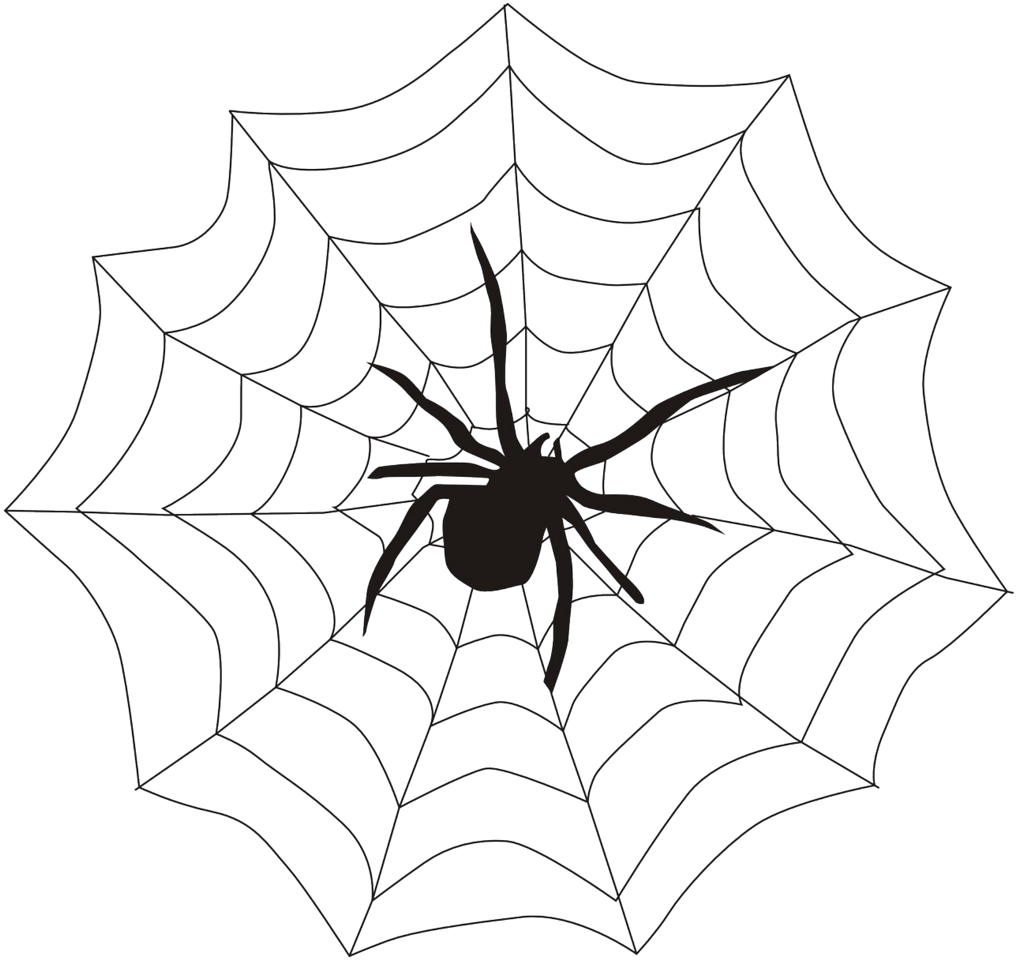
HackerFrogs Afterschool
Web App 7: Burp Suite Pt. 1 of 2

Class:
Web App Hacking

Workshop Number:
AS-WEB-07

Document Version:
1.2

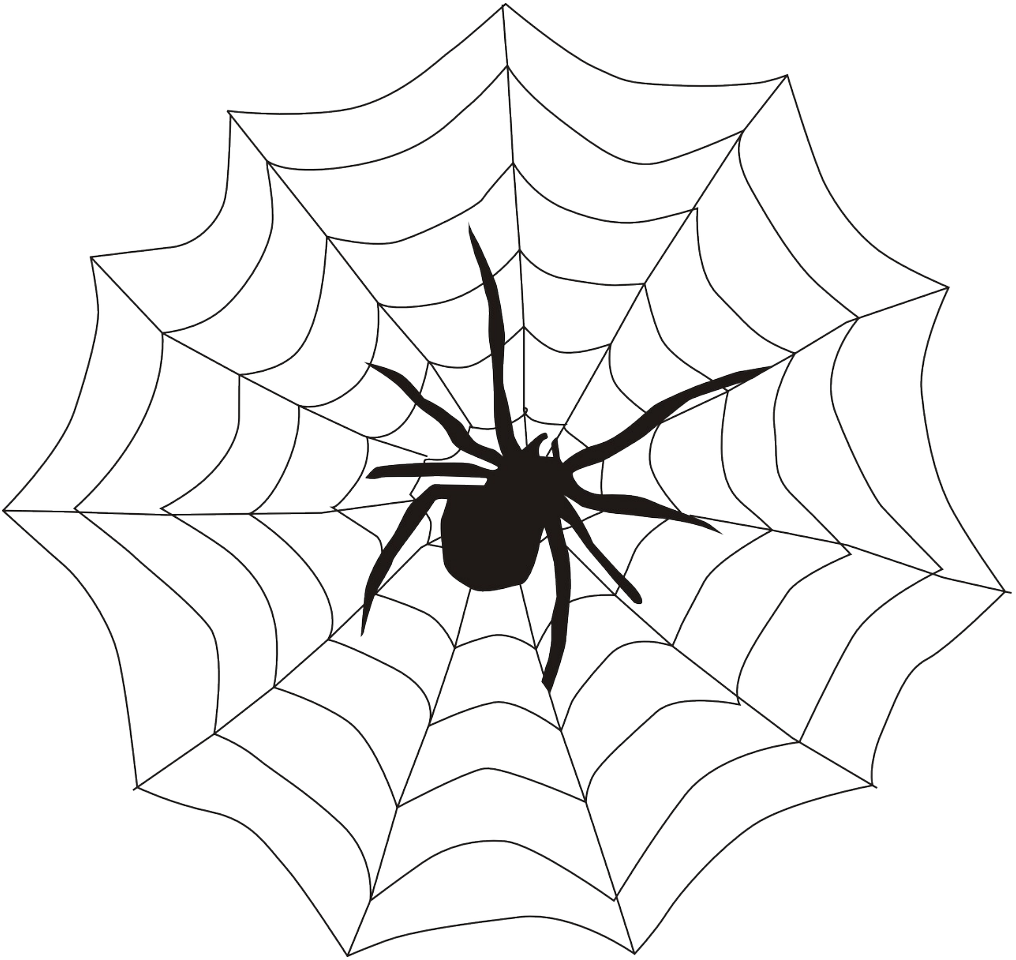
Special Requirements:
Registered account at tryhackme.com



What We Learned In The Previous Workshop

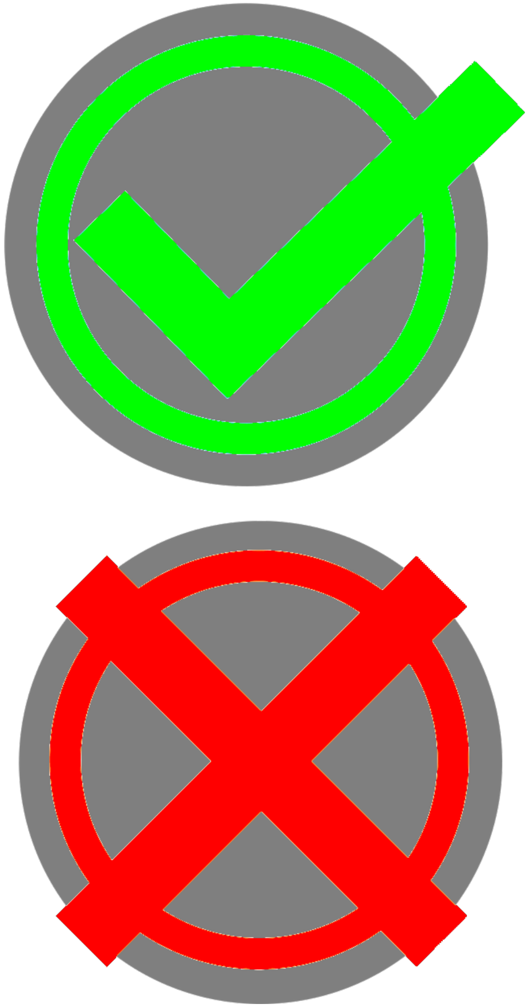
This is the seventh intro to web app hacking workshop.

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



Blind SQL Injection: Boolean Based

Boolean Based SQL Injection is a type of Blind SQL Injection where the only output that is returned after a SQL statement is whether the query returned true or false.



Blind SQL Injection: Time Based

Time Based SQL Injection is a type of Blind SQL Injection where we give the database software an instruction to return a delayed response, and if so, we know that the attack was successful.

Out-Of-Band (OOB) SQL Injection

Out-Of-Band (OOB) SQL Injection is a type of SQL injection where the output of any SQL queries can be passed to services outside of the web app's network.

Remediation

Lastly, we learned about how to remediate web apps against SQL injection vulnerability.

This Workshop's Topic

In this workshop, we'll be looking at Burp Suite, a 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/burpsuitebasics

T1 - Introduction

This TryHackMe room goes over the basics of Burp Suite, which is a Web App testing framework used by nearly every professional working in the web app security testing industry.

T2 – 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:

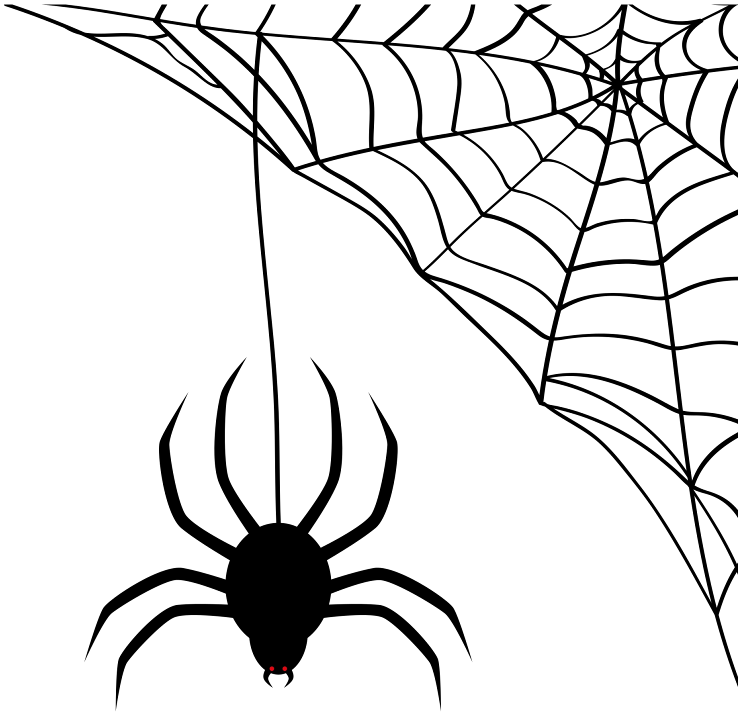
T2 – What is Burp Suite
1. Burp Proxy

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.

