



What is Burp Suite

„Burp or Burp Suite is **a set of tools used for penetration testing of web applications.**“

~ GeeksforGeeks

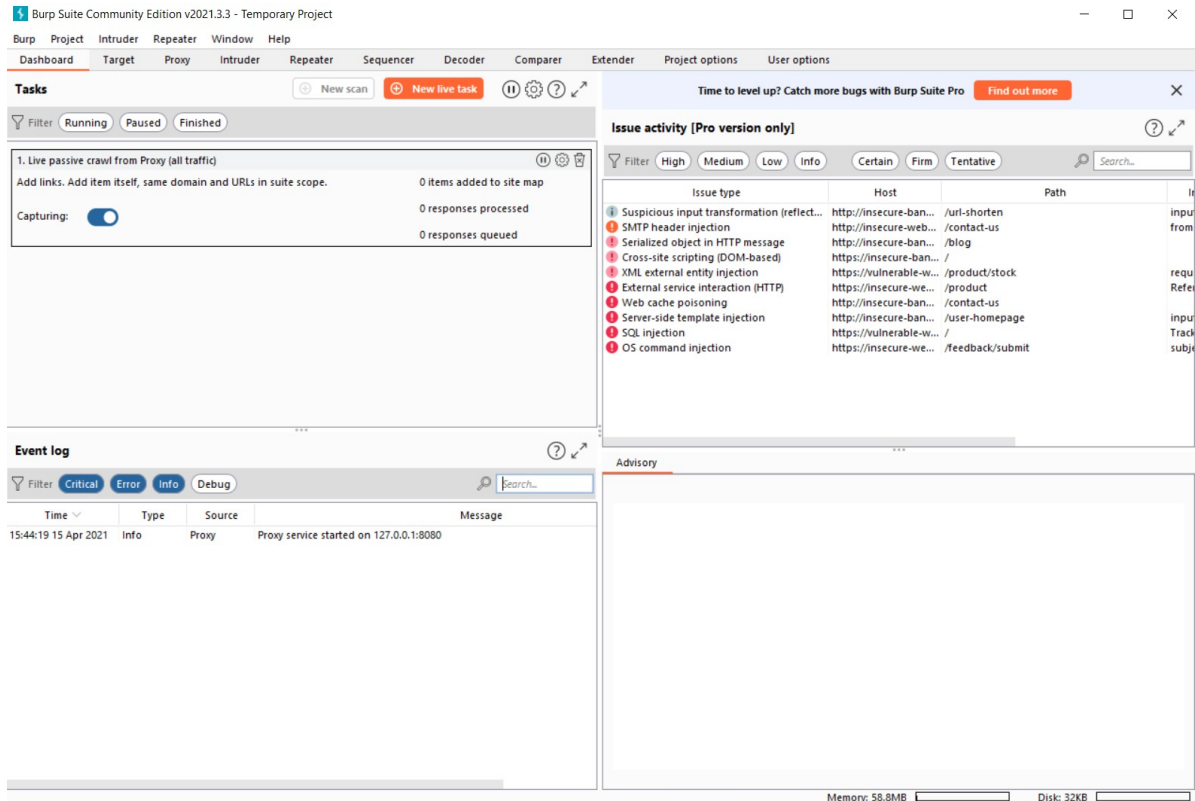
Burp Suite comes in 2 Variants.

=> A Free „Community Edition“

=> A „Professional Edition“ for which one has to Pay.

Burp Suite is available for all Common Operating Systems. Burp Suite comes with an Internal Proxy which is Used to Capture Network Packages.

First Look on Burpsuite



As We can See, Burp Suite has Several Tabs for several Purposes. In Detail we have:

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Your Overview for Burp-Suite

