Burpsuite 101: Introduction and Installation

by Md. Ashif Islam

What is Burpsuite?

Burpsuite is a powerful penetration testing tool used to test web applications. It is designed to help security professionals identify vulnerabilities in web applications and improve their overall security posture.

Why Use Burpsuite?

Web Application Security Testing

Burpsuite is a powerful penetration testing tool that allows you to test the security of web applications. It can be used to identify vulnerabilities and weaknesses in web applications, and to help secure them against attack.

Comprehensive Testing Capabilities

Burpsuite provides a wide range of testing capabilities, including passive and active scanning, intercepting traffic, analyzing requests and responses, and working with sessions. It also offers a variety of proxy options, repeater and intruder tools, and extender options for customizing and extending functionality.

Efficient and Effective Testing

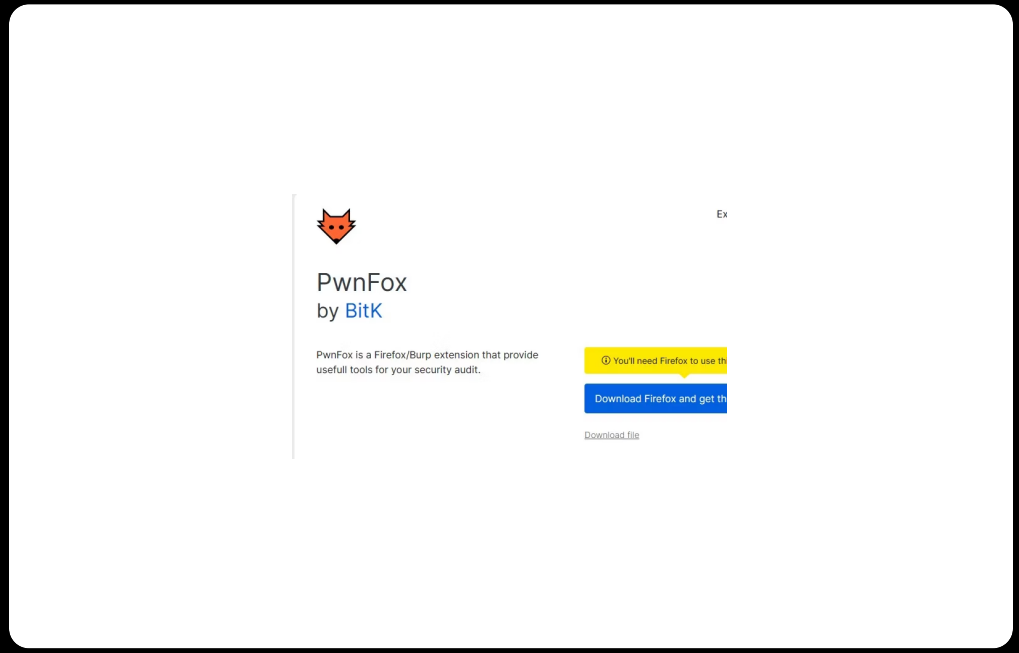
Using Burpsuite can help you conduct efficient and effective security testing of web applications. It allows you to quickly identify vulnerabilities, prioritize them based on severity, and take action to remediate them. This can help you improve the security of your web applications and protect against potential attacks.

Installation and Setup

Before you can use Burpsuite for web application penetration testing, you need to download and install Java JDK 1.8 for OLD and At last 15 for new version and install Burpsuite. Burpsuite is available for Windows, Mac, and Linux operating systems. You can download the latest version from the PortSwigger website.

Setting up Burpsuite

Once you have downloaded and Install Burpsuite, you will need to set it up Browser extension FoxyProxy or PWN Fox to work with your web browser. This involves configuring your browser to use Burpsuite as a proxy server. The exact steps for doing this will depend on your browser, but there are many tutorials available online that can help you. Once you have set up Burpsuite as a proxy, you should be able to start using it for web application penetration testing.



Intercepting Traffic

What is Intercepting Traffic?

