



Burp Suite: Sequencer

[Introduction](#)

[How to use sequencer](#)

[Into the sequencer](#)

[The attack](#)

[Analyzing the results](#)

Introduction

Burp Sequencer is a tool for analyzing the quality of randomness in a sample of data items. You can use it to test an application's session tokens or other important data items that are intended to be unpredictable, such as anti-CSRF tokens, password reset tokens, etc.

Sequencer is quite complex so i'm going to explain this topic a bit more in depth. There are no cool tricks to sequencer because sequencer is a cool trick in and off itself.

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder Repeater **Sequencer** Decoder Comparer Extender Project options User options Authorize
 Live capture Manual load Analysis 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
3	https://ferretshop.herokuapp.c...	POST /rest/user/login HTTP/1.1Host: ferretsh...

Start live capture

Token Location Within Response

Select the location in the response where the token appears.

☐ Cookie:
☐ Form field:
☒ Custom location: From ["token":] to [", "bid"] **Configure**

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

How to use sequencer

- Find a request that contains a token. This can be done in either the proxy tab or site map tab. Depending on what type of token you are trying to test you are going to need other endpoints.
 - CSRF token: The endpoint that returns CSRF token in response
 - JWT token: Usually login endpoint
 - ...
- Right click that request and sent it to the sequencer.

Burp Project Intruder Repeater Window Help
 Dashboard **Target** Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
 Site map Scope Issue definitions

Task execution is paused - Site map will not be updated

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

https://ferretshop.herokuapp.com
 /
 > api
 > assets
 favicon.ico
 main-es2015.js
 main-es5.js
 polyfills-es2015.js
 polyfills-es5.js
 > profile
 > profile
 > rest
 > admin
 > basket
 continue-code
 > continue-code
 > products
 > user
 > login
 whoami
 runtime-es2015.js
 runtime-es5.js
 > socket.io
 socket.io
 vendor-es2015.js
 vendor-es5.js

Contents

Host	Method	URL	Params	Status	Length	MIM
https://ferretshop.herokuapp.com	POST	/rest/user/login		200	1182	JSON

Request **Response**

Pretty Raw \n Actions

```

1 POST /rest/user/login HTTP/1.1
2 Host: ferretshop.herokuapp.com
3 Connection: close
4 Content-Length: 54
5 sec-ch-ua: ";Not A Brand";v="99"
6 Accept: application/json, text/plain
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36
9 Content-Type: application/json
10 Origin: https://ferretshop.herokuapp.com
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://ferretshop.herokuapp.com
15 Accept-Encoding: gzip, deflate
16 Accept-Language: nl-NL,nl;q=0.9,en;q=0.8
17 Cookie: language=en; welcomebanner=1
18
19 {
  "email": "test@gmail.com",
  "password": "test@gmail.com"
}
  
```

Scan
 Do passive scan
 Do active scan
 Send to Intruder Ctrl-I
 Send to Repeater Ctrl-R
Send to Sequencer
 Send to Comparer
 Send to Decoder
 Show response in browser
 Request in browser
 Send request to Authorize
 Send cookie to Authorize
 Send to AutoRepeater
 Engagement tools
 Copy URL
 Copy as curl command
 Copy to file
 Save item
 Convert selection
 Cut Ctrl-X
 Copy Ctrl-C
 Paste Ctrl-V
 Message editor documentation
 Site map documentation

Typ hier om te zoeken
 Search...

Into the sequencer

Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Authorize AutoRepeater
 Live capture Manual load Analysis 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
3	https://ferretshop.herokuapp.c...	POST /rest/user/login HTTP/1.1Host: ferretsh...

Remove Clear Start live capture **2**

? **Token Location Within Response**
 Select the location in the response where the token appears.

