



What is Burp Suite

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

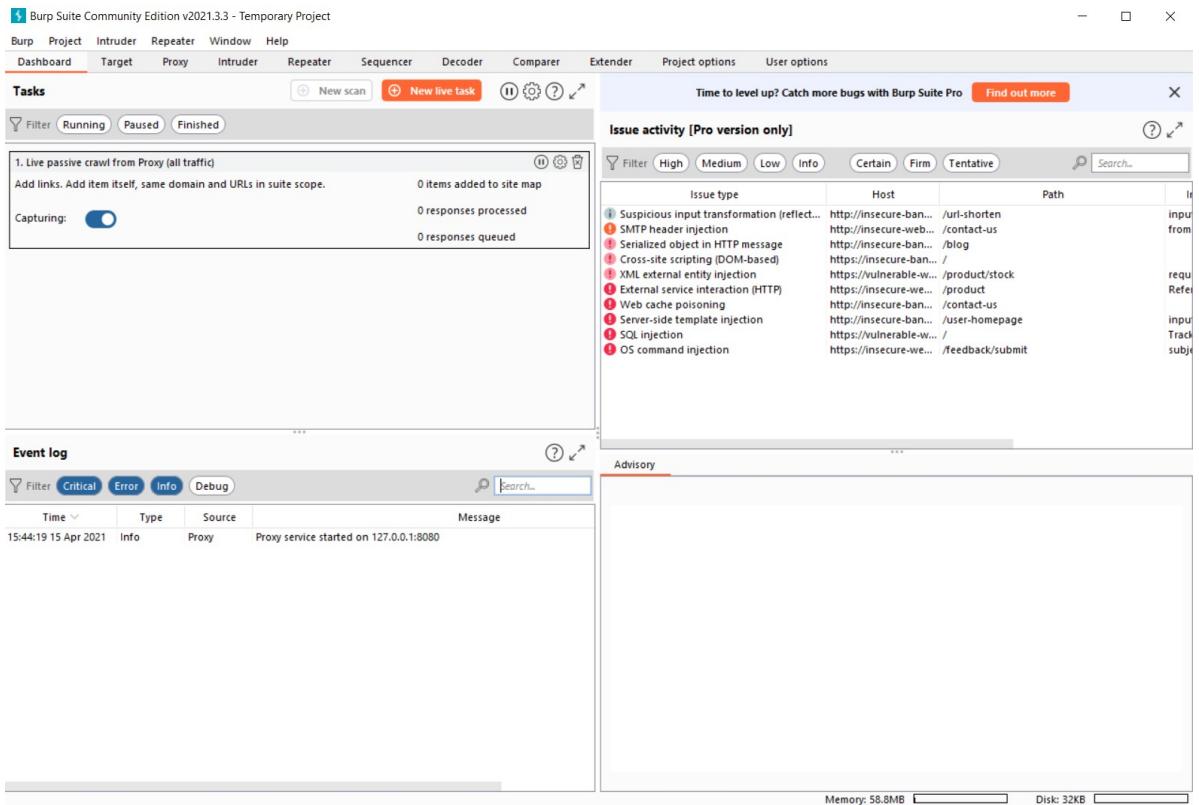
~ GeeksforGeeks

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

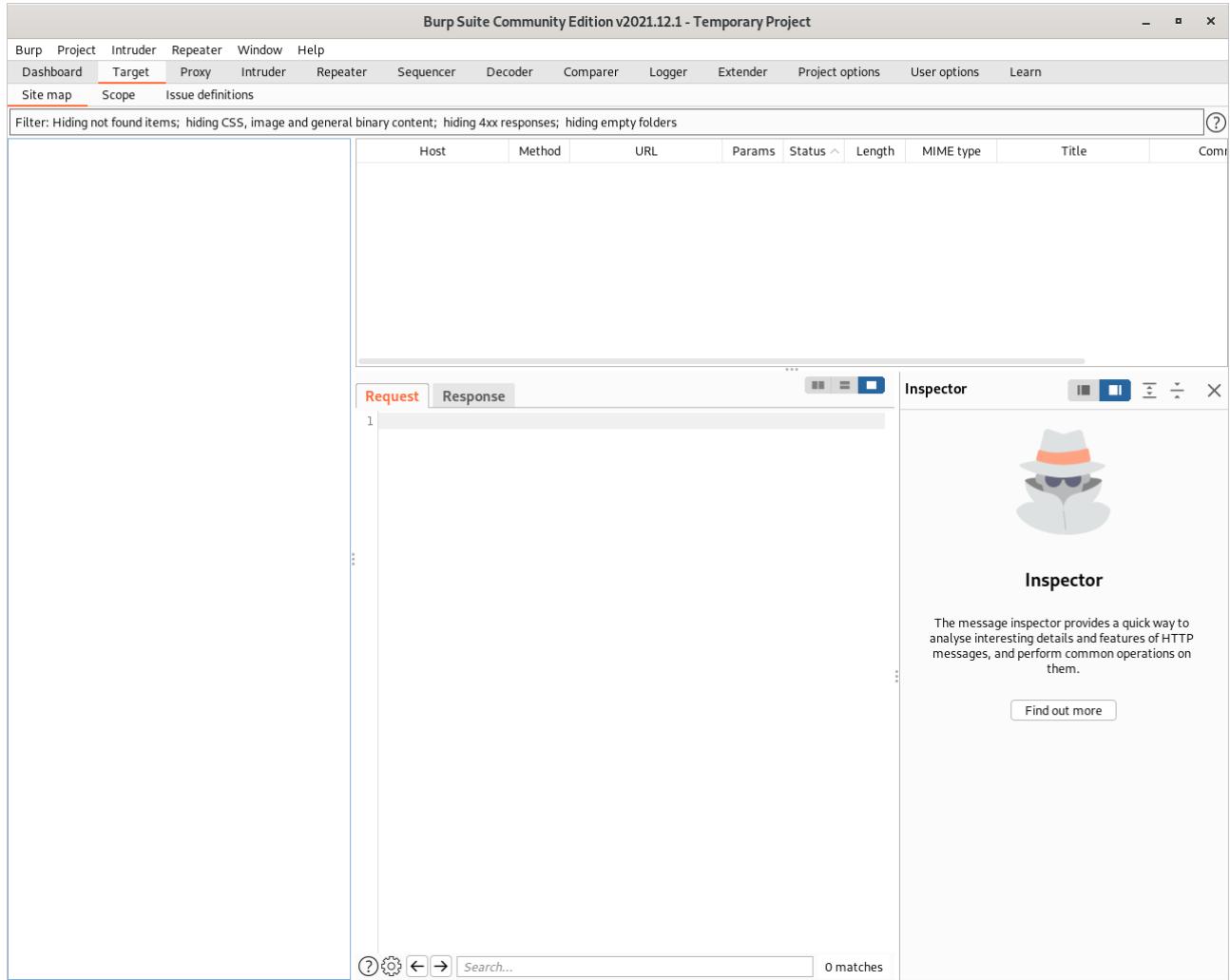
Sequencer allows us to measure the entropy (or randomness, in other words) of "tokens"

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.

Sn0wF0x CTF - Knowledge

Burp Suite Community Edition v2021.12.1 - Temporary Project

Intercept

Forward Drop Intercept is off Action Open Browser

Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

Open browser

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

View documentation

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

View

Burp Proxy options

Reference information about the different options you have for customizing Burp Proxy's behaviour.

View

Burp Proxy documentation

The central point of access for all information you need to use Burp Proxy.

View

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 :))

Sn0wF0x CTF - Knowledge

Burp Suite Community Edition v2021.12.1 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept **HTTP history** WebSockets history Options

Forward Drop Intercept is off Action Open Browser

Use Burp's embedded browser

There's no need to configure your proxy settings manually. Use Burp's embedded Chromium browser to start testing right away.

[Open browser](#)

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

[View documentation](#)

Using Burp Proxy

If this is your first time using Burp, you might want to take a look at our guide to help you get the most out of your experience.

[View](#)

Burp Proxy options

Reference information about the different options you have for customizing Burp Proxy's behaviour.

[View](#)

Burp Proxy documentation

The central point of access for all information you need to use Burp Proxy.

[View](#)

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 :))

Sn0wF0x CTF - Knowledge

The screenshot shows the Burp Suite interface with the Intruder tab selected. The target is set to `http://localhost:80`. A POST request is displayed with payload positions `p1=$p1val$`, `p2=$p2val$`, `p3=$p3val$`, and `p4=$p4val$`. The payload positions section indicates 5 payload positions with a total length of 107 bytes.