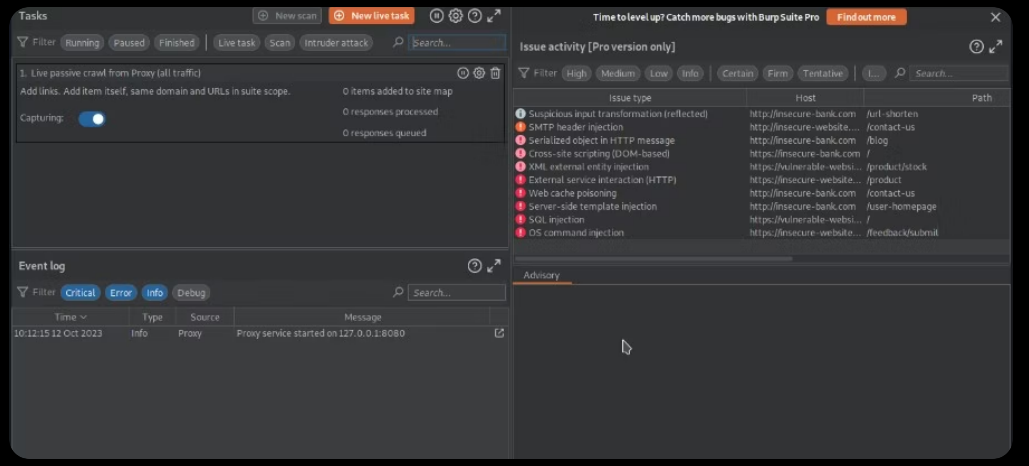
Intercepting Traffic is the process of capturing and analyzing network traffic between a client and server. Burpsuite allows you to intercept and modify this traffic in real-time, making it an essential tool for web application penetration testing.

How to Intercept Traffic with Burpsuite

To intercept traffic with Burpsuite, you must first configure your browser to use Burpsuite as a proxy. Once this is done, Burpsuite will capture all traffic between your browser and the server. You can then use Burpsuite to analyze and modify this traffic as needed.

Analyzing Requests and Responses

Burpsuite allows you to analyze requests and responses in detail, which is useful for understanding how web applications work and identifying vulnerabilities.



Intercepting Traffic

Burpsuite's proxy allows you to intercept traffic between your browser and the web application, so you can capture and analyze requests and responses.

Working with Sessions

Burpsuite allows you to manage sessions, so you can easily switch between different user accounts or testing scenarios.

Target Scope

Burpsuite allows you to define the scope of your testing, so you can focus on specific parts of the web application and avoid testing areas that are out of scope.

Passive Scanning

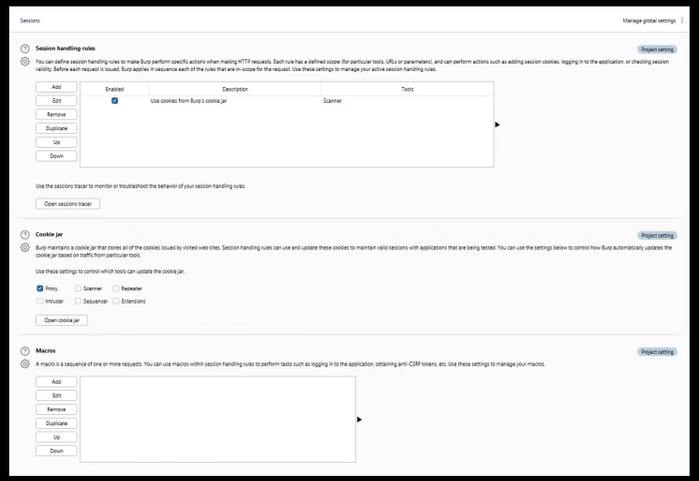
Burpsuite's passive scanner identifies potential vulnerabilities by analyzing responses and looking for known security issues.

Active Scanning

Burpsuite's active scanner sends requests to the web application and analyzes the responses, looking for vulnerabilities and potential attack vectors.

Reporting

Burpsuite allows you to generate detailed reports of your testing results, which can be useful for communicating findings to stakeholders or tracking progress over time.



Working with Sessions

Session Management

Burpsuite's session management feature allows users to save and manage sessions for later use. This is especially useful for testing web applications that require authentication or session-based interactions.

Session Options

Burpsuite offers several options for session management, including the ability to save and load sessions, view session details, and configure session handling rules.

Tips for Working with Sessions

Save sessions frequently to avoid losing progress in testing.Use session handling rules to automatically manage sessions based on specific criteria.Consider creating separate sessions for different user roles or testing scenarios.

