A Practical Guide: Your First Steps with Burp Suite

This guide will walk you through the essential first steps of using Burp Suite. By the end, you will have installed the software, configured it to intercept web traffic, and performed a basic vulnerability hunting workflow.

Step 1: Installation and Initial Setup

First, let's get Burp Suite running on your system. We'll use the free Community Edition, which is perfect for learning.

1. **Download:** Navigate to the official PortSwigger website and download the Burp Suite Community Edition for your operating system (Windows, macOS, or Linux).
2. **Install:** Run the installer you just downloaded. The default settings are suitable for most users, so you can proceed through the installation wizard.
3. **Launch and Create a Project:** Open Burp Suite. You will be prompted to select a project type.
    - Select **"Temporary project"**. This is fine for learning, as all data will be discarded when you close Burp.
    - On the next screen, choose **"Use Burp defaults"**.
    - The main Burp Suite window will now open.

Step 2: Proxy Configuration - Intercepting Traffic

The core of Burp Suite is its proxy, which sits between your browser and the internet to capture all web traffic. The easiest way to get this working is with Burp's built-in browser.

1. **Navigate to the Proxy Tab:** In Burp Suite, click on the **Proxy** tab.
2. **Open Burp's Browser:** Click the **"Open Browser"** button. A new Chromium browser window will launch.
3. **Confirm It's Working:** Any website you visit in *this specific browser window* will now have its traffic routed through Burp Suite. This method is highly recommended as it avoids the need to manually change your system's proxy settings.

Note: All subsequent steps assume you are using Burp's Browser.

Step 3: Handling HTTPS with the CA Certificate

If you try to visit a secure website (https://...), the browser will show a security warning. This is because Burp needs to decrypt the traffic, and the browser correctly sees this as a "man-in-the-middle" situation. To fix this, you must tell the browser to trust Burp's unique Certificate Authority (CA).

1. **Navigate to the Burp URL:** In the Burp Browser you opened in Step 2, go to the address http://burpsuite.
2. **Download the Certificate:** On the welcome page, click the **"CA Certificate"** link in the

top-right corner. This will download a file, likely named cacert.der.

3. **Import the Certificate into the Browser:**
    - In the Burp Browser, go to chrome://settings/security.
    - Scroll down and click on **"Manage certificates"**.
    - Go to the **"Authorities"** tab.
    - Click the **"Import..."** button.
    - Select the cacert.der file you just downloaded.
    - In the dialog box that appears, check the box for **"Trust this certificate for identifying websites"**.
    - Click **"OK"**.
4. **Test It:** You should now be able to browse any HTTPS website in the Burp Browser without security warnings.

Step 4: The Core Pentesting Workflow

Now let's put it all together and simulate a basic test. This workflow—moving from discovery to manual analysis to automated attacks—is fundamental to using Burp effectively.

1. **Define Your Target Scope:**
    - **Why?** To focus your testing and avoid cluttering your tools with traffic from other websites (like analytics or ad services).
    - **How:** In the Burp Browser, navigate to a practice website (PortSwigger's Web Security Academy is perfect for this).
    - Switch to the main Burp Suite window and click the **Target** tab.
    - In the **Site map** on the left, find the hostname of the practice website (e.g., https://portswigger.net).
    - Right-click on it and select **"Add to scope"**. Click "Yes" on the pop-up.
2. **Discover with Proxy History:**
    - **Why?** To passively observe the application's traffic and find interesting requests.
    - **How:** Click around the practice website for a minute.
    - In Burp Suite, go to the **Proxy > HTTP history** tab. You will see a log of every request your browser made. Find a request that looks interesting, perhaps one with an ID in the URL, like GET /product?id=3.
3. **Analyze and Probe with Repeater:**
    - **Why?** To manually modify a single request and see how the server responds. This is your "scalpel" for precise testing.
    - **How:** In the HTTP history, right-click the request (GET /product?id=3) and select **"Send to Repeater"**.
    - Go to the **Repeater** tab. On the left is your request; on the right will be the response.
    - Change the id=3 to id=4 and click the **"Send"** button.
    - Observe the response. Did you get a different product's page? This could indicate a potential IDOR vulnerability.
4. **Automate Attacks with Intruder:**
    - **Why?** To automate the sending of hundreds of modified requests, which is

impossible to do manually. This is your "power hammer."
    - **How:** Go back to the HTTP history or Repeater, right-click the same request, and select **"Send to Intruder"**.
    - Go to the **Intruder** tab.
    - Click on the **Positions** sub-tab. The request will be shown. Intruder may have automatically guessed where to put payloads. Click the **"Clear §"** button to remove them.
    - Now, highlight just the number 3 in the line GET /product?id=3. Click the **"Add §"** button. The request should now look like GET /product?id=§3§. This tells Intruder where to inject its payloads.
    - Click the **Payloads** sub-tab.
    - Under "Payload sets", change the "Payload type" to **"Numbers"**.
    - Set the range from 1 to 20, with a step of 1.
    - Click the **"Start attack"** button in the top-right. A new window will open.
    - **Analyze the Results:** Watch as Intruder sends 20 requests. Look at the "Status" and "Length" columns. If most requests have the same length but a few are different, it suggests those IDs returned different content, confirming a potential vulnerability.

Step 5: What's Next?

Congratulations! You have completed the core Burp Suite workflow. From here, your journey is about practice and exploration.

- **Practice, Practice, Practice:** The **PortSwigger Web Security Academy** is the best place to legally and safely practice these skills on deliberately vulnerable websites.
- **Explore the Toolkit:** Spend time with the other tools. Use **Decoder** to analyze encoded data and **Comparer** to visually diff two responses to spot subtle differences.
- **Read the Research:** Refer back to the full "Burp Suite Bible" artifact to understand the deeper concepts behind the tools and strategies.

By following these steps, you've built a solid foundation for using Burp Suite in your professional work at Breaking Circuits, LLC.