T2 – 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 Ferroxbuster



T2 – 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.

T2 – 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

T2 – What is Burp Suite
5. Burp Repeater

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

T2 – What is Burp Suite
5. Burp Repeater

Similar tools include ZAP, Postman, and Charles Proxy.

T3 – Features of Burp Community

Let's discuss the differences between the Professional version of Burp Suite and the free Community version.

T3 – Features of Burp Community

Burp Proxy, which allows capturing and modification of web content, is quite usable in Community edition

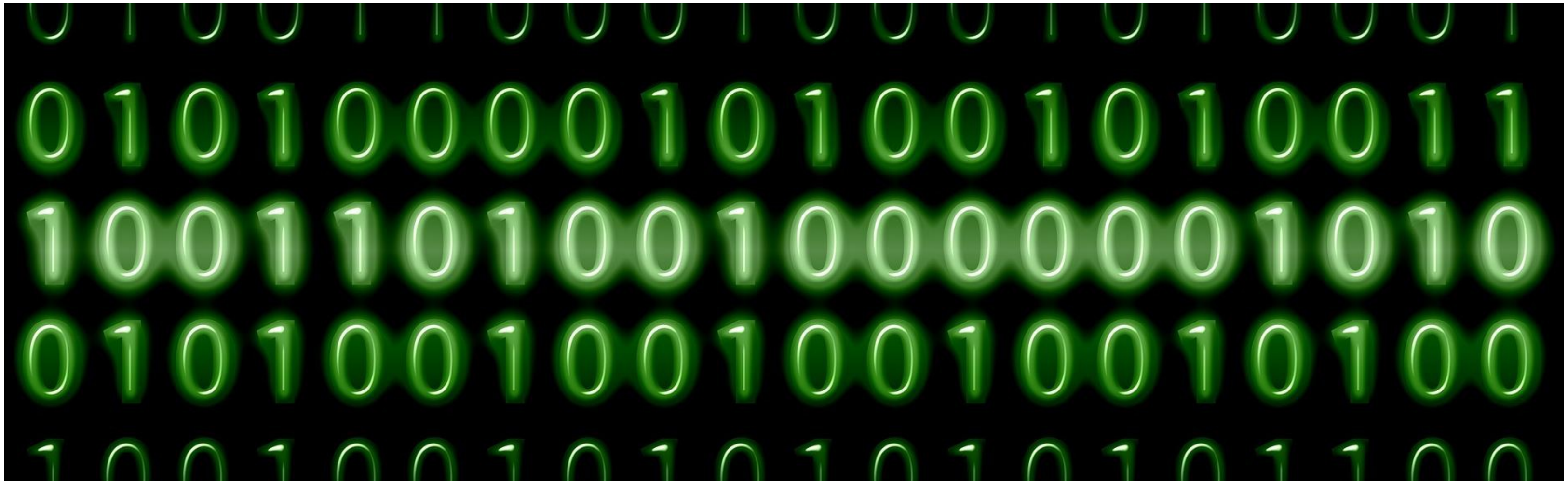
T3 – Features of Burp Community

Burp Repeater, which allows modification and re-sending of of specific web requests, is basically untouched in Community edition

T3 – Features of Burp Community

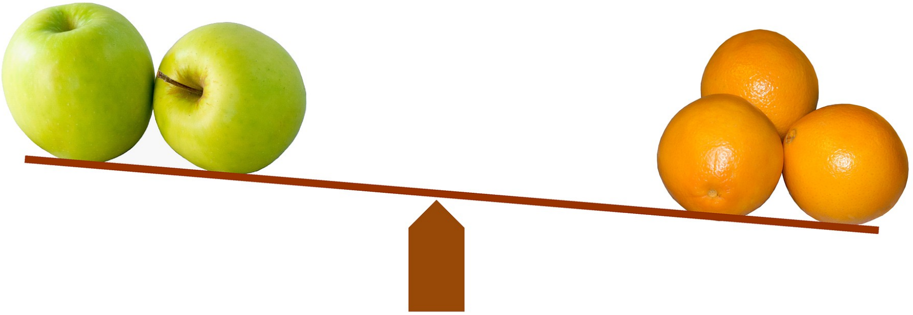
Burp Intruder, which allows brute-force attacks of web applications, is severely rate-limited, but can be used for demonstration purposes

T3 – Features of Burp Community



Burp Decoder, allows for encoding and decoding of data into various formats, such as URL, base64, binary, and more.

T3 – Features of Burp Community



Burp Comparer, allows for word or byte-level comparison between different pieces of data

T3 – Features of Burp Community

Burp Sequencer provides analysis of randomly generated data, such as sessions tokens, for flaws in its random generation.

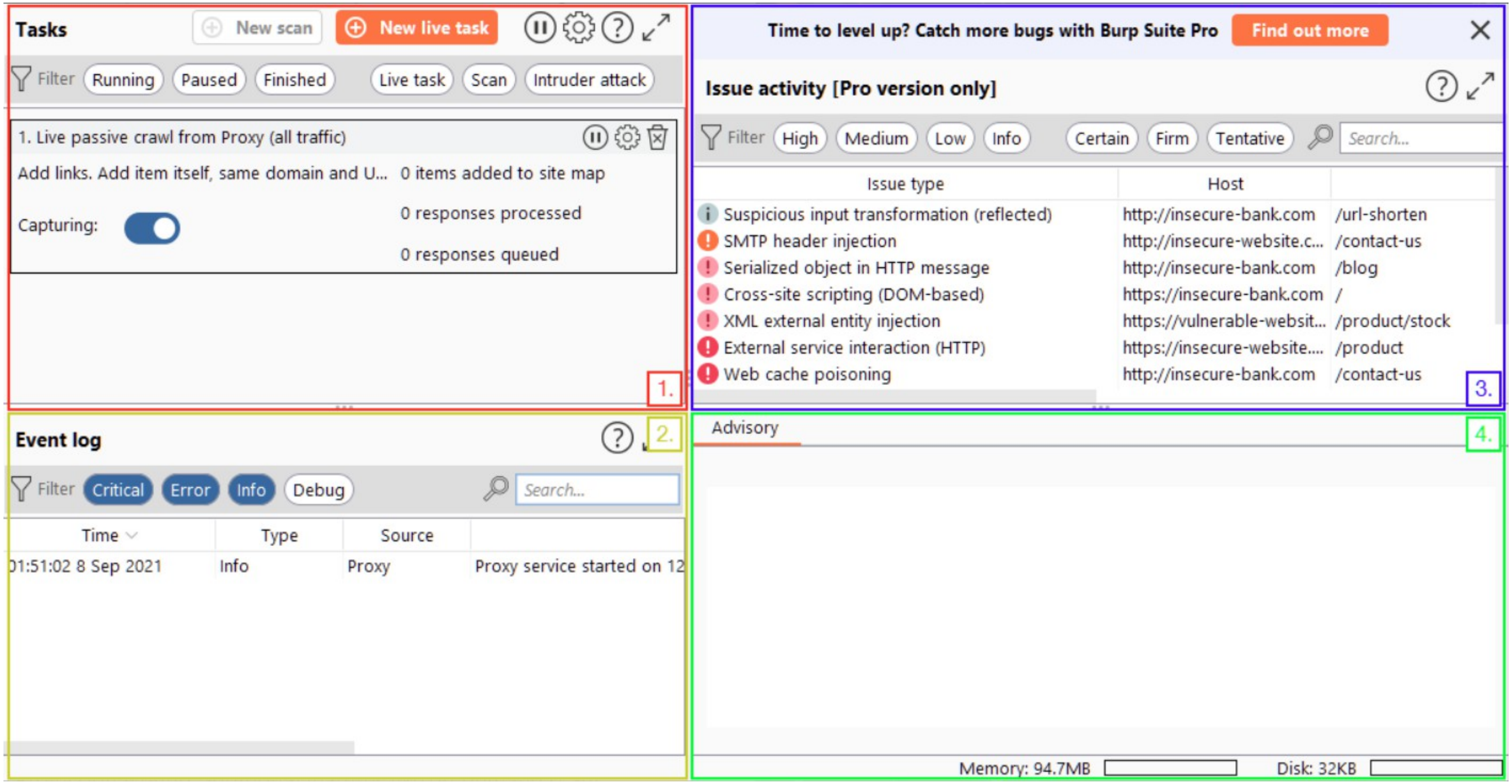
T4 – Installation

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.

T4 – Installation

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

T5 - The Dashboard



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and U... 0 items added to site map

