Shaik Kaleshavali-21BAI106

Burp suite

Table of Contents

1. Introduction

What is Burp Suite?

Burp Suite is an integrated platform for performing security testing of web applications. Developed by PortSwigger, it is widely used by security professionals, penetration testers, and developers to identify and address security vulnerabilities in web applications.

Key Uses of Burp Suite

Burp Suite offers a wide range of features and capabilities:

- Web Application Scanning: Burp Suite can automatically scan web applications for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It helps identify potential vulnerabilities that attackers could exploit.
- Proxying and Intercepting Traffic: It acts as a proxy server, allowing users to intercept and analyze HTTP requests and responses. This is useful for understanding how web applications work and identifying security issues.
- Spidering and Crawling: It can be used to automatically crawl and map the structure of a web application, helping testers identify potential entry points for testing.
- Session Management: Burp Suite can manage and manipulate session cookies and tokens, which is essential for testing authentication and authorization mechanisms.
- Intruder Tool: The Intruder tool allows testers to perform automated attacks on web applications, helping to discover vulnerabilities through brute force and parameter manipulation.
- Repeater Tool: The Repeater tool is used for manual manipulation and testing of individual HTTP requests to a web application, making it useful for testing specific vulnerabilities.

2. Getting Started

Installing Burp Suite

1. Download: Start by downloading Burp Suite Community Edition from the official PortSwigger website.
2. Installation: Follow the installation instructions for your operating system. Installation is typically straightforward and involves running the installer package.
3. Launch Burp Suite: After installation, launch Burp Suite.

Configuring Your Browser

1. Proxy Configuration: Configure your web browser to use Burp Suite as a proxy server. Set the proxy settings to use localhost and port 8080.
2. SSL/TLS Configuration: For HTTPS traffic inspection, Burp Suite generates its SSL/TLS certificates. Import Burp's CA certificate into your browser's trust store.

Setting Up a Project

1. Create a Project: In Burp Suite, create a new project. Projects help you organize your testing efforts.
2. Configure Project Scope: Define the scope of your testing by specifying target URLs, included and excluded domains, and other relevant settings.
3. Project Files: Burp Suite will create project files to store your configuration and findings.

3. Basic Usage

Intercepting Traffic

1. Start Proxy: In Burp Suite, navigate to the Proxy tab and click the "Intercept is On" button. This allows Burp Suite to intercept HTTP requests and responses.
2. Browser Interaction: Browse the web application you are testing. Burp Suite will capture and display intercepted traffic in real-time.
3. Control Flow: Use the "Forward" and "Backward" buttons in the Proxy tab to control the flow of intercepted requests and responses.

Analyzing Requests and Responses

1. Proxy History: In the Proxy tab, review and analyze intercepted requests and responses. You can see details such as HTTP headers, cookies, and parameters.
2. Request Modification: Right-click on requests to perform actions like sending to other tools, modifying, or sending to the Repeater for further testing.

Spidering and Crawling

1. Site Map: The Site Map tab displays a hierarchical view of crawled web pages. Rightclick on entries to send them to various tools for testing.
2. Spider Configuration: Configure the Spider tool by setting the target and scope. The Spider tool automatically discovers and maps the application's structure.

4. Advanced Features

Web Application Scanning

1. Configure Scan: In the Target tab, right-click on the target and select "Scan." Configure the scan settings, including authentication if required.

2. Starting the Scan: Initiate the scan to automatically identify common vulnerabilities like SQL injection and XSS.
3. Review Results: After the scan is complete, review the results in the Scanner tab. Prioritize and investigate identified issues.

Session Management

1. Session Handling Rules: In the Session Handling Rules tab, create rules to manage session tokens and cookies.
2. Session-Based Testing: Use session management to test authentication and authorization mechanisms thoroughly.

Intruder Tool

1. Configuration: In the Intruder tab, load a request, and configure attack types (e.g., Sniper, Battering Ram). Define payloads and positions.
2. Attack: Launch the attack to test parameters, fuzz inputs, and identify vulnerabilities.