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),

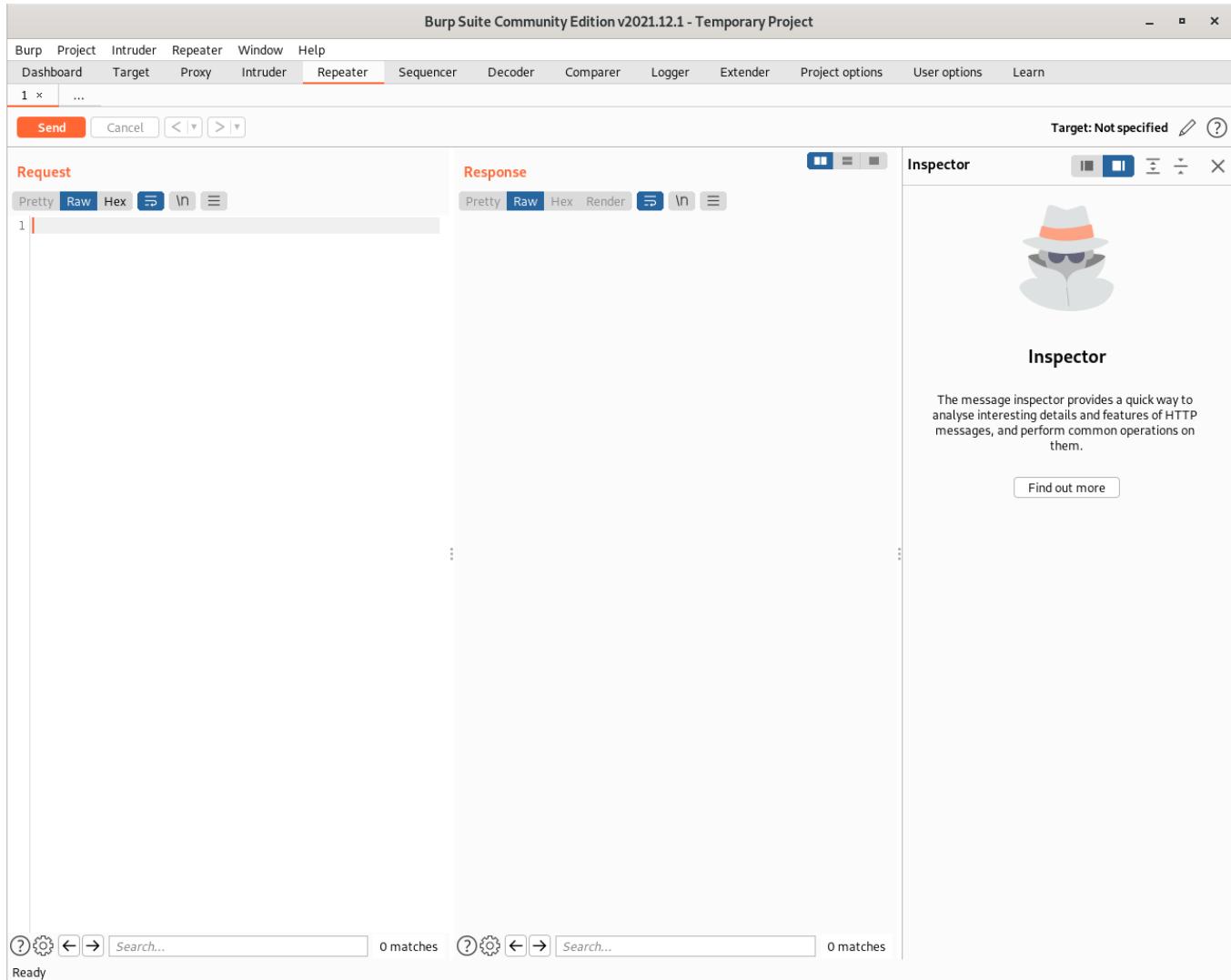
Pitchfork uses one payload set per position (up to a maximum of 20) and iterates through them all at once.

