Burp Suite

Sn0wF0x CTF-Knowledge

BURP SUITE

What is Burpsuite

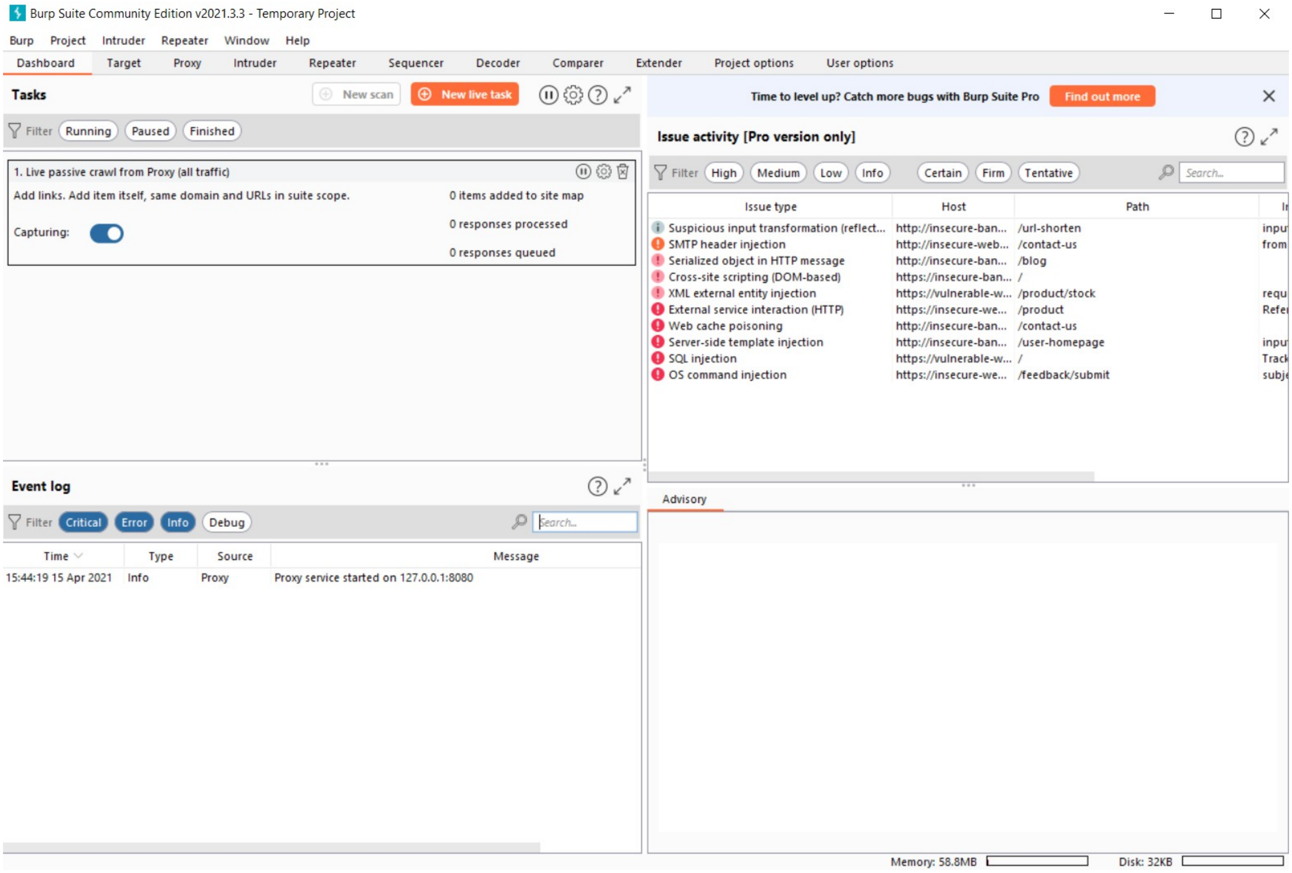
> „Burp or Burp Suite is **a set of tools used for penetration testing of web applications**.“
>
> ~ GeeksforGeeks