Here you can Create a Sitemap for a Website + Add A Scope to a speicific Website

When you captured a Request, you can see it here

Burp-Suite internal Fuzzer

Modify/Edit Income Data Packages

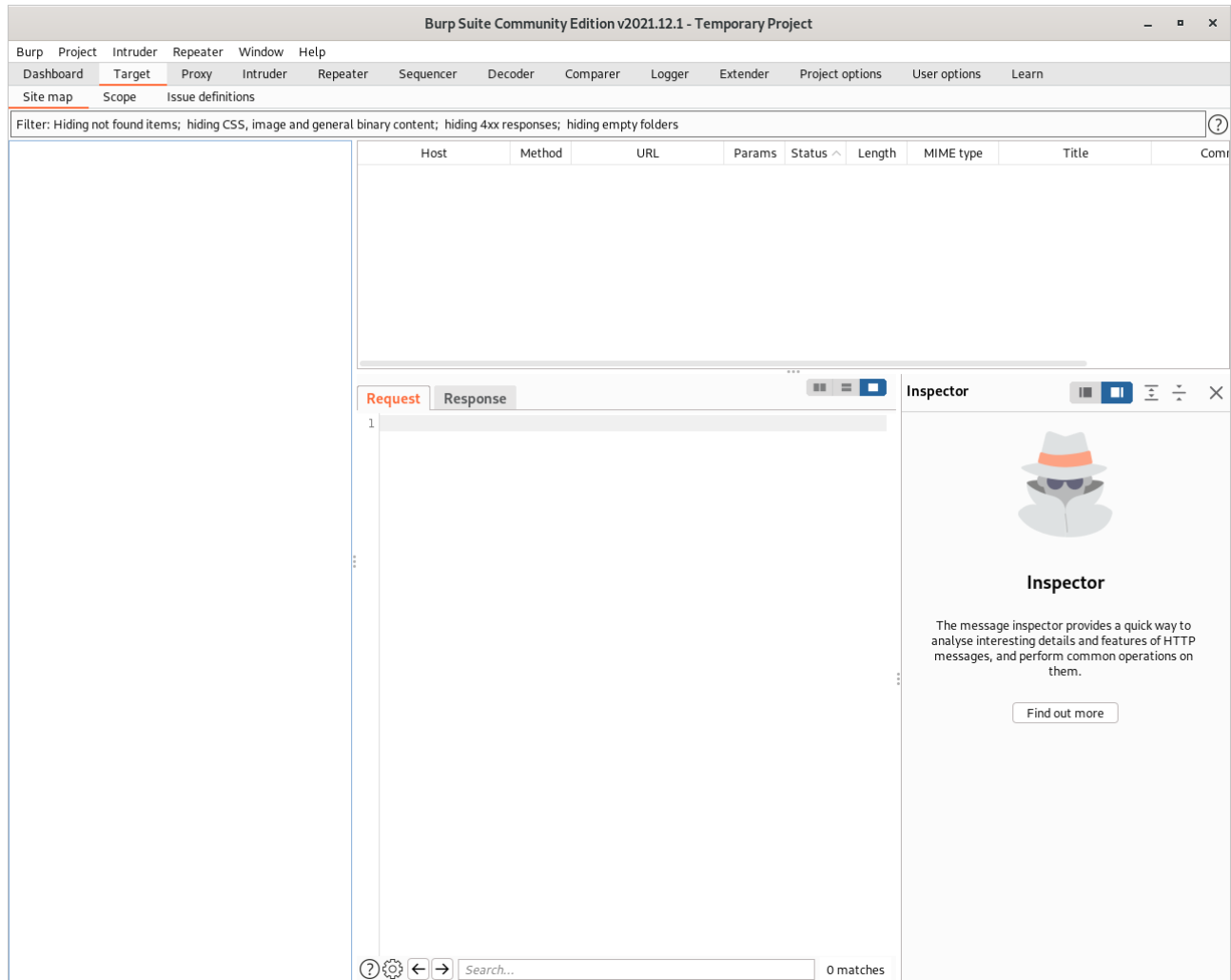
Sequencer allows us to measure the entropy (or randomness, in other words) of "tokens"