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

Cluster Bomb Attack

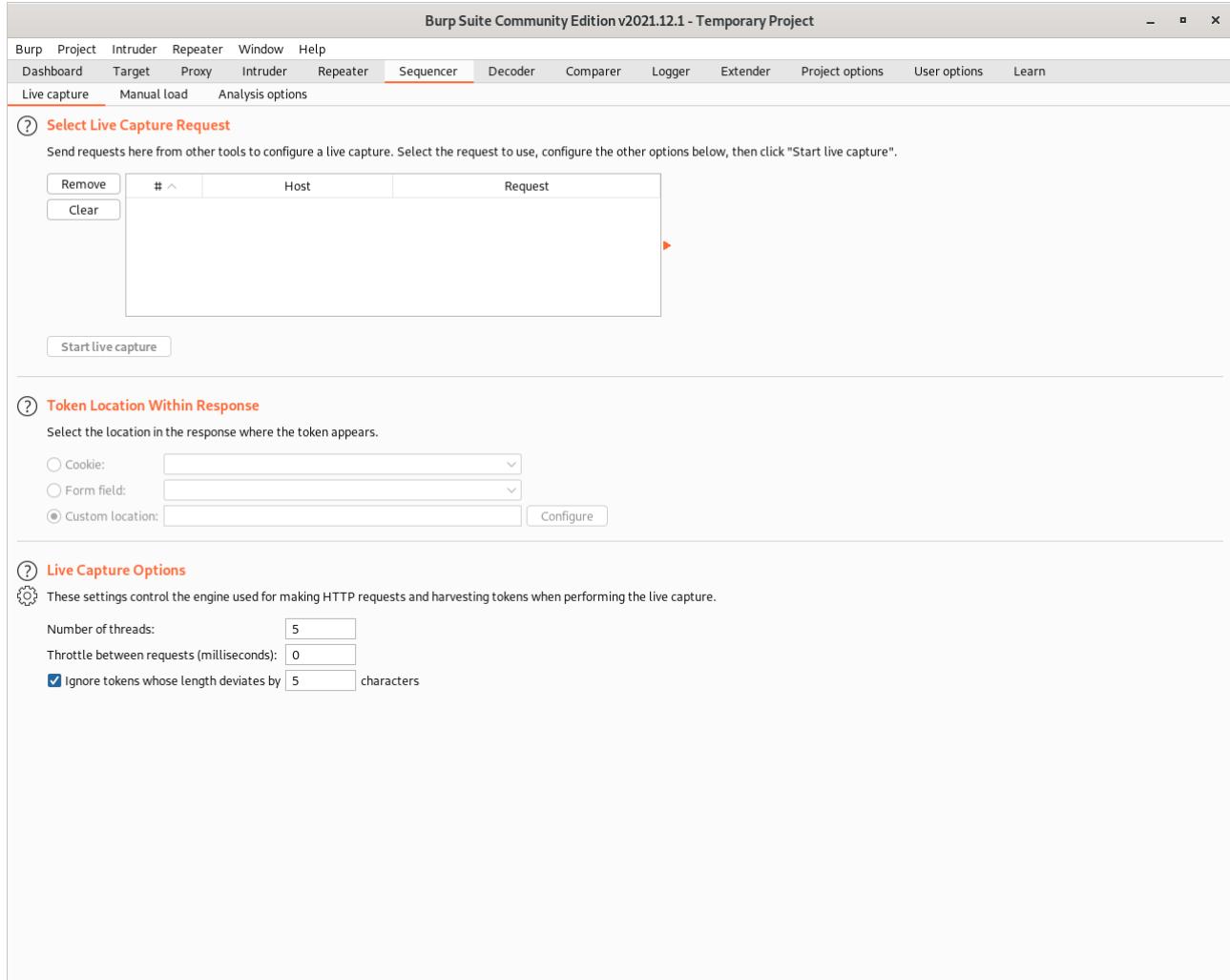
Cluster bomb iterates through each payload set individually, making sure that every possible combination of payloads is tested. this will try every combination of values.