Capturing: 0 responses processed

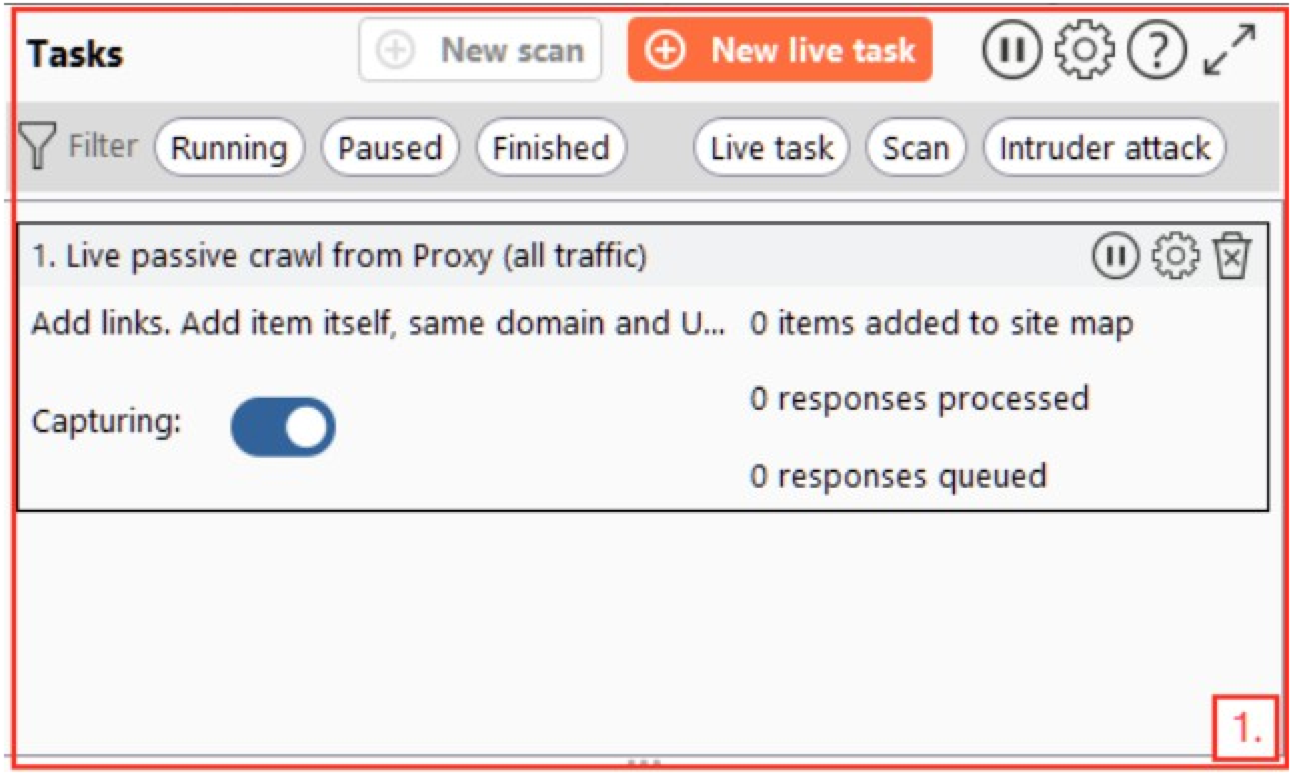
0 responses queued

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

Time	Type	Source	
01:51:02 8 Sep 2021	Info	Proxy	Proxy service started on 12

The dashboard can be subdivided into four different sections

T5 - The Dashboard



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and U...

0 items added to site map

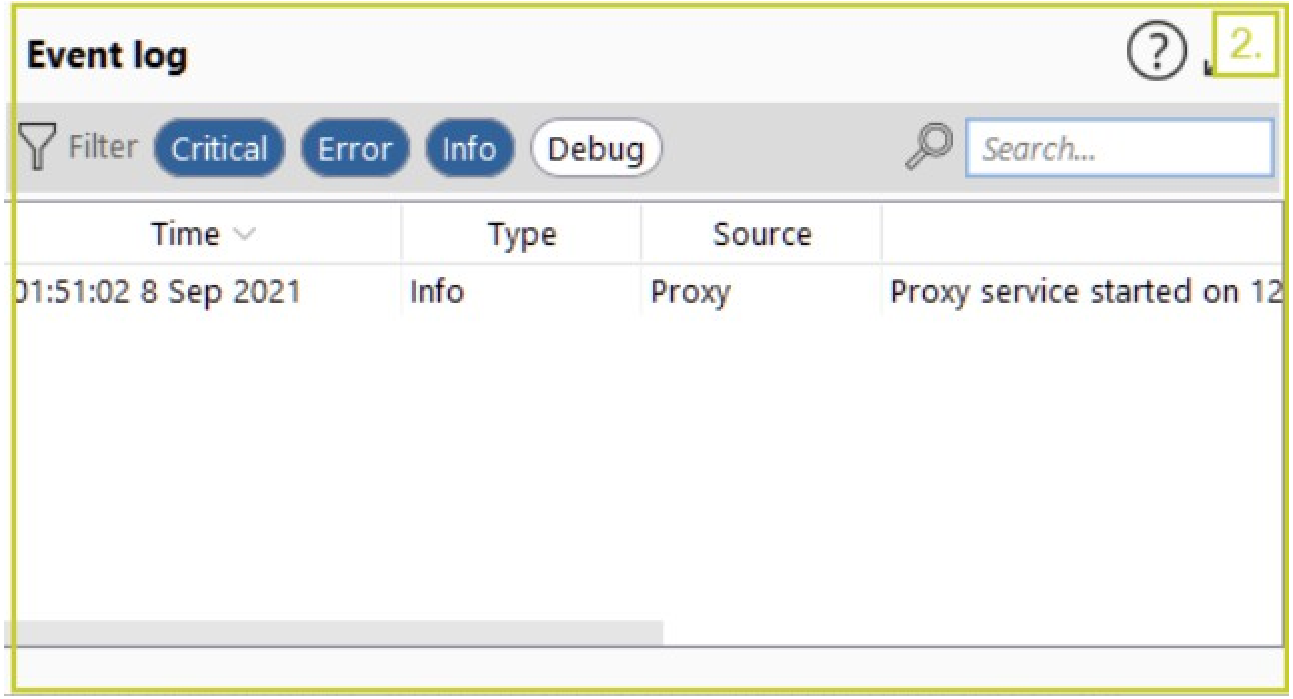
Capturing:

0 responses processed

0 responses queued

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

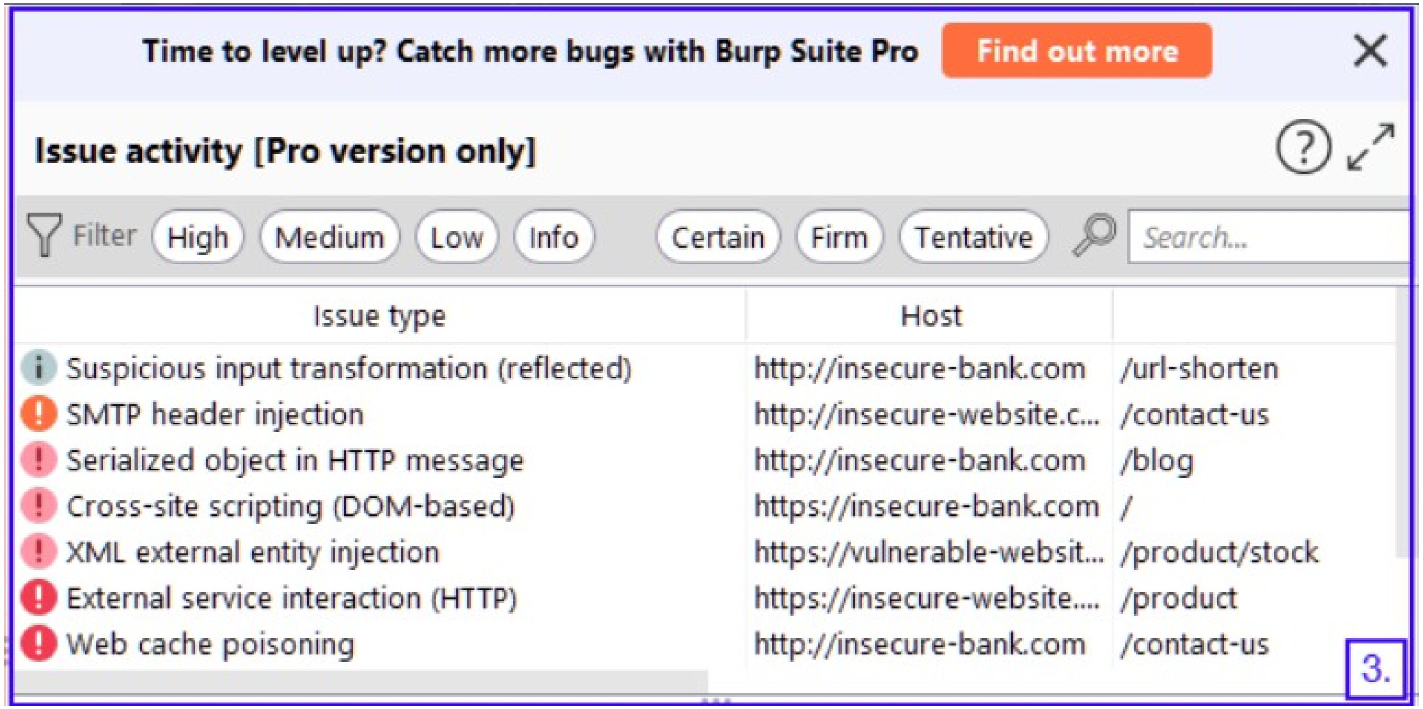
T5 - The Dashboard



Time	Type	Source	
01:51:02 8 Sep 2021	Info	Proxy	Proxy service started on 12

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

T5 - The Dashboard



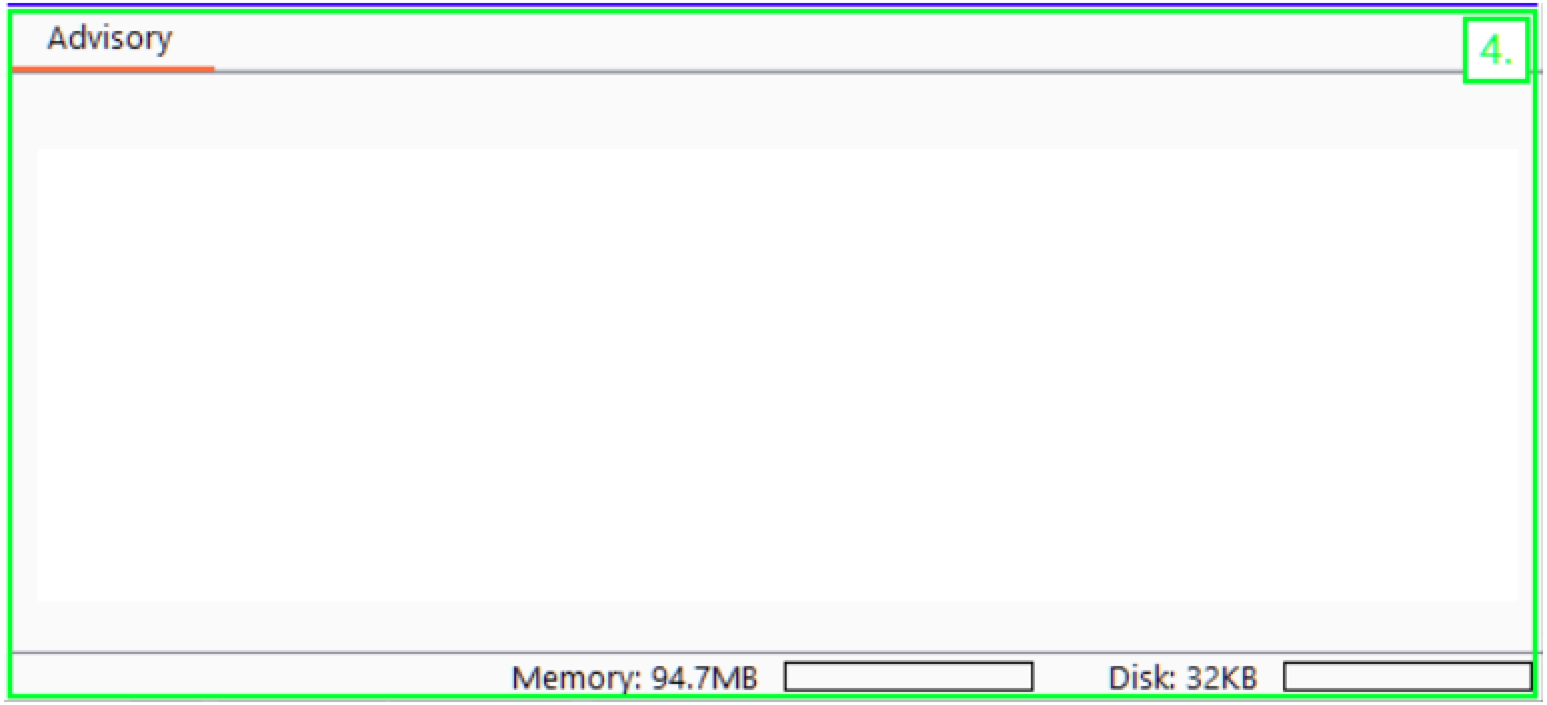
Time to level up? Catch more bugs with Burp Suite Pro

