

PicoCTF - WebDecode Writeup

Open (<http://mercury.picoctf.net:25992>) in Firefox.

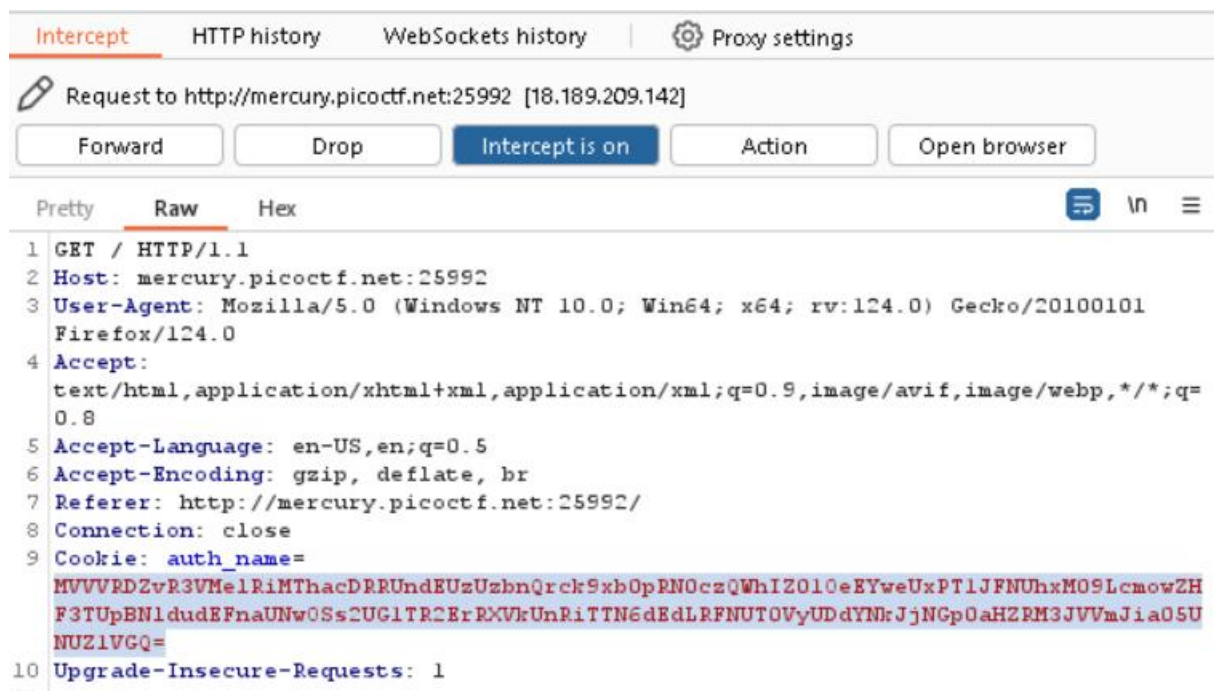
More Cookies

[Reset](#)

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

© PicoCTF

I took a peek at Burp Suite Intercept.



At the request payload, There was an interesting string at line 9, something related to cookie.

I decoded it with Base64 decoder, but it only returned another random string.

In a writeup according to

(<https://mrshan.medium.com/picoctf-more-cookies-web-exploitation-1238e29e75fe>),
there was a python script to brute force that said string into a flag.

The script was here

(<https://github.com/HHousen/PicoCTF-2021/blob/master/Web%20Exploitation/More%20Cookies/script.py>)

I need to edit the "cookie" variable first with my own cookie I got from Burp Suite.

And then I executed the script using python3 with Kali Linux.

```
(lolpotch@DESKTOP-FL6EJ09) ~  
$ python3 script.py  
Bruteforcing Bit: 100% | 96/96 [01:02<00:00, 1.54it/s]  
Bruteforcing Bit: 100% | 96/96 [01:01<00:00, 1.55it/s]  
Bruteforcing Bit: 100% | 96/96 [01:01<00:00, 1.57it/s]  
Bruteforcing Bit: 100% | 96/96 [01:02<00:00, 1.54it/s]  
Bruteforcing Bit: 100% | 96/96 [01:00<00:00, 1.58it/s]  
Bruteforcing Bit: 100% | 96/96 [01:00<00:00, 1.58it/s]  
Bruteforcing Bit: 100% | 96/96 [00:59<00:00, 1.62it/s]  
Bruteforcing Bit: 100% | 96/96 [01:01<00:00, 1.57it/s]  
Bruteforcing Bit: 100% | 96/96 [01:00<00:00, 1.59it/s]  
Bruteforcing Position: 90% | 9/10 [09:09<01:00, 60.59s/it]  
flag: picoCTF{cO0ki3s_yum_82f39377}  
Bruteforcing Bit: 1% | 1/96 [00:00<00:58, 1.63it/s]  
Bruteforcing Position: 100% | 10/10 [09:11<00:00, 55.12s/it]
```

And there you go.

Flag: picoCTF{cO0ki3s_yum_82f39377}