

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:15931/>

Hints ?

1 2

Maybe you have more than 2 choices

49,594 solves / 53,693 users attempted (92%)

81% Liked

picoCTF{FLAG}

Submit Flag

Burp Suite Community

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extens

1 x 2 x 3 x +

Send Cancel < >

Request

Raw

Hex

1 HEAD /index.php? HTTP/1.1

2 Host: mercury.picoctf.net:15931

3 Cache-Control: max-age=0

4 Upgrade-Insecure-Requests: 1

5 User-Agent: Mozilla/5.0 (X11; Linux x86_64)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0

Safari/537.36

6 Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,ima

ge/avif,image/webp,image/apng,*/*;q=0.8,application/sign

d-exchange;v=b3;q=0.7

7 Referer: http://mercury.picoctf.net:15931/index.php

8 Accept-Encoding: gzip, deflate

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

10 Connection: close

11

12

Response

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

Writeup → It was a straightforward task that involved changing the type of HTTP request from the commonly used GET or POST to the HEAD method, which was required for this specific case.