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



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

0 responses processed

0 responses queued

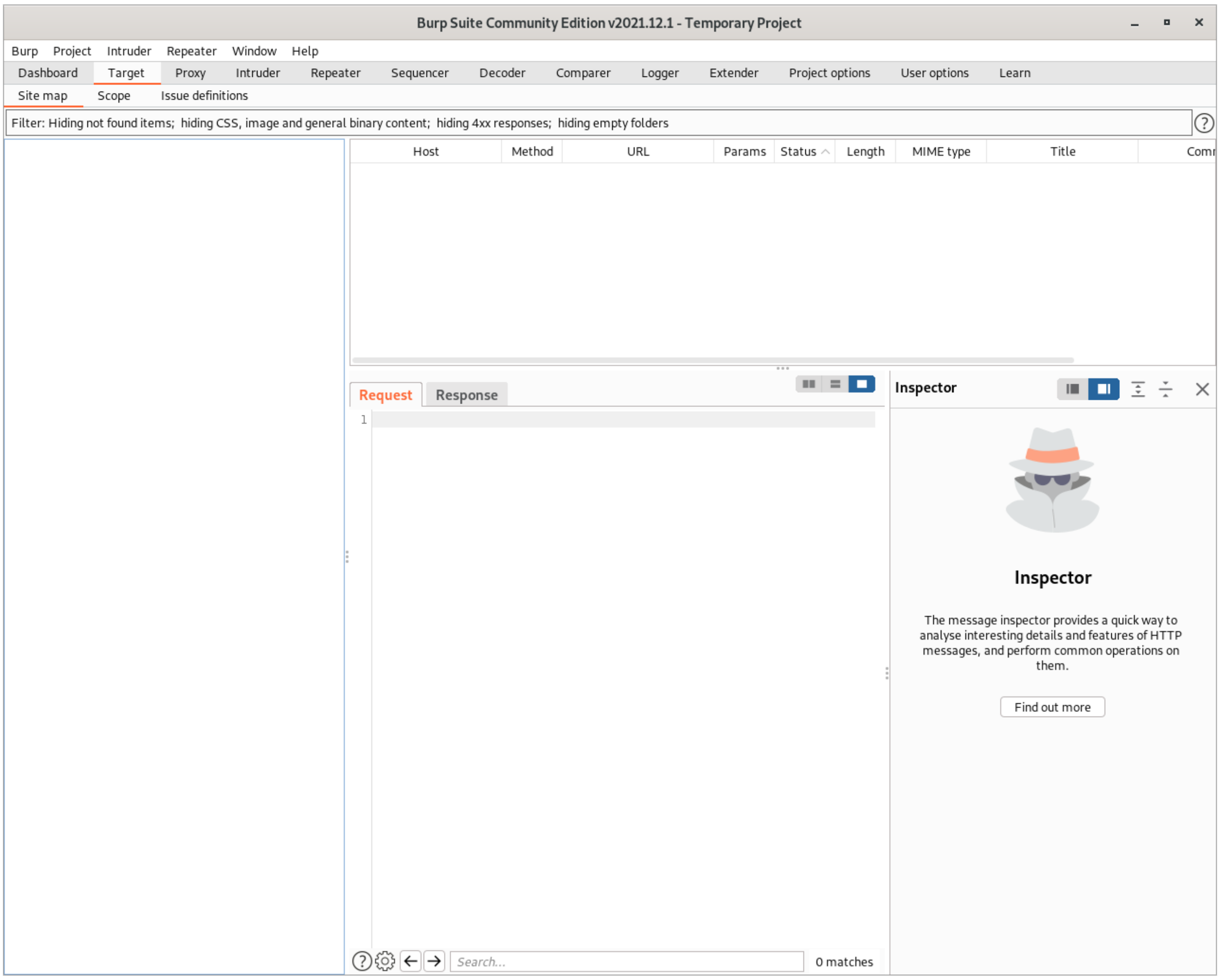
Issue type	Host	Path	I
Suspicious input transformation (reflect...	http://insecure-ban...	/url-shorten	inpu
SMTP header injection	http://insecure-web...	/contact-us	from
Serialized object in HTTP message	http://insecure-ban...	/blog	
Cross-site scripting (DOM-based)	https://insecure-ban...	/	
XML external entity injection	https://vulnerable-w...	/product/stock	requ
External service interaction (HTTP)	https://insecure-we...	/product	Refe
Web cache poisoning	http://insecure-ban...	/contact-us	
Server-side template injection	http://insecure-ban...	/user-homepage	inpu
SQL injection	https://vulnerable-w...	/	Track
OS command injection	https://insecure-we...	/feedback/submit	subje

Time	Type	Source	Message
15:44:19 15 Apr 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080

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

Dashboard	Your Overview for Burp-Suite
Target	Here you can Create a Sitemap for a Website + Add A Scope to a speicific Website
Proxy	When you captured a Request, you can see it here
Intruder	Burp-Suite internal Fuzzer
Repeater	Modify/Edit Income Data Packages
Sequencer	Sequencer allows us to measure the entropy (or randomness, in other words) of "tokens"
Decoder	En/decode Strings
Comparer	Compares The Input of Two Boxes, byte by byte
Extender	Create own Modules for Burp Suite

Deeper Look:

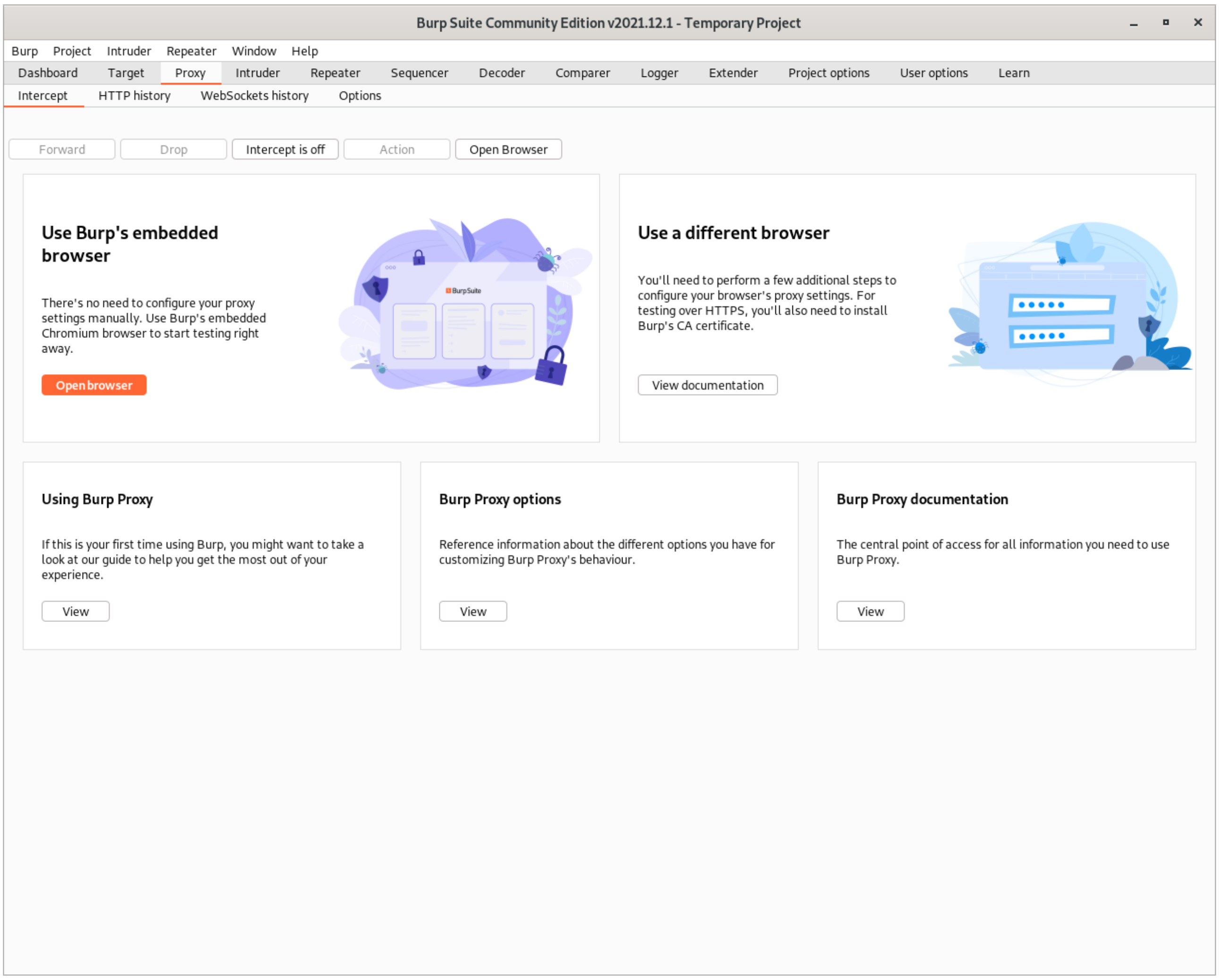

Burp Suite Community Edition v2021.12.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Host Method URL Params Status Length MIME type Title Comm
Request Response
Inspector
Find out more
Search...
0 matches

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Inspector

The message inspector provides a quick way to analyse interesting details and features of HTTP messages, and perform common operations on them.

Lets Beginn wth „Target“.
When you started scanning a Target, you may get some stuff you dont 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.


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.

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.

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.

