Introduction

Welcome to Burp Suite Basics!

This particular room aims to understand the basics of the Burp Suite web application security testing framework. Our focus will revolve around the following key aspects:

1. A thorough introduction to Burp Suite.
2. A comprehensive overview of the various tools available within the framework.
3. Detailed guidance on the process of installing Burp Suite on your system.
4. Navigating and configuring Burp Suite.

We will also introduce the core of the Burp Suite framework, which is the Burp Proxy. It is important to note that this room primarily serves as a foundational resource for acquiring knowledge about Burp Suite. Subsequent rooms in the Burp module will adopt a more practical approach. Thus, this room will contain a greater emphasis on theoretical content. If you have not yet utilised Burp Suite, it is recommended to carefully read the provided information and actively engage with the tool. Experimentation is essential for grasping the fundamentals of this framework. Combining the information presented here with hands-on exploration will establish a strong foundation for utilising the framework. This will significantly assist you in future rooms.

Answer the questions below

Let us start!

Principio del formulario

What is Burp Suite

In essence, Burp Suite is a Java-based framework designed to serve as a comprehensive solution for conducting web application penetration testing. It has become the industry standard tool for hands-on security assessments of web and mobile applications, including those that rely on **a**pplication **p**rogramming **i**nterface**s** (APIs).

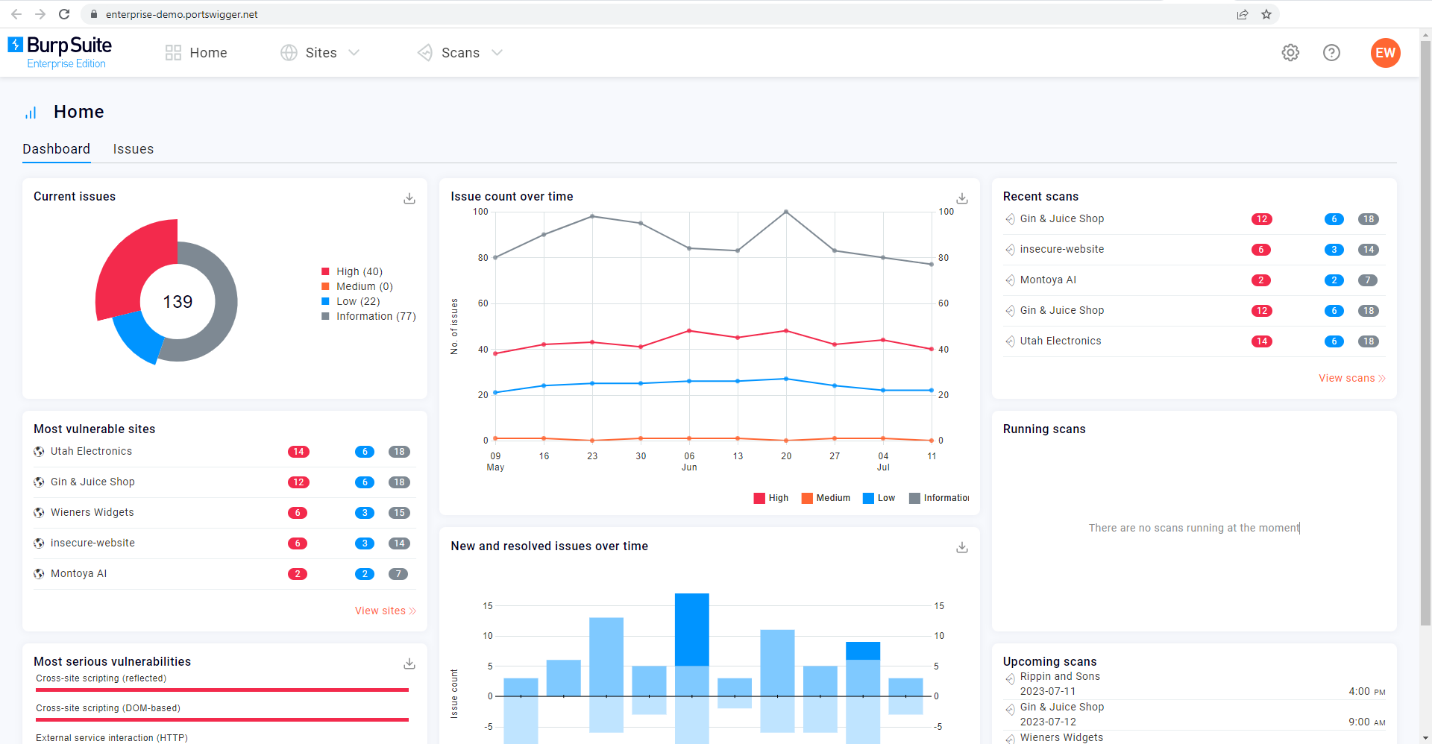
Simply put, Burp Suite captures and enables manipulation of all the HTTP/HTTPS traffic between a browser and a web server. This fundamental capability forms the backbone of the framework. By intercepting requests, users have the flexibility to route them to various components within the Burp Suite framework, which we will explore in upcoming sections. The ability to intercept, view, and modify web requests before they reach the target server or even manipulate responses before they are received by our browser makes Burp Suite an invaluable tool for manual web application testing.