En/decode Strings

Compares The Input of Two Boxes, byte by byte

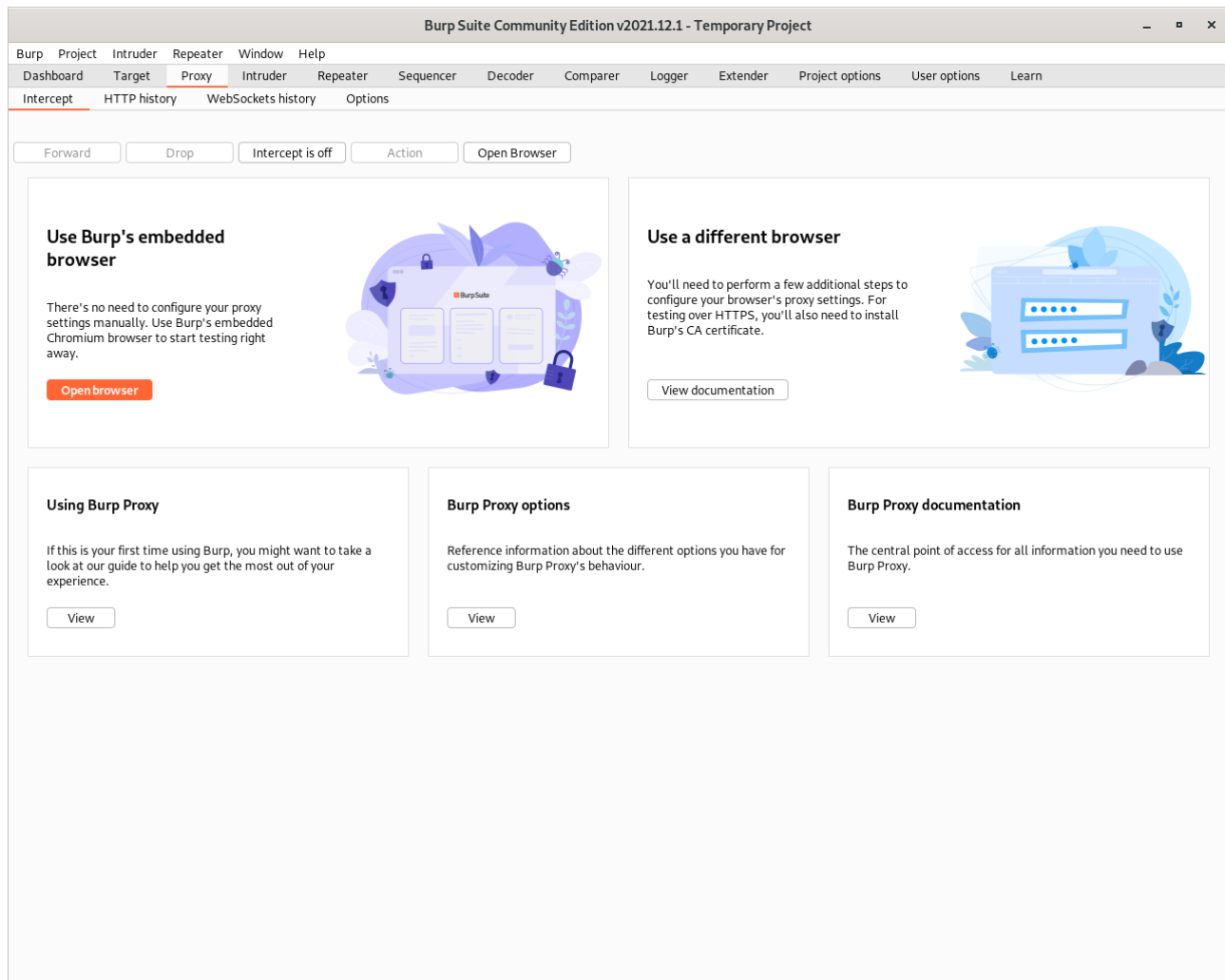
Create own Modules for Burp Suite

Deeper Look:

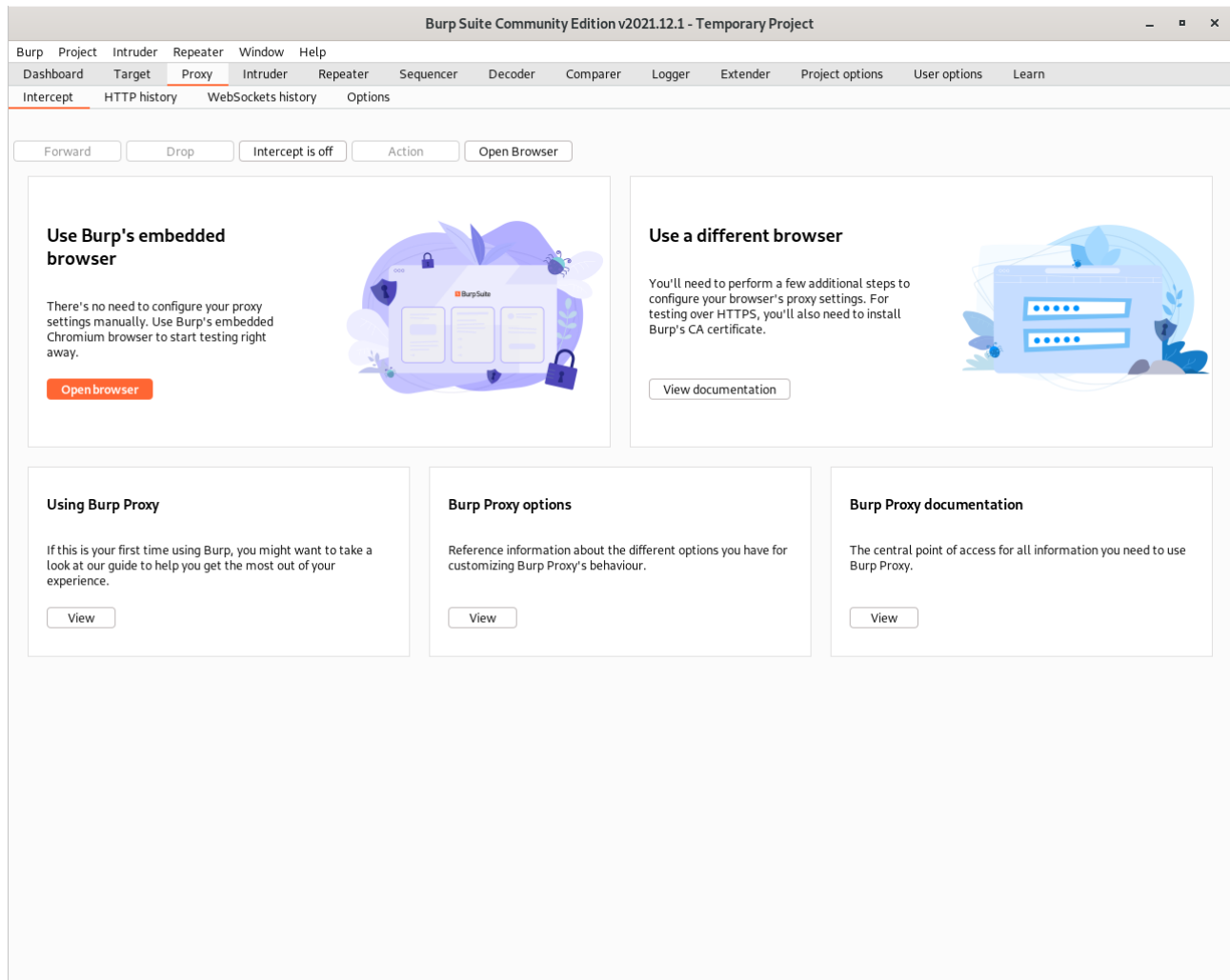


Lets Begin with „Target“.

