



SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

PicoCTF Submission

WD - Wednesday Group Submission

IE2062 – Web Security.

Submitted by:

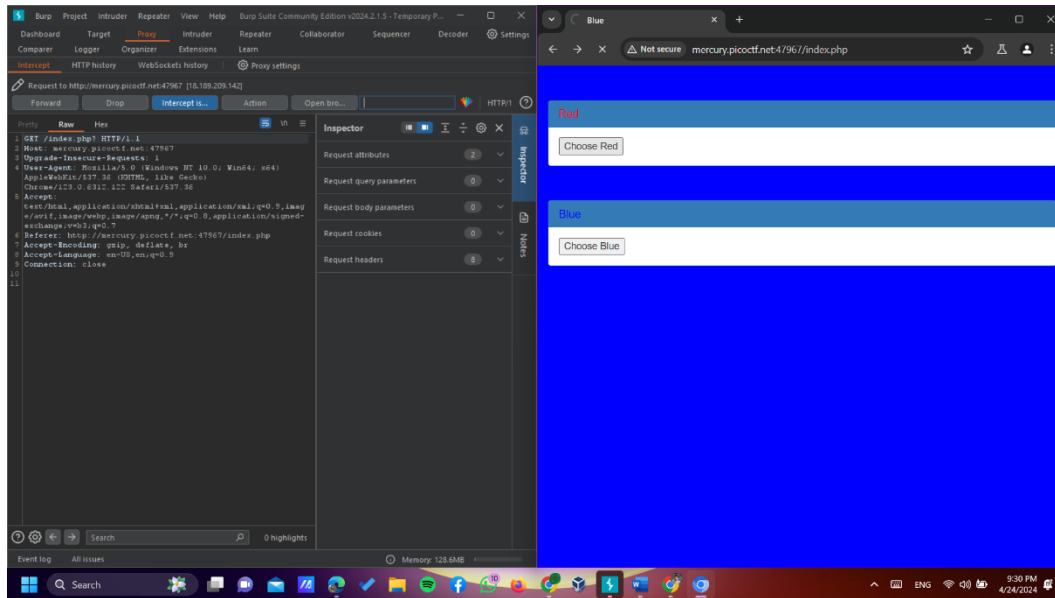
IT22199508 – Athapaththu A.M.M.I.P

Date of submission

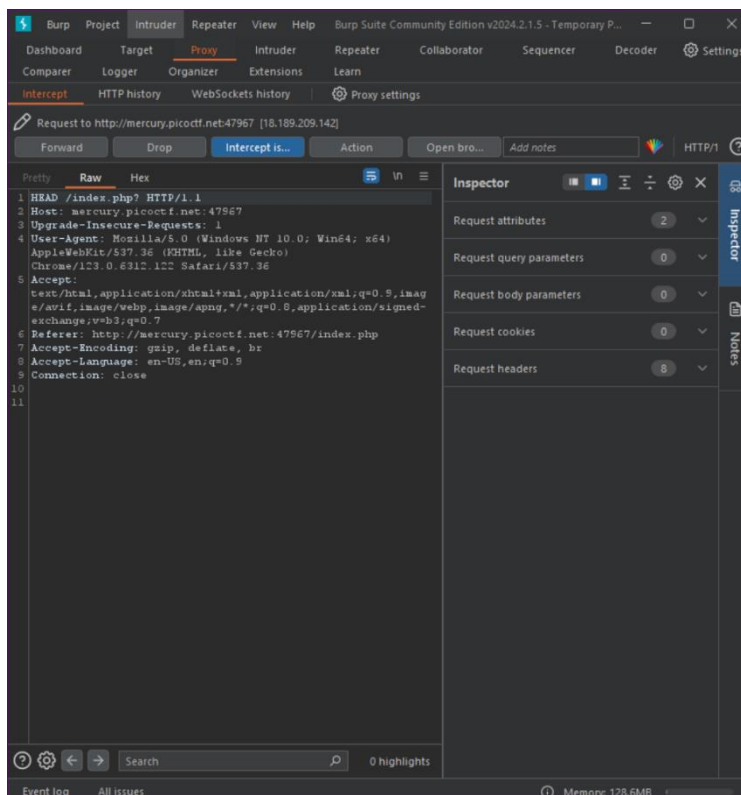
2024.04.28

1) GET aHEAD

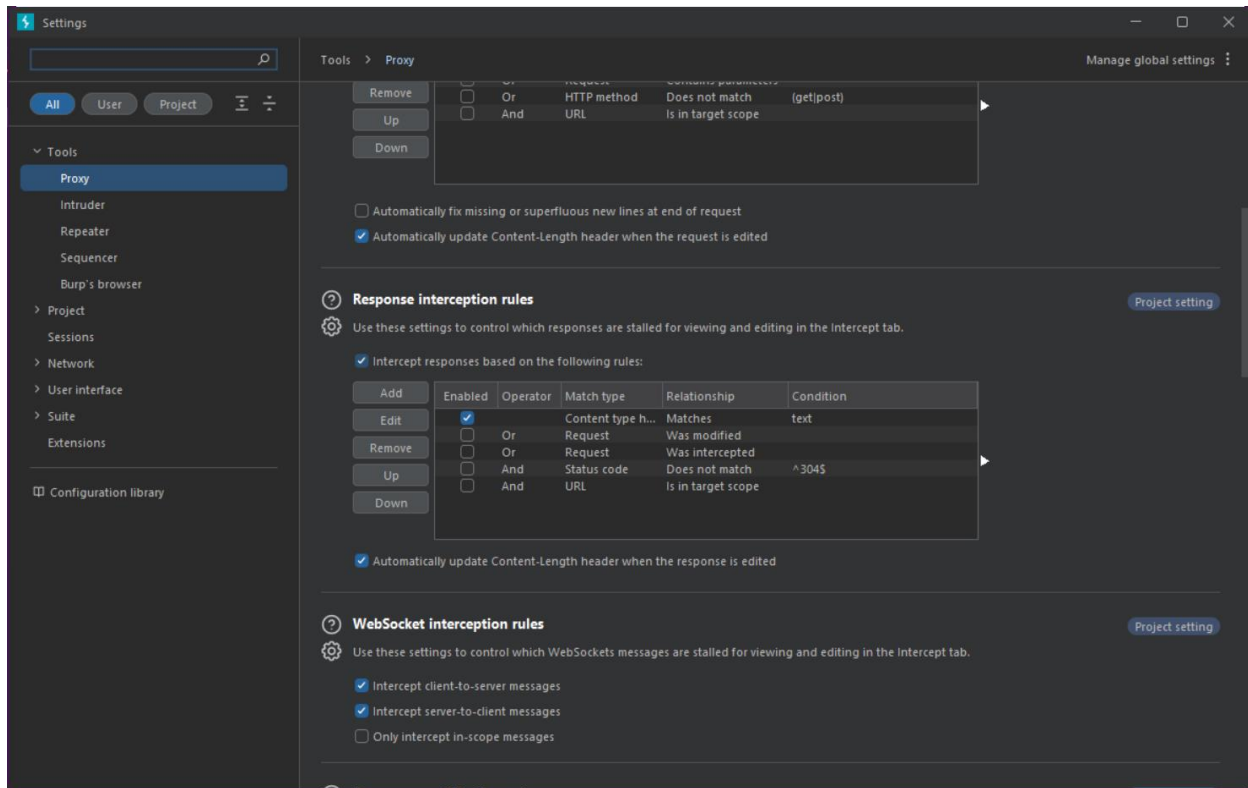
- Turn on intercept and click on choose Red and you'll receive the RAW code and you can see it is in GET method.