Issue activity [Pro version only]

Issue type	Host	
i 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

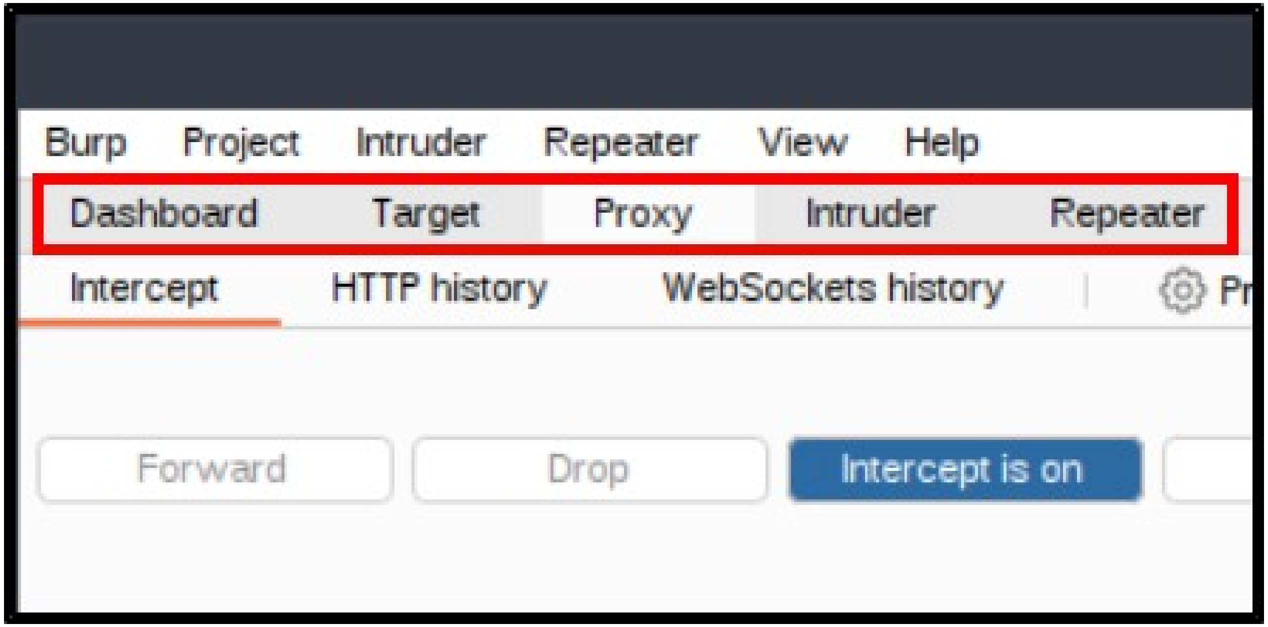
The Issue Activity window is not relevant in Community edition, but it displays vulnerabilities identified in the project scope in Pro edition.

T5 - The Dashboard



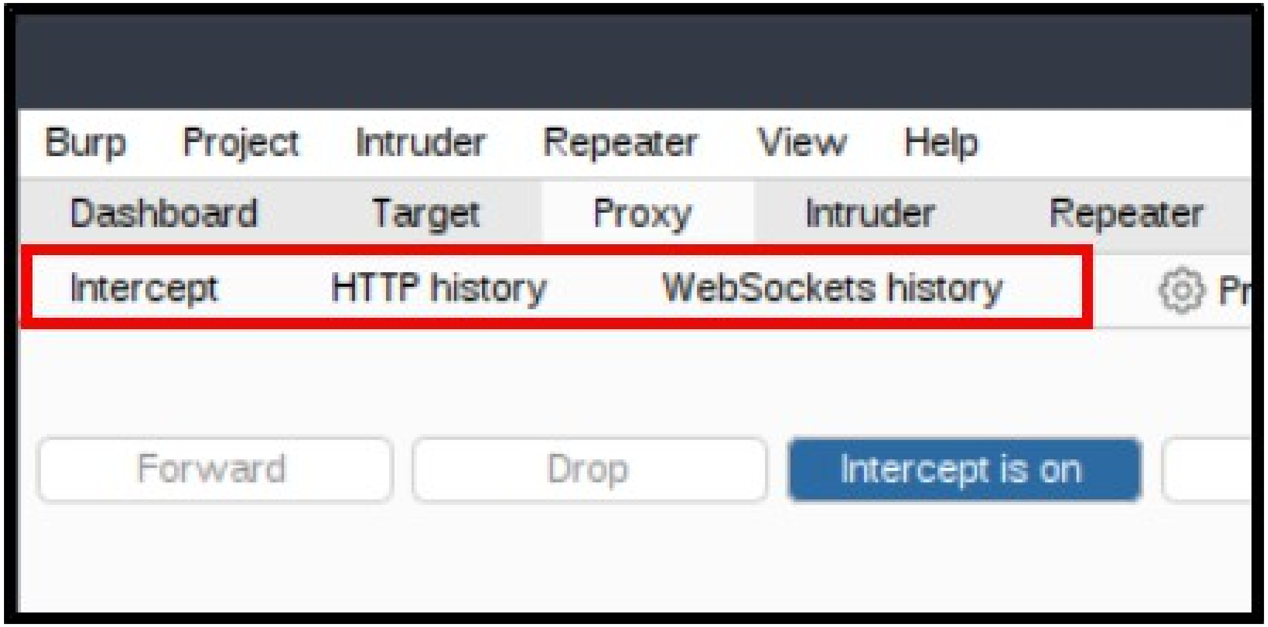
And the Advisory window provides detailed information about identified vulnerabilities, which again, is only supported in the Pro edition

T6 - Navigation



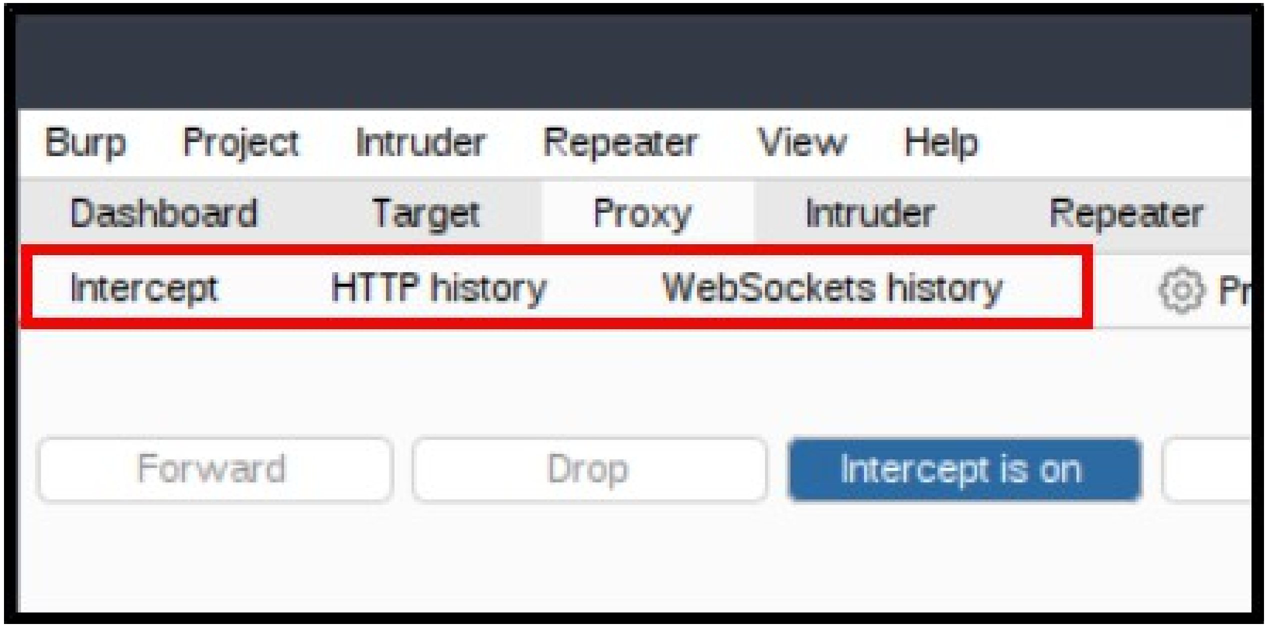
Navigating inside of Burp Suite mostly comes down to selecting the desired tab on the navigation bar, Target, Proxy, Intruder, etc.

T6 - Navigation



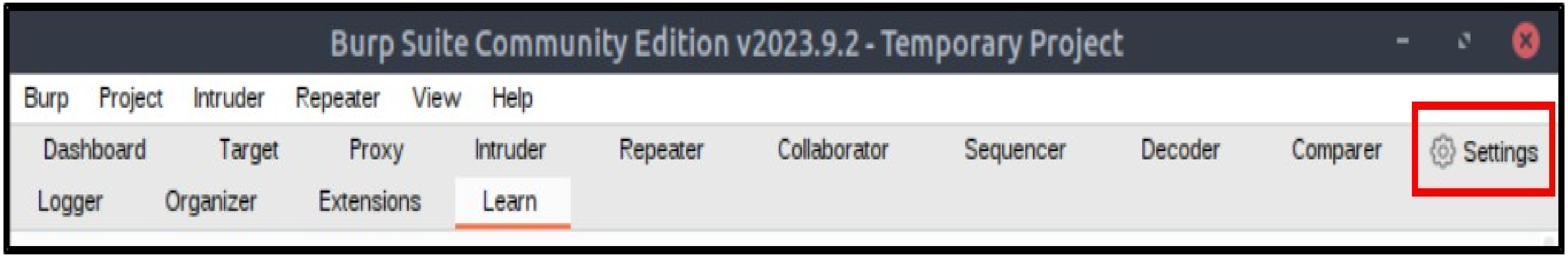
Within a specific tab, you can navigate to sub-tabs below the main tab bar.

