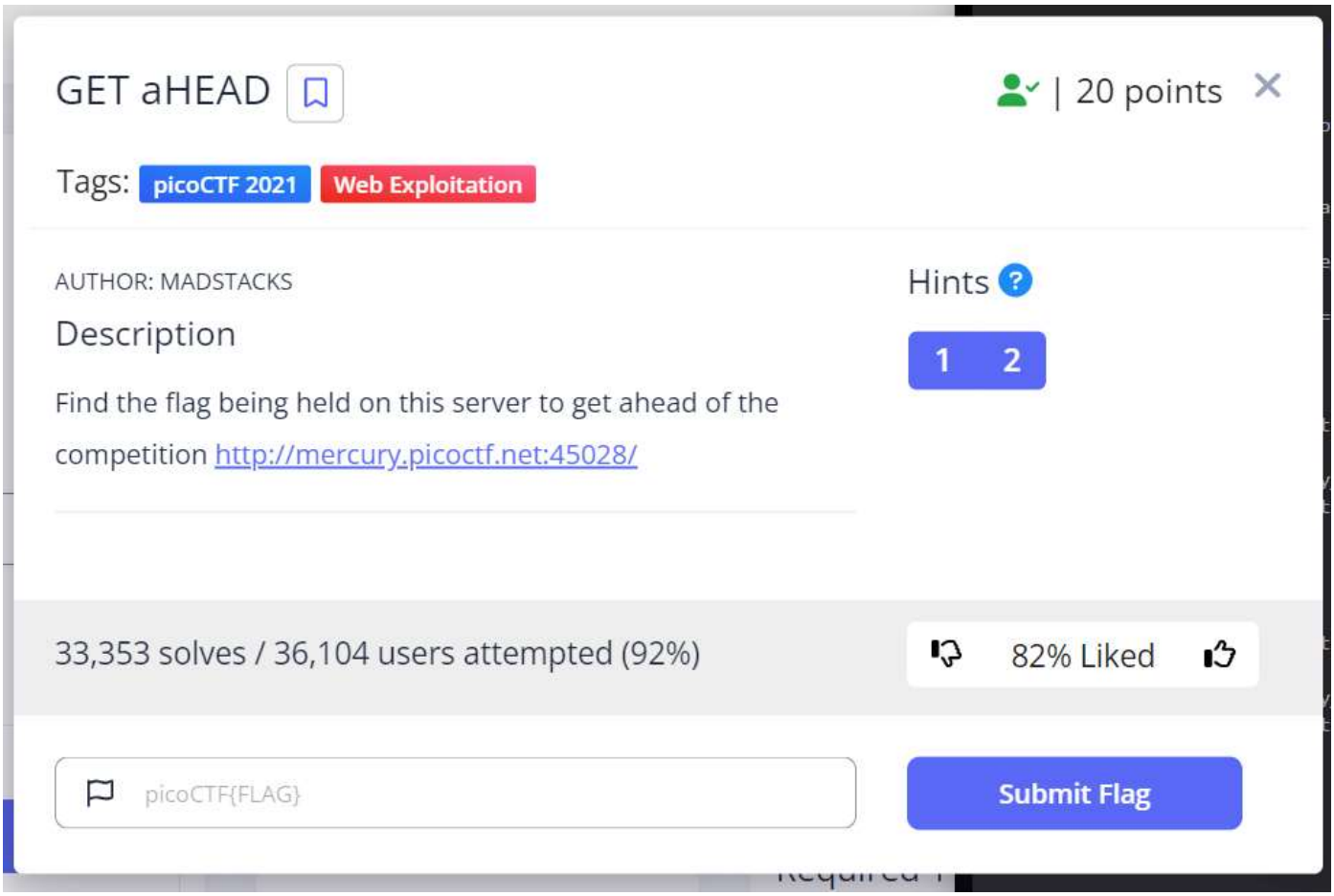
Learningwinterz
Aug 29 · 3 min read · Listen

