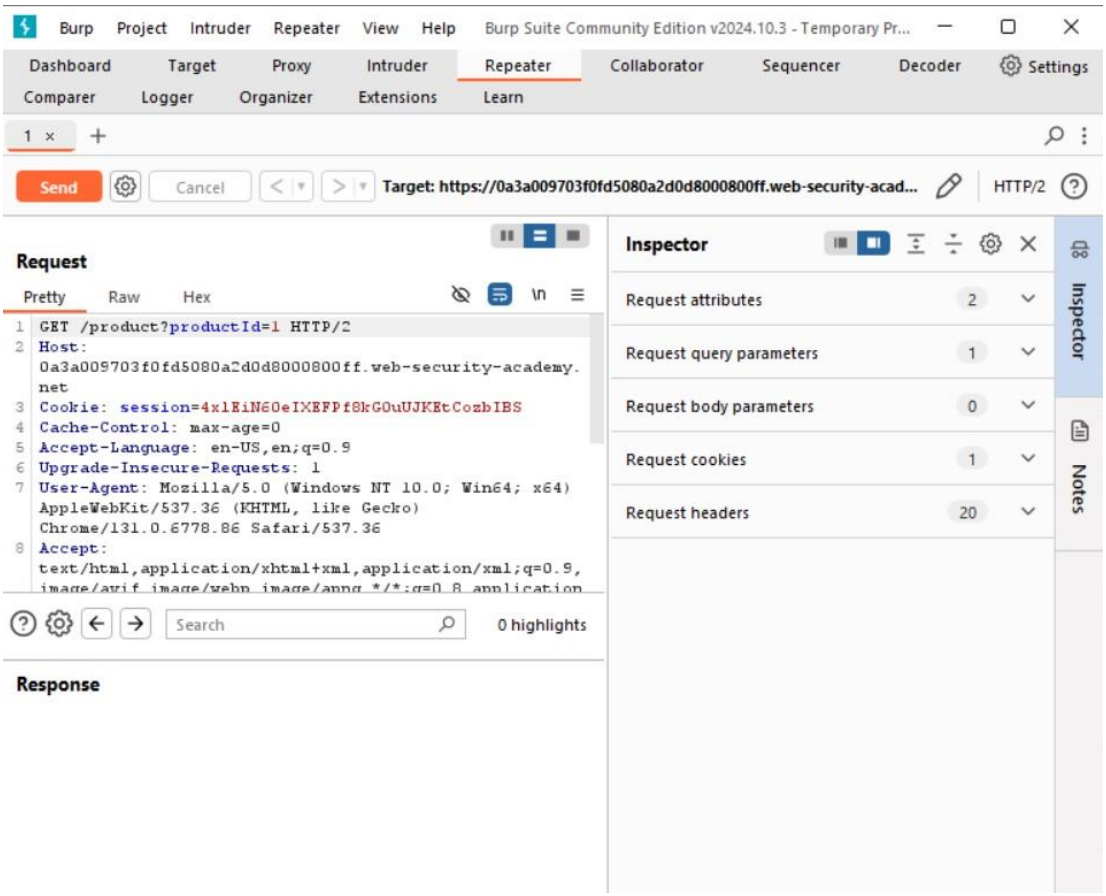
1. Intercepting HTTP Traffic

- Configured Burp Proxy to intercept HTTP requests between the browser and server.
- Observed intercepted requests, analyzed their parameters, and forwarded them to the server.



