

HackerFrogs Afterschool

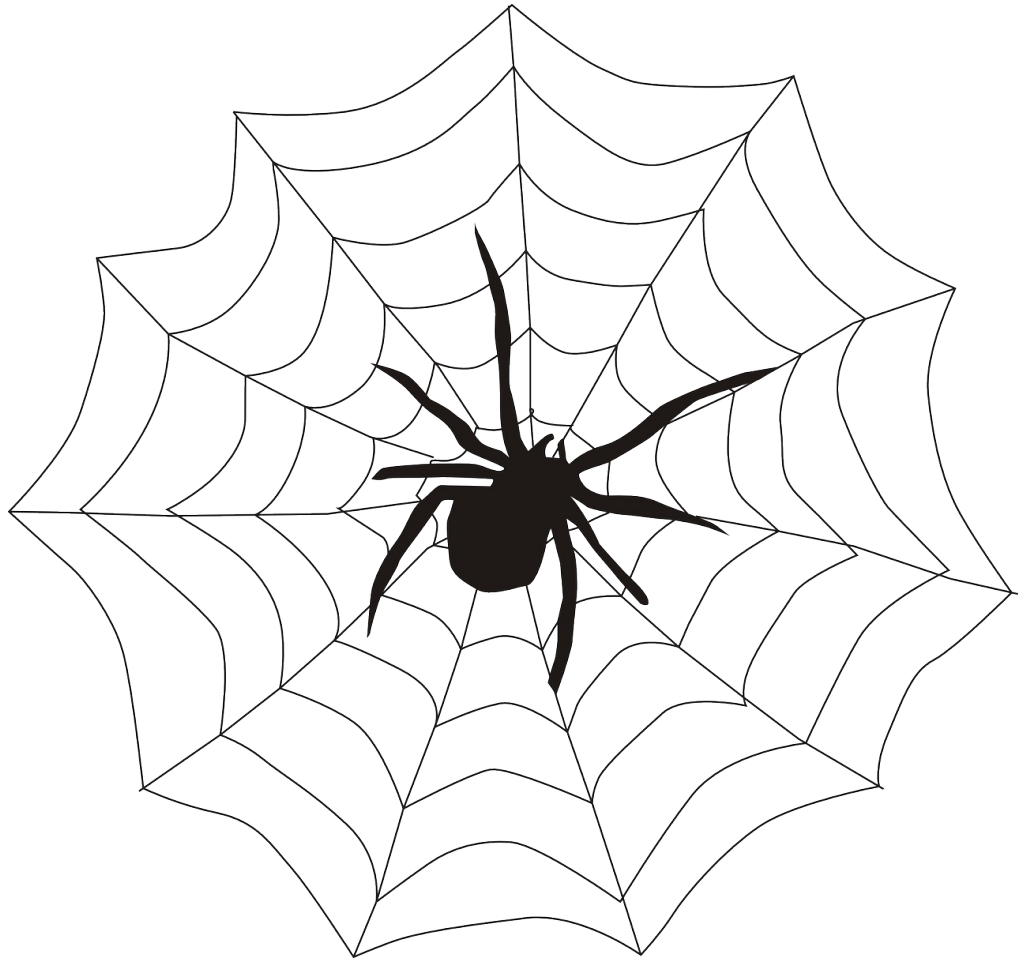
Web App 7: Burp Suite Pt. 1 of 2

Class:
Web App Hacking

Workshop Number:
AS-WEB-08

Document Version:
1.5

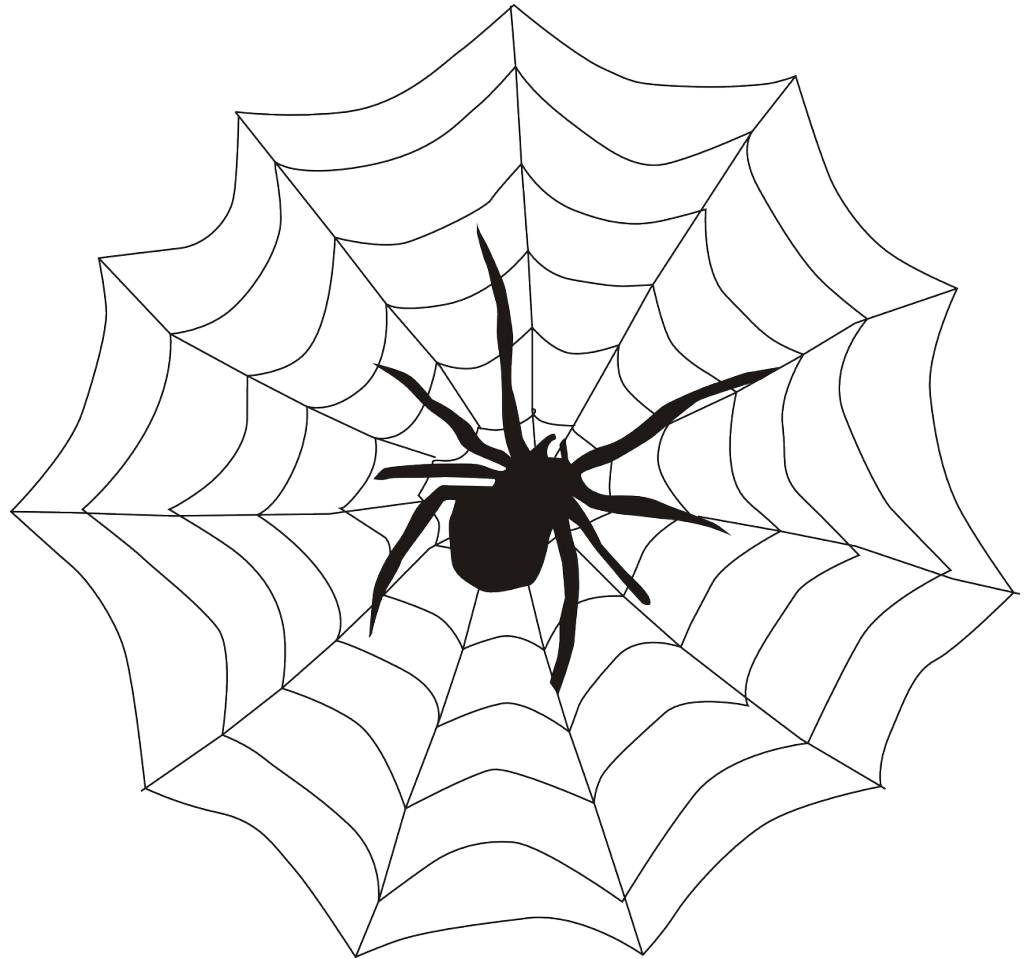
Special Requirements:
Registered account at
tryhackme.com



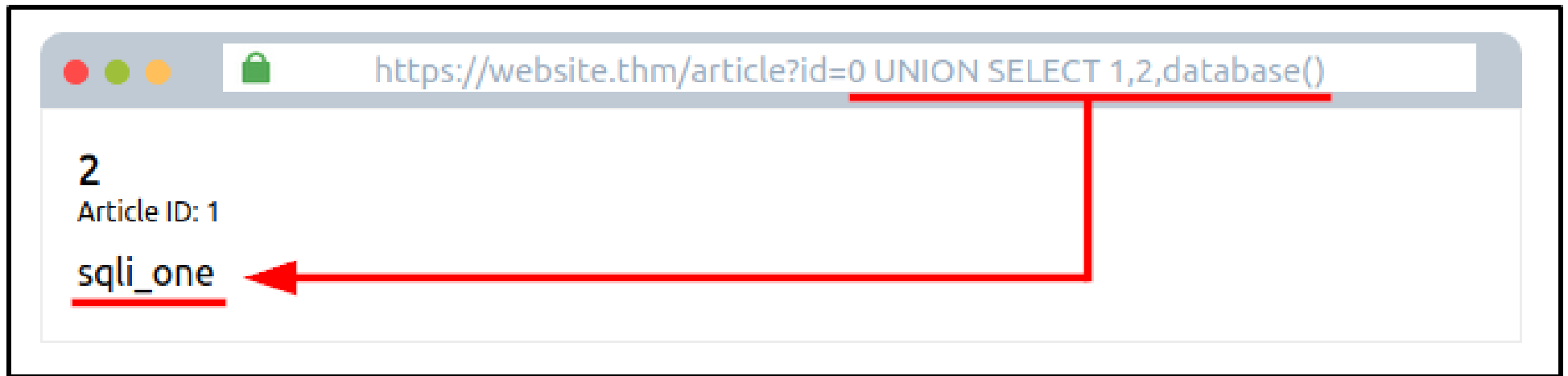
What We Learned In The Previous Workshop

This is the eight intro to web app hacking workshop.