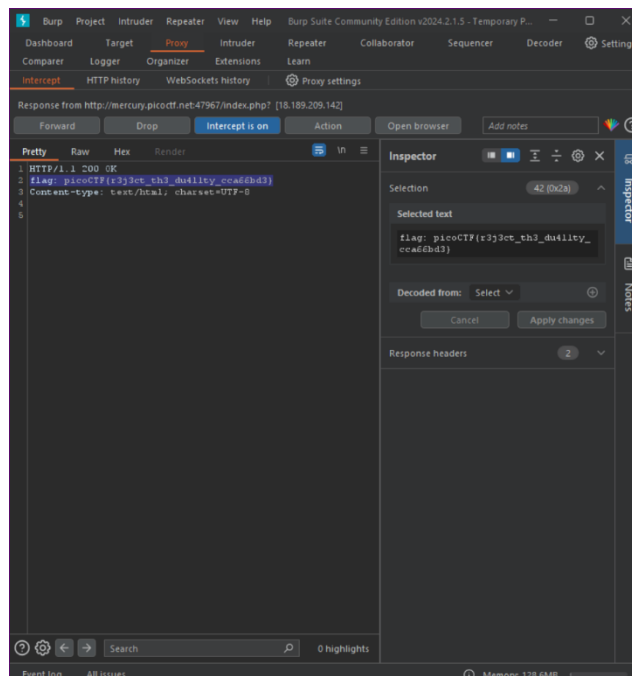
- Then change that GET method in to HEAD method and forward it.



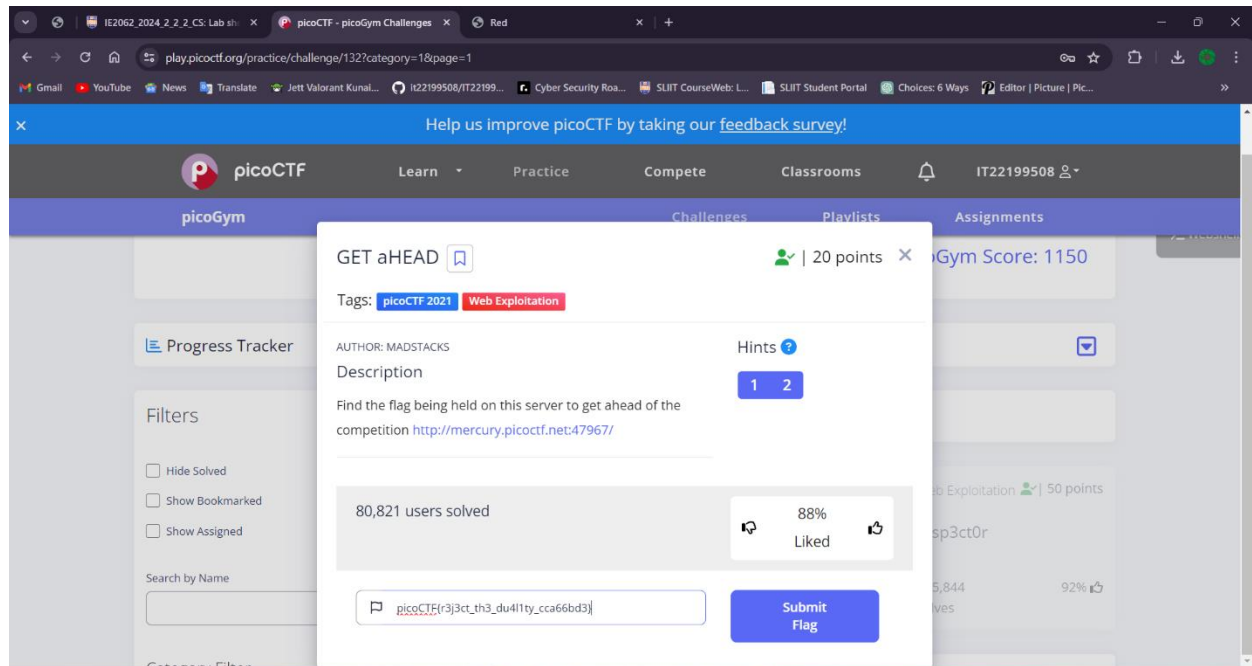
- Before forward it you put the tick in intercept responses based on the following rules in Response interception rules.



- After doing that forward it. you can see the result says HTTP/1.1 200 ok and displaying the flag.

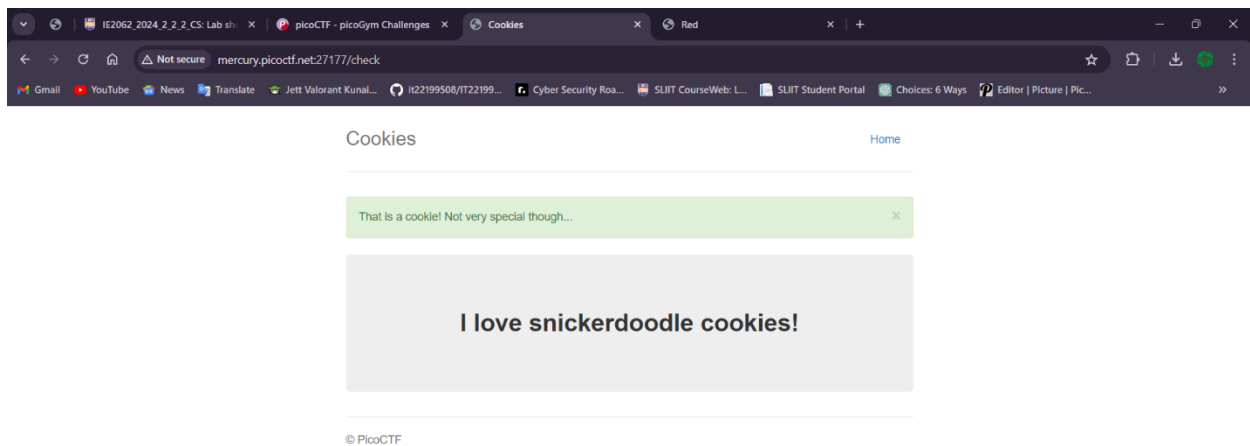
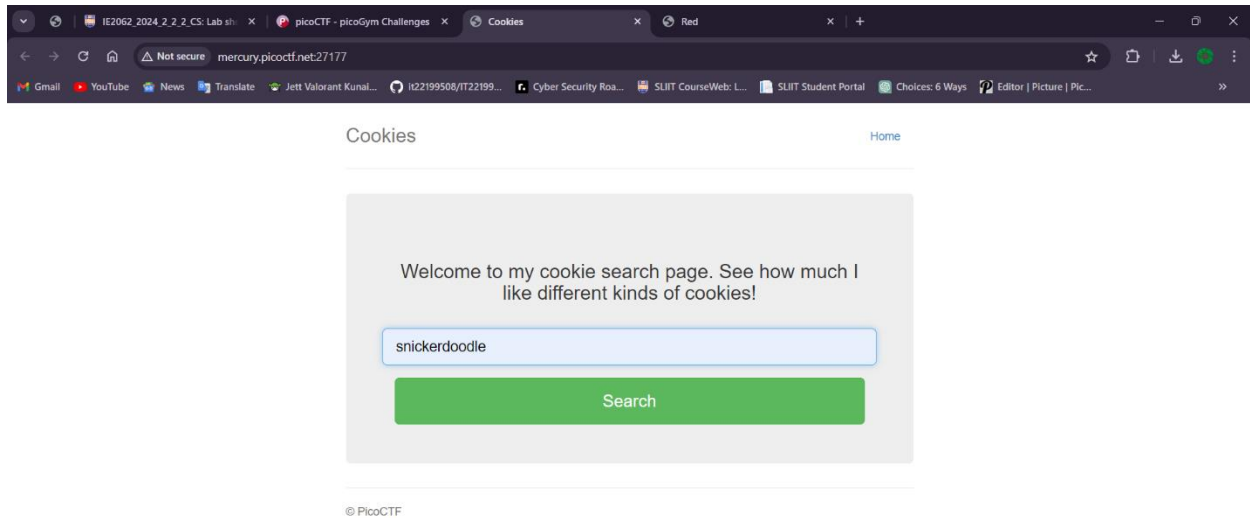


- Finally, enter the flag and get the points.