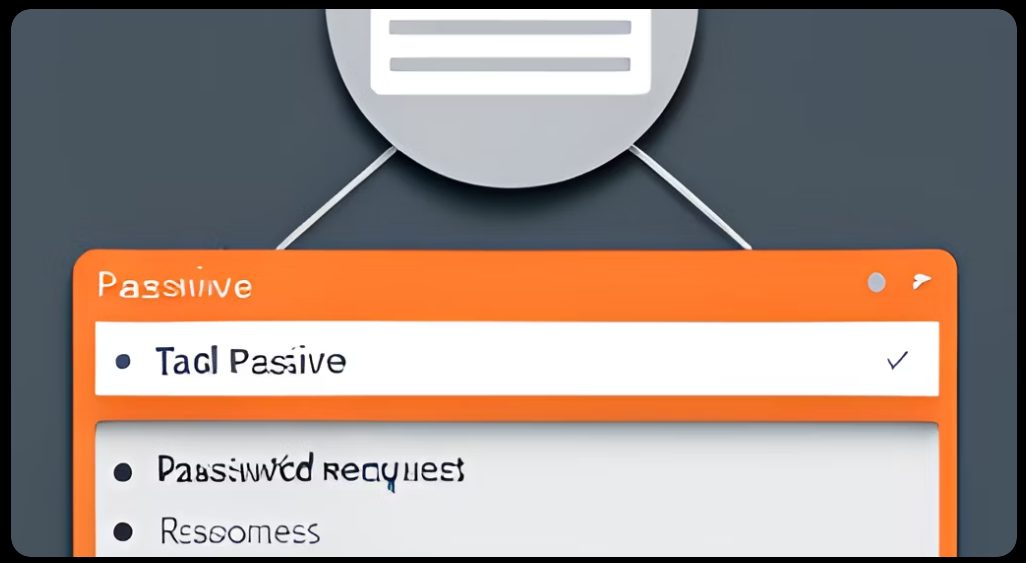
Target Scope

Before starting a web application test, it's important to define the scope of the test. The target scope defines the specific web application or website that will be tested.

- Defining the target scope helps to ensure that the testing is focused and efficient.
- It also helps to prevent unintended consequences, such as accidentally testing a production website instead of a development website.

Passive Scanning

Burpsuite's passive scanning feature allows you to monitor web traffic without actively sending requests. This is useful for identifying potential vulnerabilities in web applications without triggering any alarms or alerts.



How it Works

Burpsuite's passive scanning feature works by intercepting web traffic and analyzing the requests and responses. It looks for common vulnerabilities such as cross-site scripting (XSS), SQL injection, and sensitive data exposure.

Benefits

Passive scanning allows you to identify potential vulnerabilities in web applications without actively sending requests, which can trigger alarms or alerts. It also provides a non-intrusive way to monitor web traffic and identify security issues.

Limitations

Passive scanning has some limitations, such as the inability to identify vulnerabilities that require user interaction or dynamic content. It also may not detect all vulnerabilities, so it is important to use other testing methods in conjunction with passive scanning.

Active Scanning

Active scanning is a technique used to identify vulnerabilities and security issues in web applications by sending malicious requests and analyzing their responses. Burpsuite provides a powerful and customizable active scanning feature that can help automate the process of identifying and exploiting vulnerabilities.

Configuring Active Scanning

Before starting an active scan, it's important to configure the scan settings to ensure that the scan is effective and efficient. Burpsuite provides a variety of options for configuring active scans, including:

1. Target scope: Define the scope of the scan by specifying which pages and parameters should be included or excluded from the scan.
2. Scan speed: Choose between different scan speeds to balance the thoroughness of the scan with the time required to complete it.
3. Scan tuning: Configure the scan to use specific payloads, attack types, and other parameters to optimize the scan for the target application.

Running an Active Scan

To run an active scan in Burpsuite, follow these steps:

1. Configure the scan settings as desired.
2. Navigate to the target site in your browser and use Burpsuite to intercept a request.
3. Right-click on the intercepted request and select "Active Scan" from the context menu.
4. Wait for the scan to complete and review the results.

Active scanning can be a powerful tool for identifying vulnerabilities and security issues in web applications, but it's important to use it responsibly and ethically. Always obtain permission before scanning a target site, and be sure to follow best practices for responsible disclosure of any vulnerabilities that you discover.

Reporting

Burpsuite offers a variety of reporting options to help you document your findings and share them with others. These reports can be customized to include the information that is most relevant to your project.

Report Types

Burpsuite offers several types of reports, including:

- Site map
- Issues
- Scan
- Comparison

Customizing Reports

Burpsuite allows you to customize your reports to include only the information that is most relevant to your project. You can choose which issues to include, which columns to display, and which sections to show.

Proxy Options

Burpsuite is a powerful tool for testing web applications. One of its key features is the ability to act as a proxy server, allowing you to intercept and modify traffic between your browser and the target application.