In the previous workshop we learned about the following web app hacking concepts:



Union-Based SQL Injection



We practiced doing SQL UNION injection attacks on both the DVWA app on TryHackMe and PicoCTF.

Blind SQL Injection: Auth Bypass

And we also practiced performing SQL login bypass attacks with the PicoCTF web app challenges.



This Workshop's Topic

In this workshop, we'll be looking at Burp Suite, an industry-standard app used for web-app security testing.



Let's Learn More With TryHackMe

Navigate to the following URL:

<https://tryhackme.com/r/room/dvwa>

Introduction

Burp Suite is the web app testing tool of choice for cybersecurity professionals who test web apps. It can intercept the traffic from web apps and do all sorts of stuff with the data.



What is Burp Suite?

Burp Suite captures and enables the modification of web traffic between the browser and the server, and includes the following 5 tools for web app testing:



What is Burp Suite

1. Burp Proxy



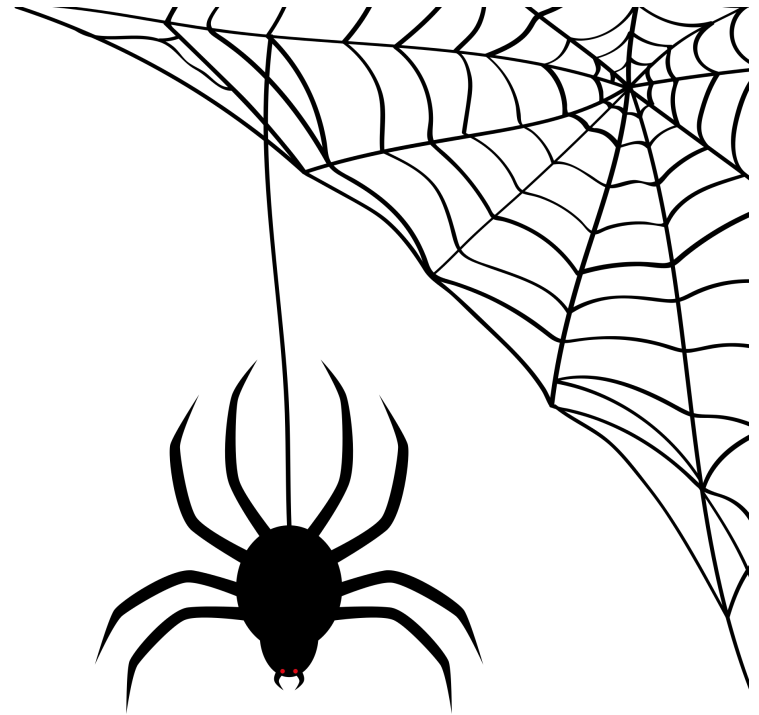
The Burp Proxy server is what enables web traffic to be captured and recorded. It sits between the browser and the server, enabling traffic capture.

What is Burp Suite

2. Burp Spider

The Burp Spider is an web app indexing robot which maps out different endpoints inside a target web app.

Similar tools in the same role include Dirb, Gobuster, and Ferretbuster



What is Burp Suite

3. Burp Intruder

Burp Intruder is a tool that can be used for different web brute forcing attacks, with modular payloads and word lists.

Similar tools include Hydra, Wfuzz, Ffuf, etc.



What is Burp Suite

4. Burp Scanner

Burp Scanner is an automated web app vulnerability scanner which tests all endpoints found in a web app for known vulnerabilities.

Similar tools include Nikto, OpenVAS, and ZAP



What is Burp Suite

5. Burp Repeater



Burp Repeater is a tool which allows for manual web request manipulation and testing.

What is Burp Suite

5. Burp Repeater



Similar tools include ZAP, Postman, and Charles Proxy.

Installation

While learning Burp Suite, it's recommended to access it via virtual machines (VM), such as the TryHackMe AttackBox VM or a Kali Linux VM.



Installation

Even so, manual installation download and installation of Burp Suite is available for all major operating systems from the Portswigger company website.



The Dashboard

The dashboard is divided into four main sections, each highlighted with a colored border and a numbered label:

- 1. Tasks (Red border):** Contains a 'New scan' button, a 'New live task' button, and a list of tasks. The first task is '1. Live passive crawl from Proxy (all traffic)'. It shows 'Capturing' is enabled (toggle switch) and '0 responses processed' and '0 responses queued'.
- 2. Event log (Yellow border):** Contains a 'Filter' dropdown, buttons for 'Critical', 'Error', 'Info', and 'Debug', and a 'Search...' field. The log shows a single entry: '01:51:02 8 Sep 2021 | Info | Proxy | Proxy service started on 12'.
- 3. Issue activity [Pro version only] (Blue border):** Contains a 'Filter' dropdown, buttons for 'High', 'Medium', 'Low', 'Info', 'Certain', 'Firm', and 'Tentative', and a 'Search...' field. It displays a table of issues:

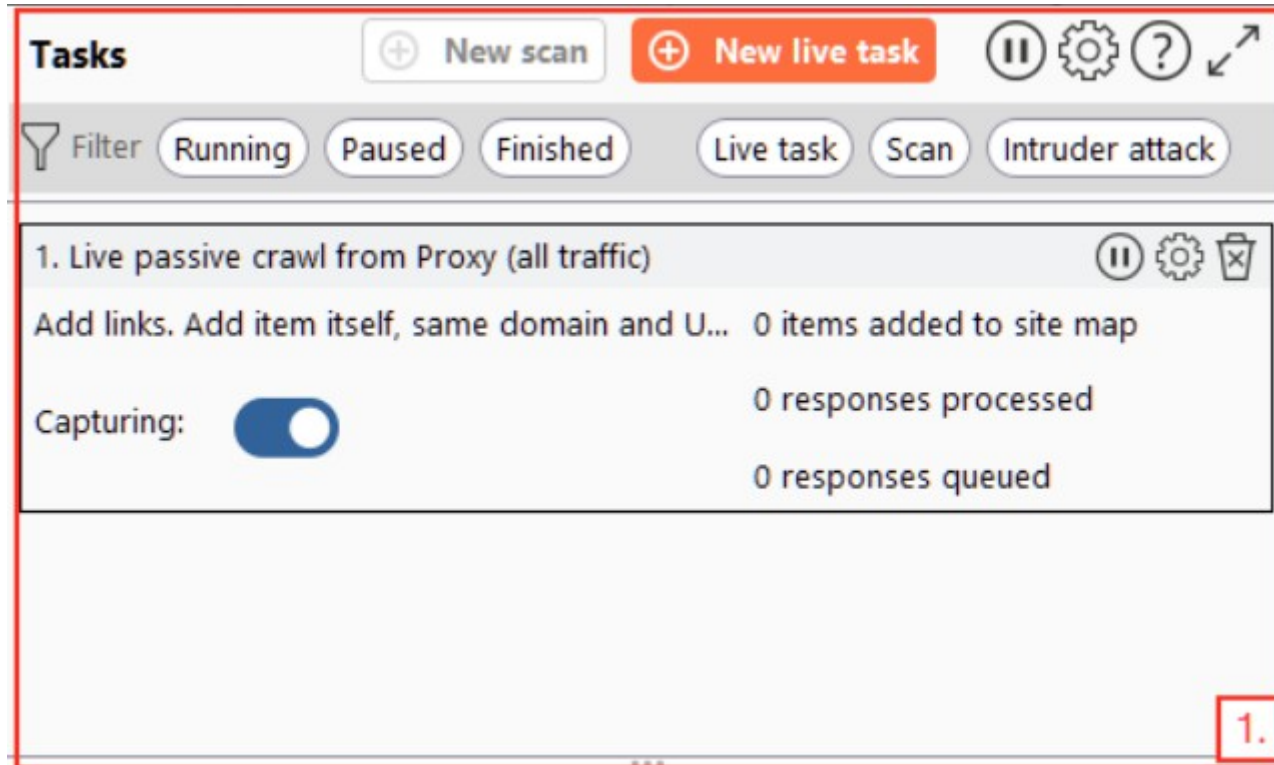
Issue type	Host
Suspicious input transformation (reflected)	http://insecure-bank.com /url-shorten
SMTP header injection	http://insecure-website.c... /contact-us
Serialized object in HTTP message	http://insecure-bank.com /blog
Cross-site scripting (DOM-based)	https://insecure-bank.com /
XML external entity injection	https://vulnerable-websit... /product/stock
External service interaction (HTTP)	https://insecure-website.... /product
Web cache poisoning	http://insecure-bank.com /contact-us

- 4. Advisory (Green border):** Contains an 'Advisory' section with a search bar and a list of advisories.

At the bottom of the dashboard, there is a status bar showing 'Memory: 94.7MB' and 'Disk: 32KB'.