picoCTF / GET aHEAD / Writeup

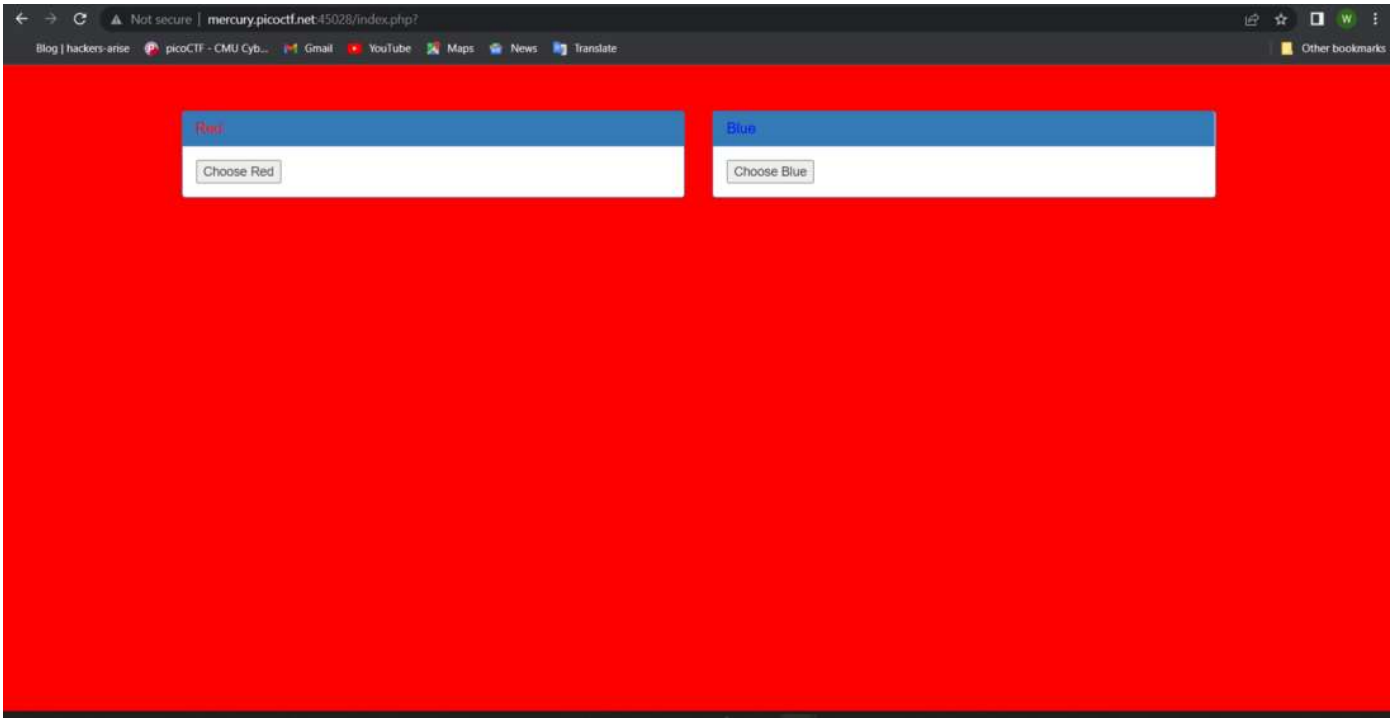


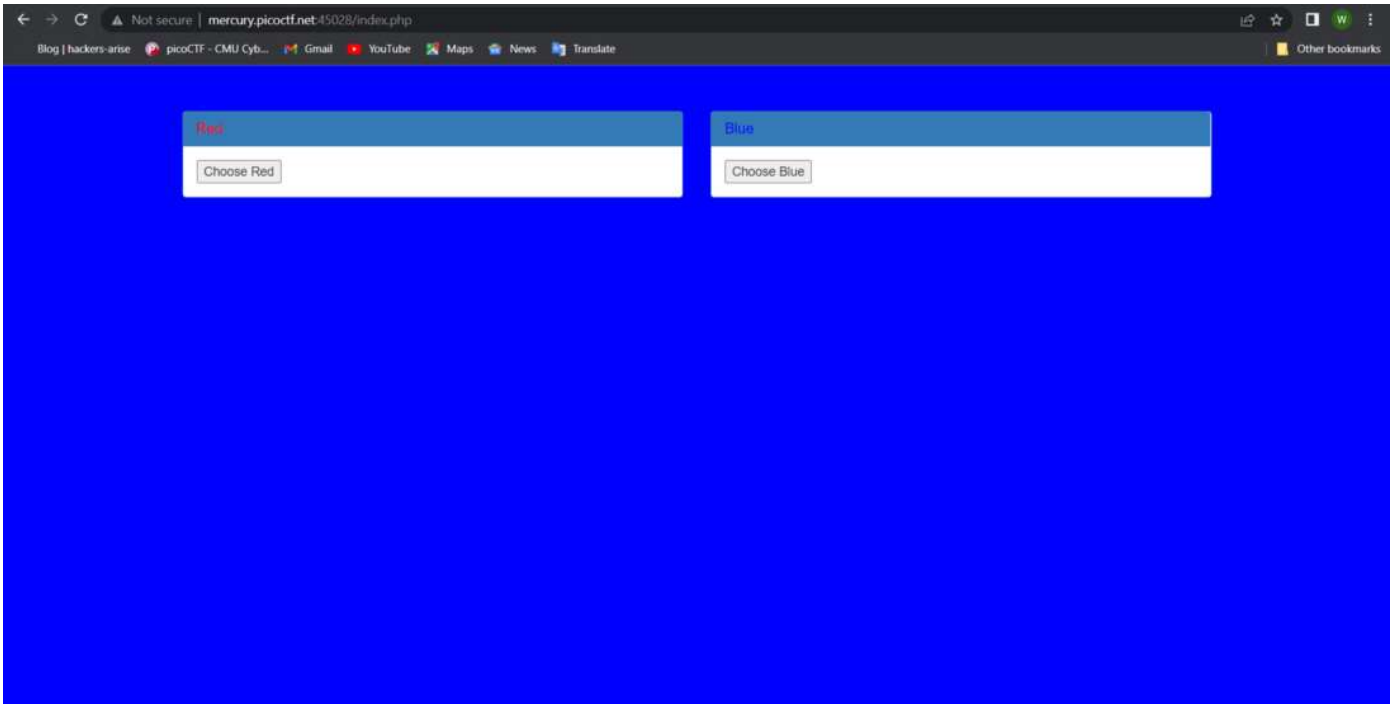
https://play.picoctf.org/practice/challenge/132?category=1&page=1