T6 - Navigation



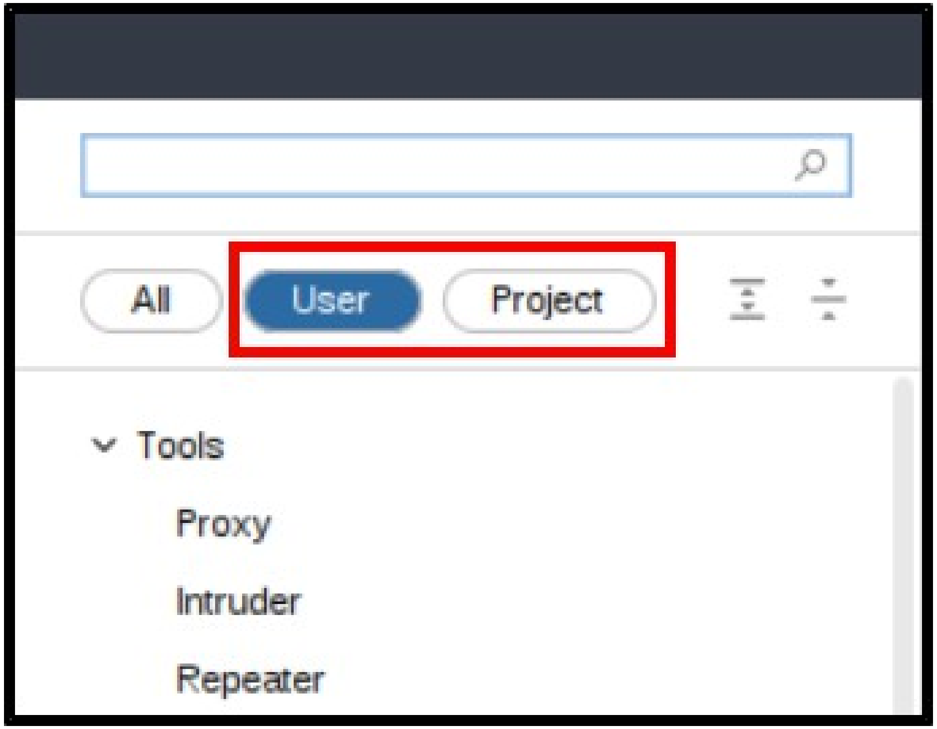
E.g., In the Proxy tab, there are the Intercept, HTTP history, and WebSockets history sub-tabs

T7 - Options



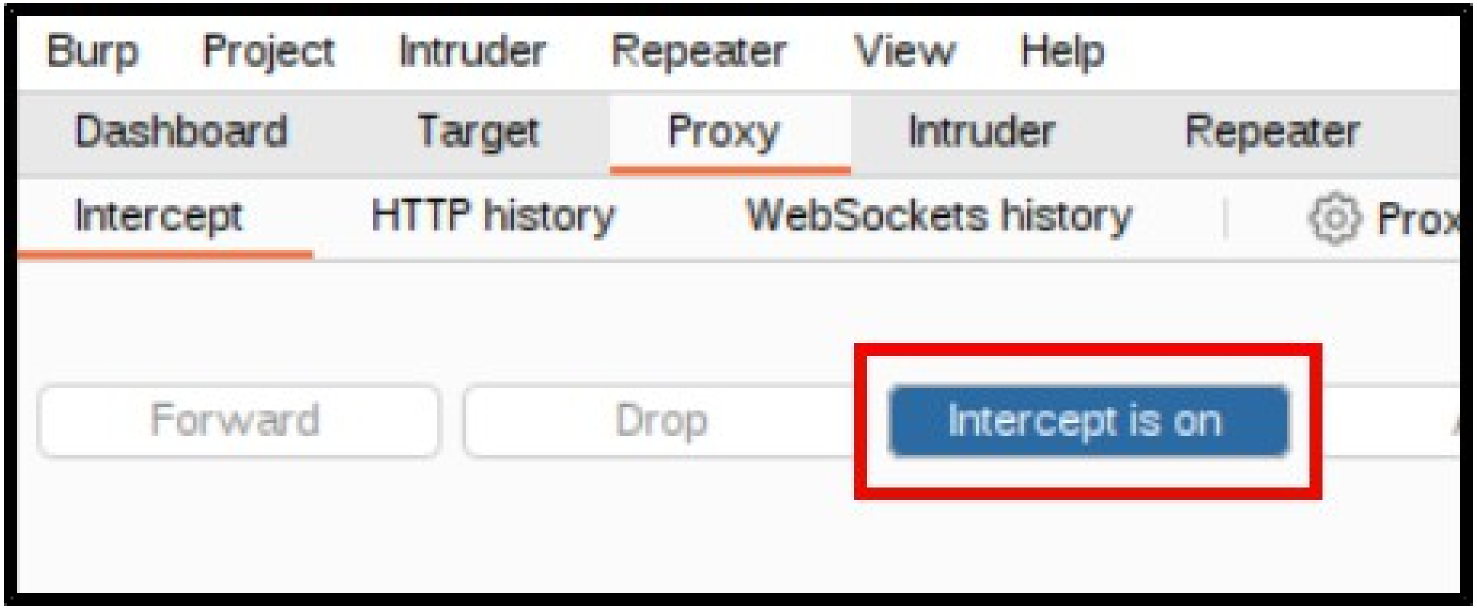
This section is actually about the Burp Suite settings page. Settings can be accessed from the settings button on the top-right corner of the UI.

T7 - Options



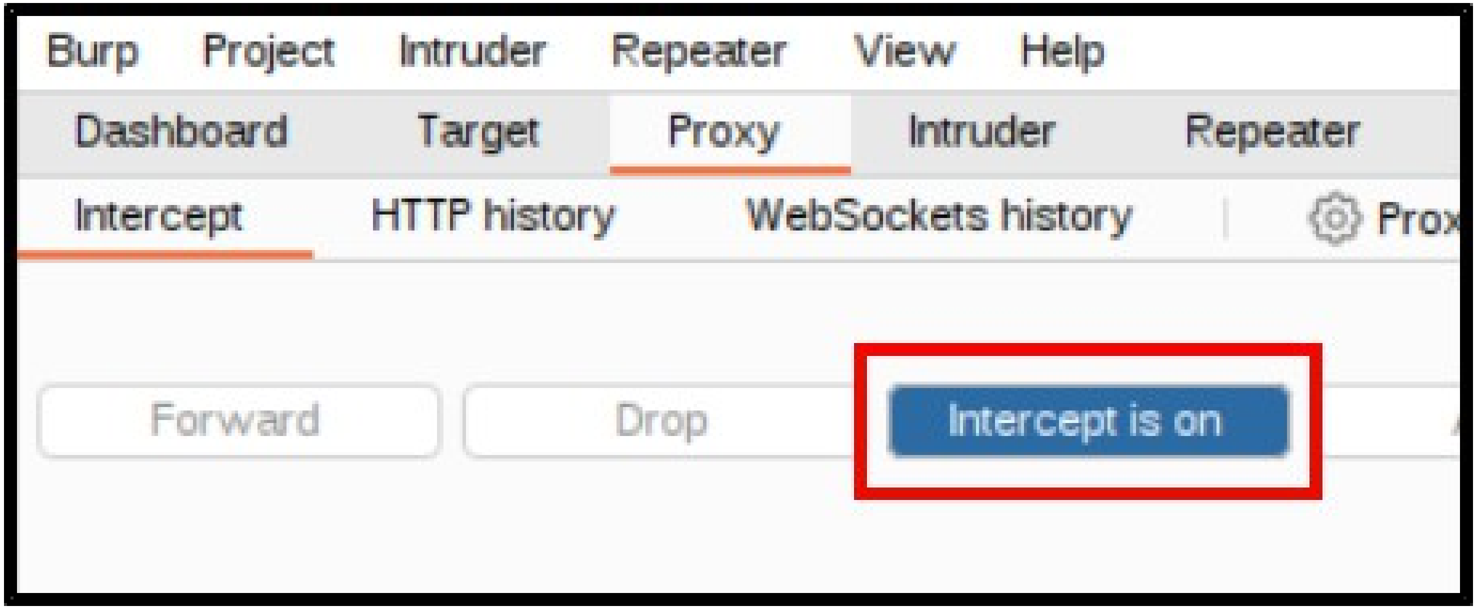
Once the settings page is opened, you can access User (global) settings or Project settings from their respective tabs at the top-left of the UI.

T8 – Introduction to Burp Proxy



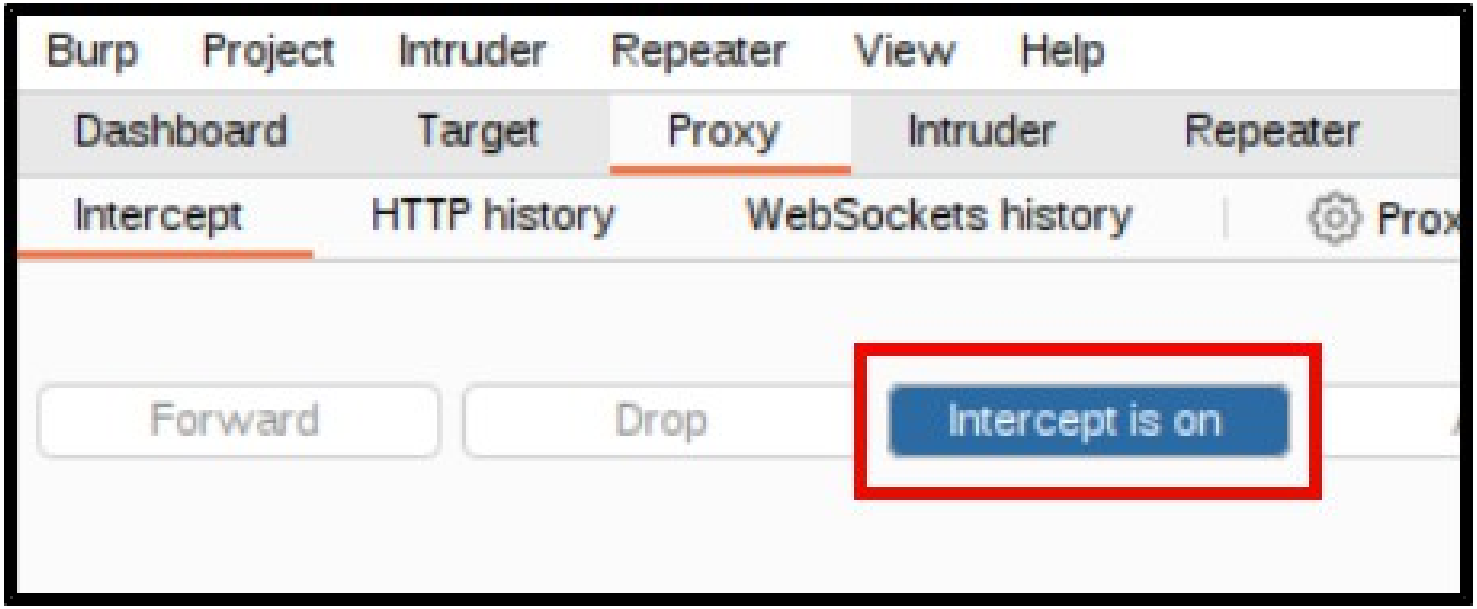
The Burp Proxy allows web traffic to be recorded, reviewed, and replayed. One thing to take note of is the Intercept → Intercept is on button