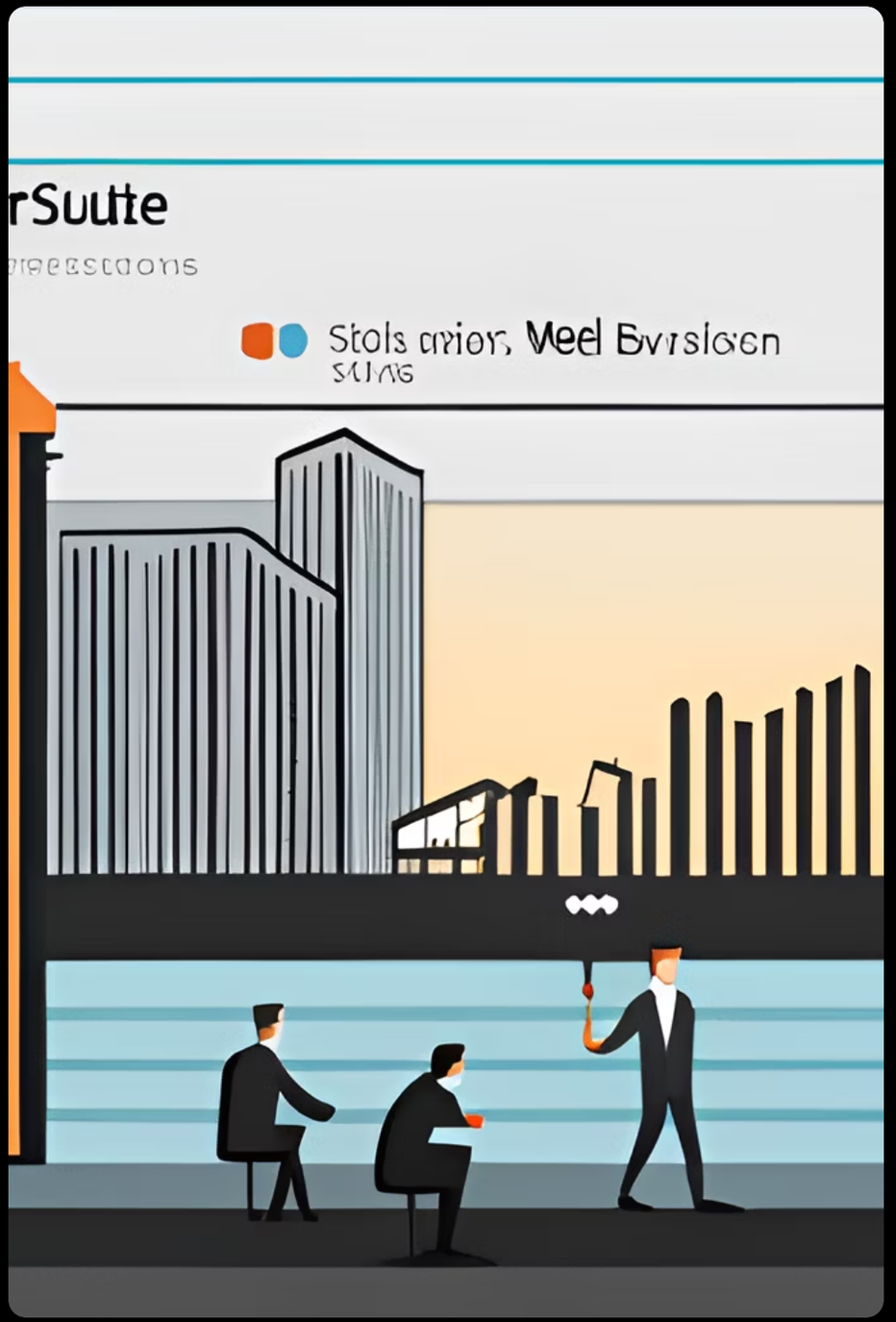
Setting up the Proxy

To use Burpsuite as a proxy, you need to configure your browser to use it. In most cases, this involves setting the HTTP proxy settings in your browser to point to the IP address and port number where Burpsuite is running.

