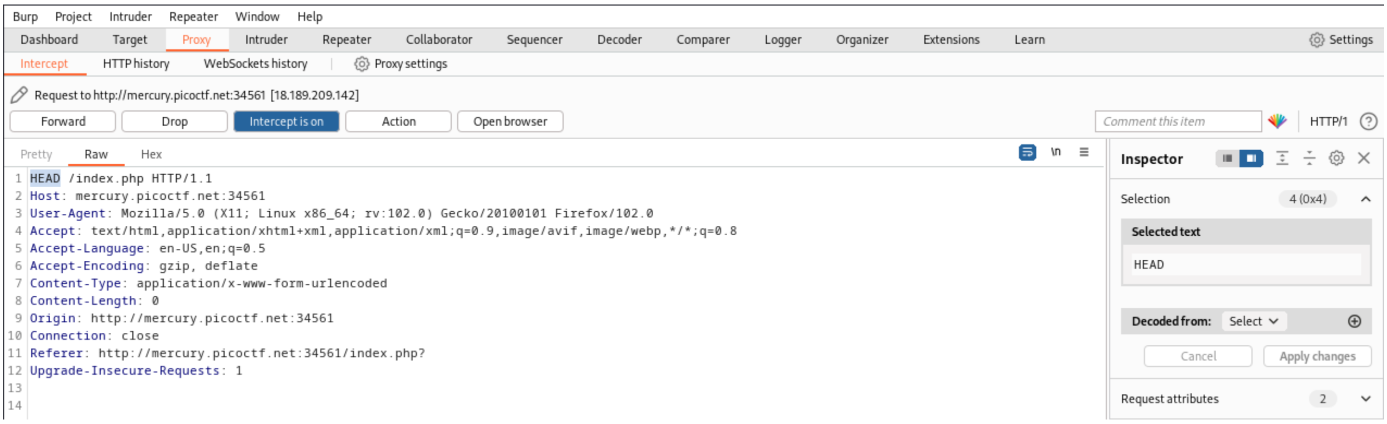
GET aHEAD

Walkthrough : https://github.com/vivian-dai/PicoCTF2021-Writeup/blob/main/Web Exploitation/Get aHead/Get aHead.md

Types of HTTP Requests : https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods

Using burpsuite, and foxy proxy, we can intercept the web traffic.
When clicking blue, we get a post request.
When clicking red, we get a get request.

Looking at the http request list, we can use burpsuite to modify the packets being sent to the website.