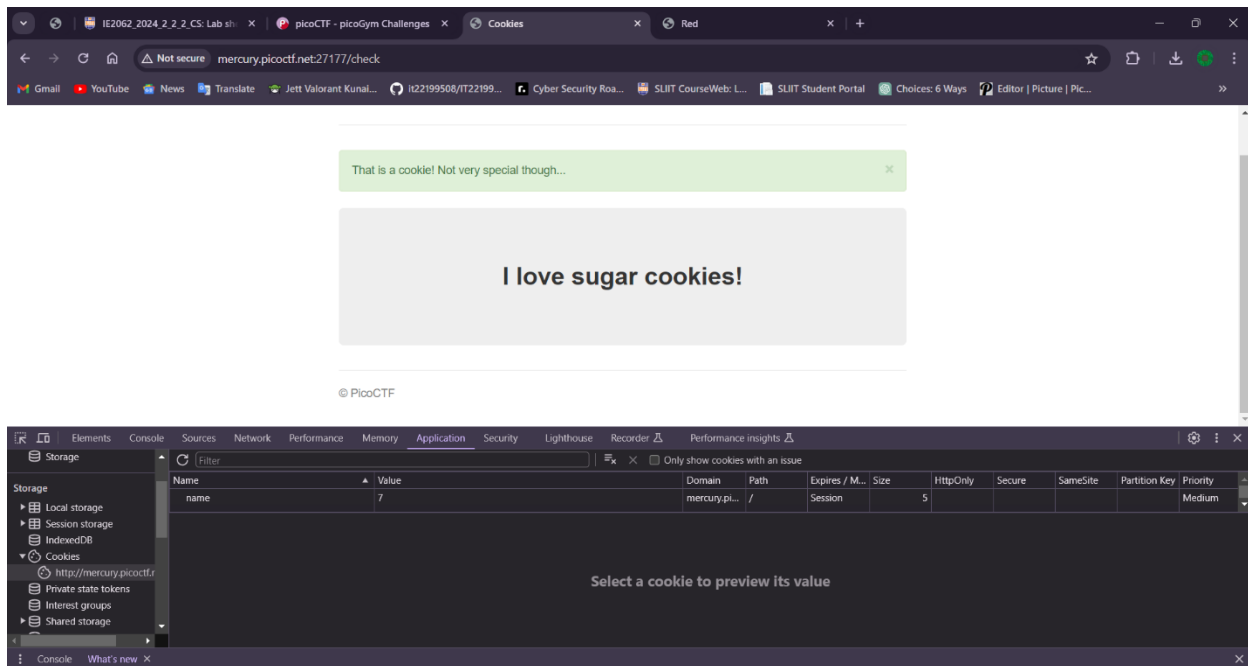


2) Cookies

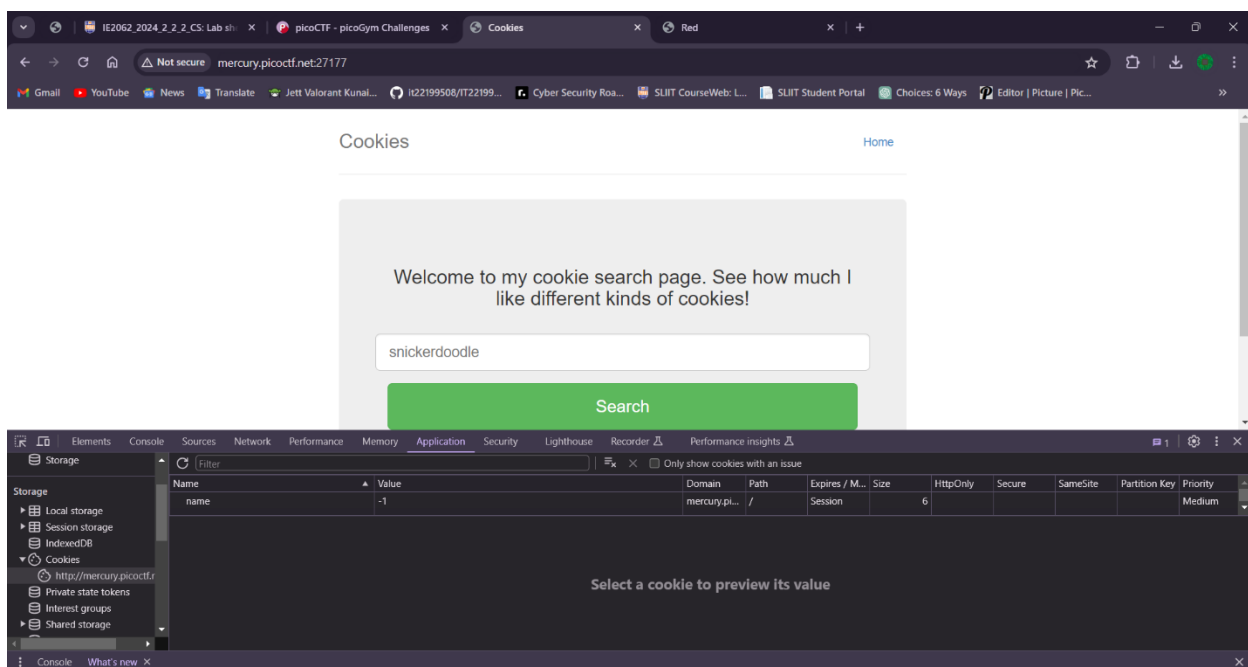
- Cookies: A way to have users store information about what they are doing and present it back to you.

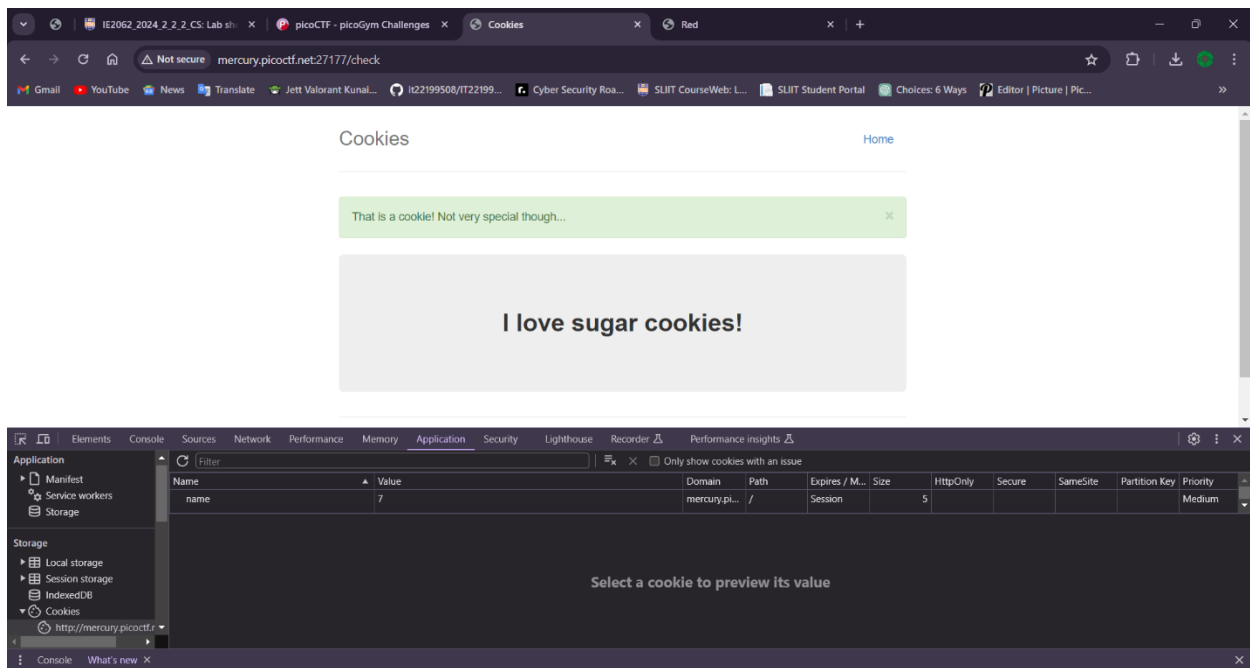


- Go to inspect and go to cookies, there you can find or see the cookie's value and other details.