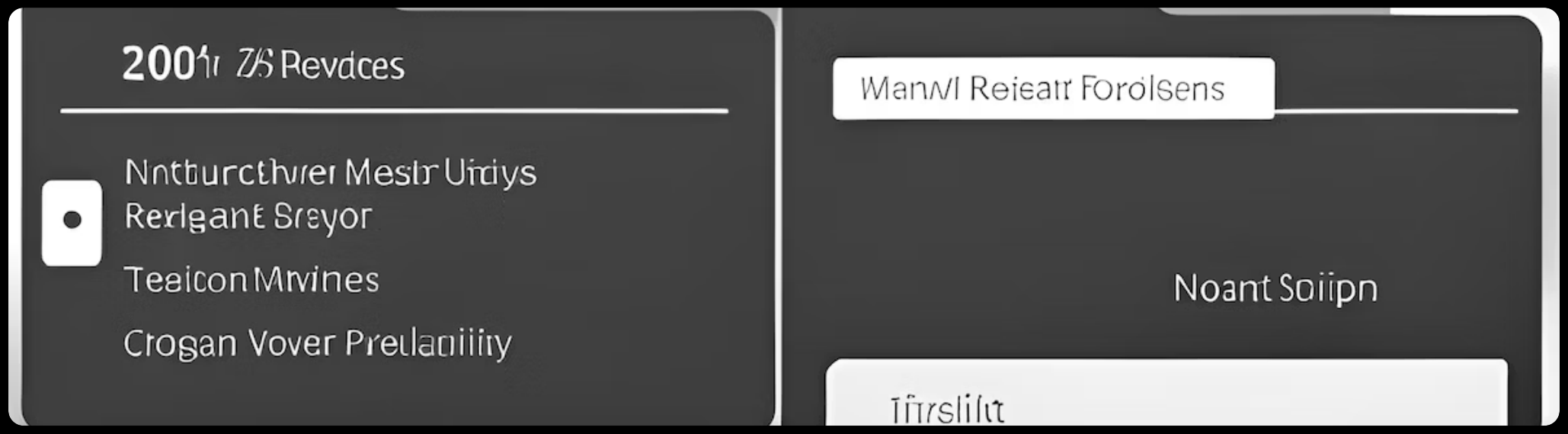
- In Burpsuite, go to the Proxy tab and select the Options sub-tab.
- Under the Proxy Listeners section, select the interface and port you want to use for the proxy.
- In your browser, go to the network settings and configure the HTTP proxy to point to the IP address and port number where Burpsuite is running.

Intercepting Traffic

Once the proxy is set up, you can intercept traffic between your browser and the target application. This allows you to view and modify requests and responses, and can be a powerful tool for identifying security vulnerabilities.



Repeater and Intruder



Repeater

Repeater is a tool used to manually repeat requests to a web application in order to test and modify parameters and observe the resulting responses. It allows for fine-tuning of requests and can be used to test for vulnerabilities such as SQL injection or cross-site scripting (XSS).

Intruder

Intruder is a tool used to automate the testing of multiple inputs and values in a web application. It can be used to test for vulnerabilities such as brute-force attacks, parameter fuzzing, and authentication bypass. Intruder allows for customization of payloads and attack types, as well as the ability to analyze and compare results.

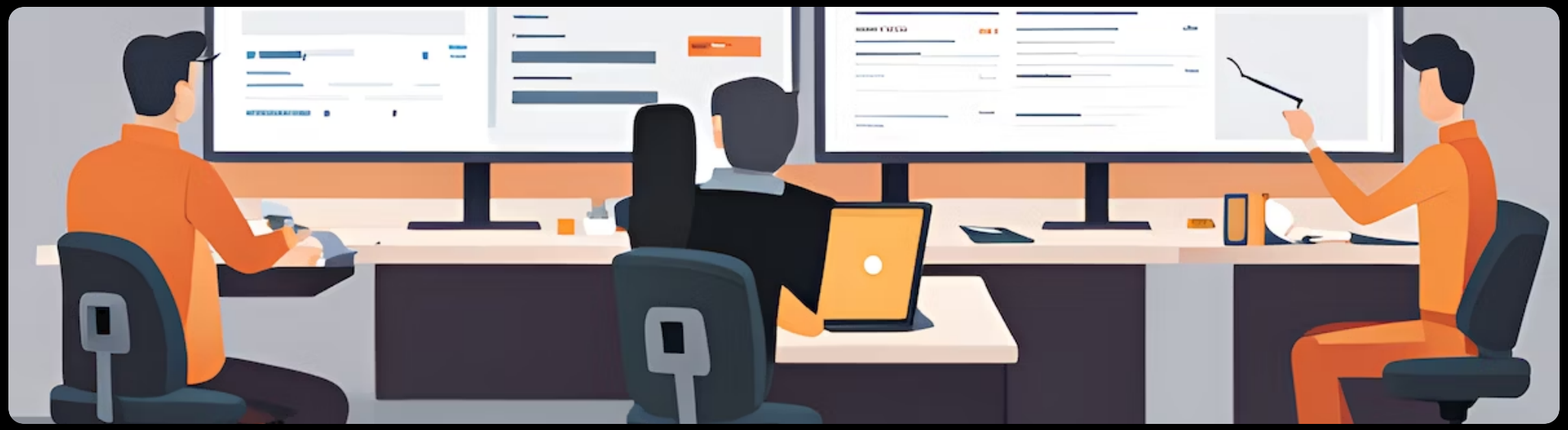
Repeater Options

Request Method: Allows for selection of HTTP method (GET, POST, etc.)URL: Displays the target URL and allows for modificationRequest Headers: Displays and allows for modification of headers sent with the requestRequest Parameters: Displays and allows for modification of parameters sent with the requestResponse: Displays the response received from the web applicationResponse Headers: Displays the headers received with the responseResponse Cookies: Displays any cookies received with the responseResponse Body: Displays the body of the responseFollow Redirects: Allows for enabling or disabling automatic following of redirectsEncode/Decode: Allows for encoding or decoding of selected parameters

Intruder Options

Target: Allows for selection of a specific request to use as the basis for the attackPositions: Allows for customization of the positions and values to be tested in the attackPayloads: Allows for customization of the payloads to be used in the attackAttack Type: Allows for selection of the type of attack to be performed (e.g. sniper, cluster bomb, pitchfork)Options: Allows for customization of various options such as threading and delaysResults: Displays the results of the attack, including successful and failed attempts

Extender



What is Extender?