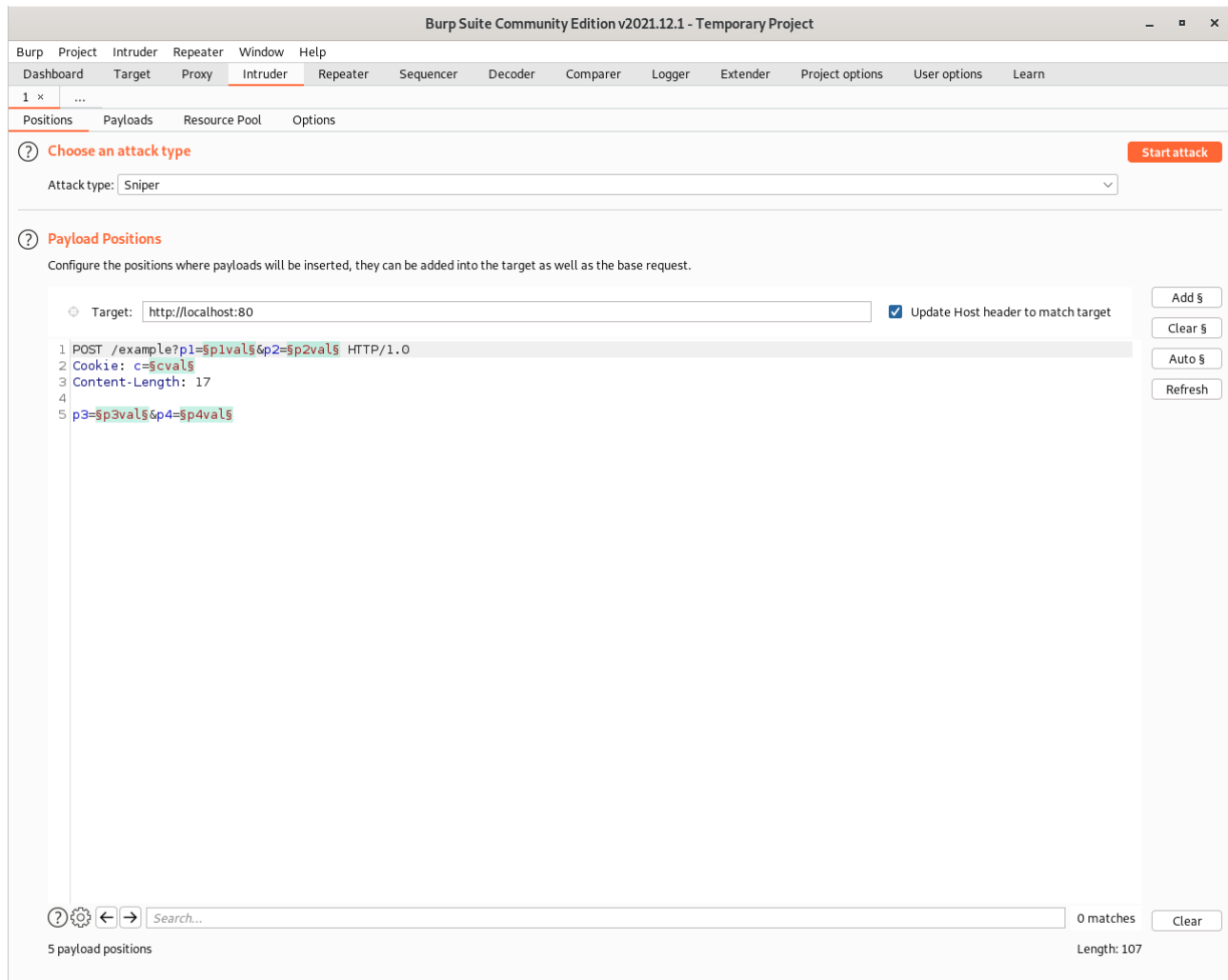
When you started scanning a Target, you may get some stuff you don't want from other websites as well. The Target Function can help you with this issue, with the „Scope“ function. Also you can Create a Sitemap of a Target here for perfect Enumeration.



This is the Proxy Area. Here you will Find all of your Captured Network Packages. From here on you can send them to Every other Sub-Tab of Burp Suite. (Remember to Turn Intercept on/off after/before using :))



This is the Proxy Area. Here you will Find all of your Captured Network Packages. From here on you can send them to Every other Sub-Tab of Burp Suite. (Remember to Turn Intercept on/off after/before using :)



Here we come to one of the most important functions of Burp Suite. The Intruder Function. The Intruder Function is the intern Fuzzing Tool of Burp Suite. It allows us to take a request (most likely captured) and sends it slightly altered back to get a result.

FUZZER:

A fuzzer is a program which injects automatically semi-random data into a program/stack and detect bugs

This Tab contains 4 Sub-Tabs to use.

- => Position
- => Payloads
- => Resource Pool
- => Options

1. **Position:**

The Positions Sub-Tab includes The Choice of the Attack (Sniper, Battering Ram, Pitchfork, Cluster bomb) as well as the Payload Position.

Sniper Attack

Sniper Attack uses 1 Set of Payloads

For Each Position you defined, the Payloads will be inserted, one by one until all positions have been tried.

This quality makes Sniper very good for single-position attacks (e.g. a password brute force if we know the username or fuzzing for API endpoints).

Battering Ram Attack

Battering ram uses 1 set of Payloads

Unlike Sniper, the Battering ram puts the same payload in every position rather than in each position in turn.

Pitchfork Attack

It may help to think of Pitchfork as being like having numerous Snipers running simultaneously.