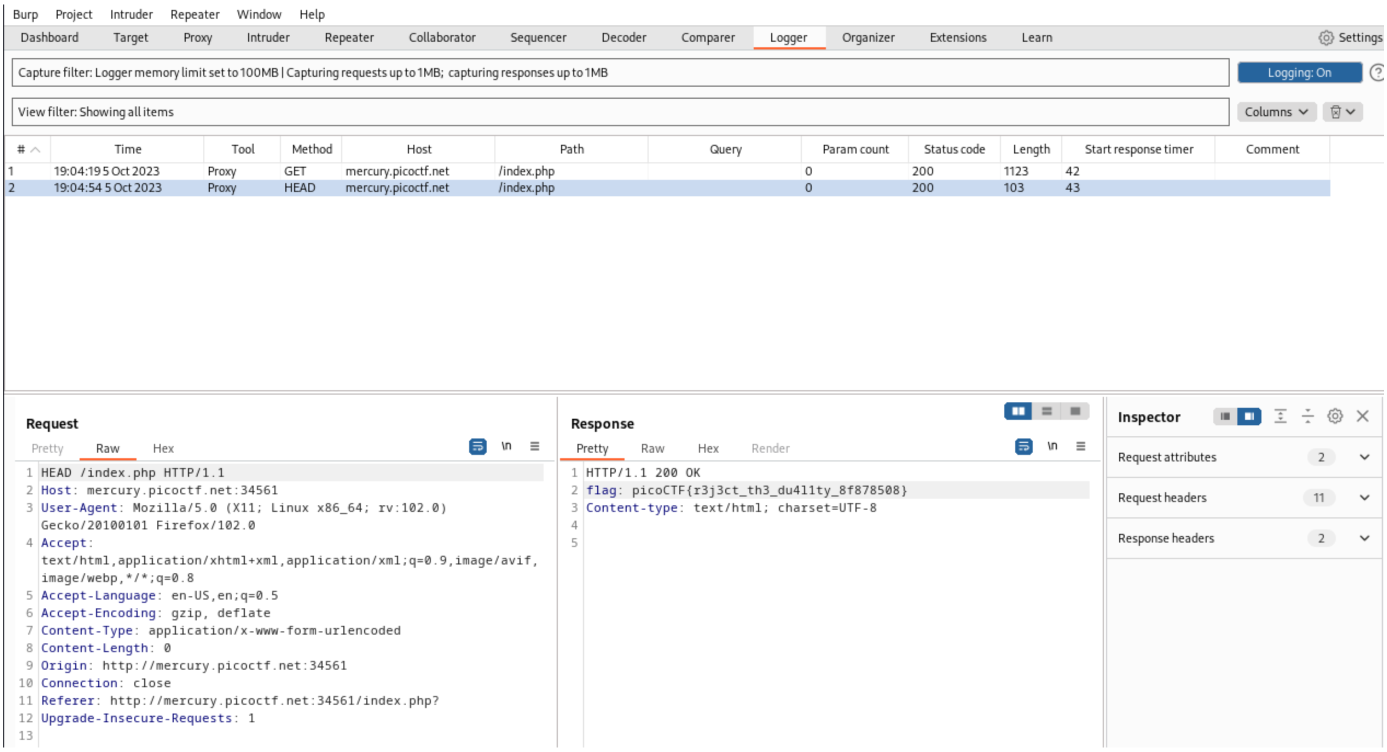
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Cancel Apply changes

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

```
HEAD /index.php HTTP/1.1
Host: mercury.picoctf.net:34561
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://mercury.picoctf.net:34561
Connection: close
Referer: http://mercury.picoctf.net:34561/index.php?
Upgrade-Insecure-Requests: 1
```

Selection 4 (0x4)
Selected text
HEAD
Decoded from: Select
Request attributes 2

So, when changing the request type to HEAD we get sent back the flag in burpsuite. Although the webpage is blank.



Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Logging: On
Columns
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector

Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
1	19:04:19 5 Oct 2023	Proxy	GET	mercury.picoctf.net	/index.php		0	200	1123	42	
2	19:04:54 5 Oct 2023	Proxy	HEAD	mercury.picoctf.net	/index.php		0	200	103	43	

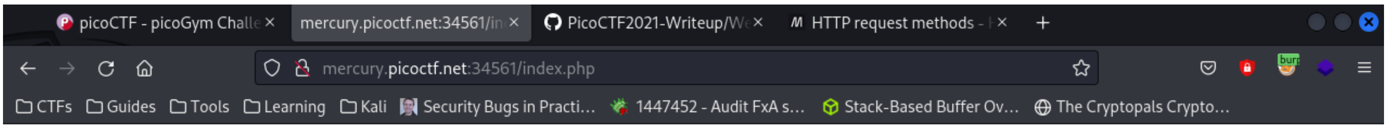
Request

```
HEAD /index.php HTTP/1.1
Host: mercury.picoctf.net:34561
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://mercury.picoctf.net:34561
Connection: close
Referer: http://mercury.picoctf.net:34561/index.php?
Upgrade-Insecure-Requests: 1
```

Response

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

Request attributes 2
Request headers 11
Response headers 2


picoCTF - picoGym Challe
mercury.picoctf.net:34561/in
PicoCTF2021-Writeup/W
HTTP request methods - I
mercury.picoctf.net:34561/index.php
CTFs
Guides
Tools
Learning
Kali
Security Bugs in Practi…
1447452 - Audit FxA s…
Stack-Based Buffer Ov…
The Cryptopals Crypto…