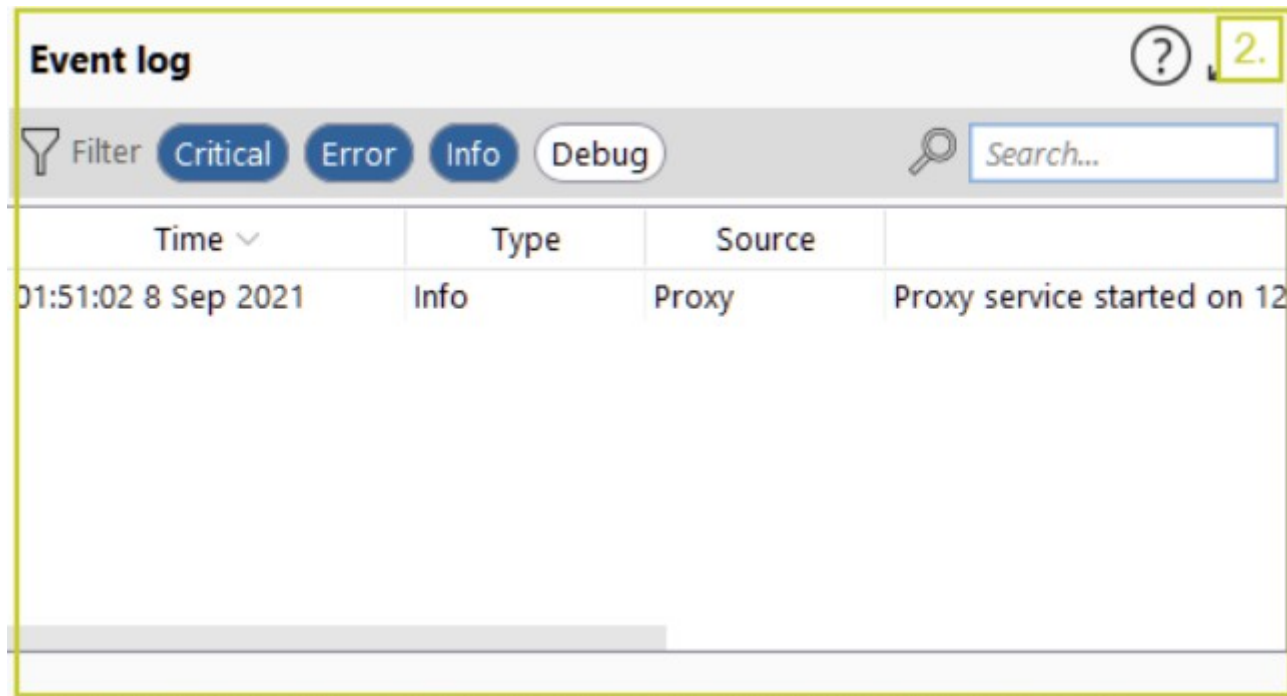
The dashboard can be subdivided into four different sections

The Dashboard



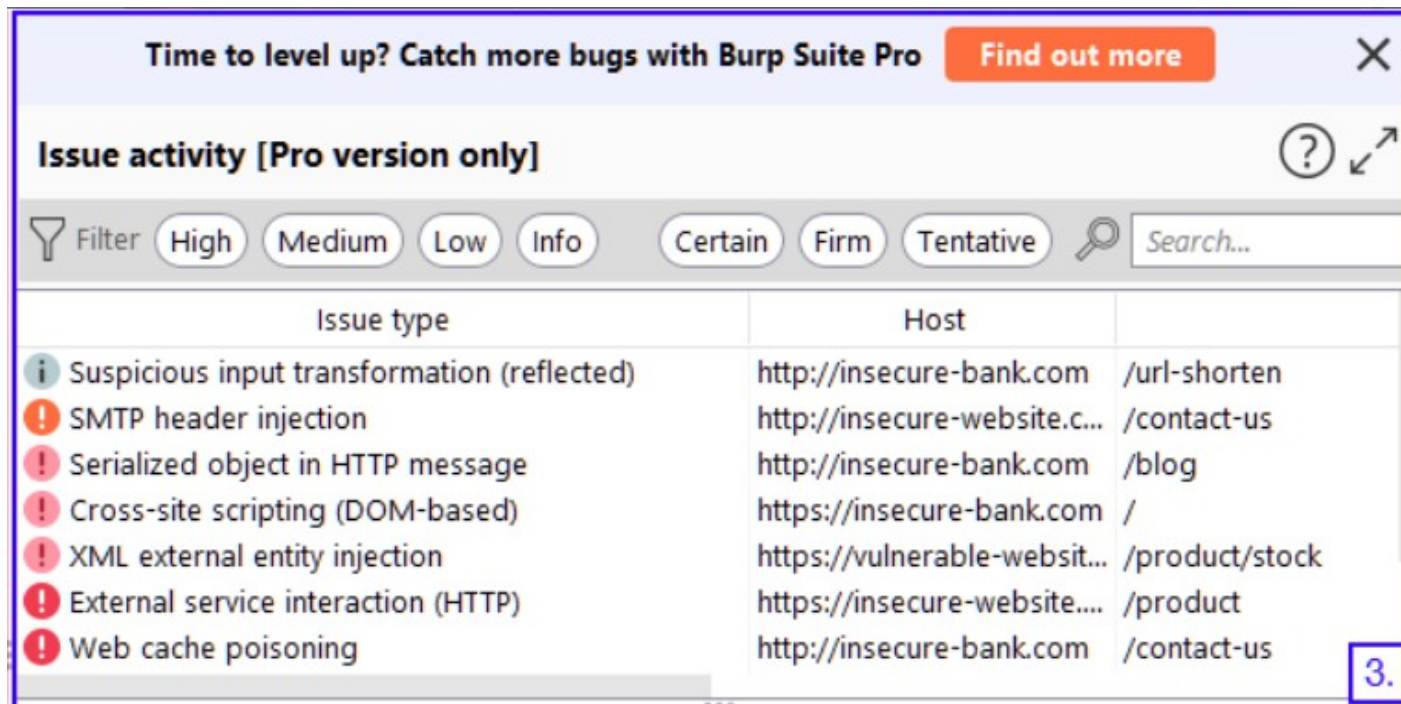
The Tasks window keeps track of visited webpages in Community edition, but in Pro edition it records scans and other tasks

The Dashboard



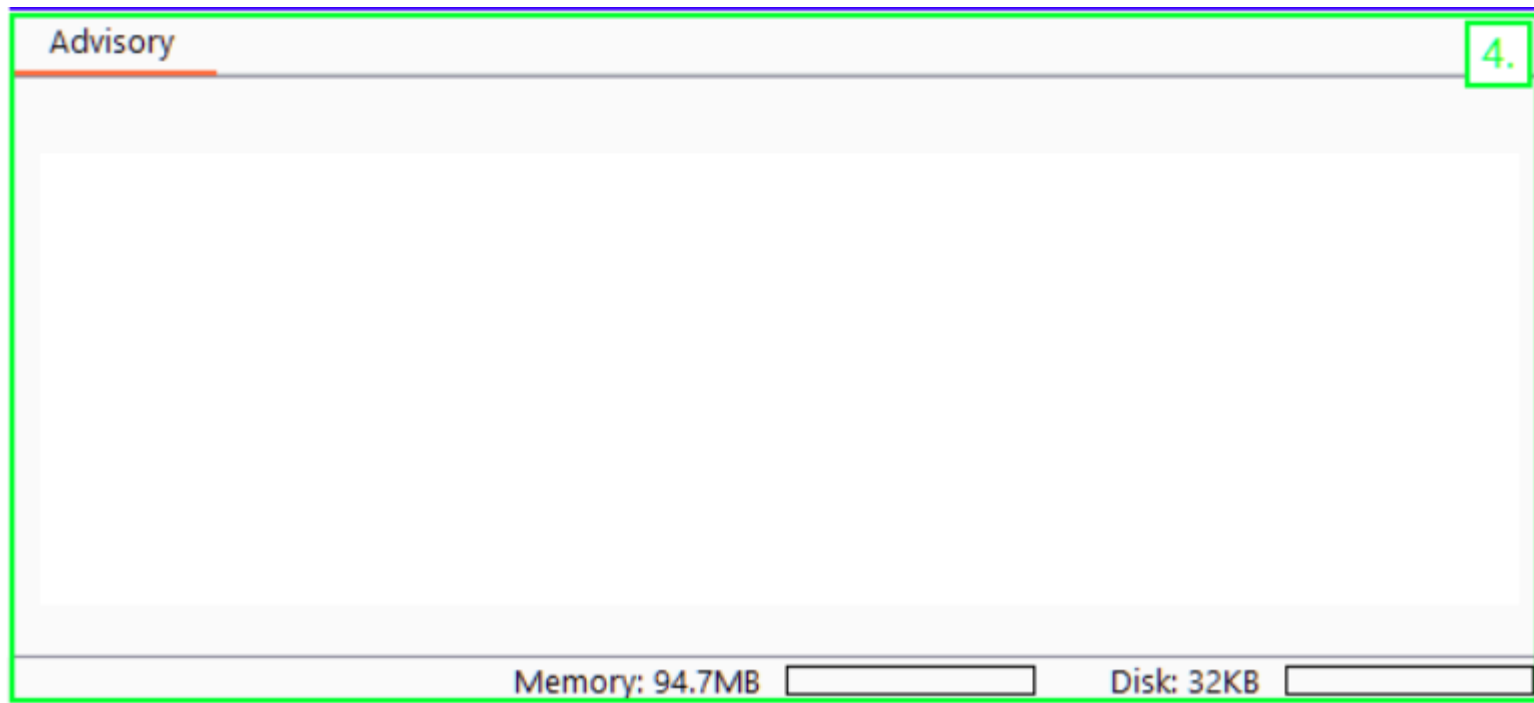
The Event Log window shows actions taken by the program for later analysis.