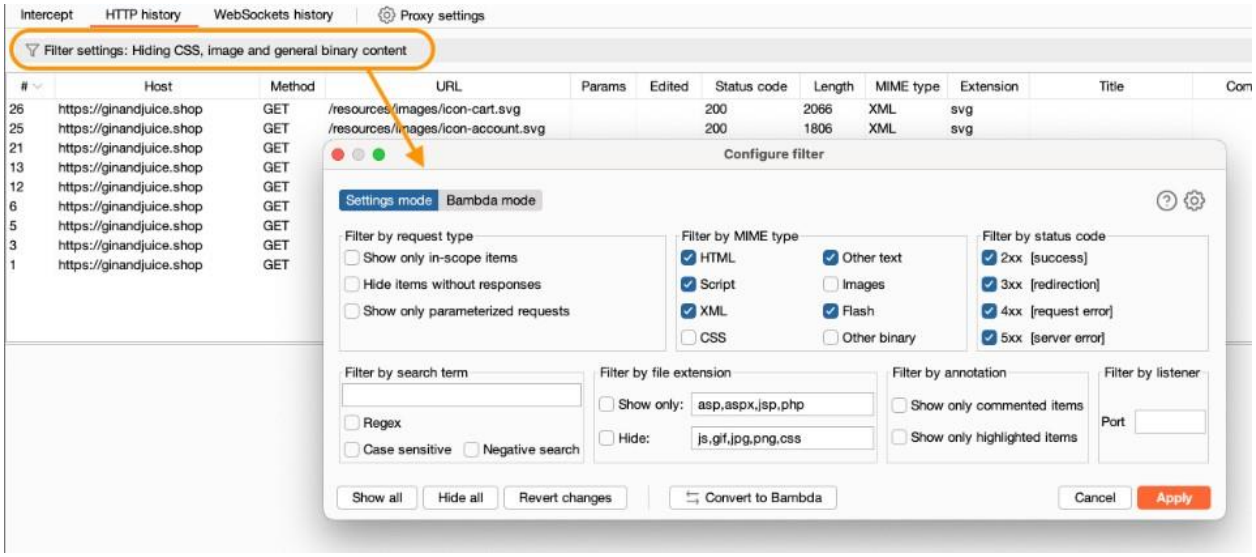
2. Modifying HTTP Requests

- Manipulated intercepted requests to explore potential vulnerabilities. For instance:
    - Adjusted pricing parameters in a POST request to simulate unauthorized discounts



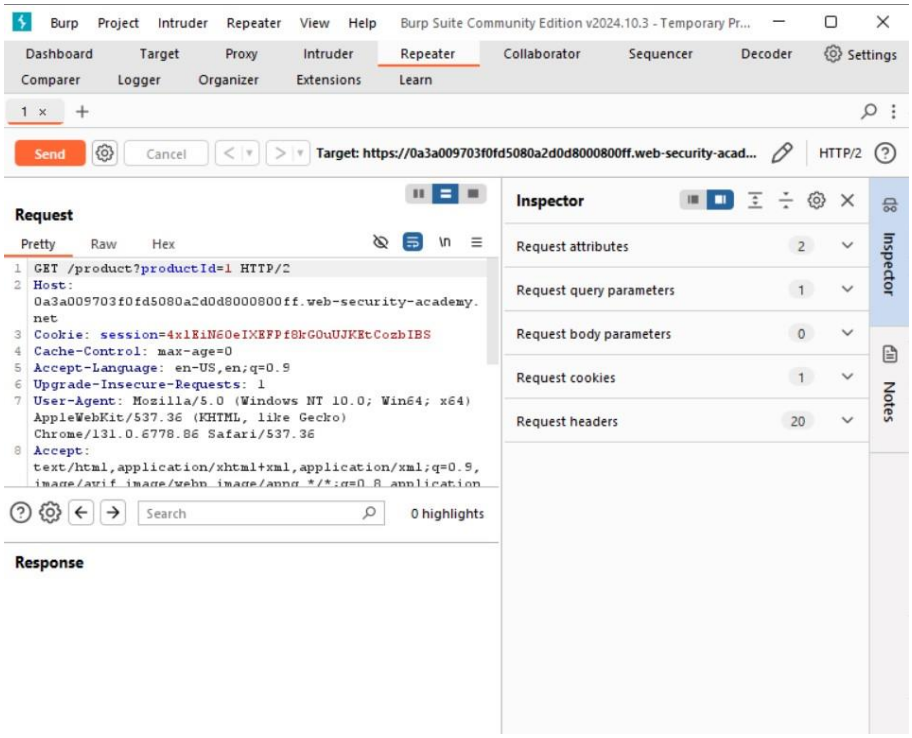
3. Analyzing HTTP History

- Reviewed the HTTP traffic log to identify patterns and unusual behavior.
- Filtered traffic to focus on the target scope, eliminating irrelevant entries.



4. Reissuing Requests with Burp Repeater

- Used Burp Repeater to resend and modify requests iteratively, validating how the server handles unexpected input.



Results and Learning Outcomes

Achievements

- Successfully exploited vulnerabilities in the test environment, including price modification and information disclosure.
- Understood the importance of secure HTTP request handling and proper input validation.

Challenges

- Initially struggled with intercepting all HTTP traffic but resolved it by refining the scope settings.
- Encountered issues with repetitive requests, which were managed by toggling interception.

Key Learnings

- Burp Suite is a versatile tool for penetration testing, enabling in-depth exploration of web vulnerabilities.
- Hands-on practice is crucial to mastering cybersecurity tools like Burp Suite.

Conclusion

This project significantly deepened my understanding of web vulnerabilities and provided hands-on experience with Burp Suite, a leading tool for web application security testing. By working through real-world scenarios, I was able to identify and exploit vulnerabilities, gaining practical insight into the complexities of web application security. The project underscored the critical role of secure coding practices in mitigating risks, as well as the importance of proactively identifying and addressing weaknesses in web applications. Furthermore, it emphasized the necessity of continuous learning and practical application to stay ahead in the dynamic and ever-evolving field of cybersecurity.