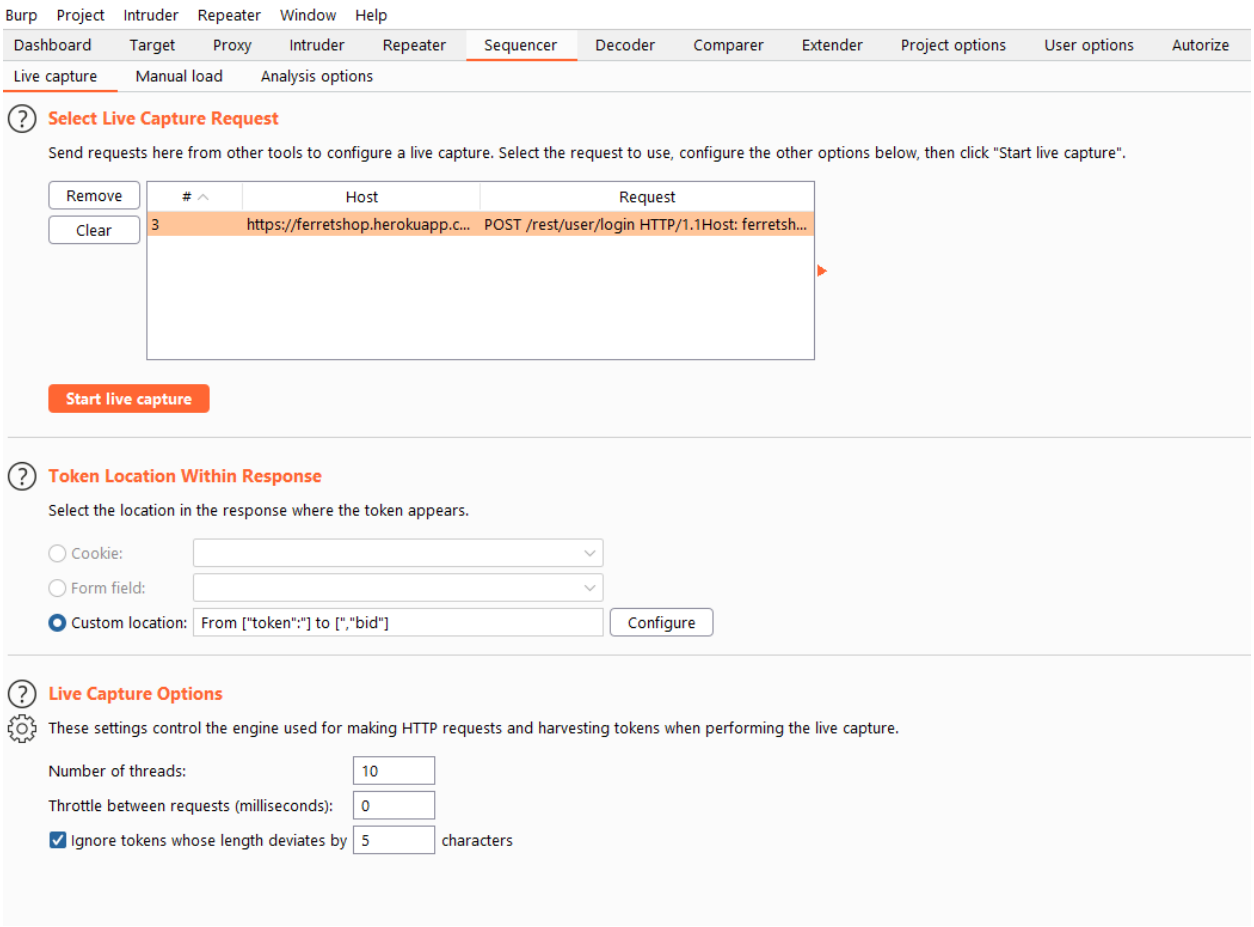
Burp Suite: Sequencer

Introduction

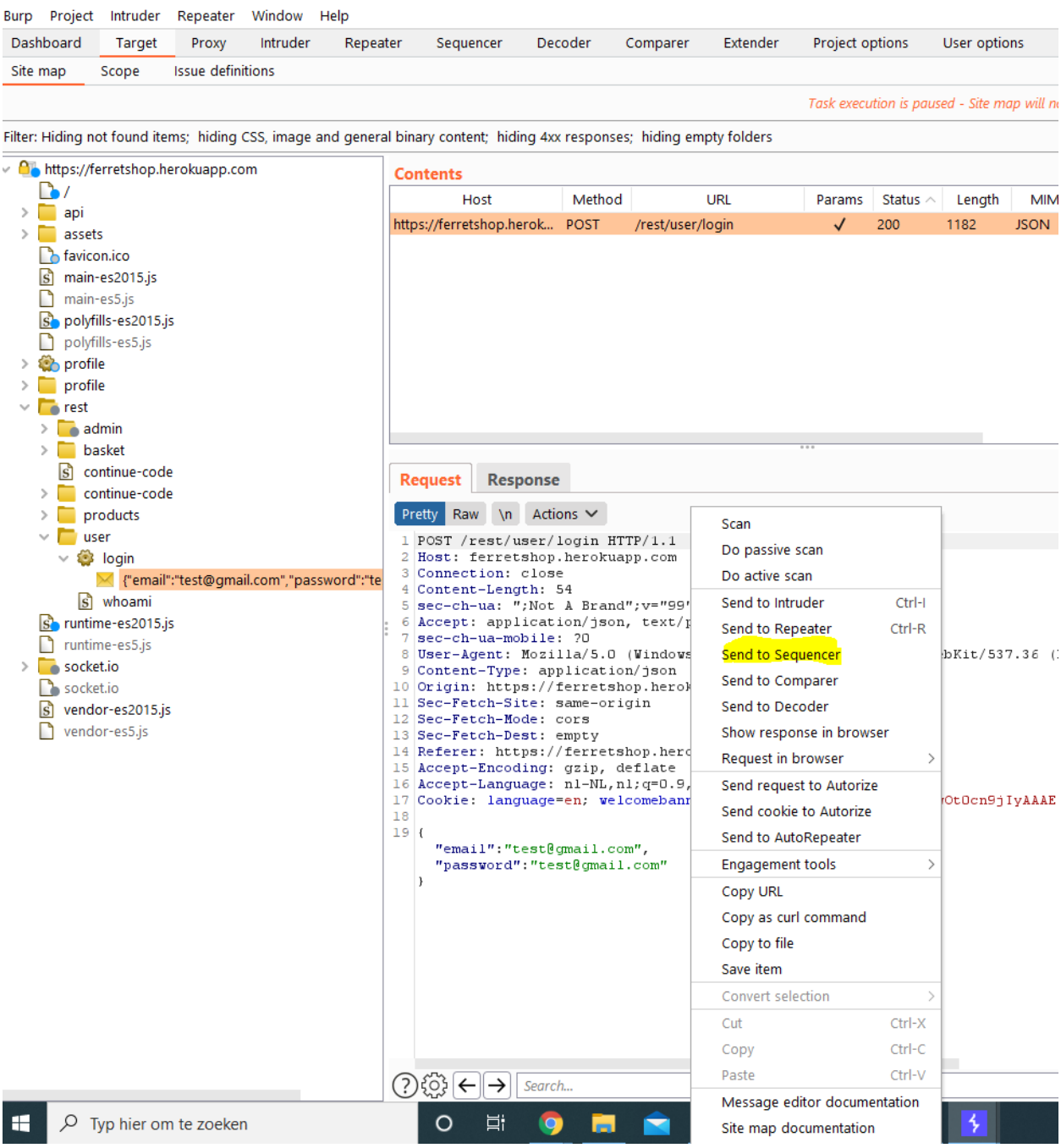
Burp Sequencer is a tool for analyzing the quality of randomness in a sample of data items. You can use it to test an application's session tokens or other important data items that are intended to be unpredictable, such as anti-CSRF tokens, password reset tokens, etc.