Burpsuite's Extender tab allows users to extend the functionality of the tool through the use of plugins and extensions.

Using Extender

To use Extender, users can browse and download available extensions from the BApp Store, or create and upload their own custom plugins. Once installed, extensions can be accessed and configured through the Extender tab.

Common Extensions

Autorize - Automated Authorization TestingActiveScan++ - Advanced Active ScanningBackslash Powered Scanner - Automated Scanning and Vulnerability DetectionSAML Raider - SAML Testing and ExploitationSQLMap - SQL Injection Detection and ExploitationWsdler - Web Services Testing and Analysis

Intruder Payloads

Intruder payloads are the inputs that are used to test a web application's vulnerability. Burpsuite provides various types of payloads that can be used to test different aspects of the application.

Payload Types

- Simple list - a list of values to be used as payloads
- Cluster bomb - combines multiple payloads to create new ones
- Pitchfork - uses two separate lists of payloads to test different parts of the application
- Battering ram - sends the same payload multiple times with different variations
- Content discovery - uses a list of common file and directory names to discover hidden content
- Payload processing - modifies payloads to test specific vulnerabilities

Intruder Attack Types

Cluster Bomb

This attack type sends multiple payloads at the same time, which can be useful for brute forcing or testing different inputs at once.

Battering Ram

This attack type sends a single payload multiple times, which can be useful for testing the stability and resilience of a target.

Pitchfork

This attack type sends multiple payloads in a sequence, which can be useful for testing different combinations of inputs.

Intruder Options

Burpsuite's Intruder tool allows for a wide range of customization and configuration. Here are some of the key options available:

Payloads

The Payloads option allows for the customization of payloads used in the attack. This can include wordlists, character sets, and custom data.

Positions

The Positions option allows for the customization of where payloads are placed within the request. This can include specific locations or using a sequential order.

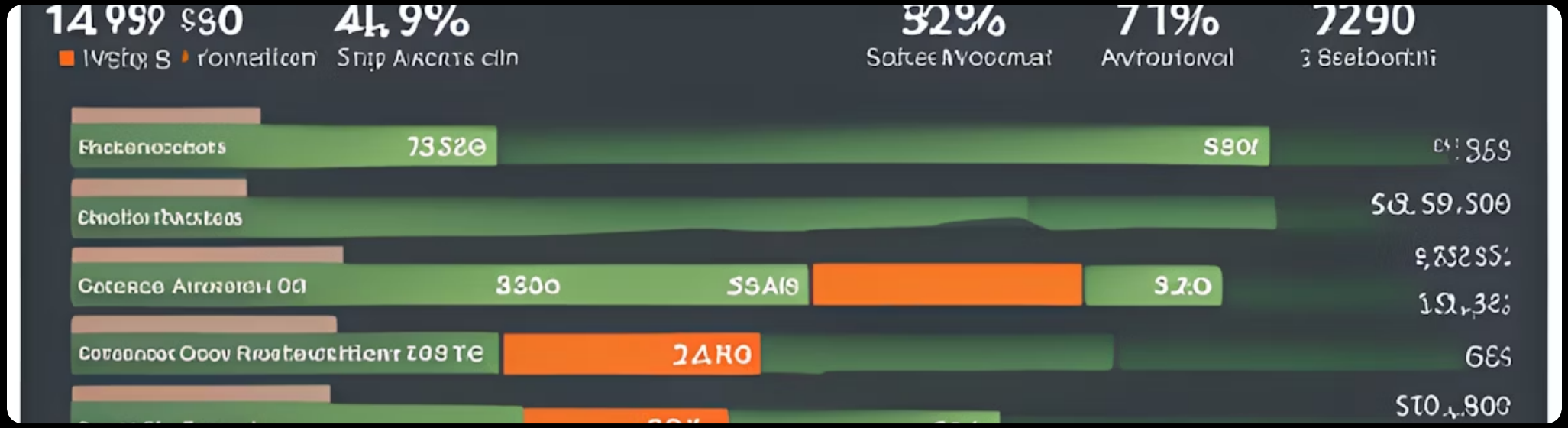
Attack Type

The Attack Type option allows for the customization of the type of attack used. This can include a Sniper attack, Battering Ram attack, and Pitchfork attack among others.