☐ Cookie:
☐ Form field:
☒ Custom location: From ["token:" to ["bid"] **Configure** **1**

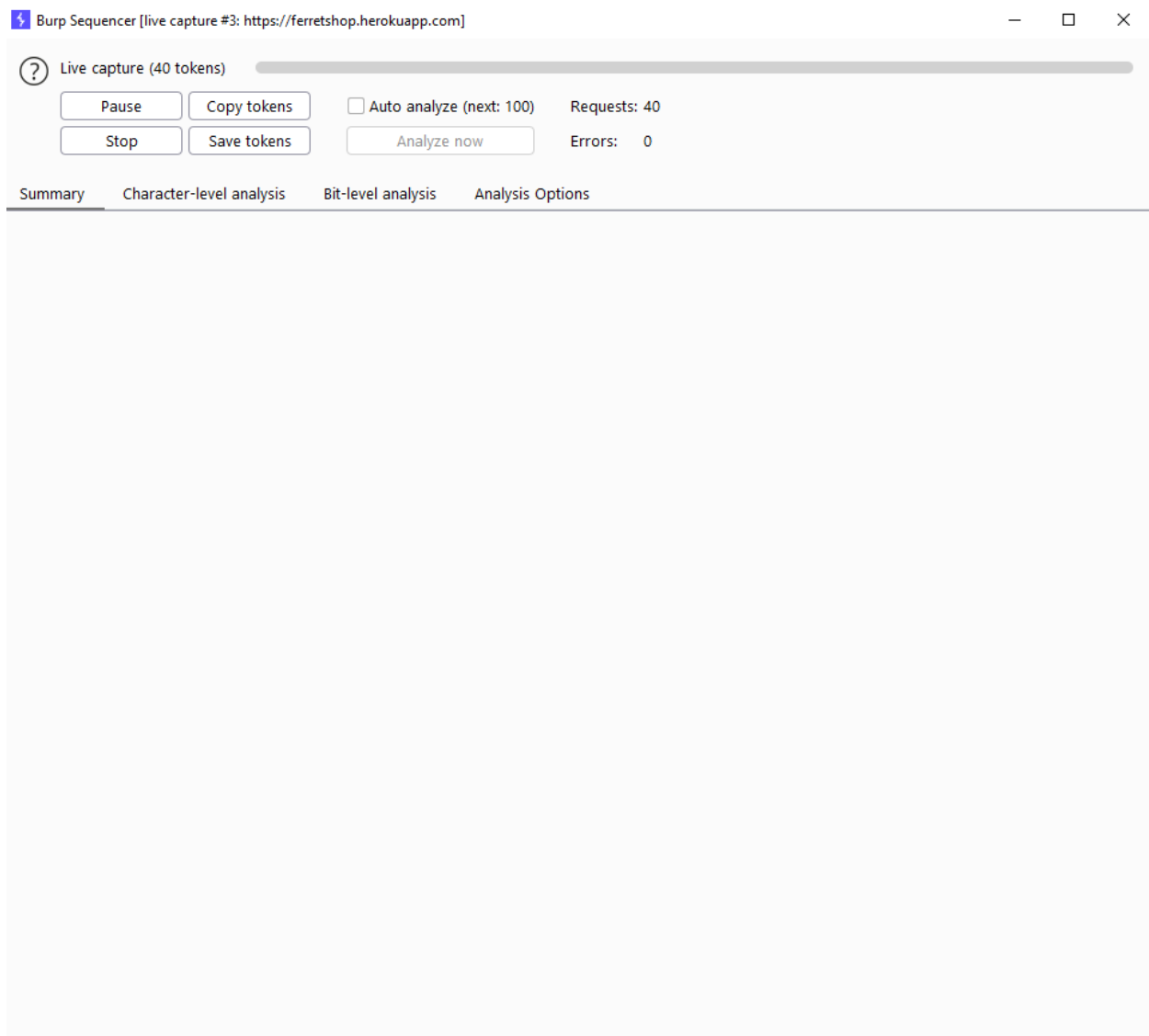
? **Live Capture Options**
 ⚙️ These settings control the engine used for making HTTP requests and harvesting tokens when performing the live capture.

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

1. When we are in the repeater the first thing we need to do is determine where the token is being returned in the response. Just select the full token, only the token itself, not the quotes
2. And then we start capturing and we wait 😊

The attack

Now burp suite is going to request a TON of tokens and try to see how predictable they are. This will take a long time, don't put the amount of threads too high as it might make the requests even slower if the server can't keep up with the number of requests.



Analyzing the results

The character level and bit level results will explain any predictability in the tokens you are testing. To explain those details is outside the scope of this course but google has enough resources for this.