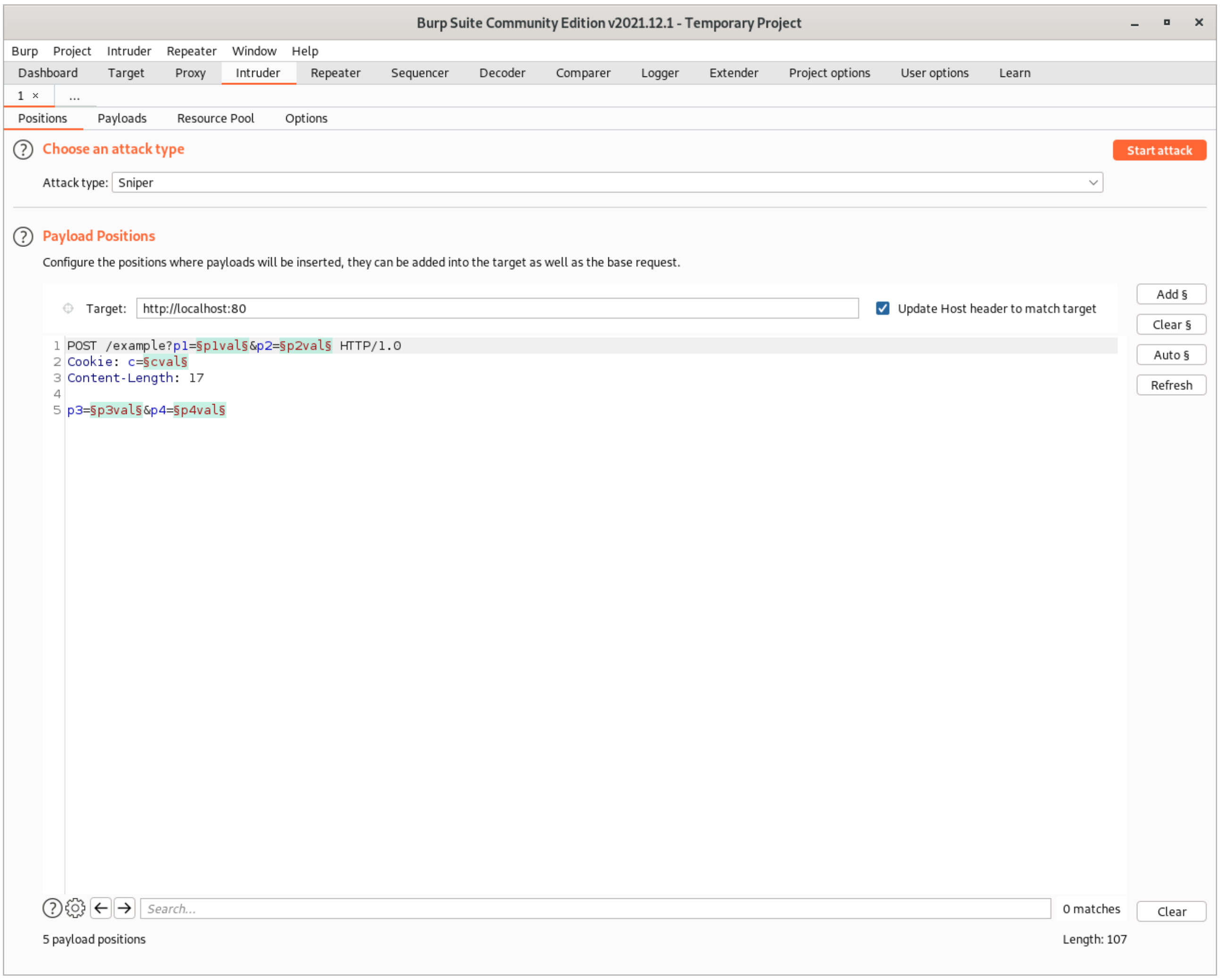
Burp Proxy options

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

Burp Proxy documentation

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

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. (Remeber to Turn Intercept on/off after/before using :))


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
1 × ...
Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
Clear

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:80

☑ Update Host header to match target

```
POST /example?p1=§p1val§&p2=§p2val§ HTTP/1.0
Cookie: c=§cval§
Content-Length: 17

p3=§p3val§&p4=§p4val§
```

0 matches

5 payload positions

Length: 107

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
=> Ressource Pool
=> Options

1. **Position:**

The Positions Sub-Tab includes The Choice of the Attack (Sniper, Battering Ram, Pitchfork, Clusterbomb) 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 untill all positions have been tried.

This quality makes Sniper very good for single-position attacks (e.g. a password bruteforce 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.

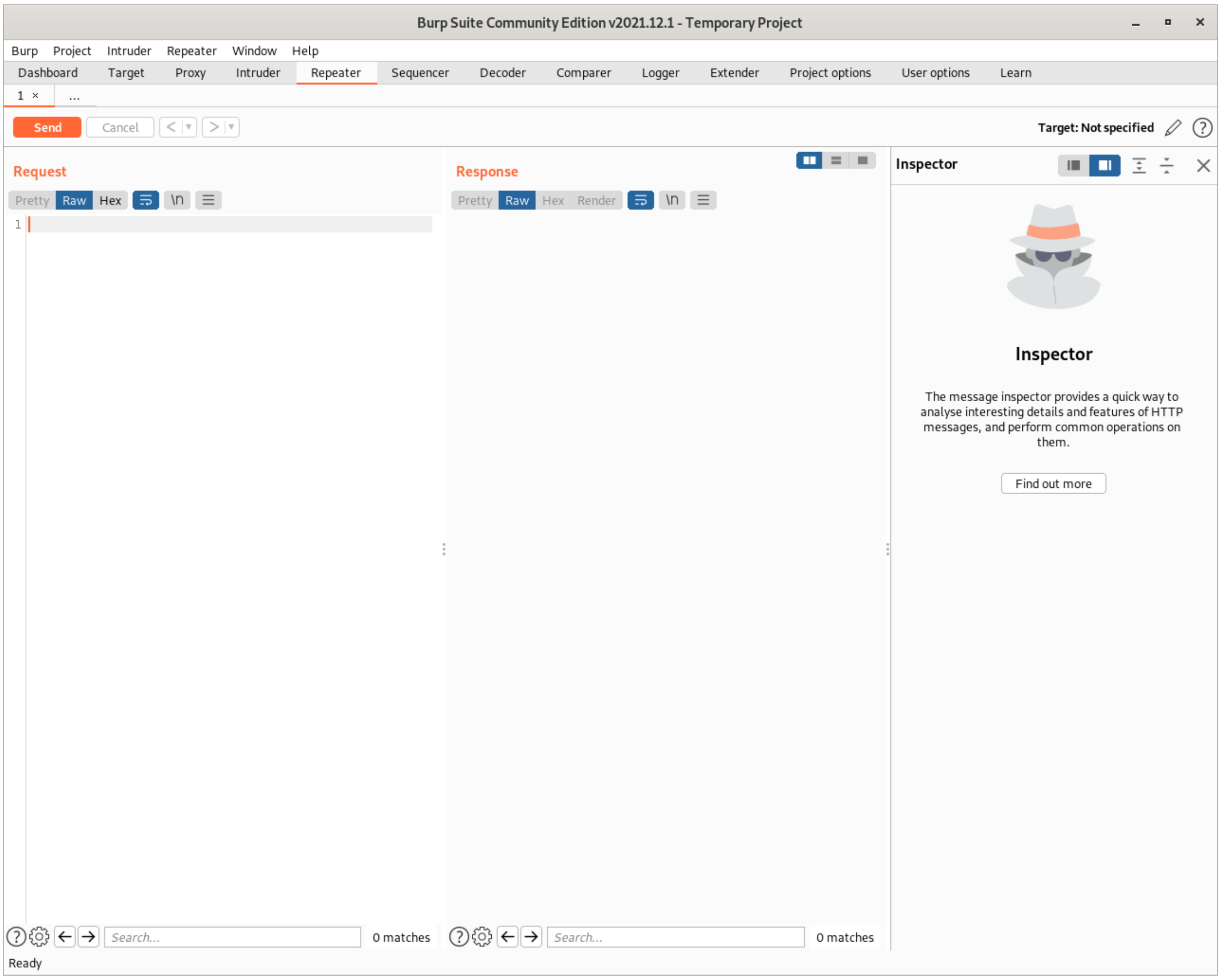
Where Sniper uses one payload set (which it uses on every position simultaneously),