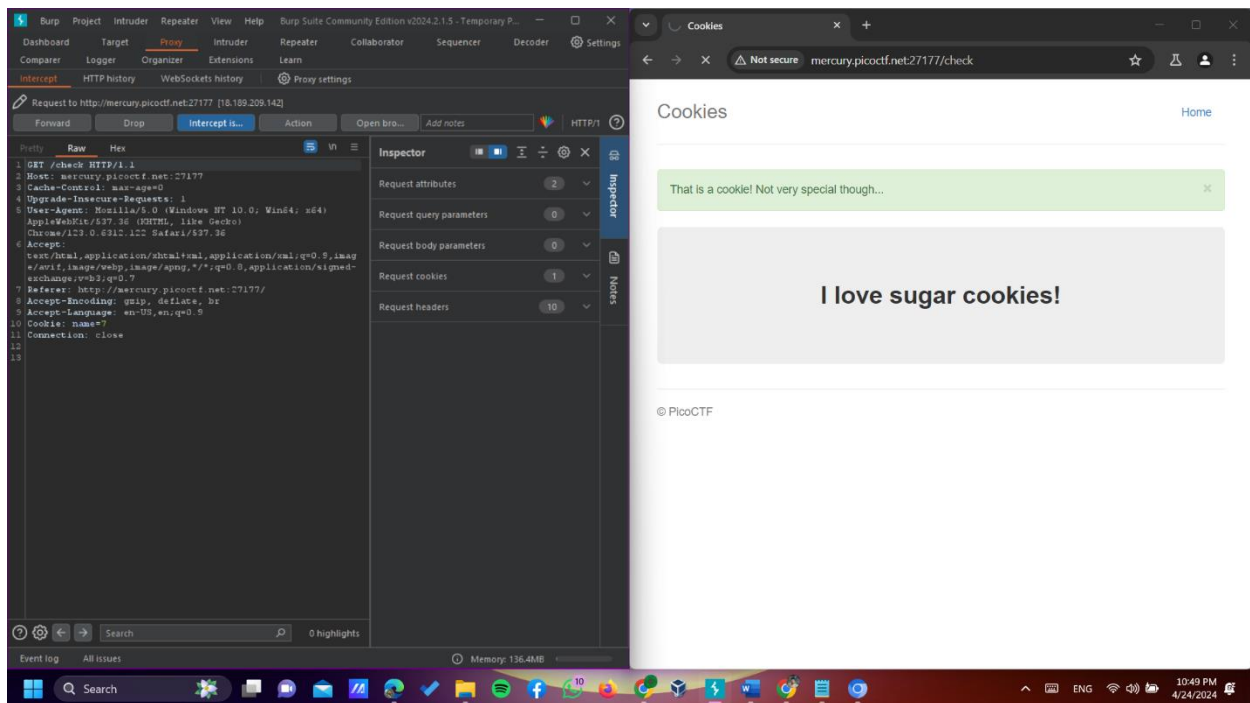


- By removing cookie or go back to home you can see changing the value bar, cause every cookie as it's own value. We can't enter any word cause, there have some specific cookies, specific means there are some general cookies with some names.





- Open burp and turn on intercept and get the RAW code.



- Go to HTTP history and check the host and send it to intruder.

The screenshot shows the Burp Suite interface with the HTTP history tab selected. A table lists several HTTP requests. The request at index 32 is highlighted, showing a GET request to `/check` with a status code of 200. The response view for this request is displayed below, showing an HTML document with a title 'Cookies' and several links. The 'Inspector' panel on the right shows the request attributes, cookies, headers, and response headers.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
21	https://macdn.bootstrapcdn.com	GET	/bootstrap/3.3.7/js/bootstrap.min.js			200	37943	script	js			✓	104.18.11.207		22:47:21 24 A...	8080
23	http://mercury.picoctf.net:27177	GET	/favicon.ico			404	319	HTML	ico	404 Not Found			18.189.209.142		22:47:32 24 A...	8080
24	http://mercury.picoctf.net:27177	POST	/search		✓	302	380	HTML		Redirecting...			18.189.209.142	name=3	22:47:41 24 A...	8080
25	http://mercury.picoctf.net:27177	GET	/check			200	1937	HTML		Cookies			18.189.209.142	session=	22:47:42 24 A...	8080
26	http://mercury.picoctf.net:27177	GET	/check			200	1937	HTML		Cookies			18.189.209.142	session=	22:47:43 24 A...	8080
27	http://mercury.picoctf.net:27177	GET	/reset			302	403	HTML		Redirecting...			18.189.209.142	name=	22:48:23 24 A...	8080
28	http://mercury.picoctf.net:27177	GET	/reset			302	403	HTML		Redirecting...			18.189.209.142	name=	22:49:05 24 A...	8080
29	http://mercury.picoctf.net:27177	GET	/			302	366	HTML		Redirecting...			18.189.209.142	name=1	22:49:06 24 A...	8080
30	http://mercury.picoctf.net:27177	GET	/			200	2129	HTML		Cookies			18.189.209.142		22:49:07 24 A...	8080
31	http://mercury.picoctf.net:27177	POST	/search		✓	302	380	HTML		Redirecting...			18.189.209.142	name=7	22:49:10 24 A...	8080
32	http://mercury.picoctf.net:27177	GET	/check			200	1932	HTML		Cookies			18.189.209.142	session=	22:49:12 24 A...	8080
33	http://mercury.picoctf.net:27177	GET	/check										18.189.209.142		22:49:16 24 A...	8080

Request

```

1 GET /check HTTP/1.1
2 Host: mercury.picoctf.net:27177
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://mercury.picoctf.net:27177/
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
10 Cookie: name=7
11 Connection: close
12
13

```

Response

```

1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Length: 1771
4 Set-Cookie: session=, Expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0; Path=/
5
6 <!DOCTYPE html>
7 <html lang="en">
8
9 <head>
10 <title>
11 Cookies
12 </title>
13
14 <link href="https://macdn.bootstrapcdn.com/bootstrap/3.2.0/css/bootstrap.min.css" rel="stylesheet">
15
16 <link href="https://getbootstrap.com/docs/3.2/examples/jumbotron-narrow/jumbotron-narrow.css" rel="stylesheet">
17
18 <script src="https://ajax.googleapis.com/ajax/libs/jquery/2.3.1/jquery.min.js">
19 </script>
20

```

Inspector

Request attributes: 2

Request cookies: 1

Request headers: 10

Response headers: 3

Memory: 136.4MB

- In intruder, there you can see the Cookie: name 7 and add §§ to the value 7

The screenshot shows the Burp Suite Intruder interface. The 'Choose an attack type' dropdown is set to 'Sniper'. The 'Payload positions' section shows a list of positions where payloads can be inserted. The 'Target' is set to `http://mercury.picoctf.net:27177`. The 'Update Host header to match target' checkbox is checked. The 'Payload positions' list shows a single position at index 10, corresponding to the 'Cookie: name=7' header. The 'Add §' button is highlighted.