Grep - Match

The Grep - Match option allows for the customization of what to match in the response. This can include specific strings or regular expressions.

Intruder Results



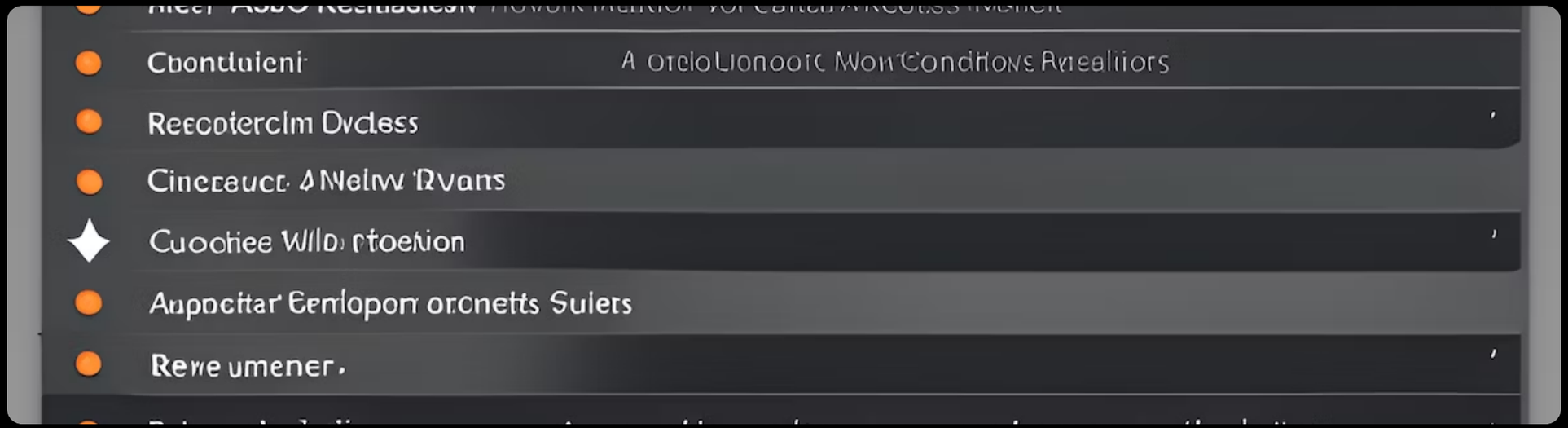
Data Analysis

Burpsuite's Intruder Results interface provides a comprehensive data analysis of the attack results. This includes a data table with sortable columns, as well as options for filtering, grouping, and exporting the data.

Vulnerability Identification

The Intruder Results interface also provides detailed information on the vulnerabilities identified during the attack. This includes the vulnerability type, severity level, and recommended remediation steps.

Repeater Options



Request Options

- Match and Replace: Replace specific text in the request with other text.
- Send to Intruder: Send the request to Intruder for further testing.
- Copy to Clipboard: Copy the request to the clipboard for use in other tools.
- Save Item: Save the request as a new item in the site map.

Response Options

- Match and Replace: Replace specific text in the response with other text.
- Send to Comparer: Send the response to Comparer for comparison with other responses.
- Copy to Clipboard: Copy the response to the clipboard for use in other tools.
- Save Item: Save the response as a new item in the site map.