Sn0wF0x CTF - Knowledge



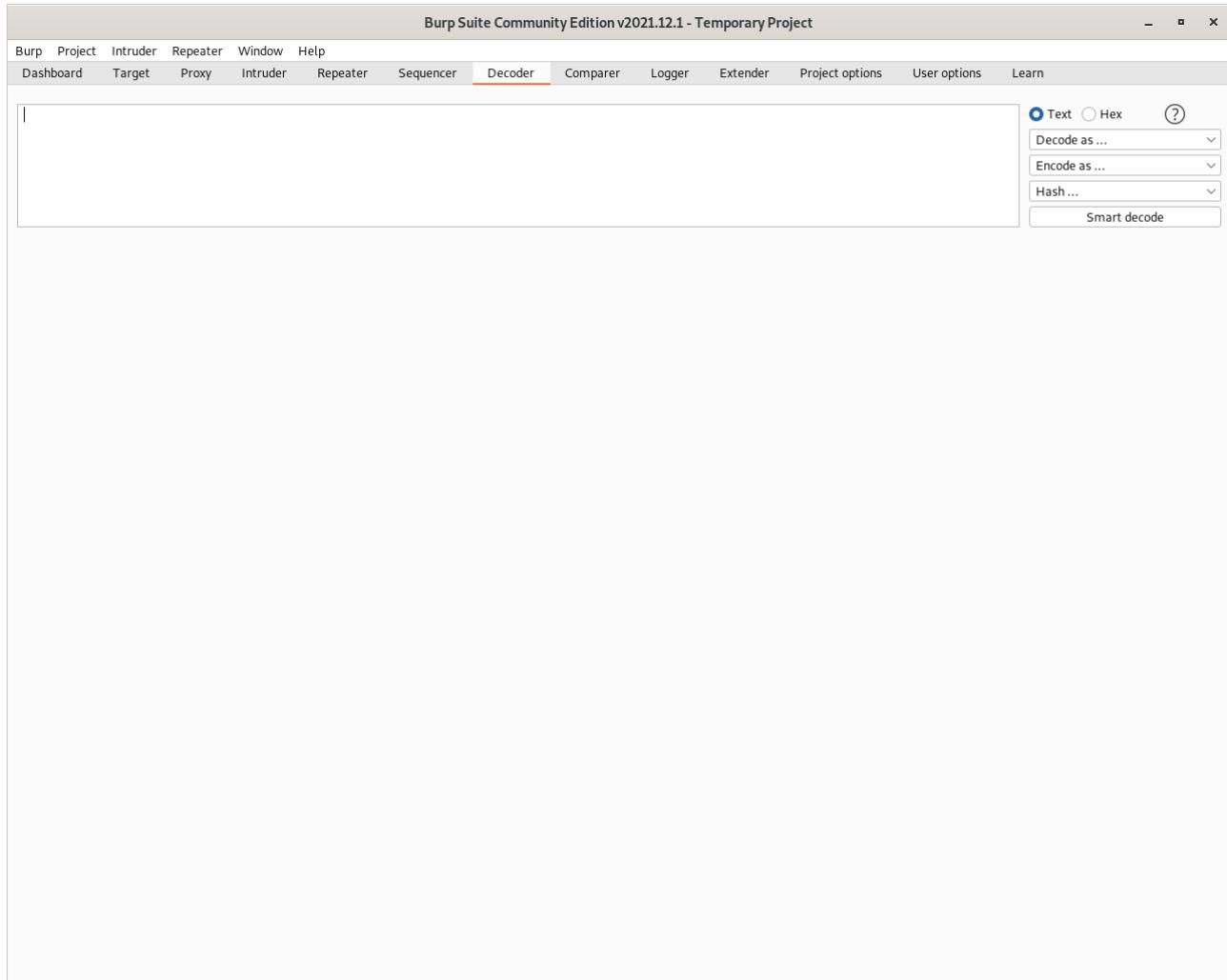
The Repeater Allows us to craft and/or manipulate intercepted Requests as often as we want. It also has a Function to quickly see the Response of altered Requests.