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://mercury.picoctf.net:27177` ☒ Update Host header to match target

1 GET /check HTTP/1.1

2 Host: mercury.picoctf.net:27177

3 Cache-Control: max-age=0

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36

6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

7 Referer: http://mercury.picoctf.net:27177/

8 Accept-Encoding: gzip, deflate, br

9 Accept-Language: en-US,en;q=0.9

10 Cookie: name=7§

11 Connection: close

12

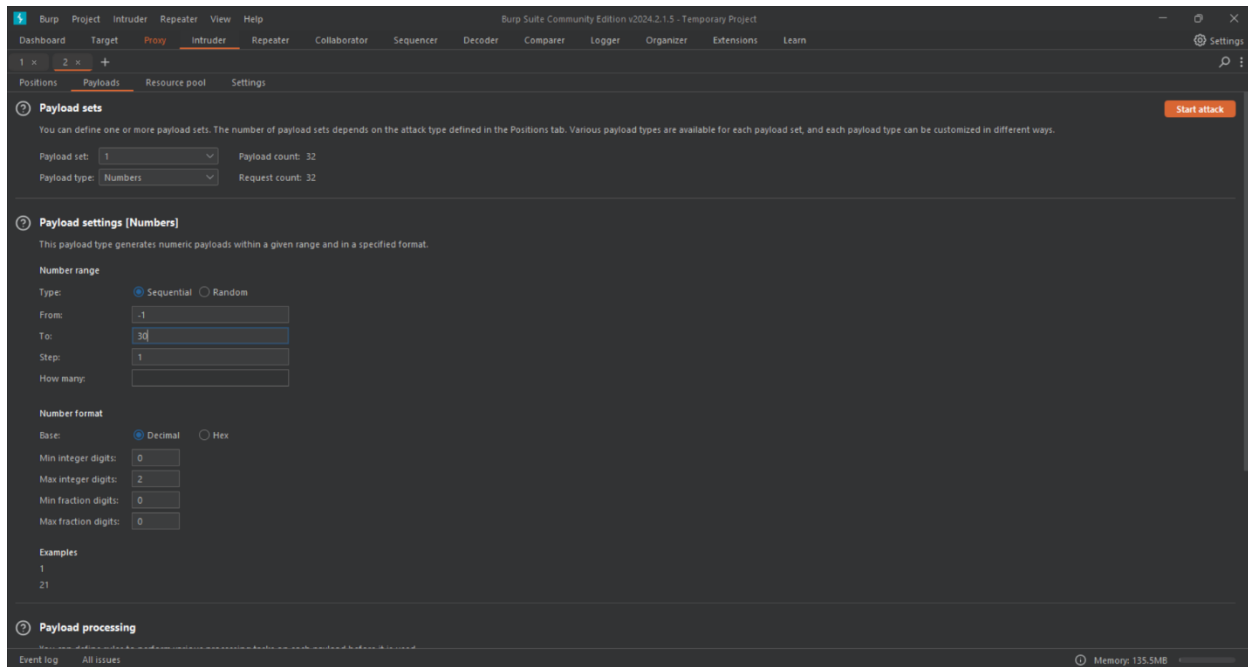
13

1 payload position

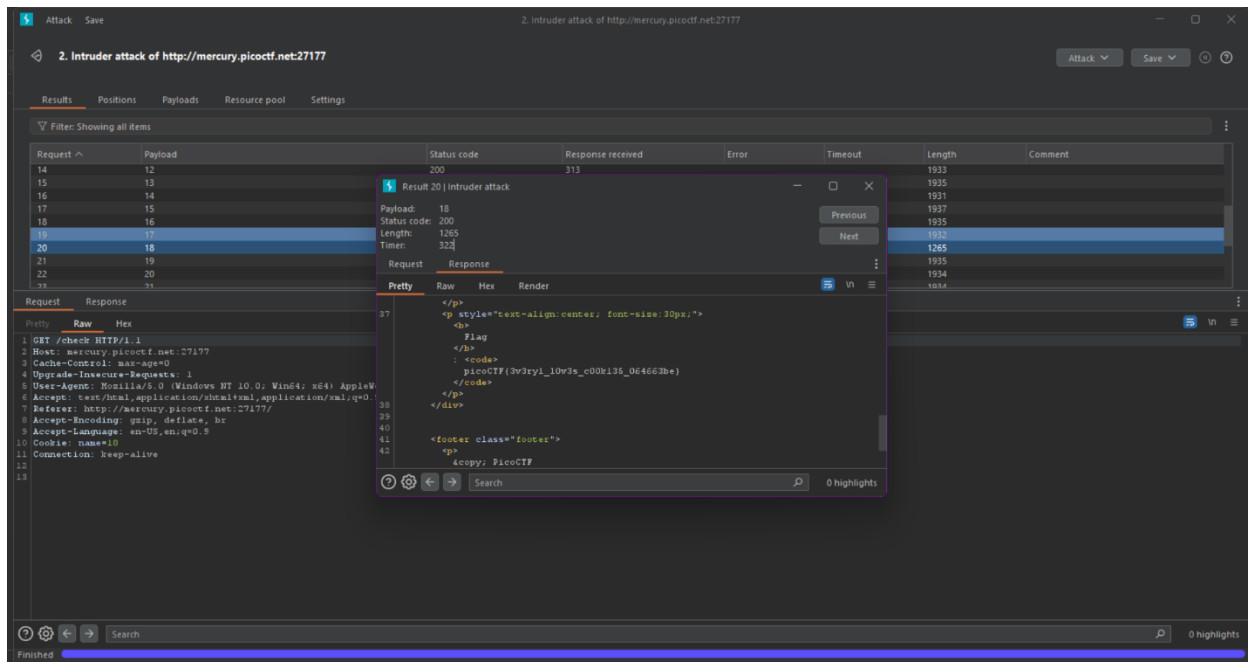
Length: 537

Memory: 136.4MB

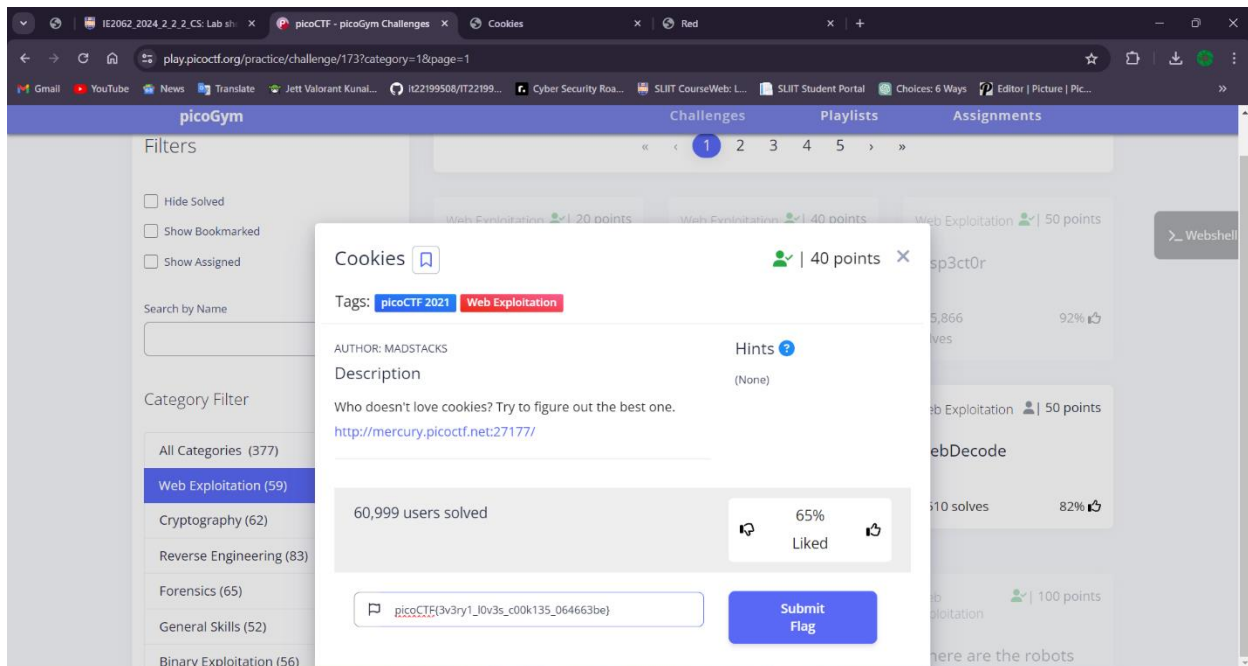
- Go to payload and set payload type as number and set payload setting as from -1 to 30 and start the attack.