Where Sniper uses one payload set (which it uses on every position simultaneously),

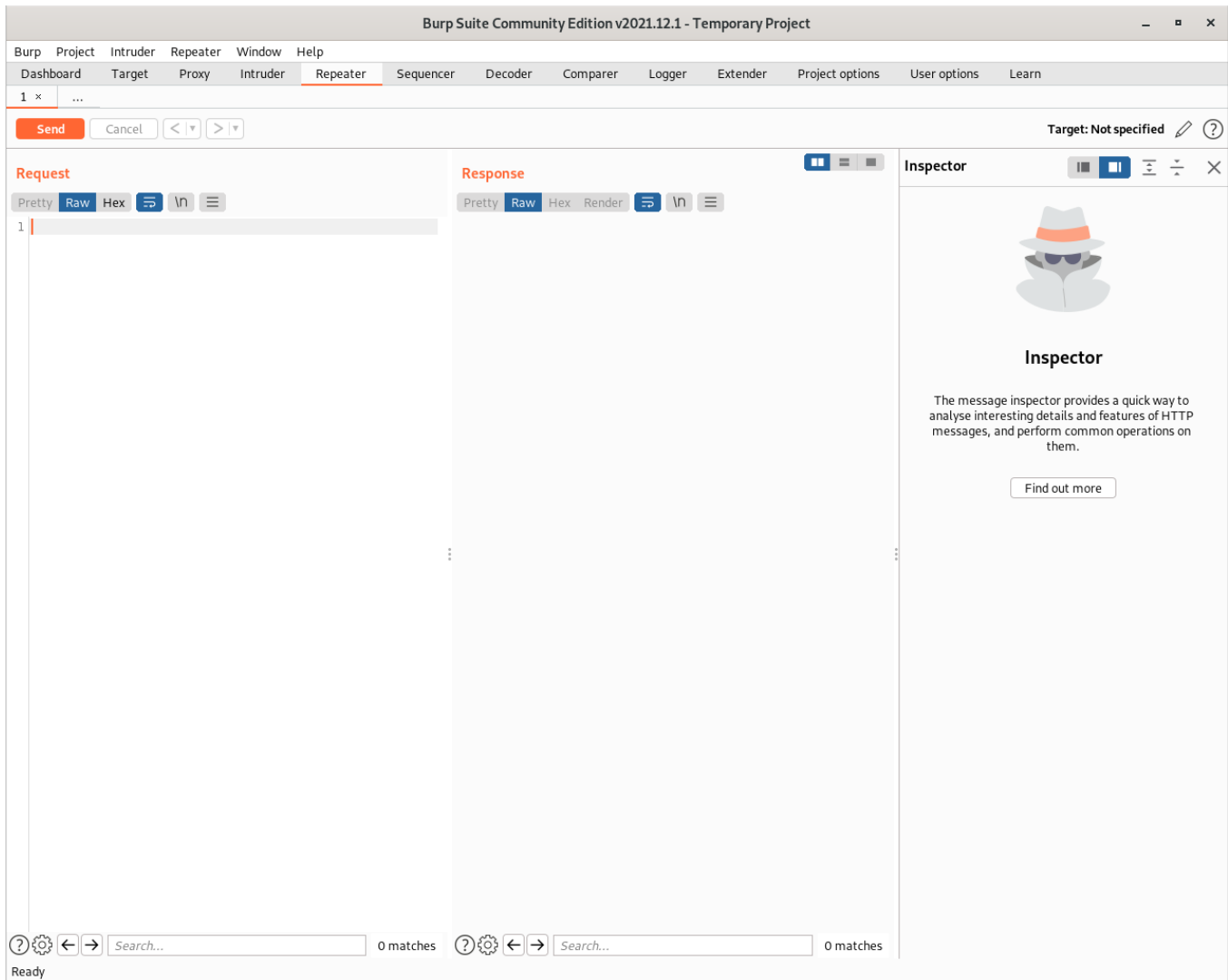
Pitchfork uses one payload set per position (up to a maximum of 20) and iterates through them all at once.

Pitchfork takes the first item from each list and puts them into the request, one per position

Cluster Bomb Attack

Cluster bomb iterates through each payload set individually, making sure that every possible combination of payloads is tested. this will try every combination of values.

Sn0wF0x CTF - Knowledge



The Repeater Allows us to craft and/or manipulate intercepted Requests as often as we want. It also has a Function to quickly see the Response of altered Requests.

The screenshot shows the Burp Suite Community Edition v2021.12.1 interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main menu bar has Dashboard, Target, Proxy, Intruder, Repeater, Sequencer (selected), Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. Below the main menu, there are sub-tabs: Live capture, Manual load, and Analysis options. The Sequencer tab is active, displaying three sections: 'Select Live Capture Request', 'Token Location Within Response', and 'Live Capture Options'.

Select Live Capture Request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".

#	Host	Request
---	------	---------

Buttons: Remove, Clear, Start live capture

Token Location Within Response

Select the location in the response where the token appears.