Sn0wF0x CTF - Knowledge



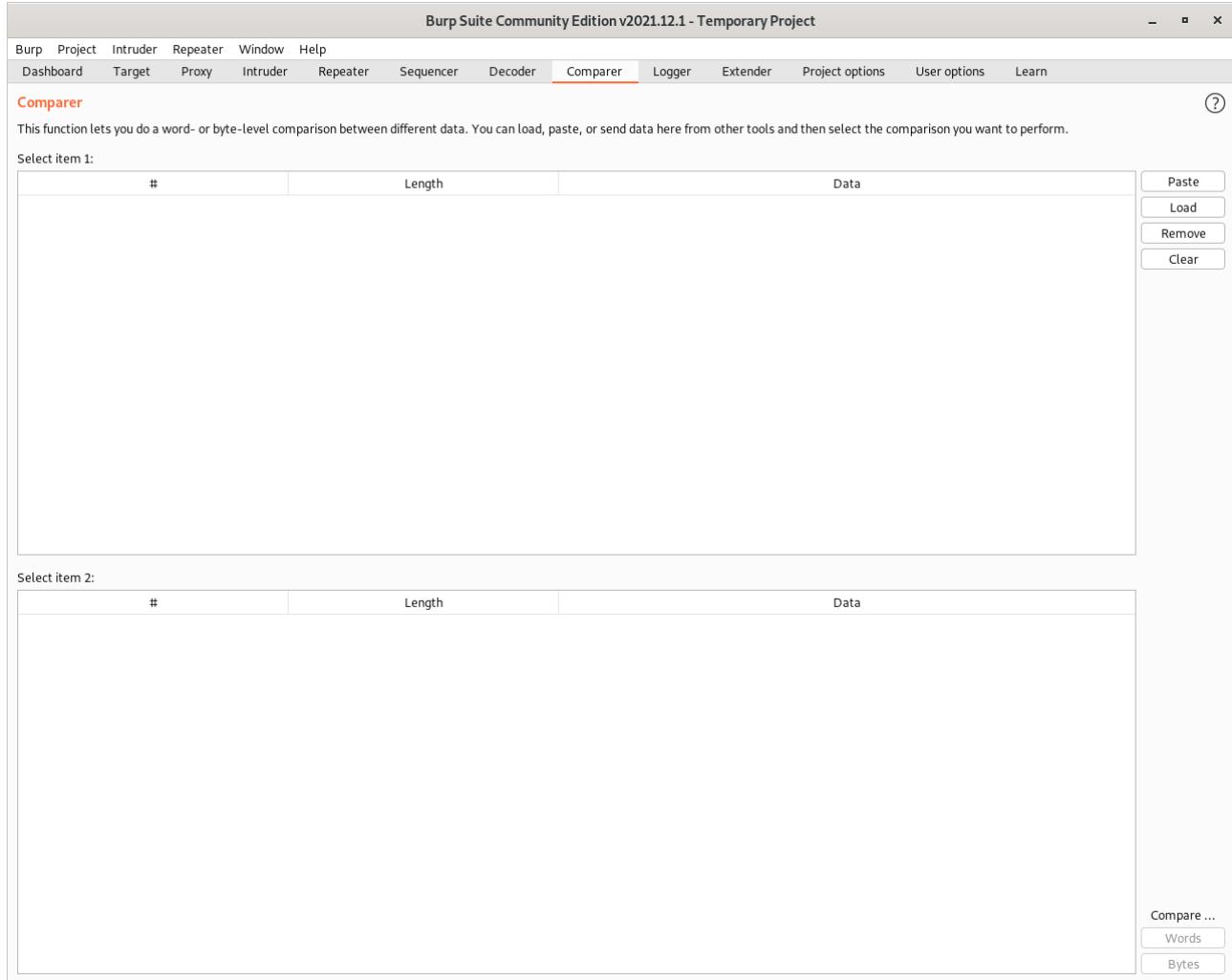
The Sequencer allows us to measure the entropy (or randomness, in other words) of "tokens"