T8 – Introduction to Burp Proxy



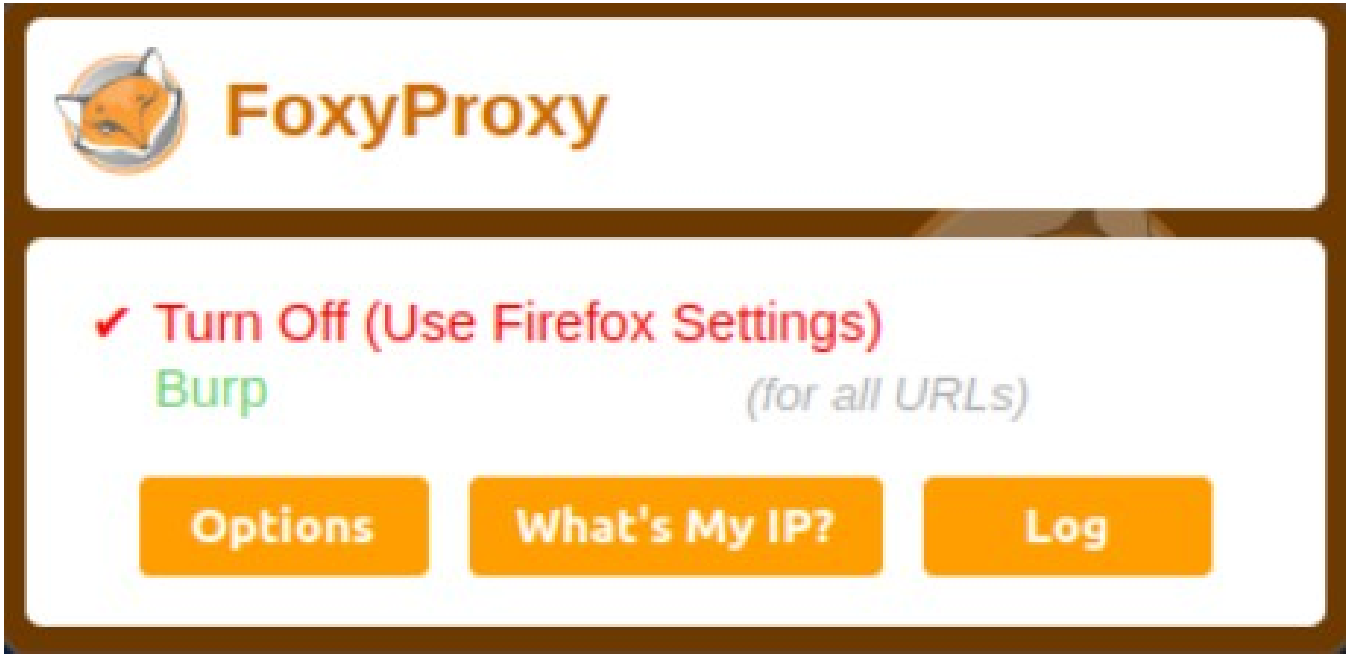
When Intercept is on, each web request has to be manually allowed or dropped before the next can be sent.

T8 – Introduction to Burp Proxy



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

T9 – Connecting through the Proxy

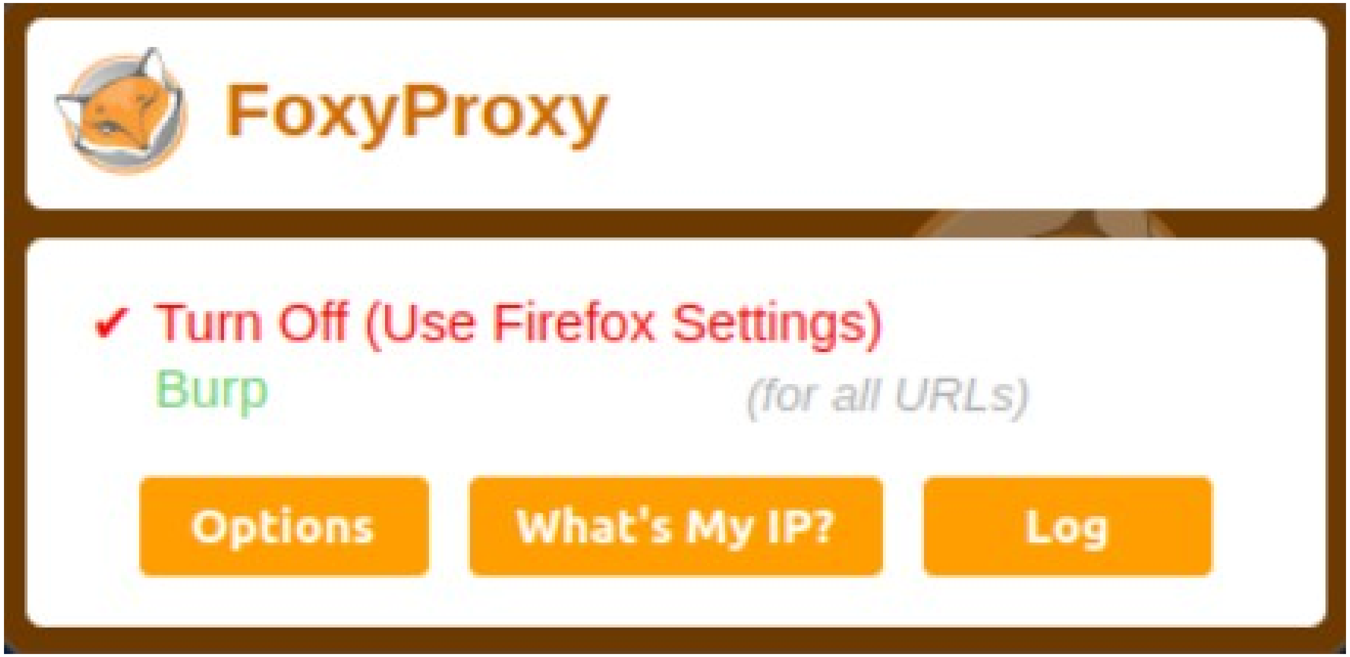

FoxyProxy

✓ Turn Off (Use Firefox Settings)

Burp (for all URLs)

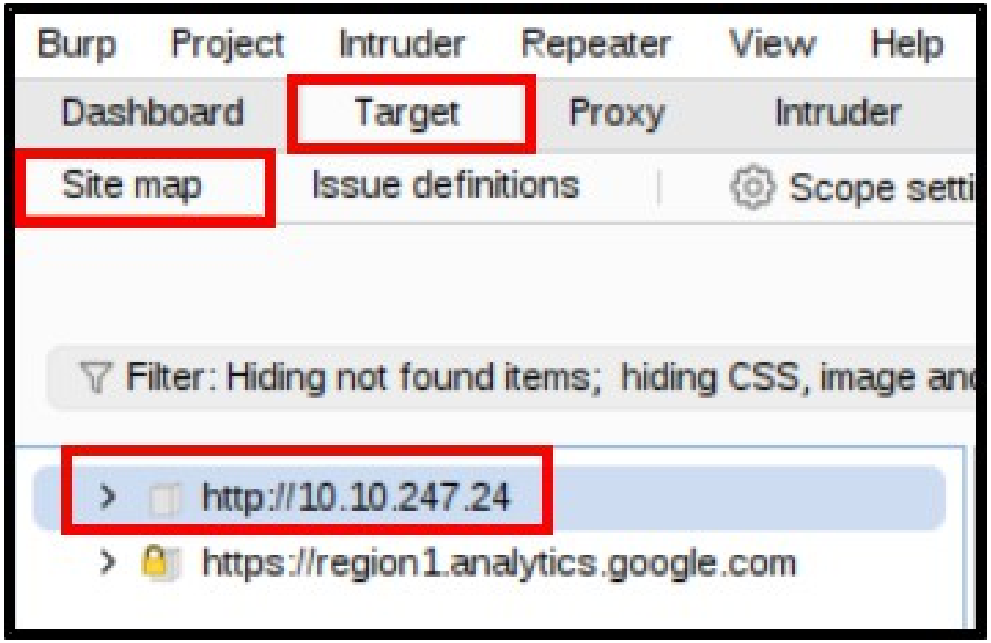
Before the release of the Burp Browser, Burp Proxy needed to be linked to a proxy configuration in a regular web browser, like Firefox or Chrome.

T9 – Connecting through the Proxy



One common browser extension used to configure a proxy is FoxyProxy.