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.

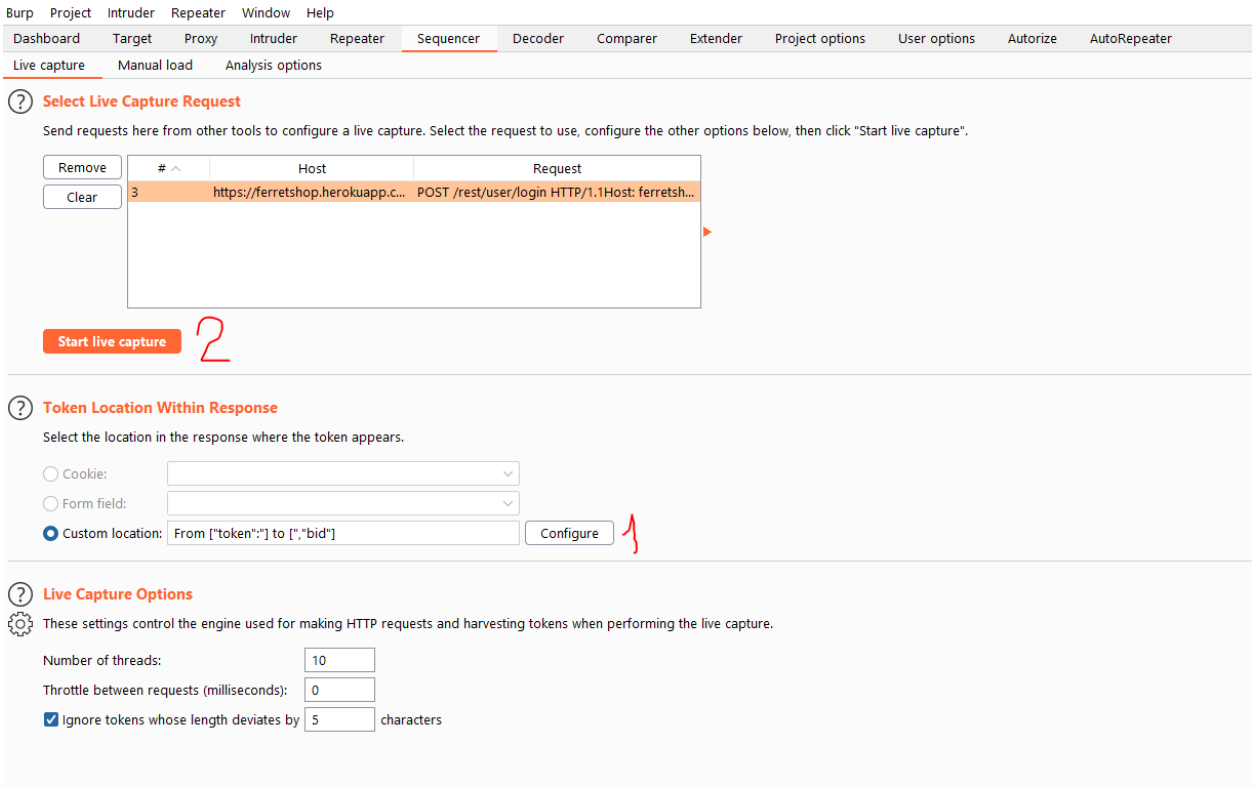


How to use sequencer

1. 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.
    1. CSRF token: The endpoint that returns CSRF token in response
    2. JWT token: Usually login endpoint
    3. ...
2. Right click that request and sent it to the sequencer.