The Dashboard



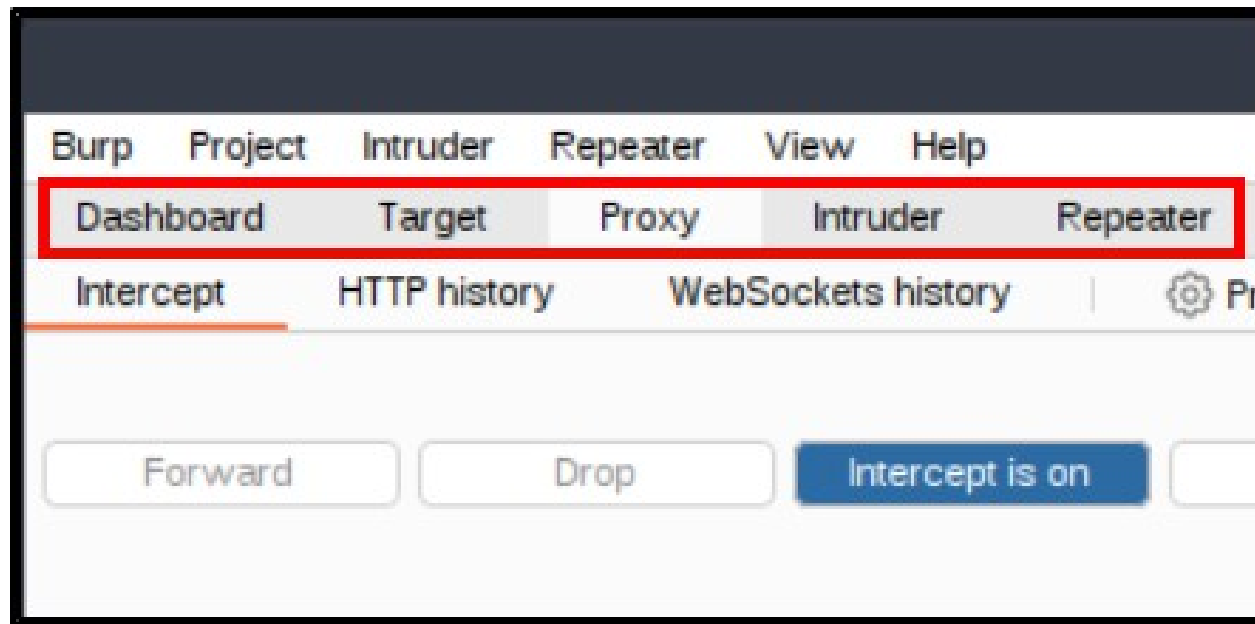
The Issue Activity window is not relevant in Community edition, but it displays vulnerabilities identified in the project scope in Pro edition.

The Dashboard



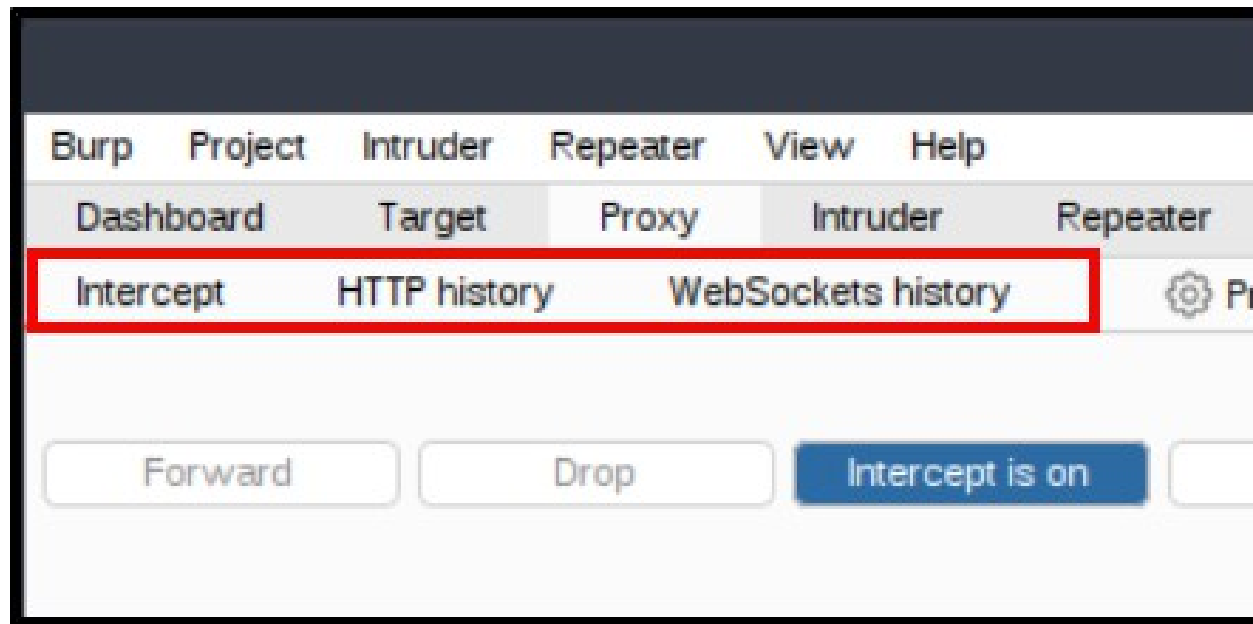
And the Advisory window provides detailed information about identified vulnerabilities, which again, is only supported in the Pro edition

Navigation



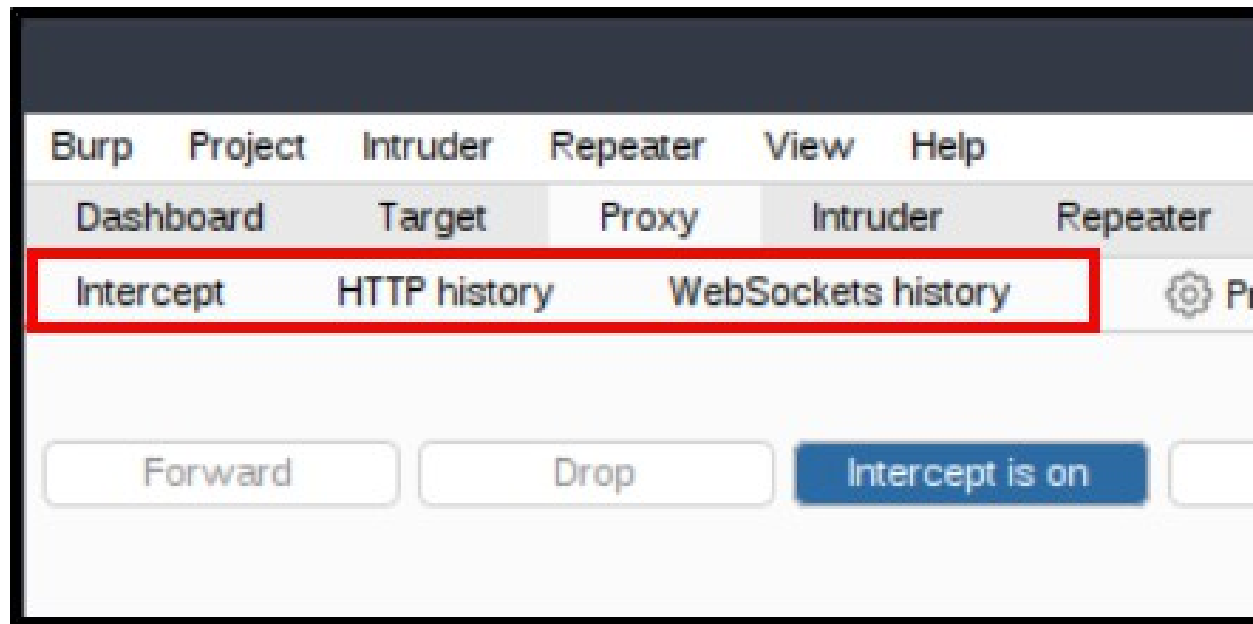
Navigating inside of Burp Suite mostly comes down to selecting the desired tab on the navigation bar, Target, Proxy, Intruder, etc.