T10 – Site Map and Issue Definitions



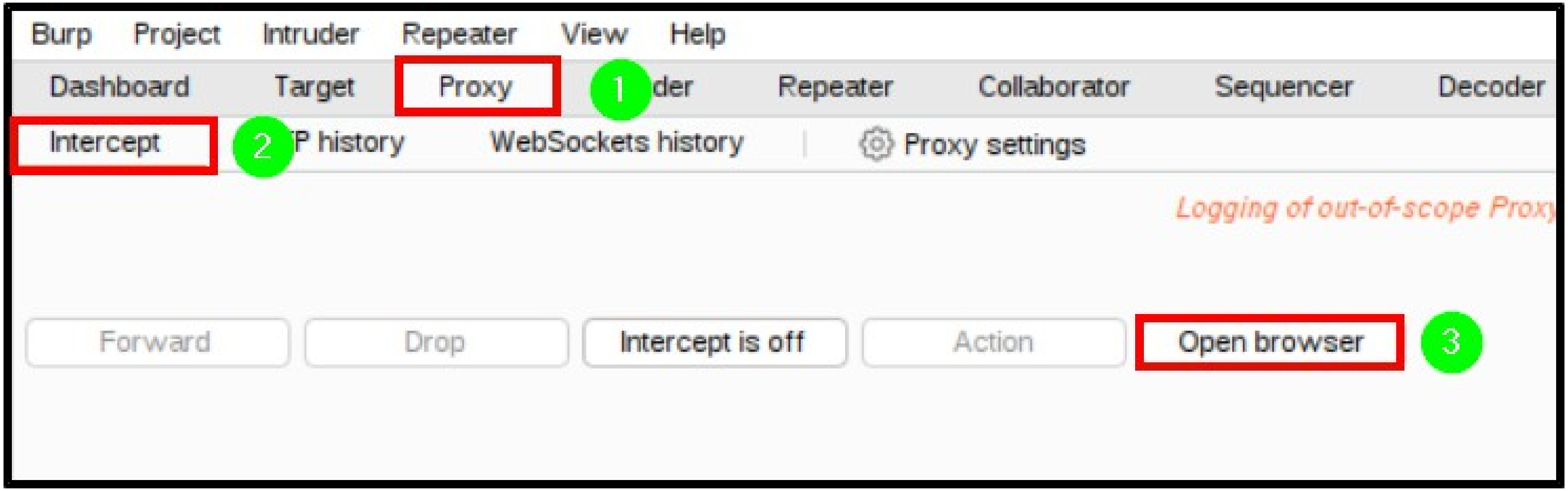
Filter: Hiding not found items; hiding CSS, image and

http://10.10.247.24

https://region1.analytics.google.com

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

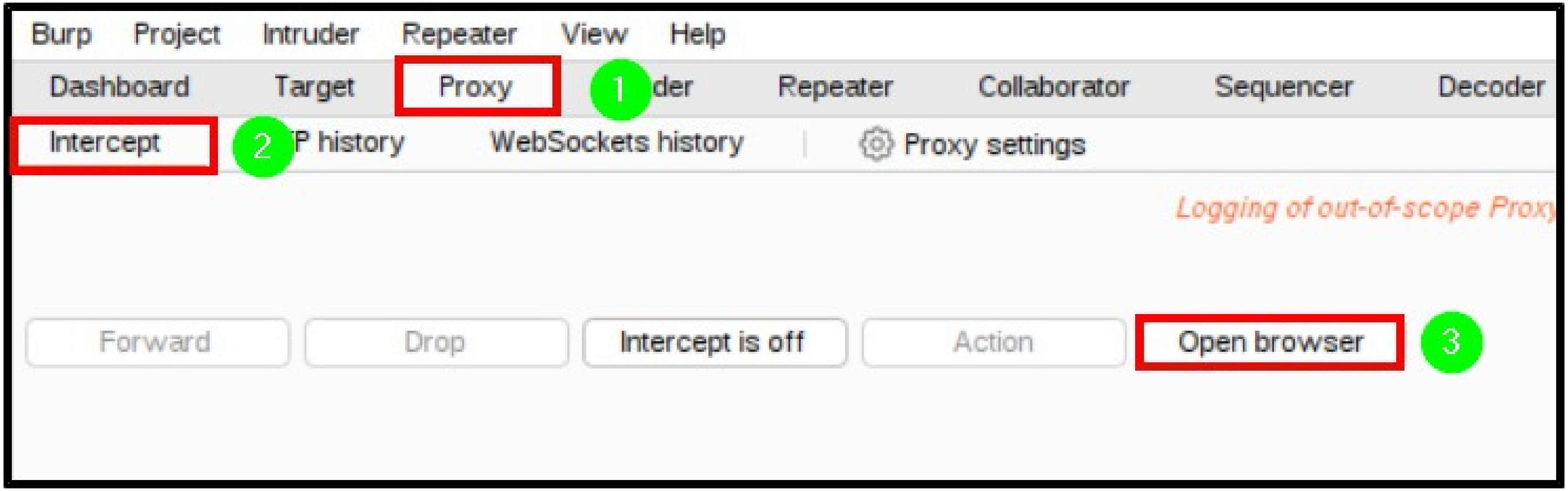
T11 – The Burp Suite Browser



Logging of out-of-scope Proxy

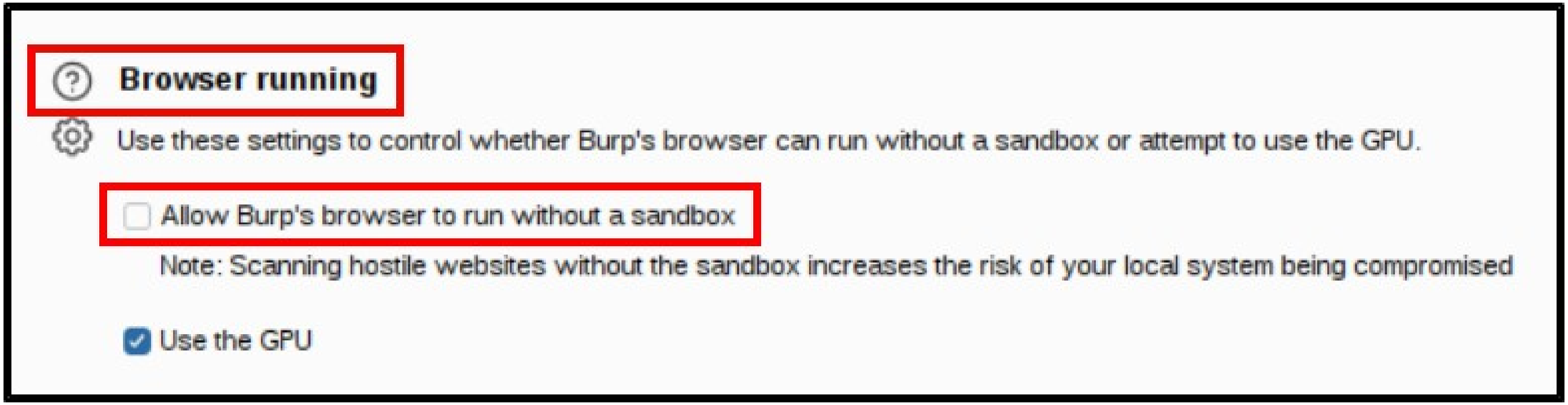
Using the Burp Suite Browser to proxy web traffic is the more convenient option over using regular web browser proxies.

T11 – The Burp Suite Browser



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

T11 – The Burp Suite Browser



Browser running

Use these settings to control whether Burp's browser can run without a sandbox or attempt to use the GPU.

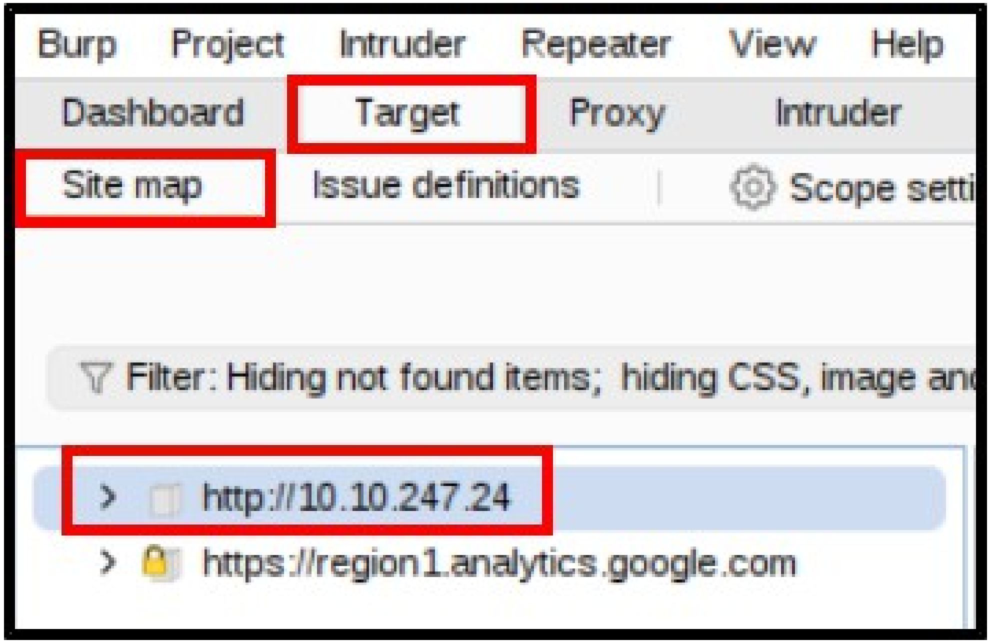
□ Allow Burp's browser to run without a sandbox

Note: Scanning hostile websites without the sandbox increases the risk of your local system being compromised

☑ Use the GPU

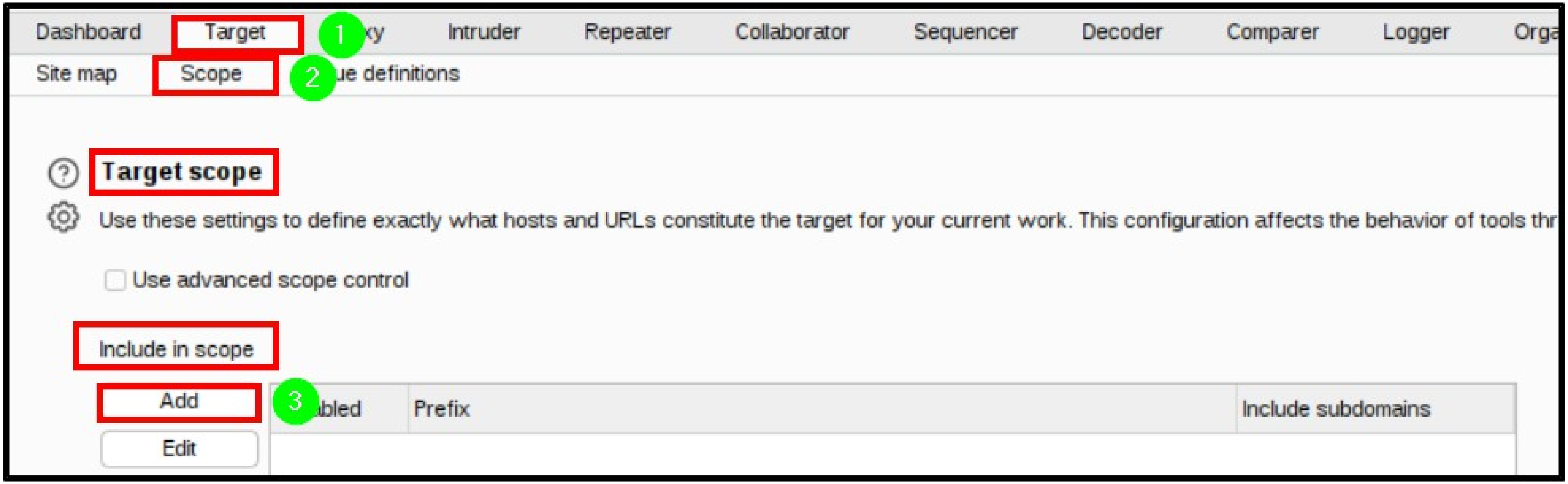
In the AttackBox, you'll have to go into Settings → Burp's browser → Browser running → Allow Burp's browser to run without a sandbox.

