findme

Web Exploitation

Description:

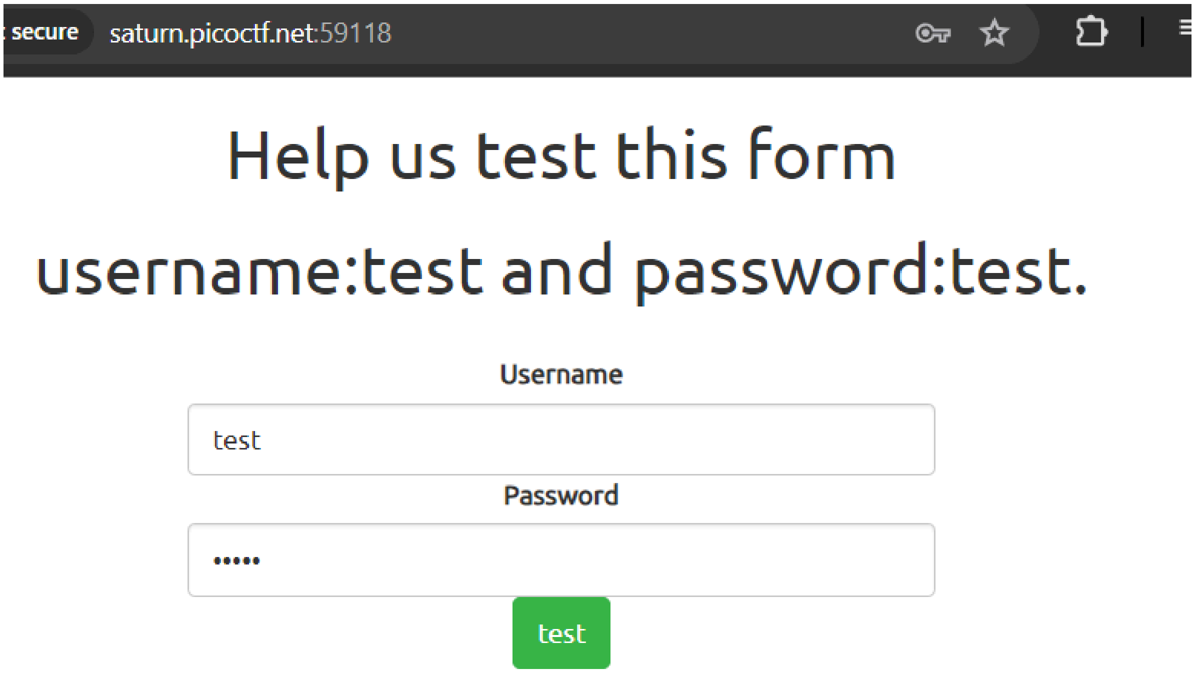
Help us test the form by submitting the username as `test` and password as `test!`

Additional details will be available after launching your challenge instance.

Hints:

1) any redirections?

Solution:



Help us test this form

username:test and password:test.