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

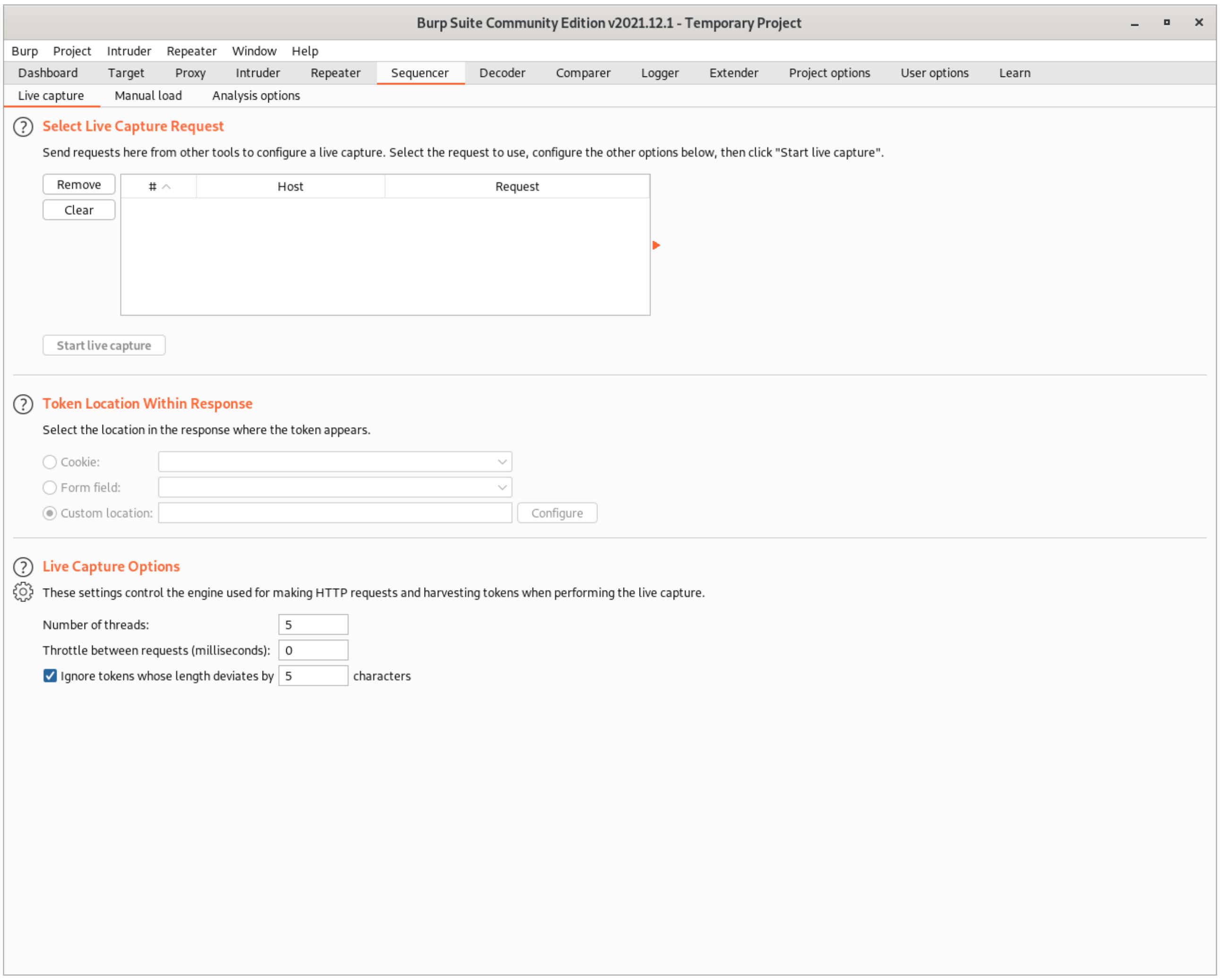
Cluster bomb iterates through each payload set individually, making sure that every possible combination of payloads is tested. this will try every combination of values.


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
1 × ...
Send
Cancel
Target: Not specified
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Find out more
Search...
0 matches
Search...
0 matches
Ready

Inspector

The message inspector provides a quick way to analyse interesting details and features of HTTP messages, and perform common operations on them.

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


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
Live capture Manual load Analysis options
Remove
Clear
# Host Request
Start live capture
Configure

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".

Token Location Within Response

Select the location in the response where the token appears.