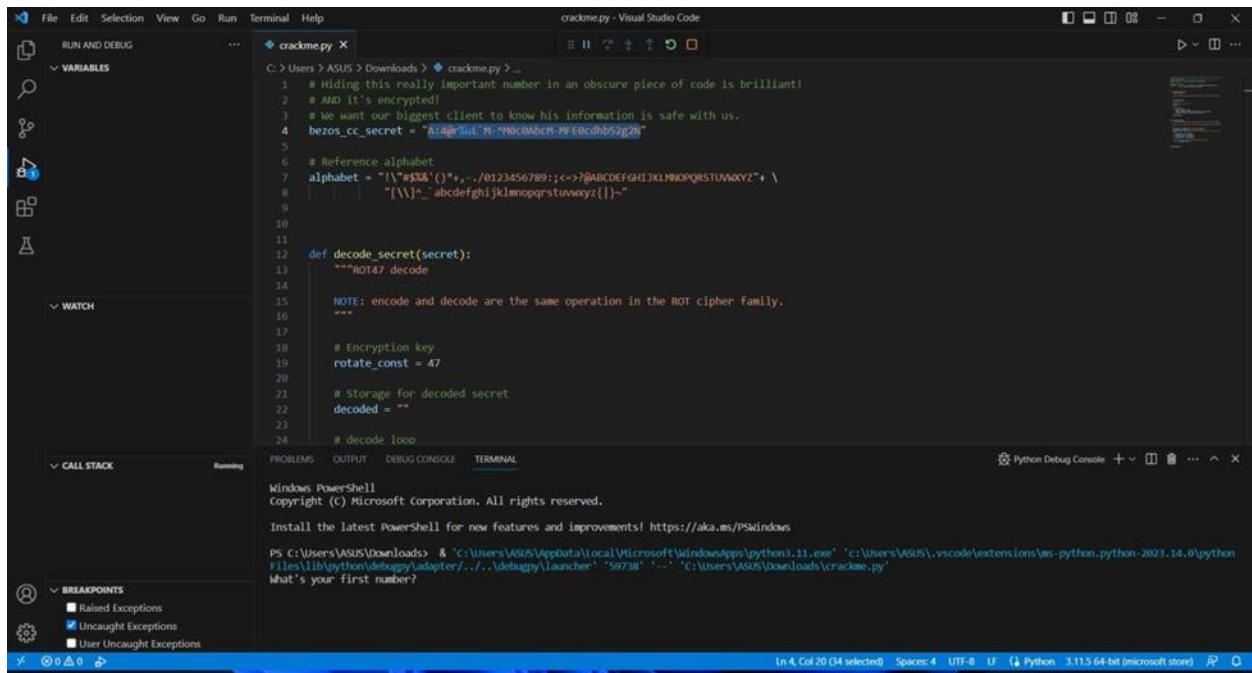
- After the attack, see the results. You can see in 20th position in 18th payload, click it and go to response and check the code, there you can see the flag in there.



- Flag is : picoCTF{3v3ry1_10v3s_c00k135_064663be} and submit the flag and earn the points.