Repeater Tool

1. Using Repeater: In the Repeater tab, load a request, modify it, and resend it to the target. Use it for manual testing and analysis of individual requests.

Sequencer Tool

1. Collecting Data: Use the Sequencer tool to analyze the randomness and quality of tokens, such as session cookies.
2. Start Analysis: Start the analysis and review the results to identify weak tokens.

5. Reporting and Remediation

Generating Reports

1. Report Generation: Burp Suite allows you to generate detailed reports summarizing your findings.
2. Report Types: Choose from various report templates, including HTML, PDF, and XML.
3. Share Reports: Share reports with stakeholders, including developers and security teams.

Collaborating with Developers

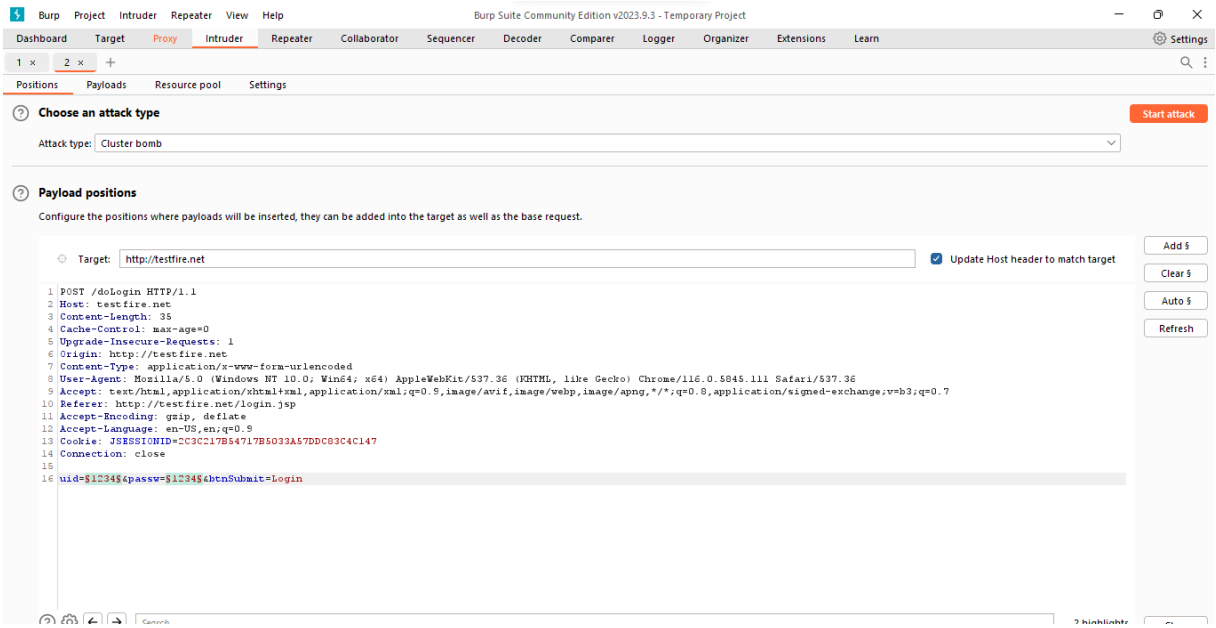
1. Issue Tracking: Use the findings in Burp Suite to create issues or tickets in your organization's issue tracking system.