Sn0wF0x CTF - Knowledge



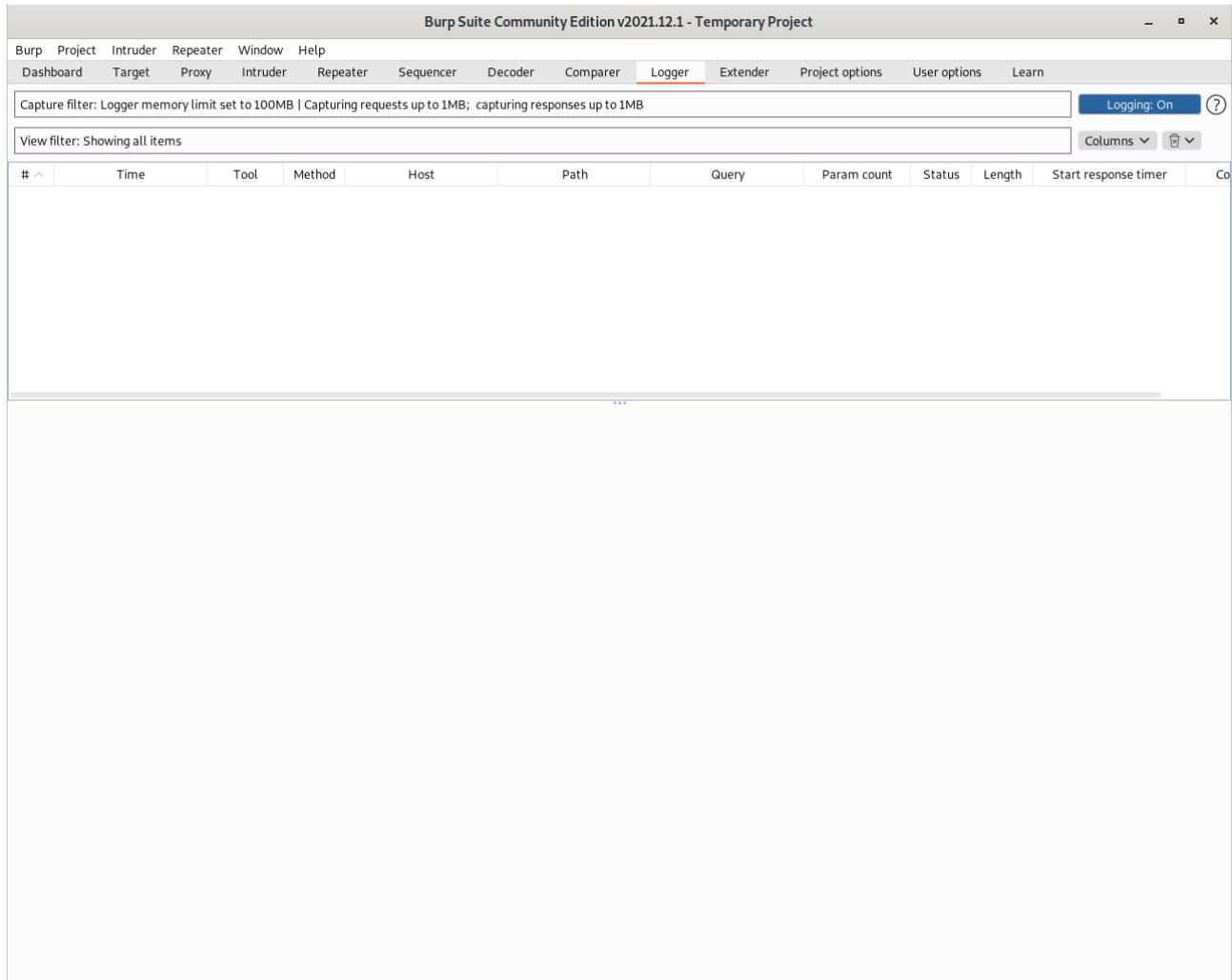
Similar to „Cyberchef“ the Decoder En/Decodes Values.