Navigation



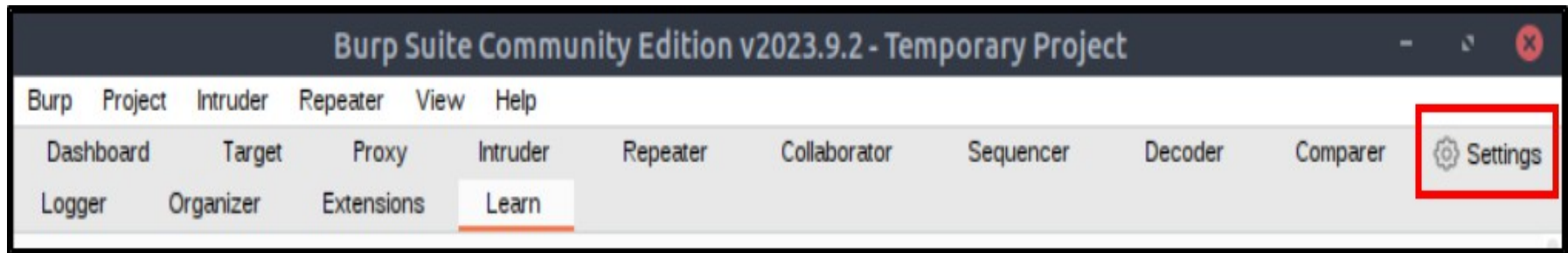
Within a specific tab, you can navigate to sub-tabs below the main tab bar.

Navigation



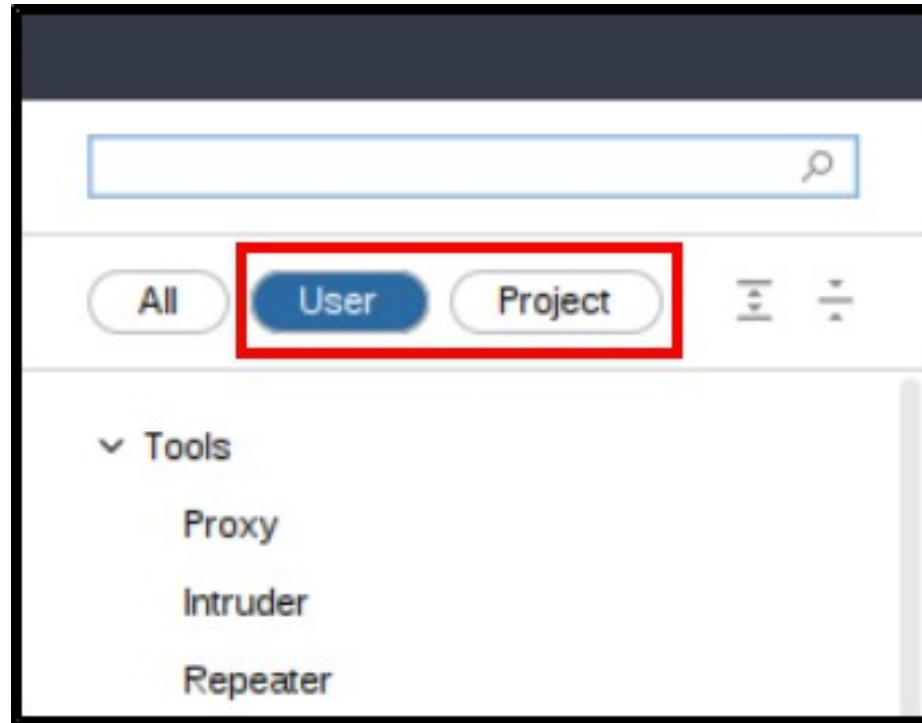
E.g., In the Proxy tab, there are the Intercept, HTTP history, and WebSockets history sub-tabs

Options



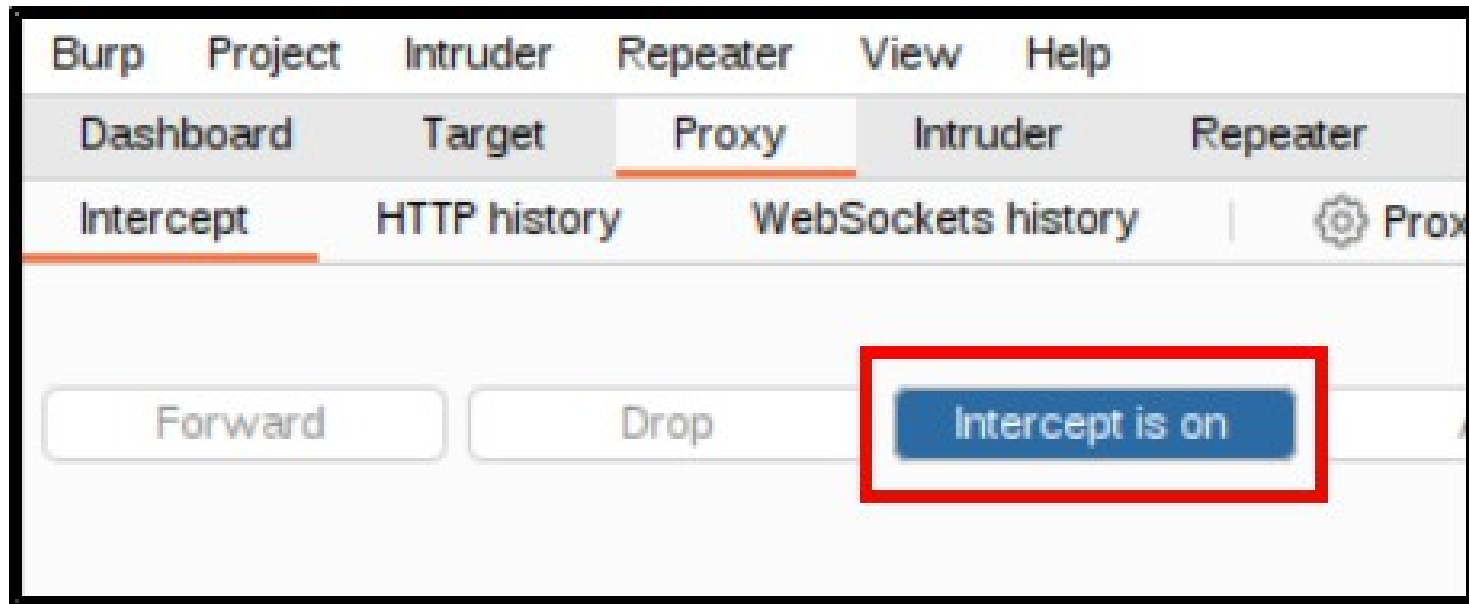
This section is actually about the Burp Suite settings page. Settings can be accessed from the settings button on the top-right corner of the UI.

Options



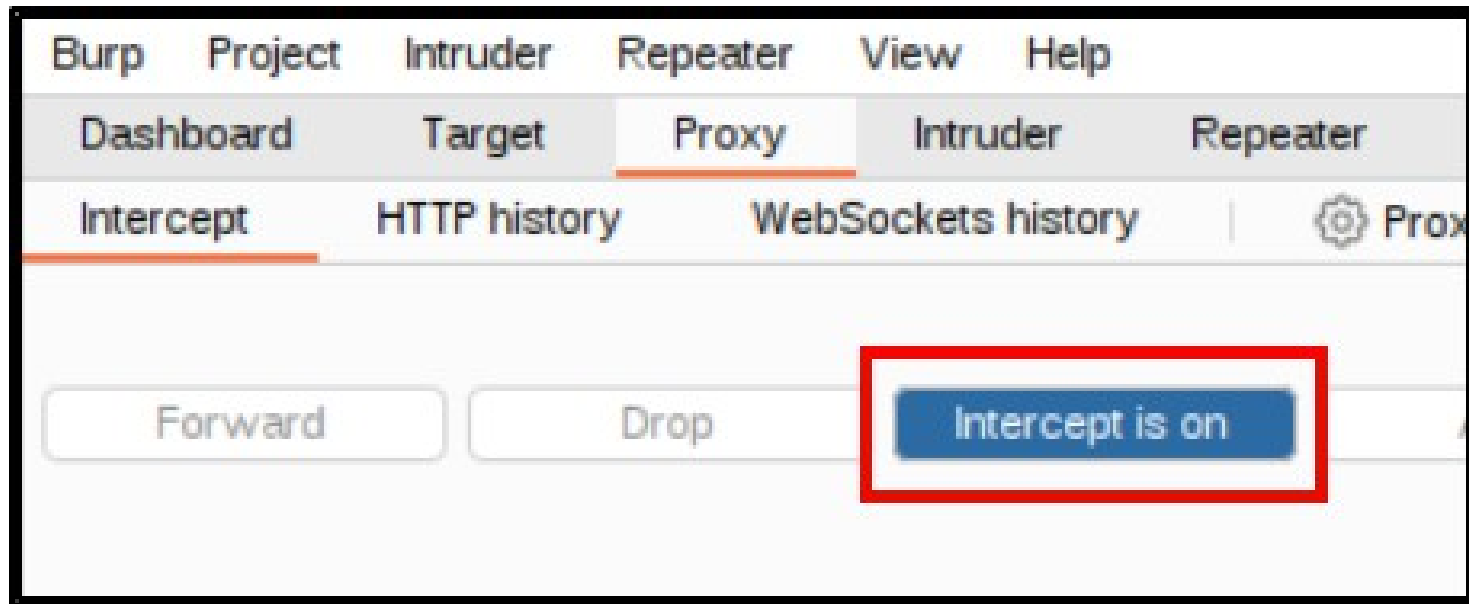
Once the settings page is opened, you can access User (global) settings or Project settings from their respective tabs at the top-left of the UI.

