

GET aHEAD

Web Exploitation

Description:

Find the flag being held on this server to get ahead of the competition <http://mercury.picoctf.net:15931/>

Hints:

- 1) Maybe you have more than 2 choices
- 2) Check out tools like Burpsuite to modify your requests and look at the responses

Solution:



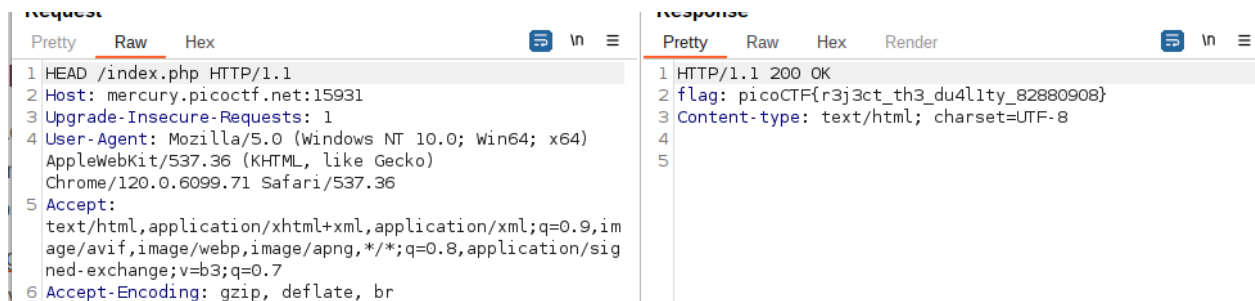
request

Pretty Raw Hex



```
1 GET /index.php HTTP/1.1
2 Host: mercury.picoctf.net:15931
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
```

- 1) We open the website using burpsuite and send it to the repeater.
- 2) We see that both the red and blue look similar.
- 3) In the repeater we see that there is a HEAD prefix and as the name of the challenge suggests we need to change it to HEAD.
- 4) After doing so we get the flag.



The screenshot displays the Burp Suite interface with two panels: 'request' on the left and 'response' on the right. The 'request' panel shows a HEAD request to /index.php with various headers including Host, Upgrade-Insecure-Requests, User-Agent, Accept, and Accept-Encoding. The 'response' panel shows the corresponding 200 OK response with a flag in the body and a Content-type header.

```
request
Pretty Raw Hex
1 HEAD /index.php HTTP/1.1
2 Host: mercury.picoctf.net:15931
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,im
  age/avif,image/webp,image/apng,*/*;q=0.8,application/sig
  ned-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br

response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 flag: picoCTF{r3j3ct_th3_du4l1ty_82880908}
3 Content-type: text/html; charset=UTF-8
4
5
```

Flag:

picoCTF{r3j3ct_th3_du4l1ty_82880908}