Burp Suite is available in different editions. For our purposes, we will focus on the **Burp Suite Community Edition**, which is freely accessible for non-commercial use within legal boundaries. However, it's worth noting that Burp Suite also offers Professional and Enterprise editions, which come with advanced features and require licensing:

1. **Burp Suite Professional** is an unrestricted version of Burp Suite Community. It comes with features such as:
   * An automated vulnerability scanner.
   * A fuzzer/brute-forcer that isn't rate limited.
   * Saving projects for future use and report generation.
   * A built-in API to allow integration with other tools.
   * Unrestricted access to add new extensions for greater functionality.
   * Access to the Burp Suite Collaborator (effectively providing a unique request catcher self-hosted or running on a Portswigger-owned server).

In short, Burp Suite Professional is a highly potent tool, making it a preferred choice for professionals in the field.

1. **Burp Suite Enterprise**, in contrast to the community and professional editions, is primarily utilized for continuous scanning. It features an automated scanner that periodically scans web applications for vulnerabilities, similar to how tools like Nessus perform automated infrastructure scanning. Unlike the other editions, which allow manual attacks from a local machine, Burp Suite Enterprise resides on a server and constantly scans the target web applications for potential vulnerabilities.



Due to requiring a license for the Professional and Enterprise editions, we will focus on the core feature set provided by the Burp Suite Community Edition.

**Note:** The provided demonstrations utilize Burp Suite for Windows. However, the functionality remains consistent with the version installed on the AttackBox.

Answer the questions below

Which edition of Burp Suite runs on a server and provides constant scanning for target web apps?

Principio del formulario

Submit

Final del formulario

Burp Suite is frequently used when attacking web applications and \_\_\_\_\_\_ applications.

Principio del formulario

Final del formulario

Features of Burp Community

Although Burp Suite Community offers a more limited feature set compared to the Professional edition, it still provides an impressive array of tools that are highly valuable for web application testing. Let's explore some of the key features:

* **Proxy**: The Burp Proxy is the most renowned aspect of Burp Suite. It enables interception and modification of requests and responses while interacting with web applications.
* **Repeater**: Another well-known feature. [Repeater](https://tryhackme.com/room/burpsuiterepeater) allows for capturing, modifying, and resending the same request multiple times. This functionality is particularly useful when crafting payloads through trial and error (e.g., in SQLi - Structured Query Language Injection) or testing the functionality of an endpoint for vulnerabilities.
* **Intruder**: Despite rate limitations in Burp Suite Community, [Intruder](https://tryhackme.com/room/burpsuiteintruder) allows for spraying endpoints with requests. It is commonly utilized for brute-force attacks or fuzzing endpoints.
* **Decoder**: [Decoder](https://tryhackme.com/room/burpsuiteom) offers a valuable service for data transformation. It can decode captured information or encode payloads before sending them to the target. While alternative services exist for this purpose, leveraging Decoder within Burp Suite can be highly efficient.
* **Comparer**: As the name suggests, [Comparer](https://tryhackme.com/room/burpsuiteom) enables the comparison of two pieces of data at either the word or byte level. While not exclusive to Burp Suite, the ability to send potentially large data segments directly to a comparison tool with a single keyboard shortcut significantly accelerates the process.
* **Sequencer**: [Sequencer](https://tryhackme.com/room/burpsuiteom) is typically employed when assessing the randomness of tokens, such as session cookie values or other supposedly randomly generated data. If the algorithm used for generating these values lacks secure randomness, it can expose avenues for devastating attacks.