Sn0wF0x CTF - Knowledge



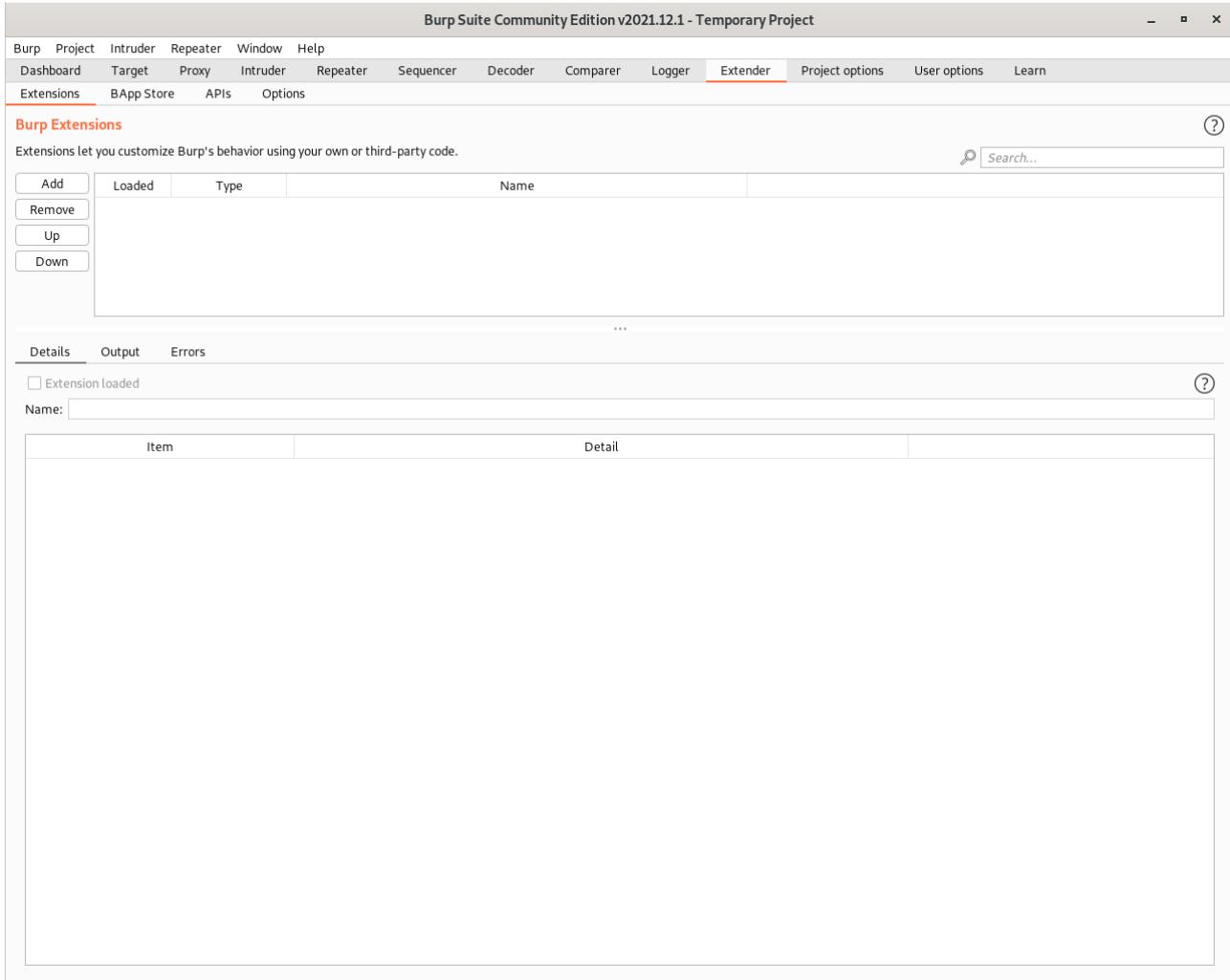
The Comparer does, what it sounds like. It compares the Input of the Two Boxes and shows you the Differences.

Sn0wF0x CTF - Knowledge



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

Sn0wF0x CTF - Knowledge



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.

Credits:

I Hope this might Help Someone on their Journey through Infosec :)

If so, feel free to contact me on Twitter : <https://twitter.com/MarcusChachuls1>

```
,,%          ..@  
**/(*(. *.. /  %@(.,&  
,/*/, *%*,... ..*/..%  
. *@(*,#,..      ,#,...  
./*/*,..        ##,&  
.**//...        . #  
.#/(*,. @*    @@@  .  
.**,*//,.       ..  
.,#//**..,*%,   *  .(  
,,***,...,*..,*  #  ..  
.*((),...      #./  
.%((),...      .  
.(((),...      #  
.*/...,...     ..  
.%,/(),...     .%  
.*/%,..       ...  
.#//,..      .*,...,.,.#  
.///,,,/,..  ..%,...,%,..(#. ...  
.#,,*//%***,,**/#.  #.. ./,,, ,* .  
.****,,,...,/,*//****,%*/ .. #.. ,..,* , #(.  
.**.....,(%,.....,* ,.,#/.. ,*/*. .(.  
.,... ...../&*/**//,,*,/,,#, ./&*,*/**#  
.##...  /*, .... #.,,,***,**#. /*//**,%,%*#  
.%,...      #,****,*/*#,/*#,#/ /  
.(..,... ... (      **,*//,**&,.. ,*,  
.***,,..... ,,, ,,*%#/,,#*#, ***/%.  
.***,,..... #.. ....,...,...,* ,*%%***%%(/*#  
.##.. .(****//****/(%%****/((((((/%#/#. ....,##..,/,,****/*****#, ..  
.. .*,..
```

Created by Sn0wF0x