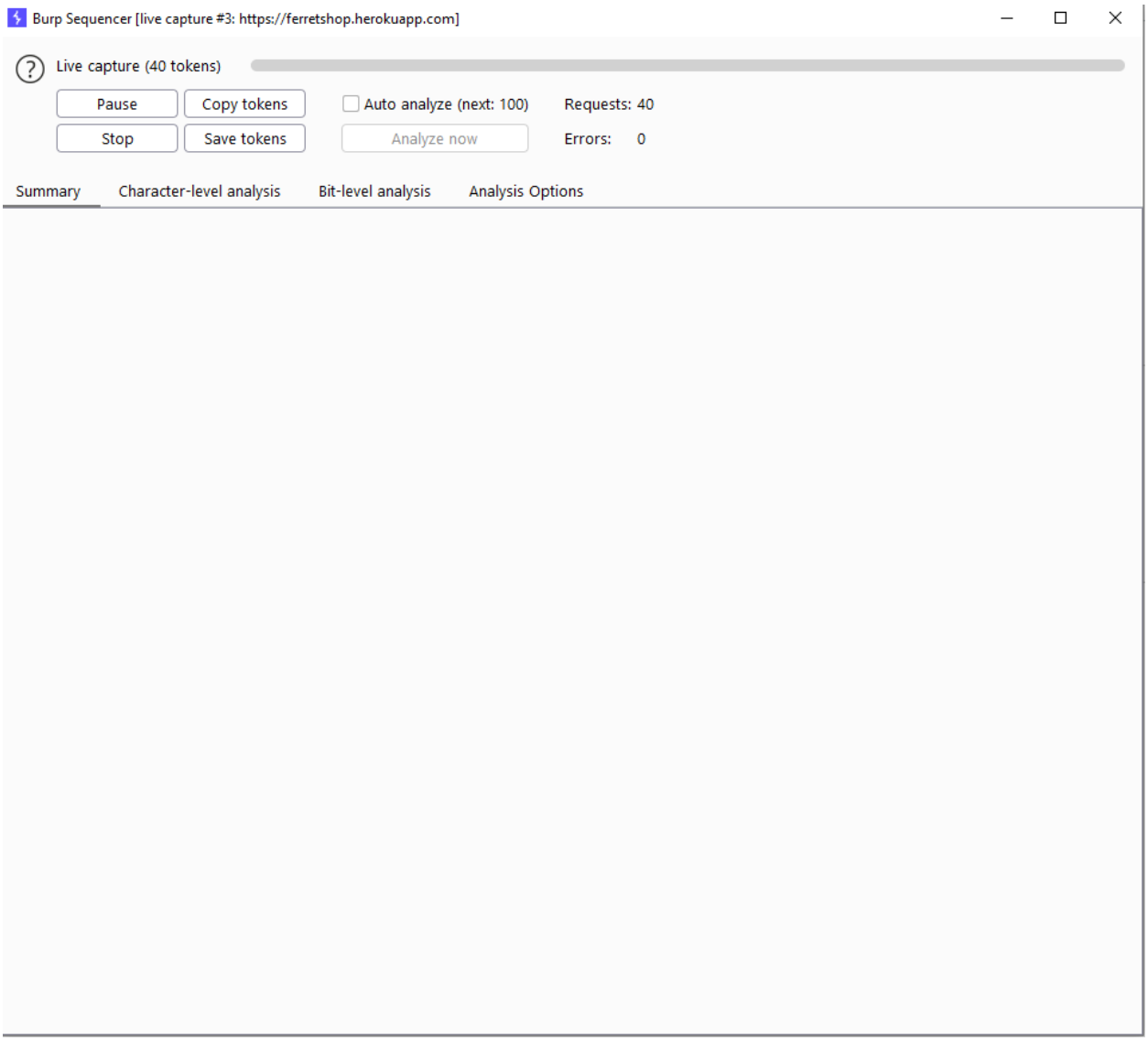
Into the sequencer



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.