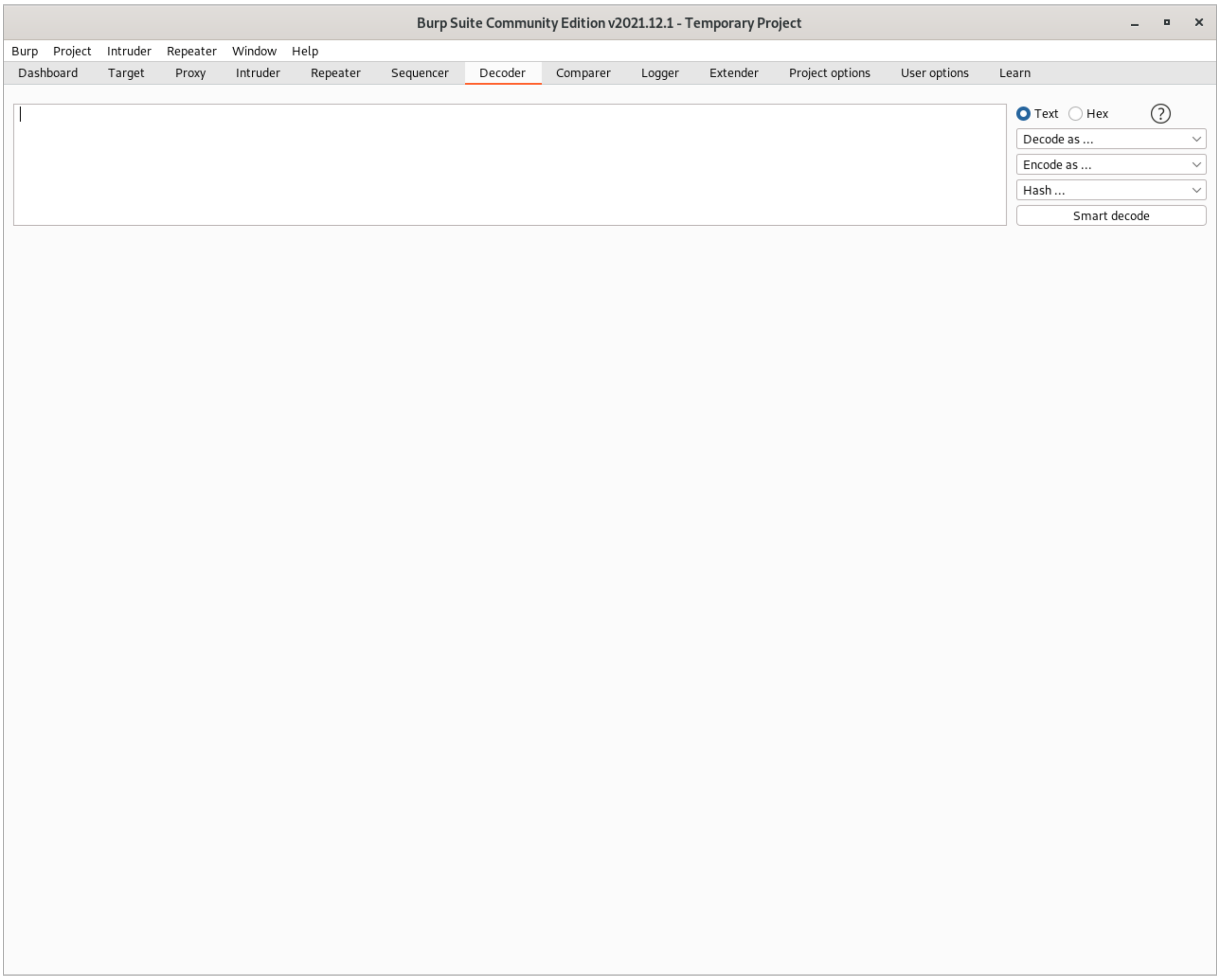
○ Cookie:
○ Form field:
● Custom location:

Live Capture Options

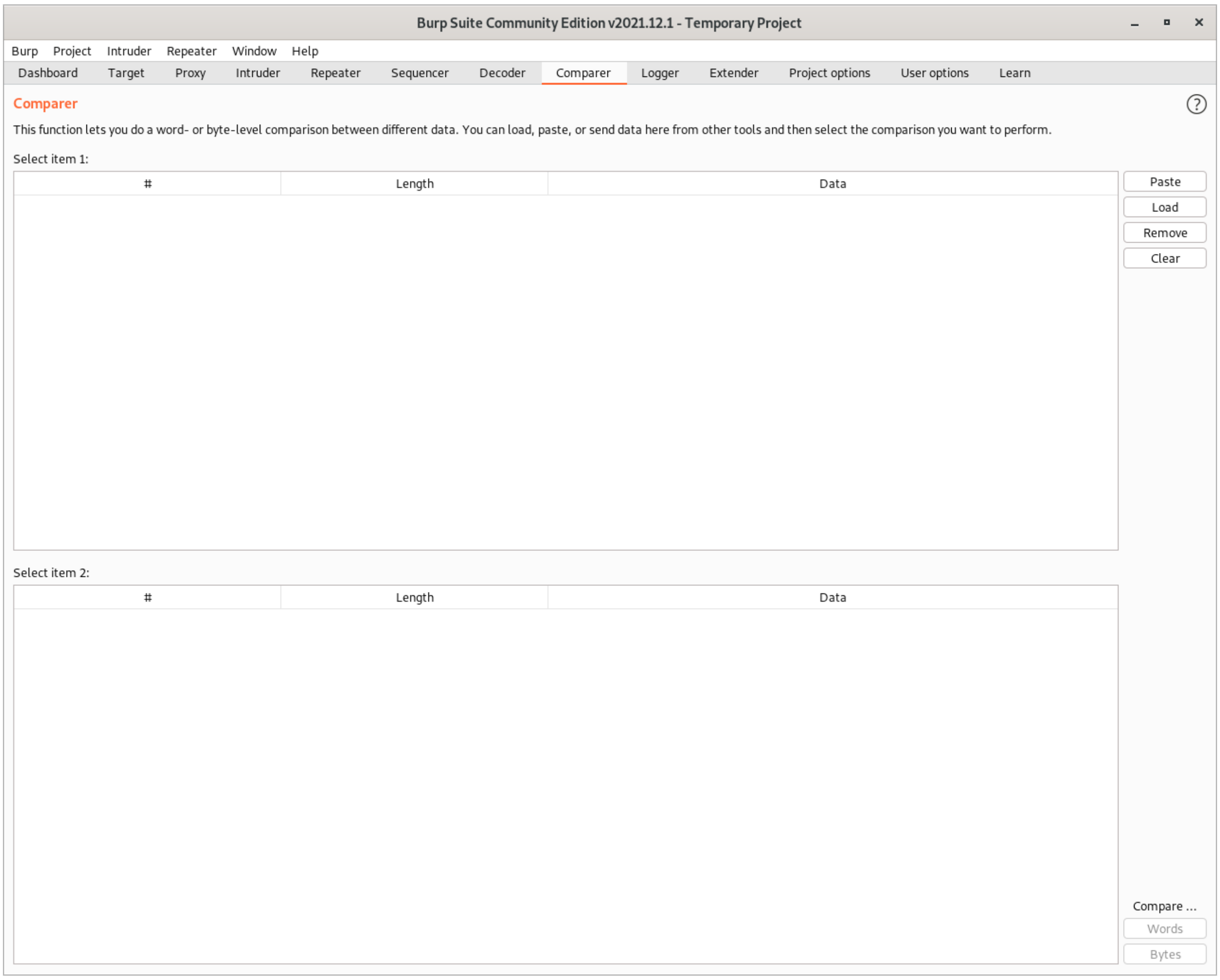
These settings control the engine used for making HTTP requests and harvesting tokens when performing the live capture.

Number of threads: 5
Throttle between requests (milliseconds): 0
☑ Ignore tokens whose length deviates by 5 characters