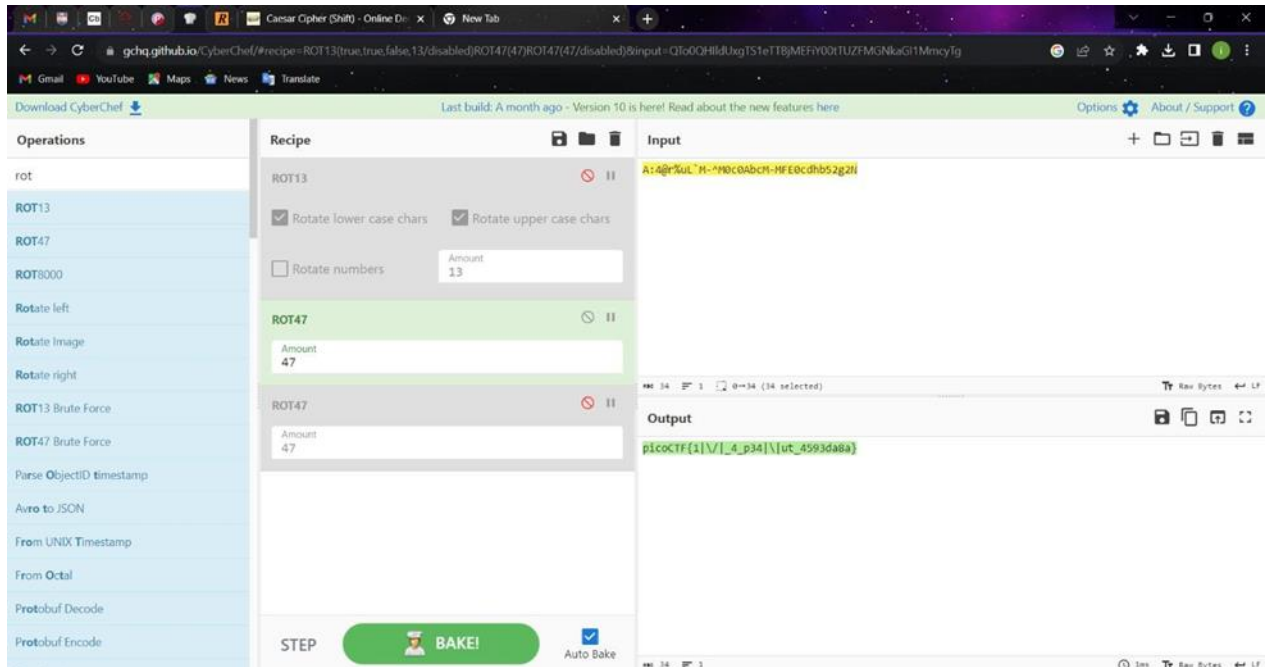


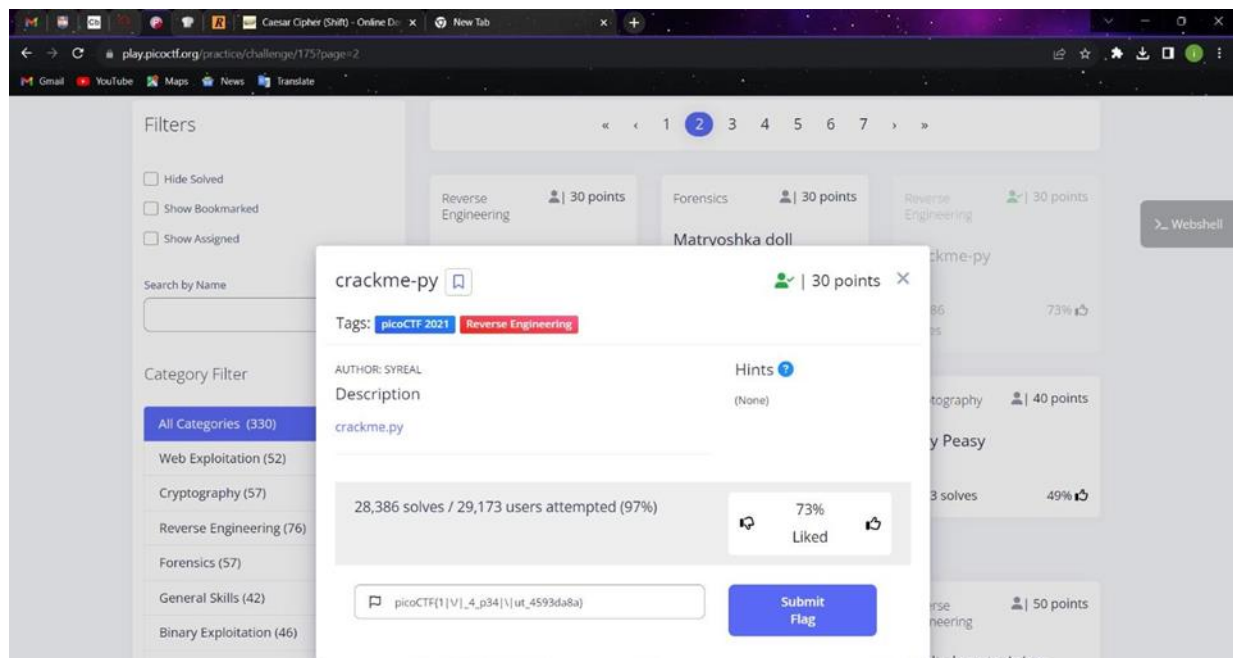
3) Crackme-py



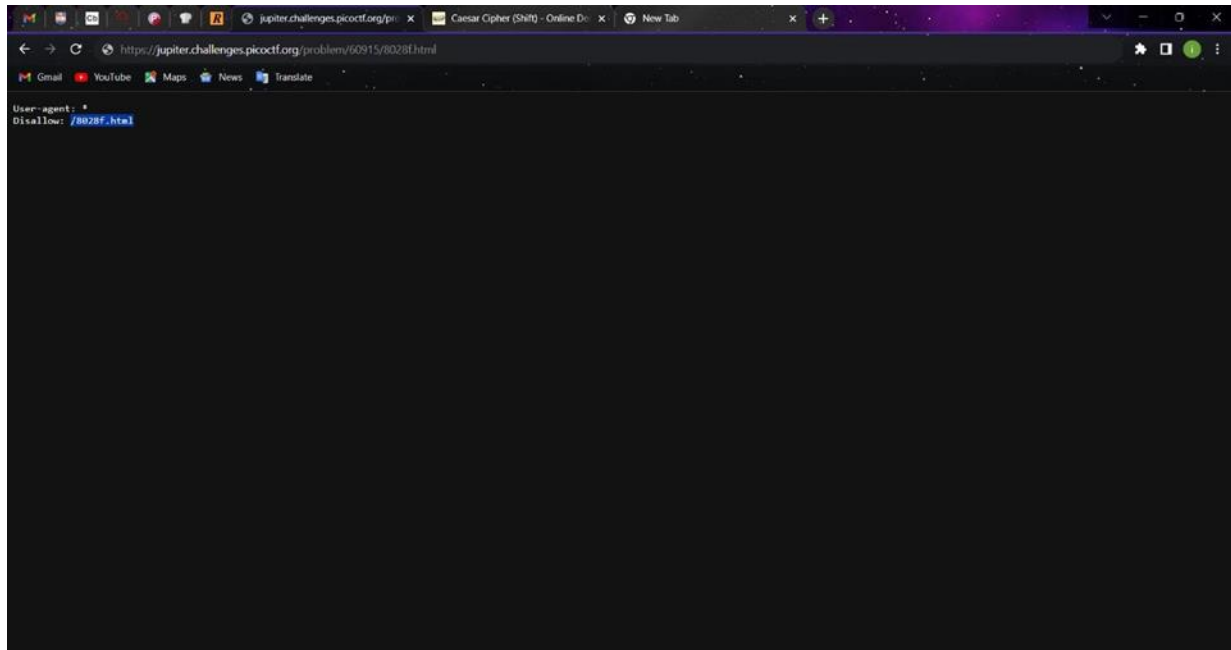
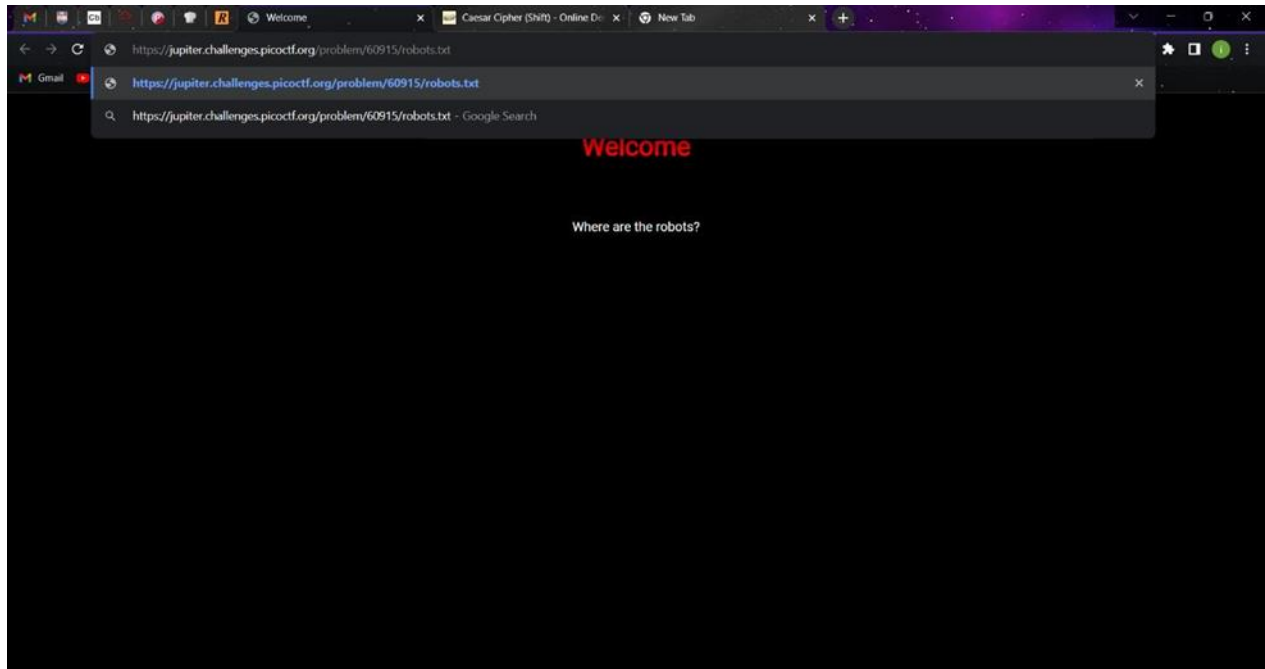
```
1 # Hiding this really important number in an obscure piece of code is brilliant!
2 # And it's encrypted!
3 # We want our biggest client to know his information is safe with us.
4 bezos_cc_secret = "A:4@r%uL"R~^NKC0ABCH-MFE0cdhb52g2l"
5
6 # Reference alphabet
7 alphabet = "1\\\"s3X'()*+,-./0123456789:;<=>@ABCDEFGHIJKLMNPQRSTUWXYZ+ \
8           \"[\\]_`abcdefghijklmnopqrstuvwxyz{|}~\"
9
10
11
12 def decode_secret(secret):
13     """ROT47 decode
14
15     NOTE: encode and decode are the same operation in the ROT cipher family.
16     """
17
18     # Encryption key
19     rotate_const = 47
20
21     # Storage for decoded secret
22     decoded = ""
23
24     # decode loop
```