Introduction to Burp Proxy



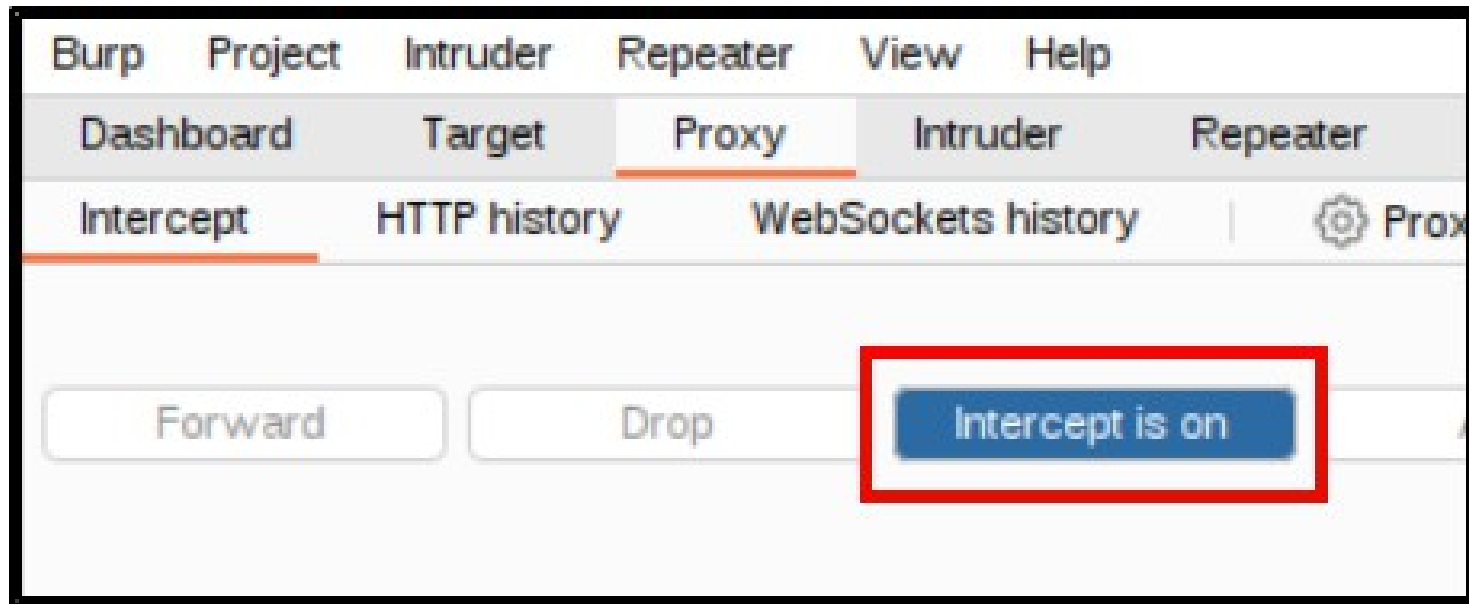
The Burp Proxy allows web traffic to be recorded, reviewed, and replayed. One thing to take note of is the Intercept → Intercept is on button

Introduction to Burp Proxy



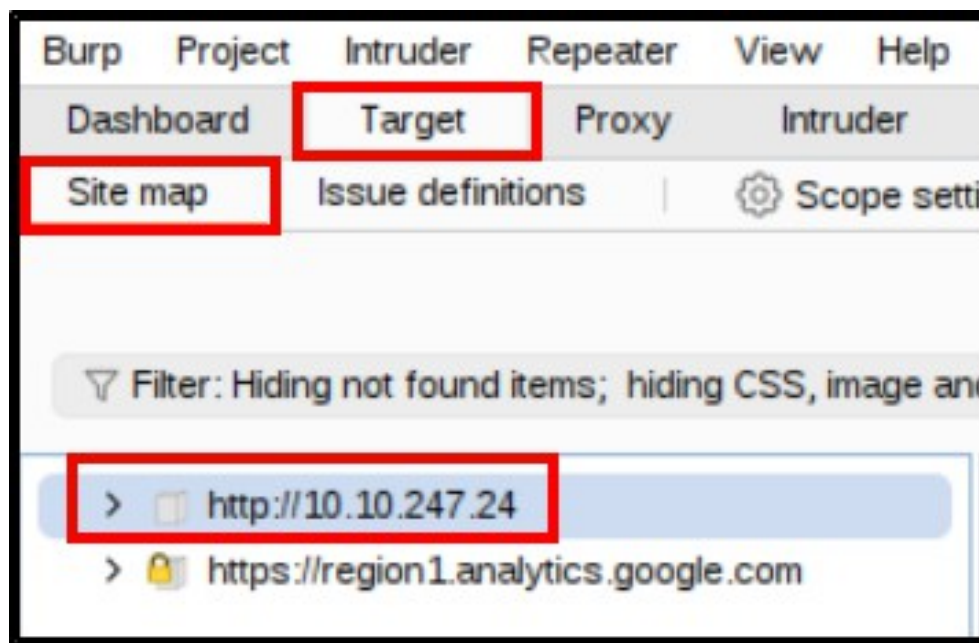
When Intercept is on, each web request has to be manually allowed or dropped before the next can be sent.

Introduction to Burp Proxy



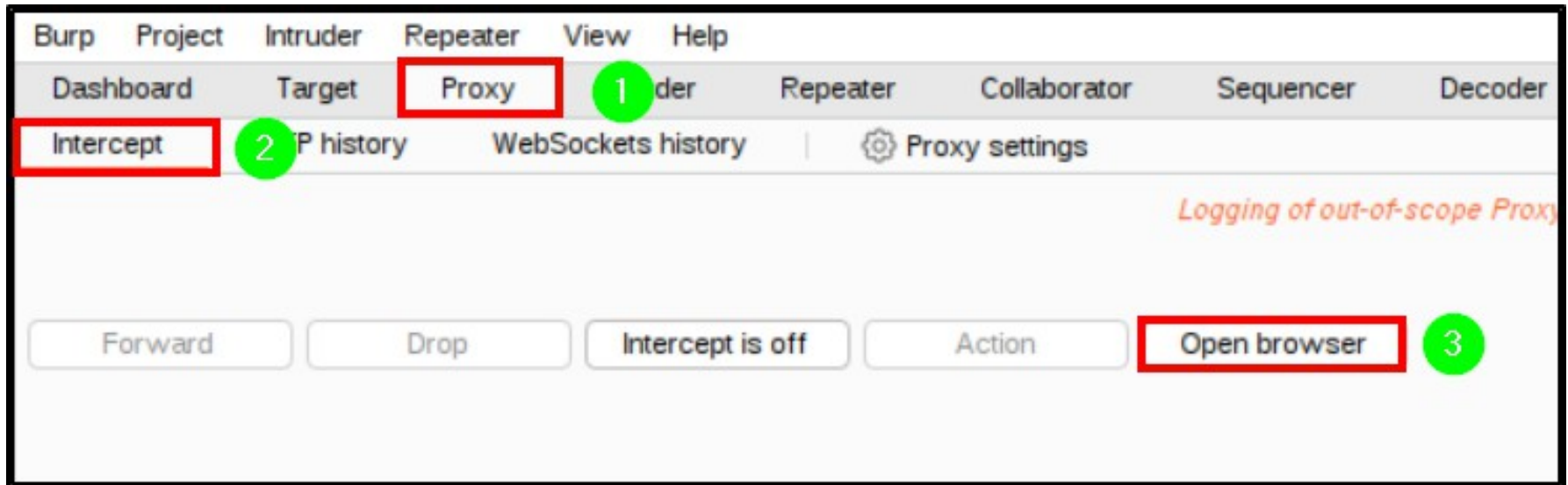
In most cases, we do not want this, and we should ensure the Intercept is on button is toggled off.