T12 – 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.

T12 – Scoping and Targeting



Target scope

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of tools thr

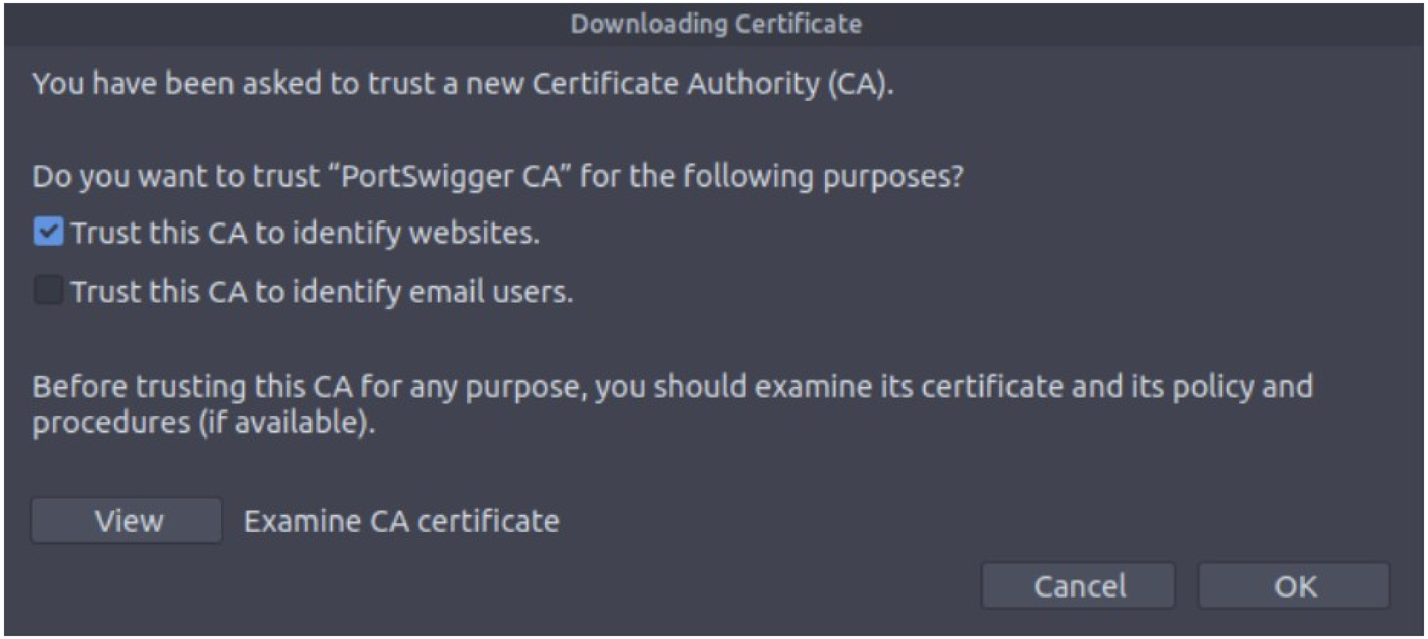
□ Use advanced scope control

Include in scope

bled	Prefix	Include subdomains

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

T13 – Proxying HTTPS



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust “PortSwigger CA” for the following purposes?

☑ Trust this CA to identify websites.

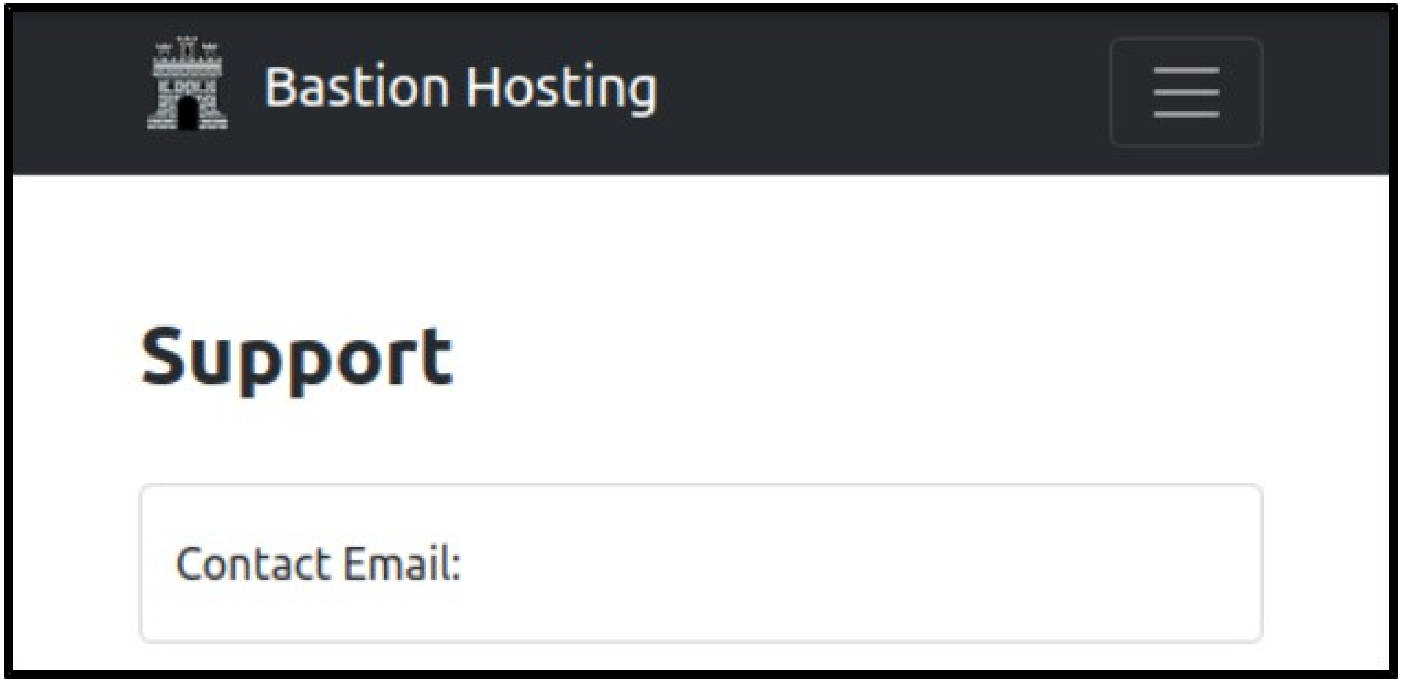
☐ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

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.

T14 – Example Attack



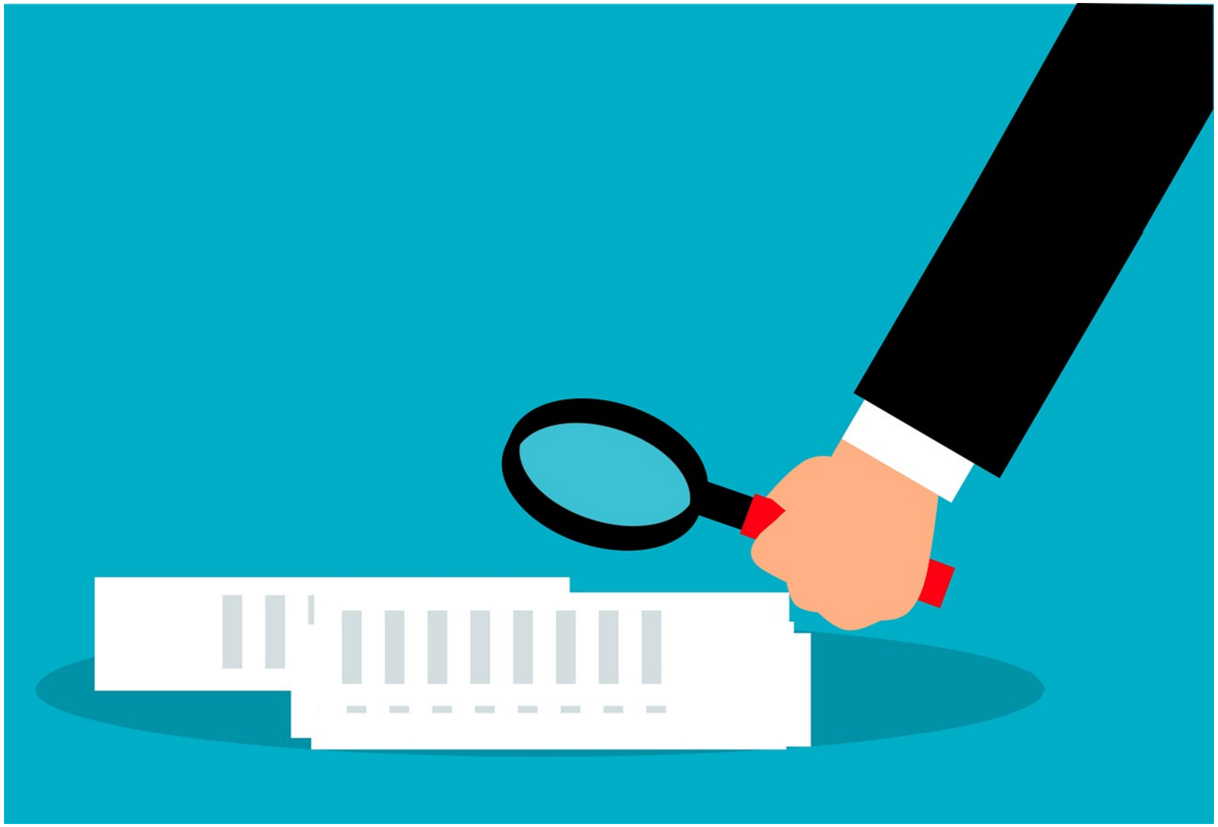
Bastion Hosting

Support

Contact Email:

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!