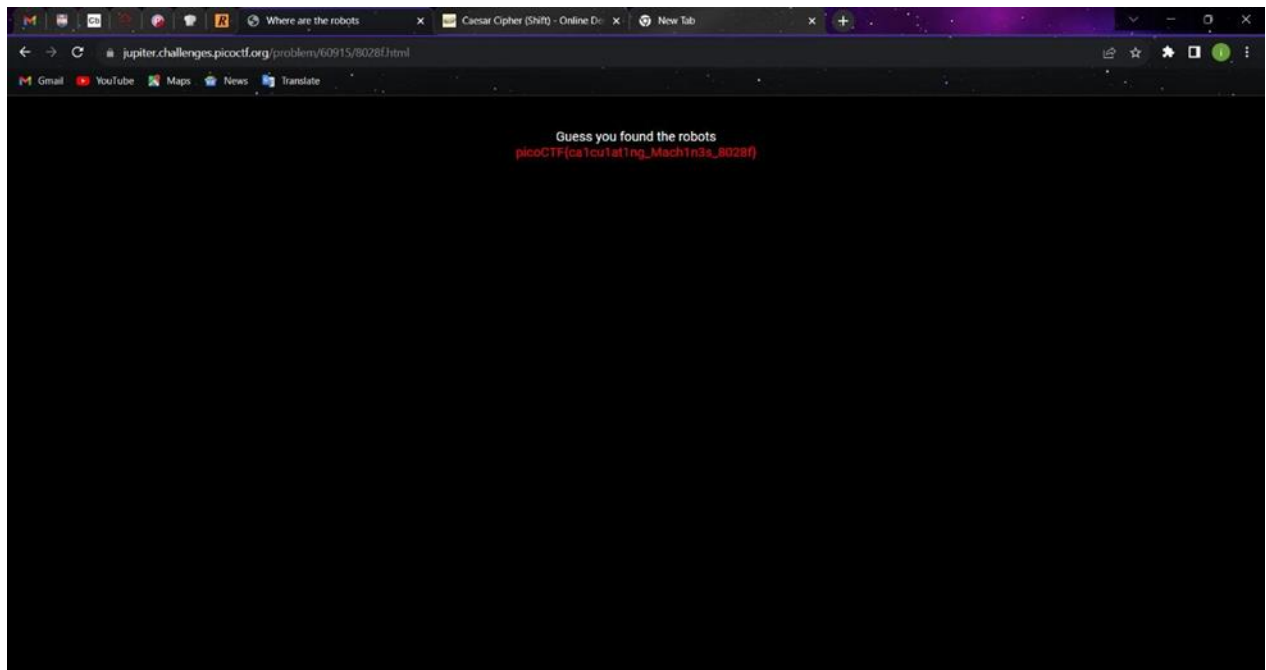
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>
PS C:\Users\ASUS\Downloads> & "C:\Users\ASUS\AppData\Local\Microsoft\WindowsApps\python3.11.exe" "C:\Users\ASUS\.vscode\extensions\ms-python.python-2023.14.0\pythonFiles\lib\python\debugpy\adapter\..\..\debugpy\launcher" "59738" "-:" "C:\Users\ASUS\Downloads\crackme.py"
What's your first number?



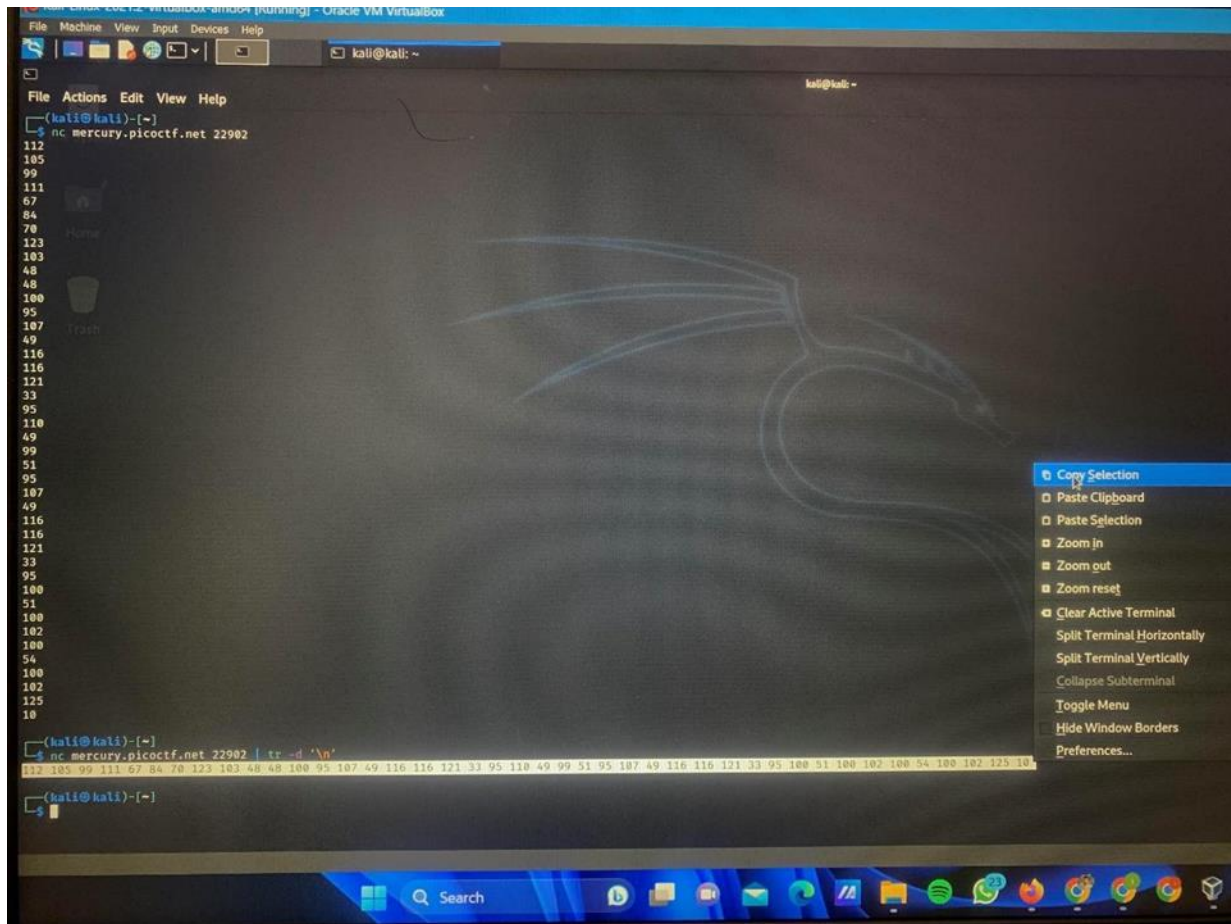


4) Where are the robots





5) Nice netcat...



Caesar Cipher (Shift) - Online D... x New Tab

rapidtables.com/convert/number/ascii-hex-bin-dec-converter.html

0x/0b prefix

ASCII text

picoCTF{g00d_k1tty!_n1c3_k1tty!_d3df6d6f}

Hex (bytes)

70 69 63 6F 43 54 46 78 67 30 30 64 5F 68 31 74 74 79 21 5F 6E
31 63 33 5F 68 31 74 74 79 21 5F 64 33 64 66 64 36 64 66 7D 0A

Binary (bytes)

01110000 01101001 01100011 01101111 01000011 01010100 01000110
01111011 01100111 00110000 00110000 01100100 01011111 01101011

Decimal (bytes)

112 105 99 111 67 84 78 123 105 48 48 100 95 107 49 116 116 121 33 95 100 51 100
121 33 95 110 49 99 51 95 107 49 116 116 121 33 95 100 51 100
102 100 54 100 102 125 10

Base64

cG1jb0NURntnMDBkX2sxdHR5IV9uMzZsX2sxdHR5IV9kM2RmZDZkZn0K

Length (bytes)

42

Checksum

8-bit Sum 67

Sign up

INTUIT quickbooks

NUMBER CONVERSION

- ASCII,Hex,Binary,Decimal converter
- ASCII to binary
- ASCII to hex
- Base converter
- Binary converter
- Binary to ASCII
- Binary to decimal
- Binary to hex

Caesar Cipher (Shift) - Online D... x New Tab

play.picoctf.org/practice/challenge/156/page=1

Filters

Hide Solved
Show Bookmarked
Show Assigned

Search by Name

Category Filter

All Categories (330)

Web Exploitation (52)
Cryptography (57)
Reverse Engineering (76)
Forensics (57)
General Skills (42)
Binary Exploitation (46)

Nice netcat... 15 points

Tags: picoCTF 2021 General Skills

AUTHOR: SYREAL

Description

There is a nice program that you can talk to by using this command in a shell: `$ nc mercury.picoctf.net 22907`, but it doesn't speak English...

96,410 solves / 100,533 users attempted (96%)

89% Liked

Submit Flag

picoCTF{g00d_k1tty!_n1c3_k1tty!_d3df6d6f}