Site Map and Issue Definitions



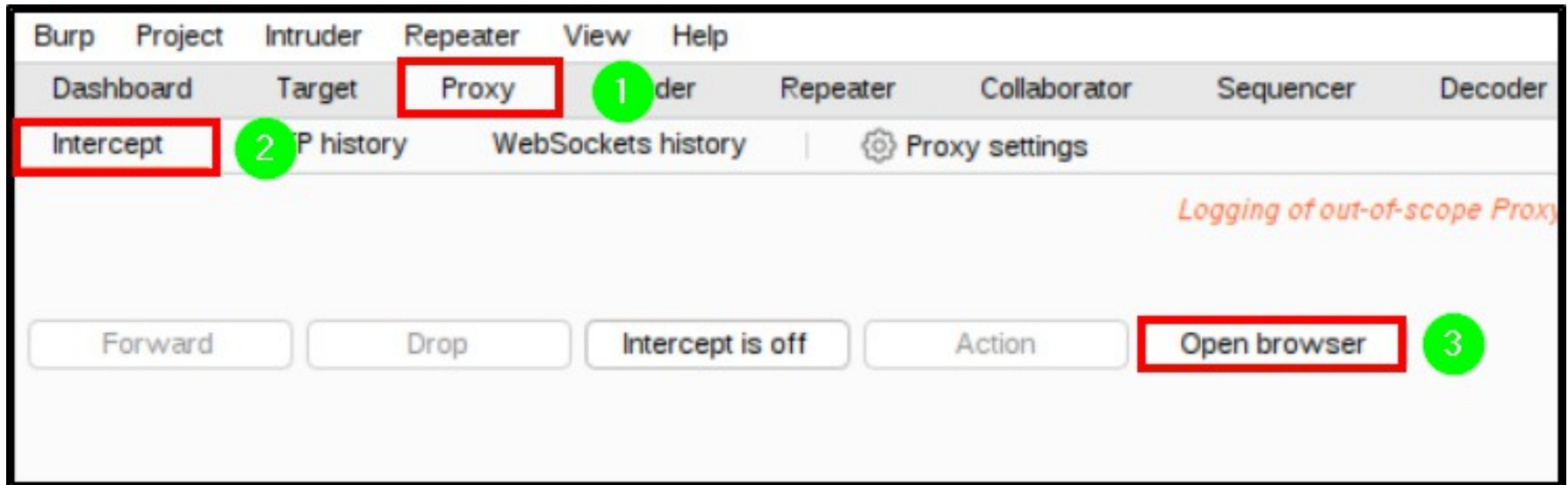
The Burp Target tab allows us to define which IP addresses and / or URLs are considered in-scope for web traffic proxy and capture.

The Burp Suite Browser



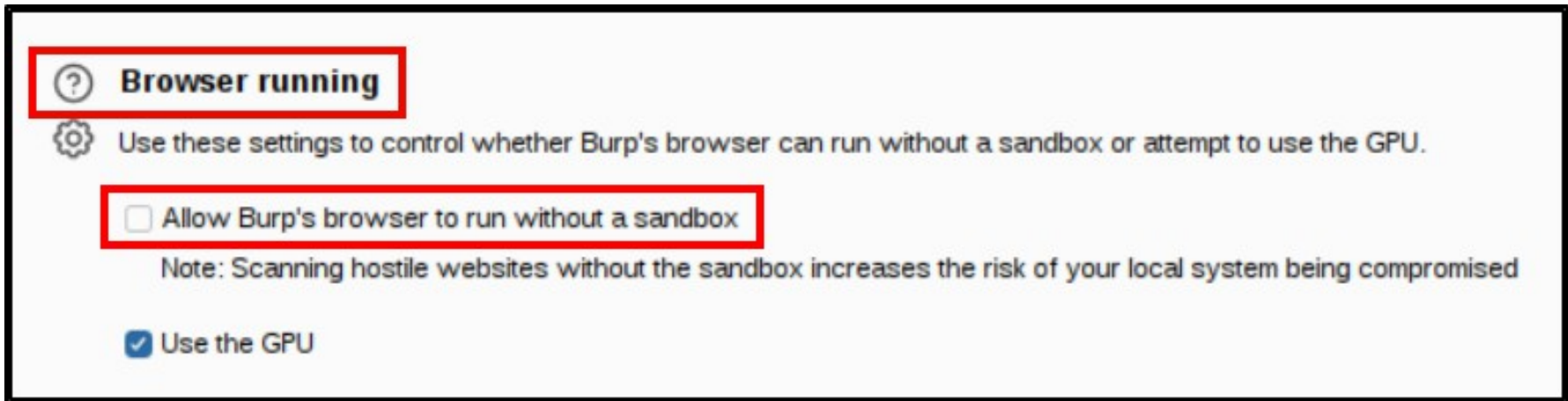
Using the Burp Suite Browser to proxy web traffic is the more convenient option over using regular web browser proxies.

The Burp Suite Browser



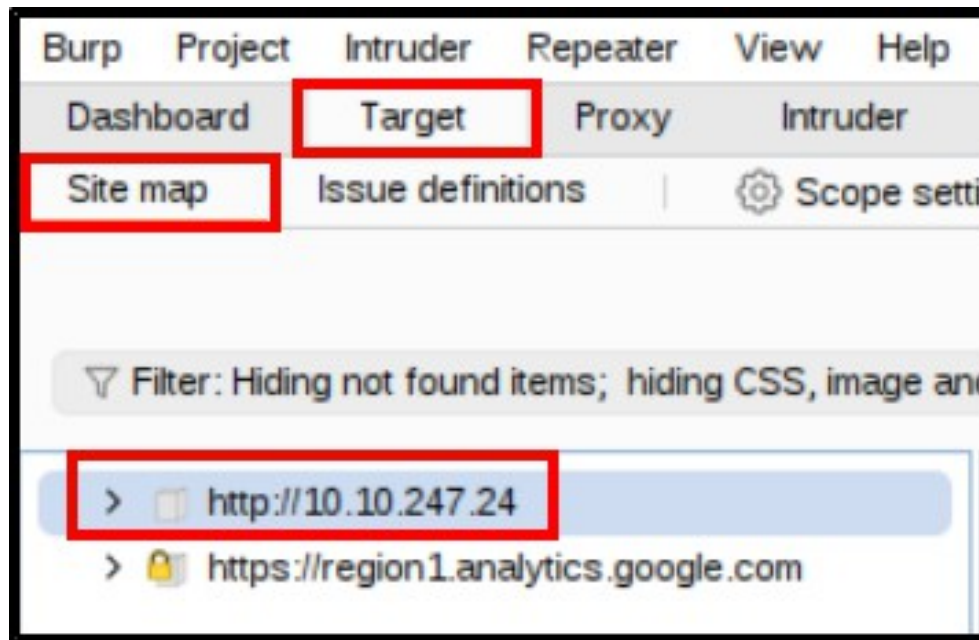
It can be accessed under the Proxy tab, then the Intercept sub-tab, then the Open browser button.