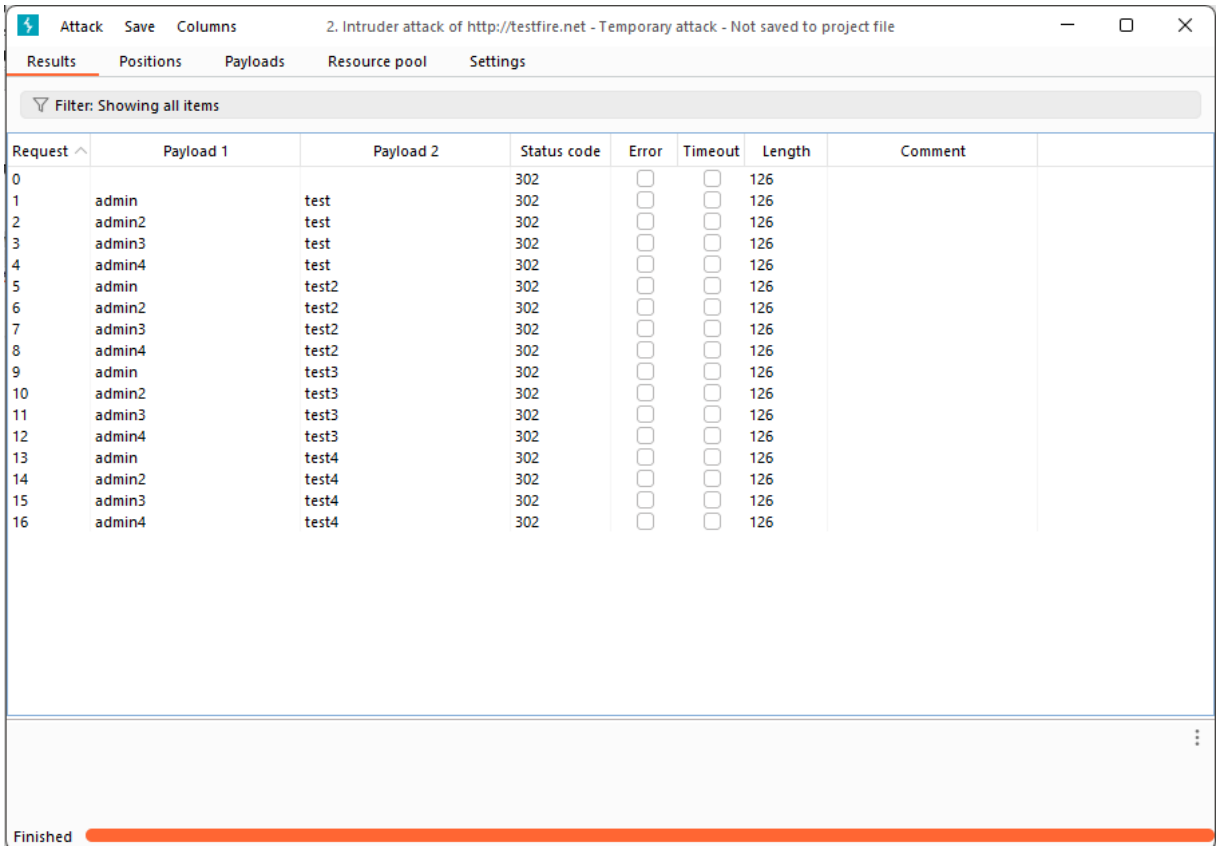
2. Developer Collaboration: Work closely with developers to understand and address identified vulnerabilities.

Tips and Best Practices

1. Regular Backups: Periodically back up your Burp Suite project files to prevent data loss.
2. Stay Updated: Keep Burp Suite up to date by installing updates and patches from PortSwigger.
3. Continuous Learning: Stay informed about the latest web application security threats and testing techniques.

Brute force Login using Proxy:




Attack
Save
Columns
2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Request
Payload 1
Payload 2
Status code
Error
Timeout
Length
Comment
0 302 126
1 admin test 302 126
2 admin2 test 302 126
3 admin3 test 302 126
4 admin4 test 302 126
5 admin test2 302 126
6 admin2 test2 302 126
7 admin3 test2 302 126
8 admin4 test2 302 126
9 admin test3 302 126
10 admin2 test3 302 126
11 admin3 test3 302 126
12 admin4 test3 302 126
13 admin test4 302 126
14 admin2 test4 302 126
15 admin3 test4 302 126
16 admin4 test4 302 126
Finished