☐ Cookie:

☐ Form field:

☒ Custom location:

Live Capture Options

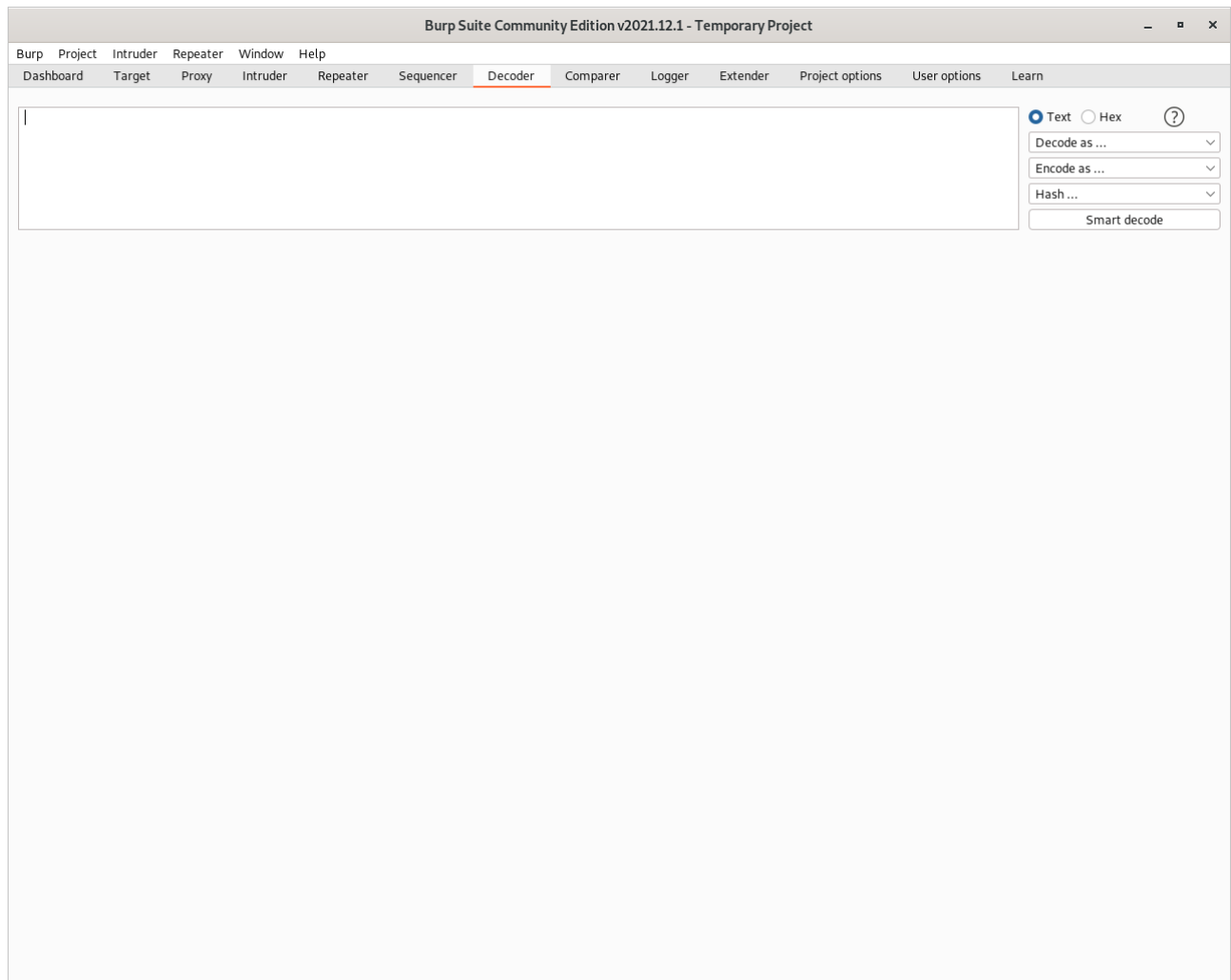
These settings control the engine used for making HTTP requests and harvesting tokens when performing the live capture.

Number of threads:

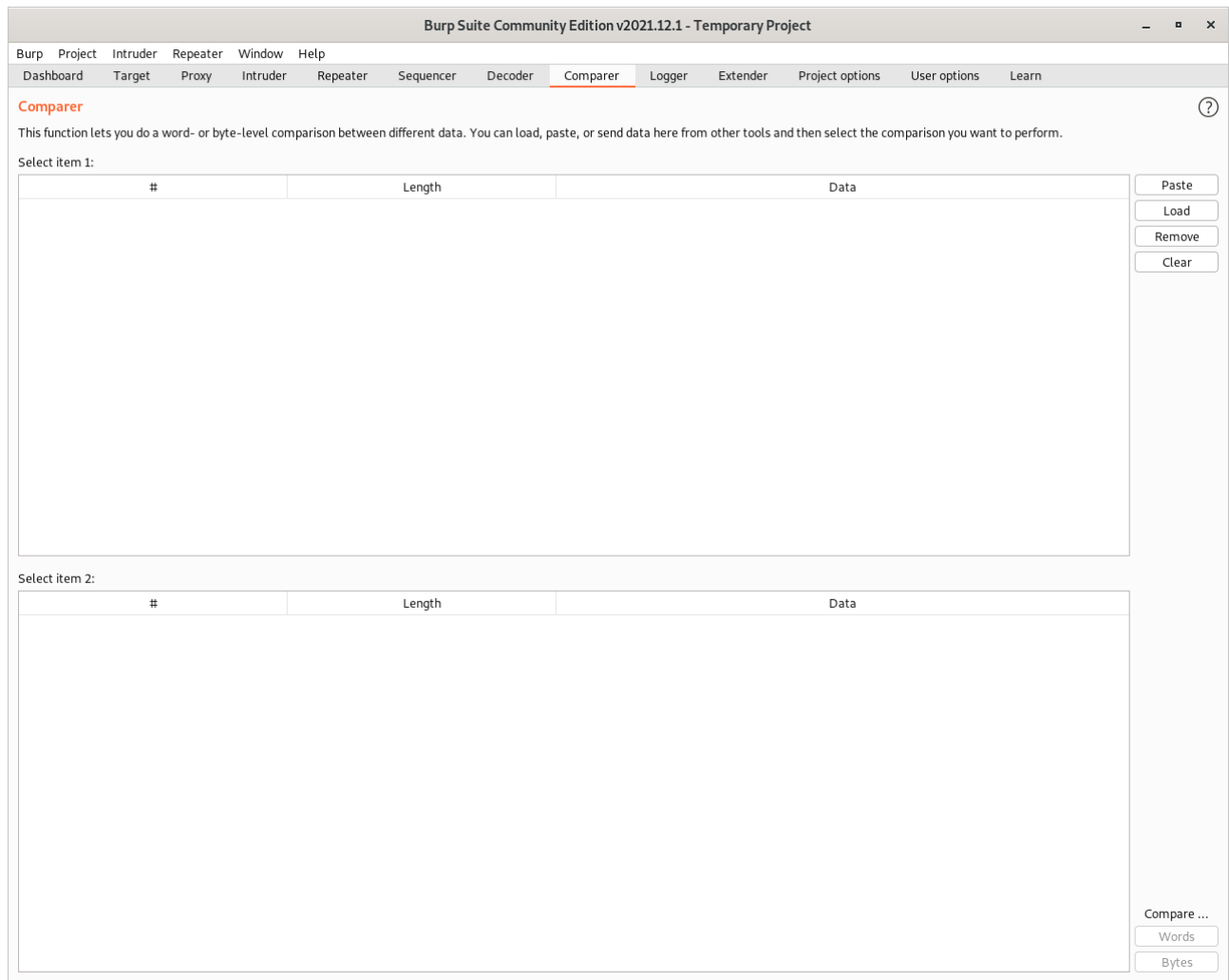
Throttle between requests (milliseconds):

☒ Ignore tokens whose length deviates by characters

The Sequencer allows us to measure the entropy (or randomness, in other words) of "tokens"