The Burp Suite Browser



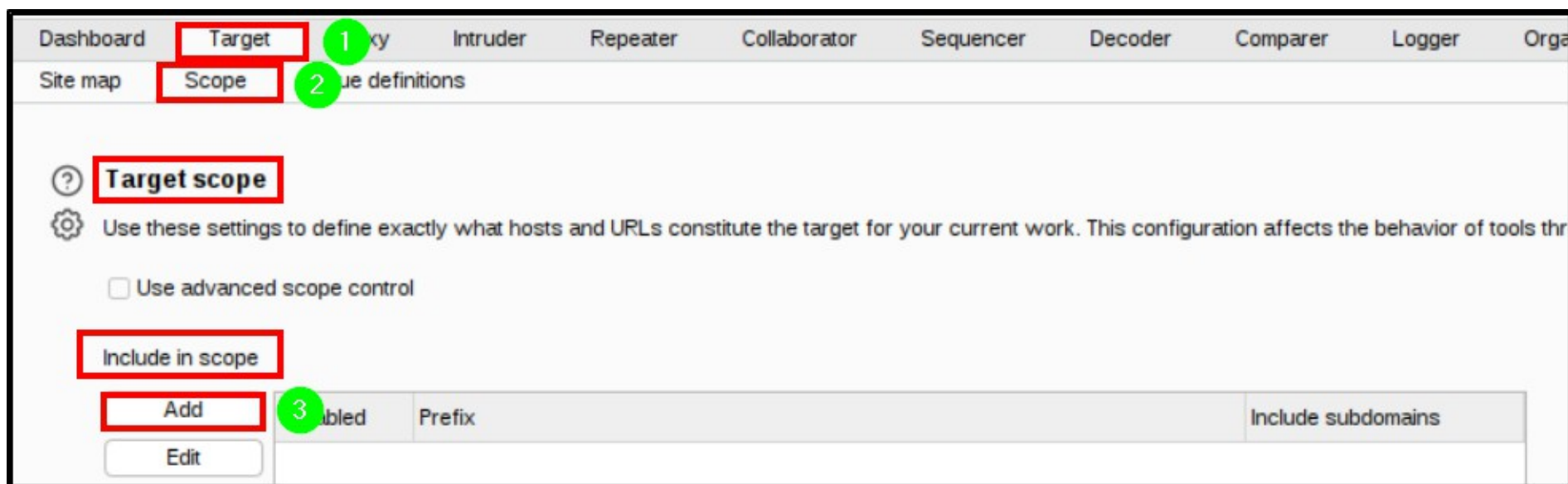
In the AttackBox, you'll have to go into Settings → Burp's browser → Browser running → Allow Burp's browser to run without a sandbox.

Scoping and Targeting



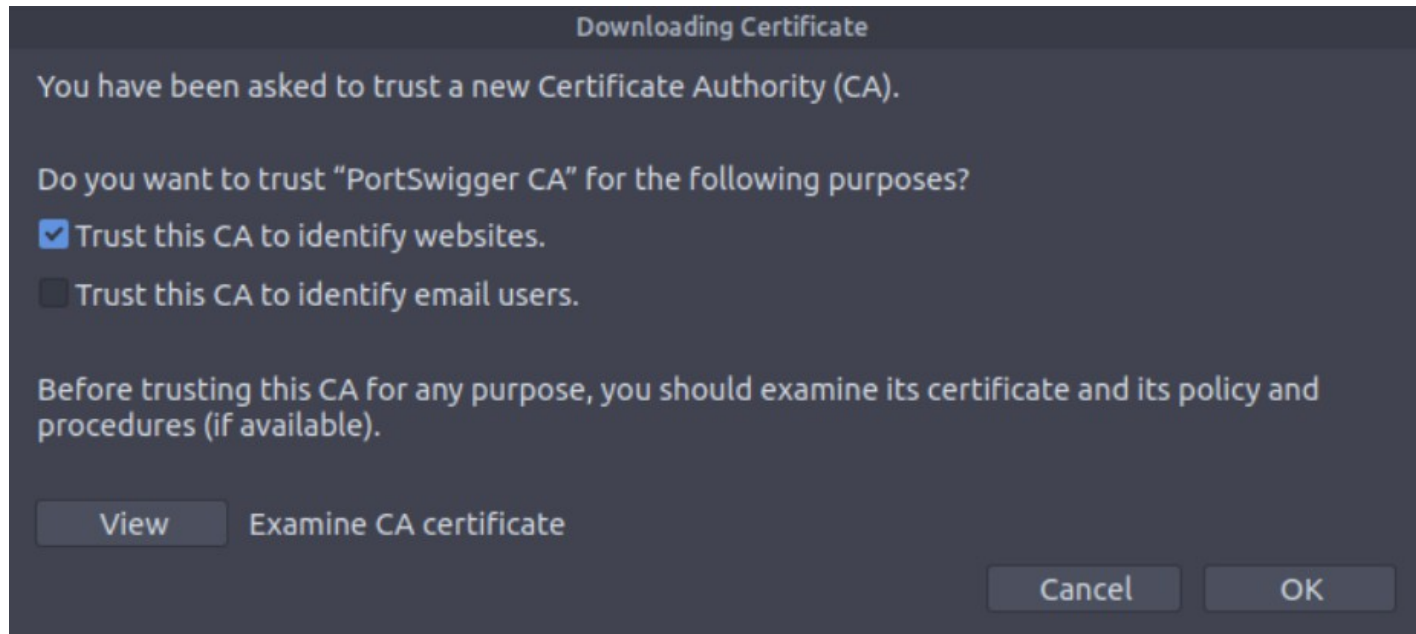
In most cases, we want to set a scope for our testing, and exclude all traffic that is outside the URL / IP address of the scope.

Scoping and Targeting



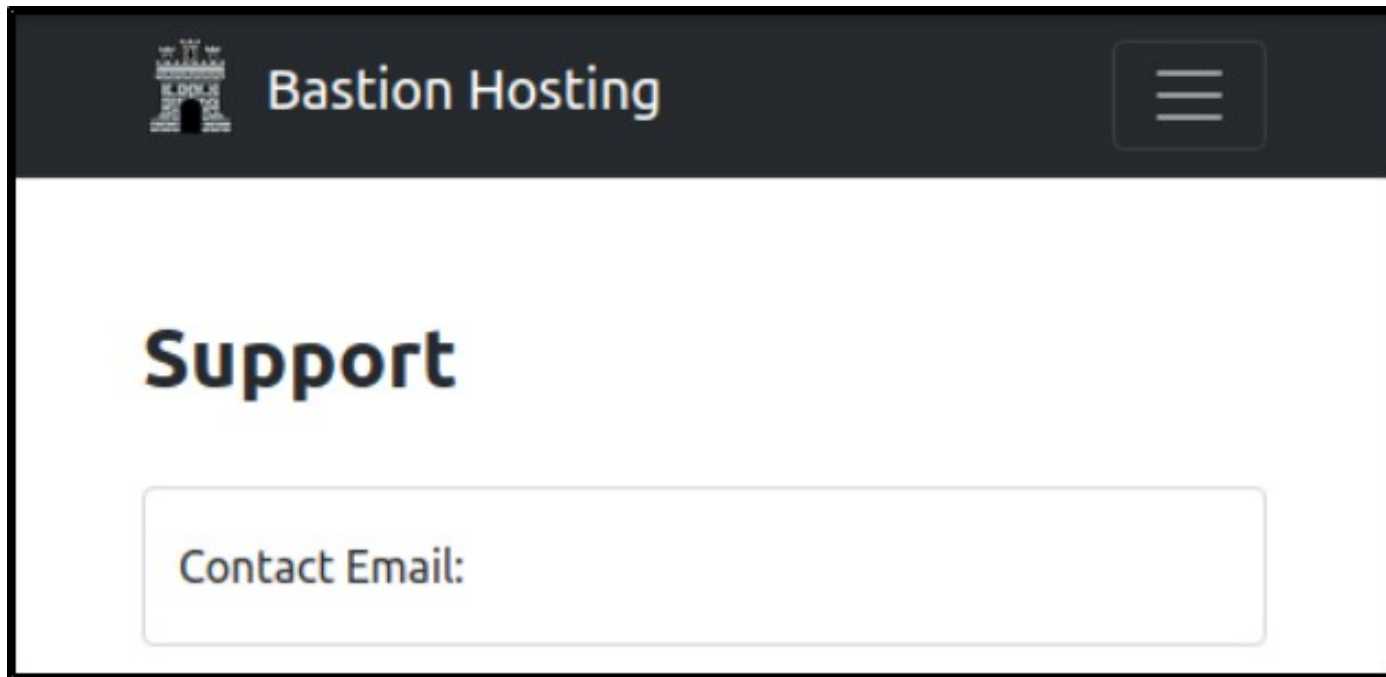
We can manually set a scope by using the Target
→ Scope → Target scope → Include in scope →
Add button.

Proxying HTTPS



One reason why it's preferable to use Burp's Browser to proxy web traffic is because it avoids some setup steps such as downloading and configuring HTTPS certificates.

Example Attack



The image shows a web browser window displaying the 'Bastion Hosting' support page. The header is dark grey with a castle icon on the left, the text 'Bastion Hosting' in the center, and a hamburger menu icon on the right. The main content area is white and features the word 'Support' in a large, bold, dark blue font. Below this, there is a light grey rectangular input field with the placeholder text 'Contact Email:' in a dark blue font.

Our last task in this room is to perform a web attack on the room's associated web app.

Summary



Let's review the web exploitation concepts we learned in this workshop:

Burp Suite

Burp Suite is the industry-standard software framework for testing web apps. It includes many different tools, but the Burp tool that enables the rest of the framework is...



Burp Proxy



The Burp Proxy server is what enables web traffic to be captured and recorded. It sits between the browser and the server, enabling traffic capture.

What's Next?

In the next HackerFrogs Afterschool web app hacking workshop, we'll learn continue learning about Burp Suite, more specifically, the Burp Repeater tool.



Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!



Until Next Time, HackerFrogs!