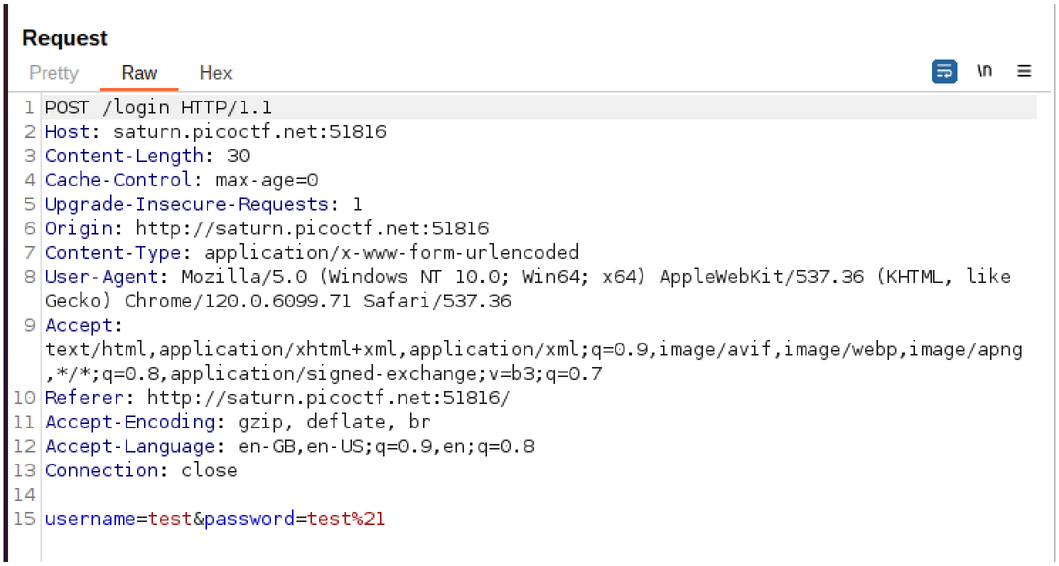
Username

test

Password

•••••

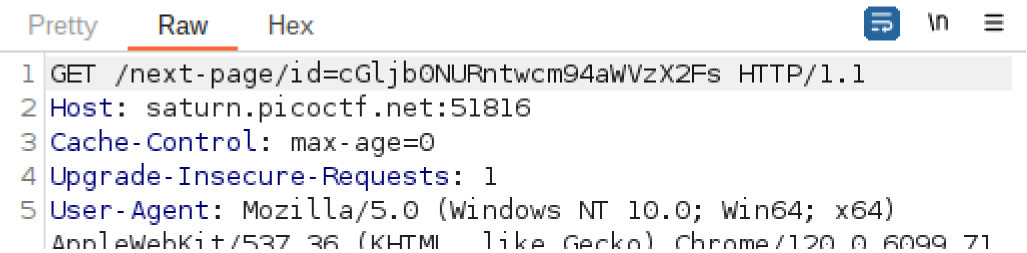
1) We open the website in burpsuite.



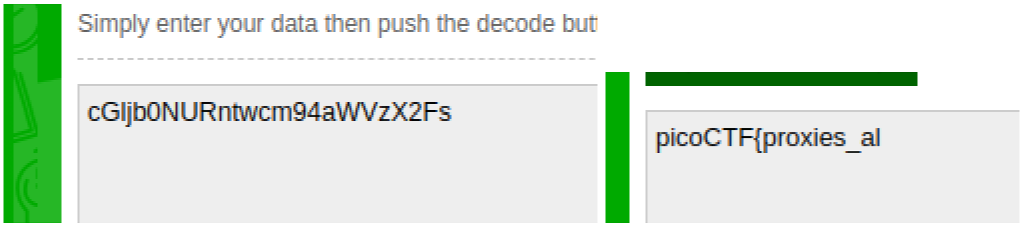
```
POST /login HTTP/1.1
Host: saturn.picoctf.net:51816
Content-Length: 30
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://saturn.picoctf.net:51816
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/120.0.6099.71 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
Referer: http://saturn.picoctf.net:51816/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

username=test&password=test%21
```

2) When we send the initial request in the repeater we get the first half of the flag encoded in base64.
3) And then when we send it again we get the second half of the flag in base64.

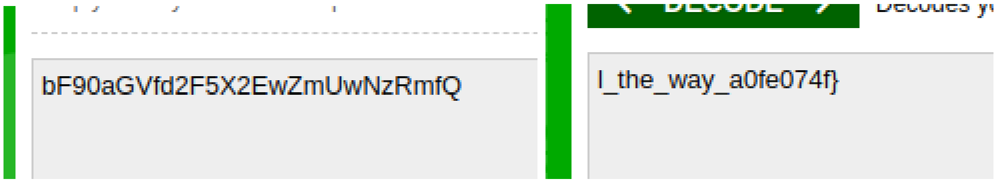


```
GET /next-page/id=cGljb0NURntwcm94aWVzX2Fs HTTP/1.1
Host: saturn.picoctf.net:51816
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71
```


Simply enter your data then push the decode but

cGljb0NURntwcm94aWVzX2Fs

picoCTF{proxies_al



bF90aGVfd2F5X2EwZmUwNzRmfQ

l_the_way_a0fe074f}

Flag:
picoCTF{proxies_all_the_way_a0fe074f}