

## [PicoCtf Web- (Get aHEAD)]

-->So lets see the Description:

GET aHEAD 

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/>

-->So the flag is in server-side. The hint are saying that.

Hints 

1 2


Maybe you have more than

2 choices 

Hints 

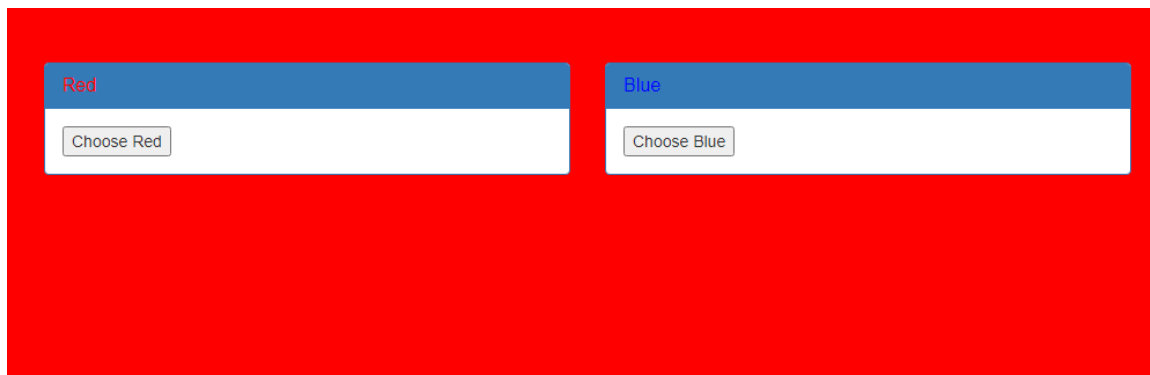
1 2

Check out tools like

Burpsuite to modify your requests and look at the responses 

-->There is something that are two and in 2nd hint we have to use burpsuit tool to modify request and see the response.

-->The website which is in description look,s like this.



-->When we choose Red or Blue it take me no where but it is changing path here.



-->After view source page i got this thing.

```
<form action="index.php" method="GET">
  <input type="submit" value="Choose Red"/>
</form>
</div>
<
<div class="col-md-6">
  <div class="panel panel-primary" style="margin-top:50px">
    <div class="panel-heading">
      <h3 class="panel-title" style="color:blue">Blue</h3>
    </div>
    <div class="panel-body">
      <form action="index.php" method="POST">
        <input type="submit" value="Choose Blue"/>
      </form>
    </div>
  </div>
</div>
```

-->Mean the two things that was in description was the two http request methods. So i got that third method willbe HEAD and also in description ahead is pointing towards HEAD request method.

-->Then i send HEAD request using curl.

```
picotf@webshell:~$ curl -I HEAD -i http://mercury.picotf.net:34561/
```

-->SO after sending HEAD request using curl to given website. I found this.

```
curl: (6) Could not resolve host: HEAD flag  
HTTP/1.1 200 OK  
flag: picoCTF{r3j3ct_th3_du4l1ty_8f878508} ←  
Content-type: text/html; charset=UTF-8
```

-->Hurry we found the flag. Well done brother...

By -->[PlayExploits]