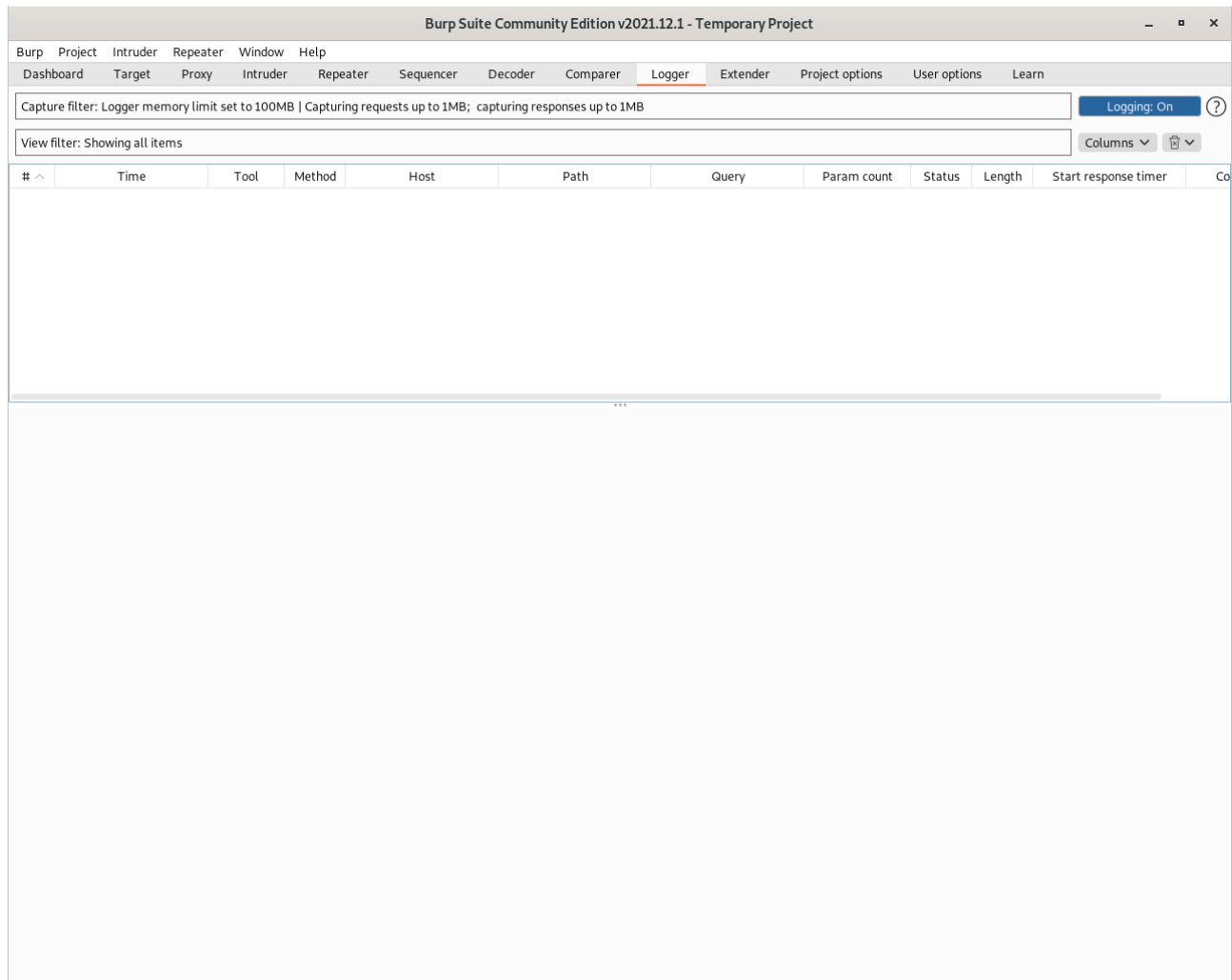


Similar to „Cyberchef“ the Decoder En/Decodes Values.

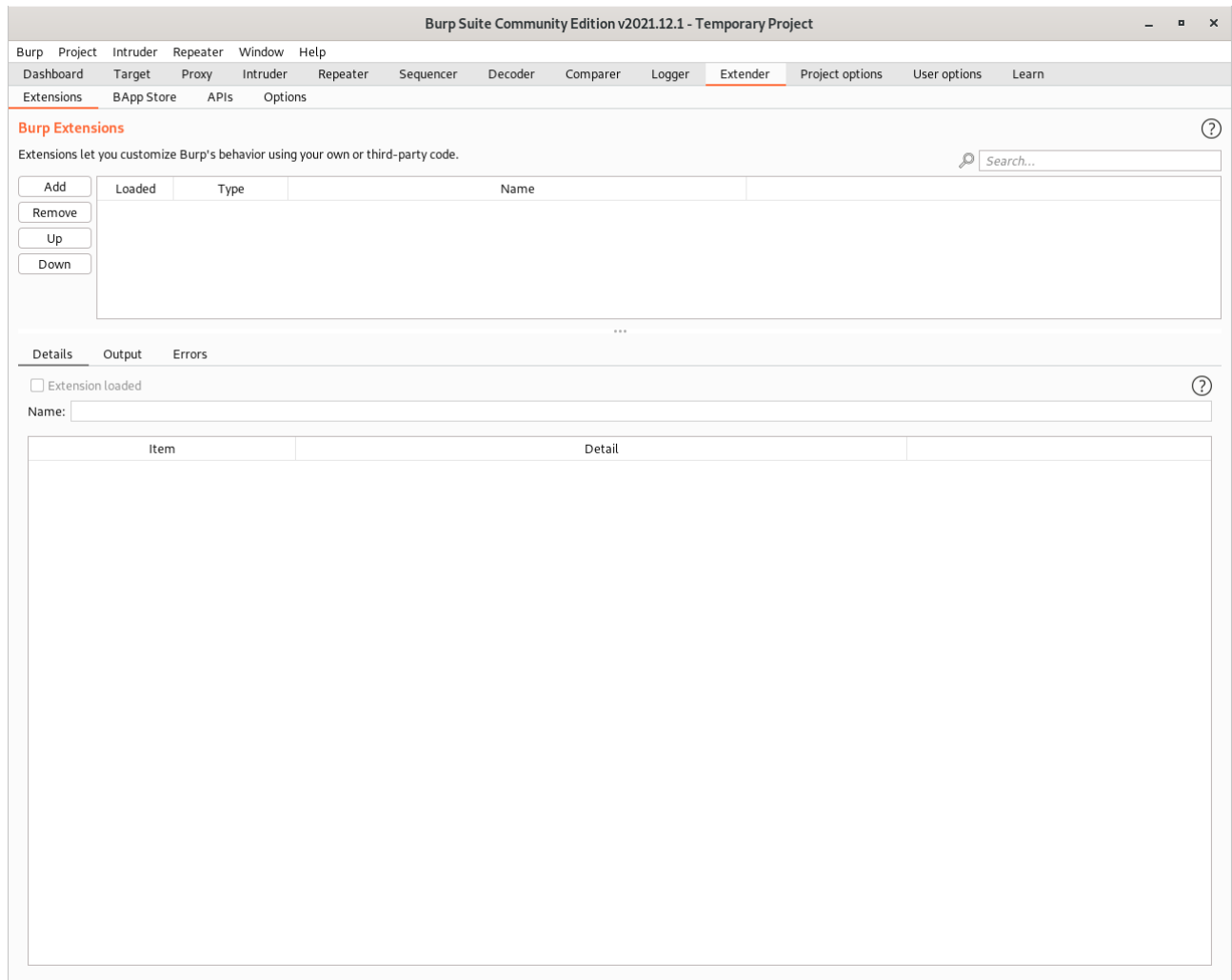


The Comparer does, what it sounds like. It compares the Input of the Two Boxes and shows you the Differences.

Sn0wF0x CTF - Knowledge



The Logger is Pretty much Self Explained I guess. You can also filtered Logged Data.



If (by Chance) you will feel the need to include Functions to Burp Suite, that are not already there, here is your spot. You can Include new Cool Stuff that might (or might not) help you.