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

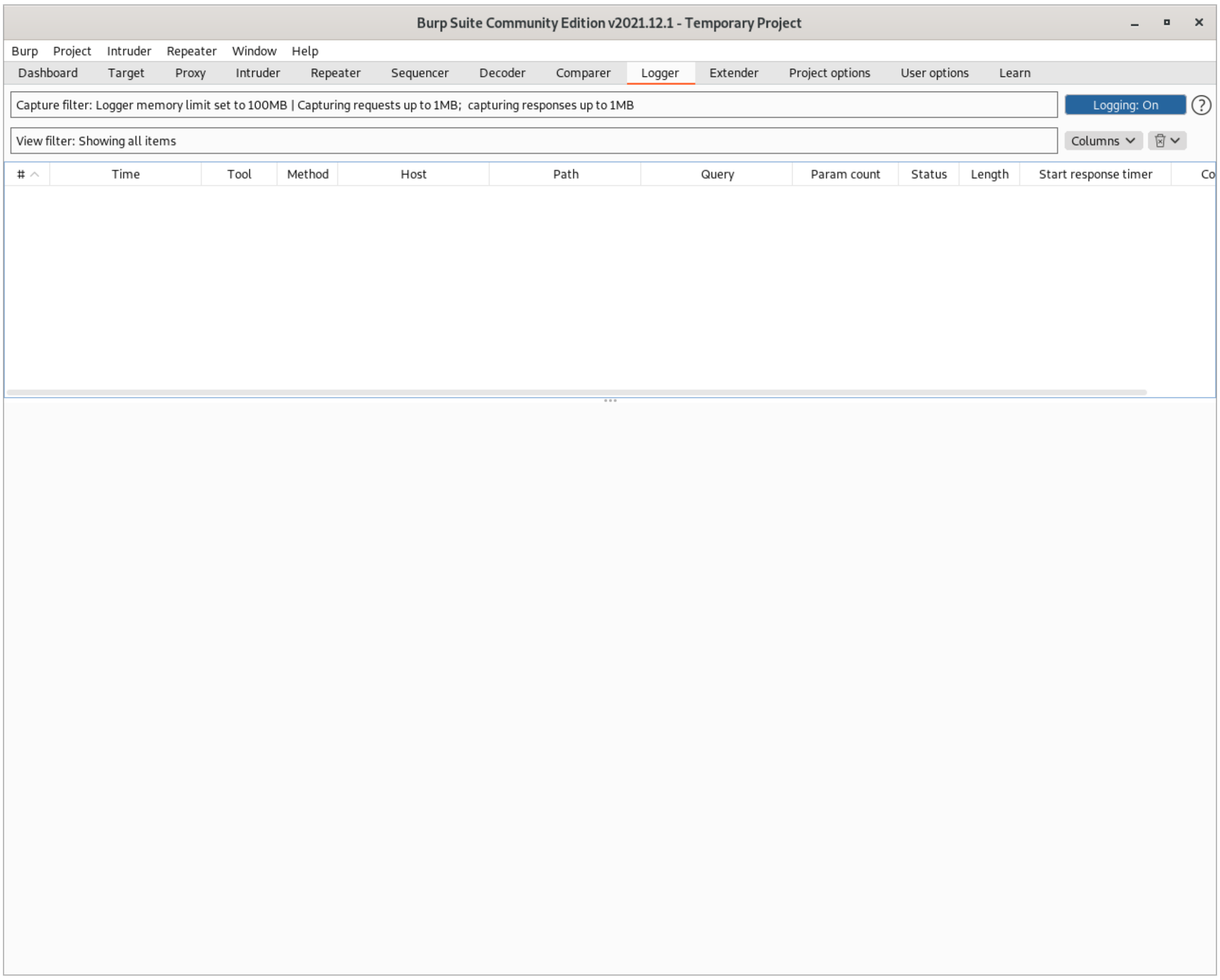


Similar to „Cyberchef“ the Decoder En/Decodes Values.


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
Comparer
Select item 1:
# Length Data
Paste
Load
Remove
Clear
Select item 2:
# Length Data
Compare ...
Words
Bytes

This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.

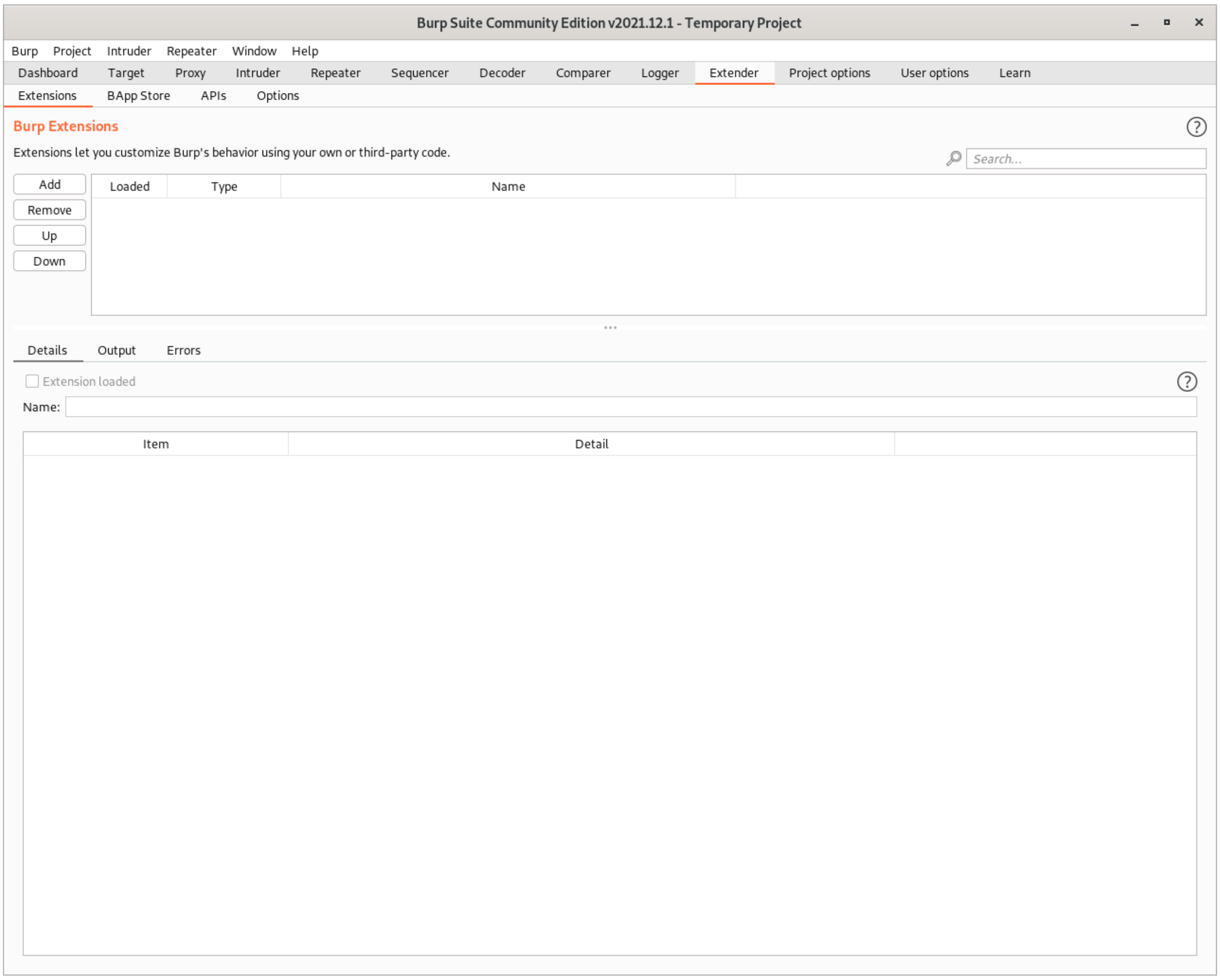
The Comparer does, what it sounds like. It compares the Input of the Two Boxes and shows you the Differences.



Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

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


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
Extensions BApp Store APIs Options
Search...
Add
Remove
Up
Down
Loaded Type Name
Details Output Errors
Extension loaded
Name:
Item Detail

Burp Extensions

Extensions let you customize Burp's behavior using your own or third-party code.

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