enc challenge | medium

when I start this challenge I didn’t see anything in the page but I see in the cookies cookie called id and it has base64 encode value and when I decode it I see jwt token like this

that base64 encode → eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6IjEiLCJpYXQiOjE1MTYyMzkwMjJ9.1EUw90A2xwL40wJOlE5gNDBCLdDDMG3JkW5f5ChoYKI

and that is decode → {"alg":"HS256","typ":"JWT"}{"id":"1","iat":[1516239022}E0@6](mailto:1516239022}E0@6)##NN`40B-0mɑn\_(h`

we can split jwt token to 3 part

firtst part → eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

second part → eyJpZCI6IjEiLCJpYXQiOjE1MTYyMzkwMjJ9

third part → 1EUw90A2xwL40wJOlE5gNDBCLdDDMG3JkW5f5ChoYKI

first part has data for the type of encryptino

second part has the data that website use it

third part has the encryptino value so if the user edit the data this part has to change

I decode each part and in second part I see parameter called id and its value is 1 so

I try to change this value each time and encode it in burp suite

so I craete python script to build list for jwt token have different value for id in jwt token

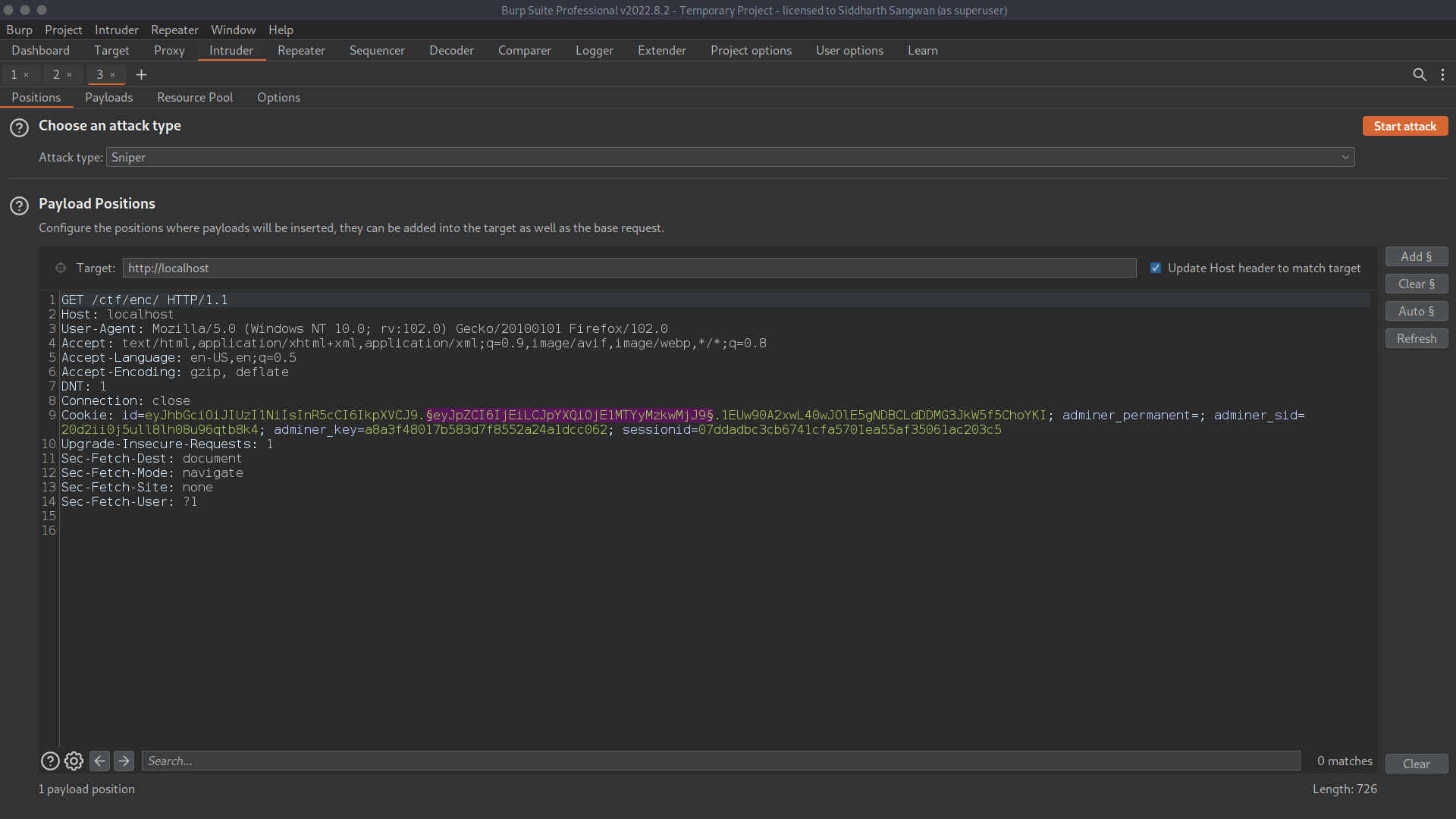
started from 0 to 10000

>>> for i in range(10000):

... a = '{"id":"'+str(i)+'","iat":1516239022}'

... print(a)

then I save this value in file and I intercept the request

Then I put the list in intruder then in the Payload processing I click on add then encode then base64 encode to do encode to each payload then I started attack and in the request 1500 the length for request is changed and when I see his response I see the flag