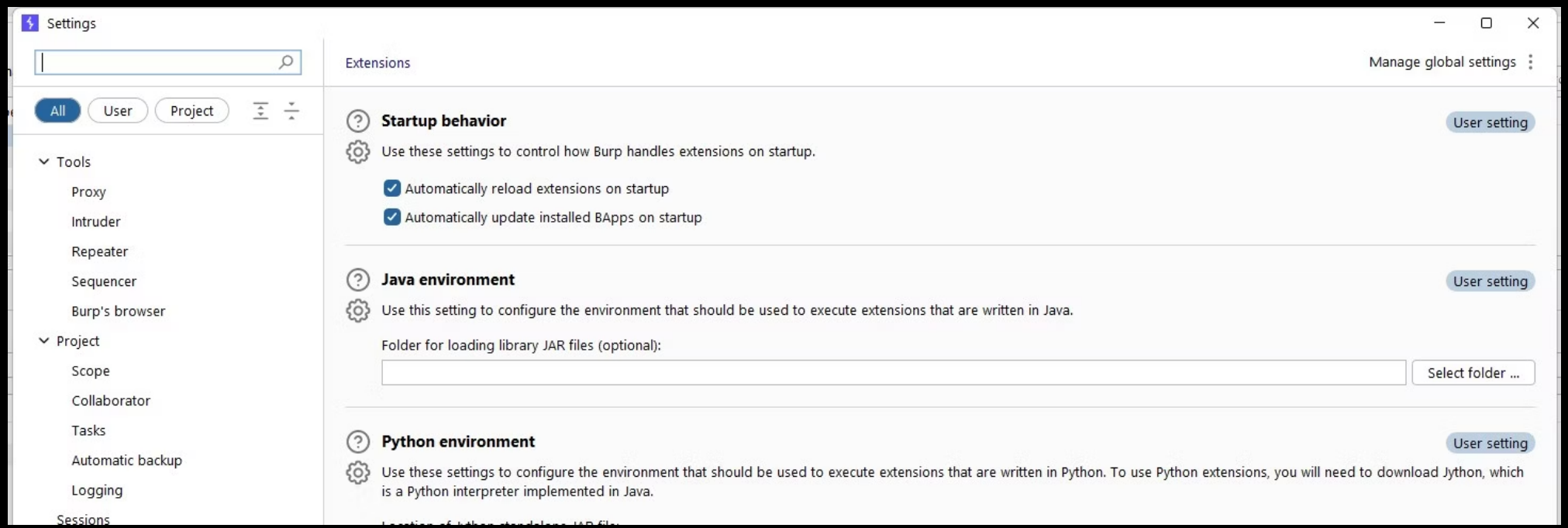
Repeater Results

Response Tab

The Response tab displays the server's response to the request. It includes the status code, headers, and body of the response.

Request Tab

The Request tab displays the details of the request that was sent. It includes the HTTP method, URL, headers, and body of the request.



Extender Options

Overview

The Extender is a powerful feature of Burpsuite that allows users to extend the functionality of the tool. This section covers some of the available options and how they can be used.

BApp Store

The BApp Store is a marketplace for Burpsuite extensions, or BApps. Users can browse and download BApps to add new functionality to Burpsuite.

API

Burpsuite's API allows users to interact with the tool programmatically. This can be useful for automating tasks or integrating Burpsuite into a larger workflow.

Extender Results

Extension Output

The Extension Output tab displays the results of any extensions that have been run. This can include custom scripts or plugins that have been developed to extend Burpsuite's functionality.

Alerts

The Alerts tab displays any security issues or vulnerabilities that Burpsuite has identified during scanning. These issues should be addressed as soon as possible to ensure the security of the application.

Using Burpsuite with Other Tools

Web Vulnerability Scanners

Burpsuite can be used in conjunction with other web vulnerability scanners to provide more comprehensive testing coverage. Some popular scanners that work well with Burpsuite include:

- Acunetix
- Nessus
- OpenVAS

Debuggers

Burpsuite can also be used as a debugger to troubleshoot issues with web applications. By intercepting and analyzing traffic, developers can identify and fix problems more quickly. Some popular debuggers that work well with Burpsuite include:

- Visual Studio Debugger
- Eclipse Debugger
- Xdebug

Integrated Development Environments (IDEs)

Burpsuite can be integrated with IDEs to provide developers with a more streamlined workflow. By using Burpsuite in conjunction with an IDE, developers can easily switch between coding and testing without having to switch between different tools. Some popular IDEs that work well with Burpsuite include:

- Eclipse
- Visual Studio
- IntelliJ IDEA

Common Use Cases

Identifying Vulnerabilities

One of the primary use cases for Burpsuite is to identify vulnerabilities in web applications. By intercepting traffic and analyzing requests and responses, security professionals can identify potential weaknesses in an application's security.

Testing Authentication Mechanisms

Burpsuite can also be used to test authentication mechanisms in web applications. By manipulating requests and responses, security professionals can test the strength of login pages, password reset mechanisms, and other authentication features.

Auditing Access Controls

Burpsuite can also be used to audit access controls in web applications. By manipulating requests and responses, security professionals can test the effectiveness of access controls and identify potential weaknesses in the application's authorization process.

Best Practices

Stay Up-to-Date

Make sure to keep Burpsuite updated with the latest version to ensure maximum security and efficiency.

Set Up a Proxy

Using a proxy can help you better understand the traffic between your web application and server, and can aid in identifying vulnerabilities.

Use Authentication

If your web application requires authentication, make sure to set up Burpsuite to handle it properly in order to accurately test the application's security.

Resources and Further Reading

To learn more about Burpsuite and penetration testing, check out the following resources:

Burpsuite Documentation: The official documentation provides in-depth information on all aspects of the tool.Web Application Hacker's Handbook: This book is a comprehensive guide to web application security and includes a section on using Burpsuite.OWASP: The Open Web Application Security Project is a community-driven organization that provides resources and best practices for web application security.