> ***Description :***

Find the flag being held on this server to get ahead of the competition http://mercury.picoctf.net:45028/

Hint 2: Check out tools like Burpsuite to modify your requests and look at the responses





SOLUTION :

Hint 1: Maybe you have more than 2 choices

let us look at the HTML code for this
PRESS F12 (OR) RIGHT CLICK → INSPECT

```
<!doctype html>
<html>
<head>
<title>Red</title>
<link rel="stylesheet" type="text/css"
href="//maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">
<style>body {background-color: red;}</style>
</head>
<body>
<div class="container">
<div class="row">
<div class="col-md-6">
<div class="panel panel-primary" style="margin-top:50px">
<div class="panel-heading">
<h3 class="panel-title" style="color:red">Red</h3>
</div>
<div class="panel-body">
<form action="index.php" method="GET">
<input type="submit" value="Choose Red"/>
</form>
</div>
</div>
</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>
```

```
<input type="submit" value="Choose Blue"/>
</form>
</div>
</div>
</div>
</div>
</div>
</body>
</html>
```

now we can see there are two methods.
"GET" — RED
"POST" — BLUE

so the hint is probably referring to a third method and lets try it with "HEAD" as it is in the title.
let's try "HEAD" request

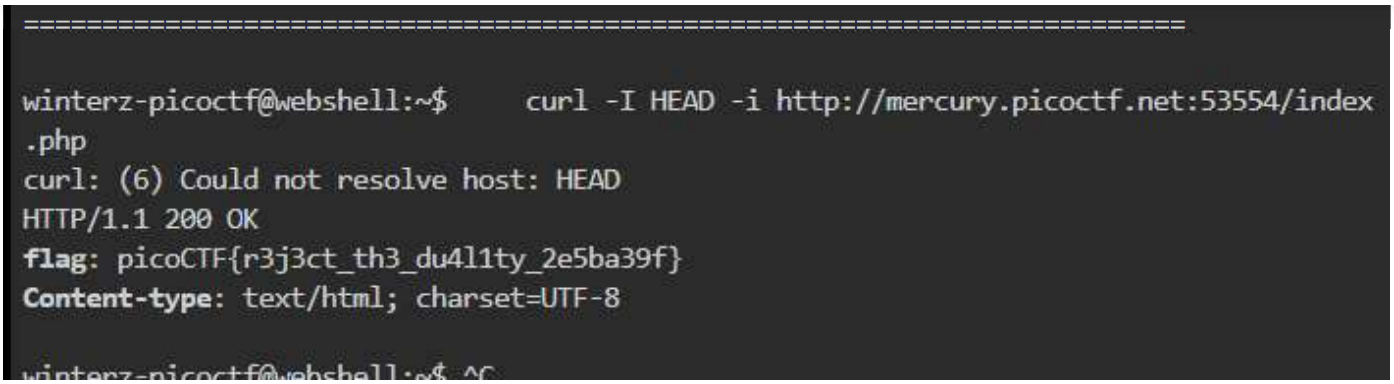
```
$ curl -I HEAD -i http://mercury.picoctf.net:53554/index.php
```

curl :

A command line tool and library for transferring data with URL syntax, supporting DICT, FILE, FTP,FTPS, GOPHER, GOPHERS, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP,
SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET and TFTP. libcurl offers a myriad of powerful features

which stands for client URL, is a command line tool that developers use to transfer data to and from a server. At the most fundamental, cURL lets you talk to a server by specifying the location (in the form of a URL) and the data you want to send

- ***I HEAD :*** *"-I" show document info only of HEAD*



> *NOTE:*

the url “http://mercury.picoctf.net:53554/index.php" will be different for diffenrnt users so check the url
while solving.