Beyond the built-in features, the Java codebase of Burp Suite facilitates the development of extensions to enhance the framework's functionality. These extensions can be written in Java, Python (using the Java Jython interpreter), or Ruby (using the Java JRuby interpreter). The **Burp Suite Extender** module allows for quick and easy loading of extensions into the framework, while the marketplace, known as the **BApp Store**, enables downloading of third-party modules. While certain extensions may require a professional license for integration, there are still a considerable number of extensions available for Burp Community. For instance, the **Logger++** module can extend the built-in logging functionality of Burp Suite.

Answer the questions below

Which Burp Suite feature allows us to intercept requests between ourselves and the target?

Principio del formulario

Submit

Final del formulario

Which Burp tool would we use to brute-force a login form?

Installation

Burp Suite is one of those tools that is very useful to have around, whether for web or mobile application assessments, pentesting, bug bounty hunting, or even debugging features in web app development. Here's a guide on installing Burp Suite on different platforms:

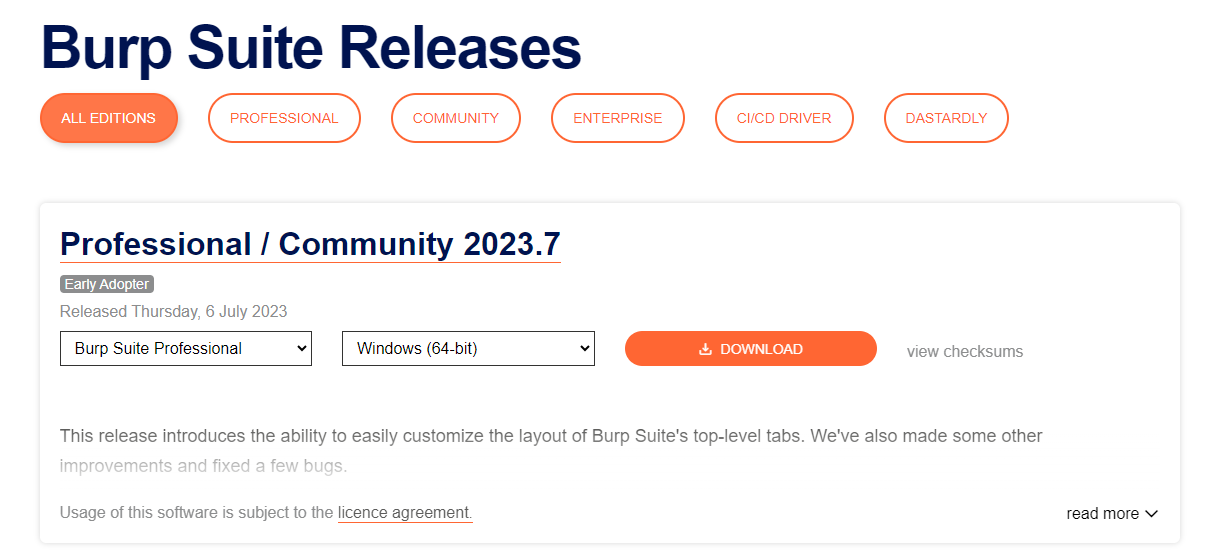
**Note:** If you use the AttackBox, Burp Suite is already installed, so you can skip this step.

Downloads

To download the latest version of Burp Suite for other systems, you may click this [button](https://portswigger.net/burp/releases/) to go to their download page.

**Kali Linux:** Burp Suite comes pre-installed with Kali Linux. In case it is missing on your Kali installation, you can easily install it from the Kali apt repositories.

**Linux, macOS, and Windows:** For other operating systems, PortSwigger provides dedicated installers for Burp Suite Community and Burp Suite Professional on the Burp Suite downloads page. Choose your operating system from the dropdown menu and select **Burp Suite Community Edition**. Then, click the **Download** button to initiate the download.



Installation

Install Burp Suite using the appropriate method for your operating system. On Windows, run the executable file, while on Linux, execute the script from the terminal (with or without sudo). If you choose not to use sudo during installation on Linux, Burp Suite will be installed in your home directory at ~/BurpSuiteCommunity/BurpSuiteCommunity and will not be added to your PATH.

The installation wizard provides clear instructions, and it is generally safe to accept the default settings. However, it is always recommended to review the installer carefully.

With Burp Suite successfully installed, you can now launch the application. In the next task, we will explore the initial setup and configuration.

Answer the questions below

If you have chosen not to use the AttackBox, ensure that you have a copy of Burp Suite installed before proceeding.