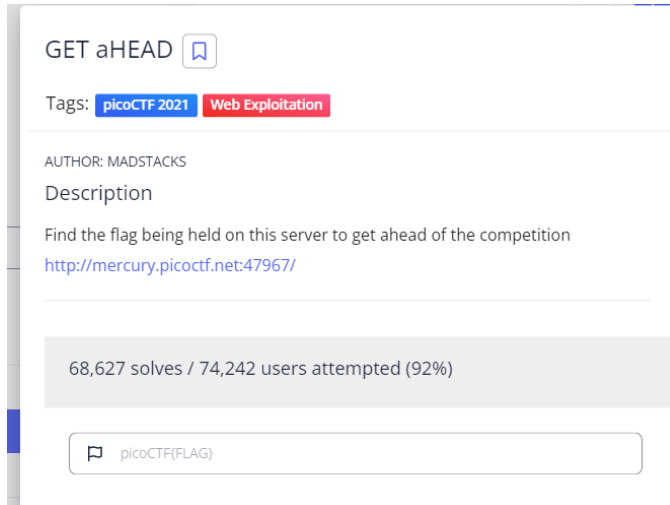
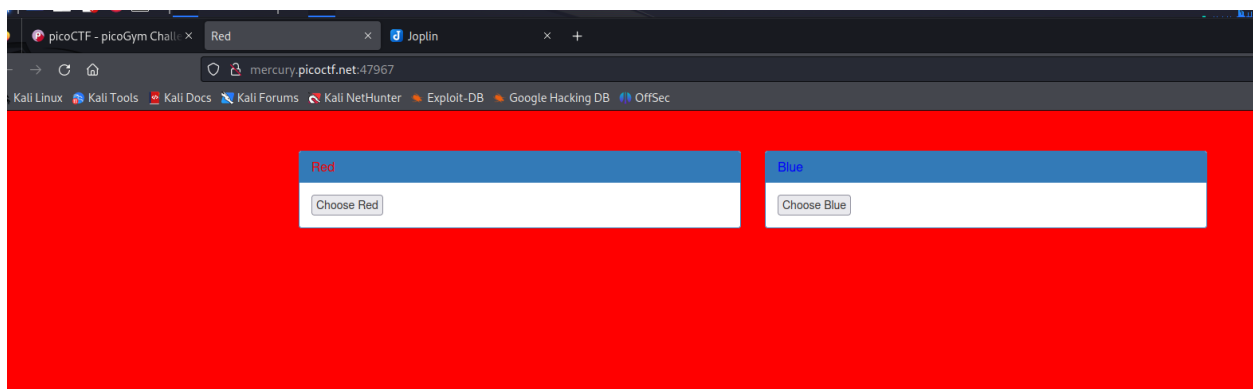


Pico CTF GET aHEAD

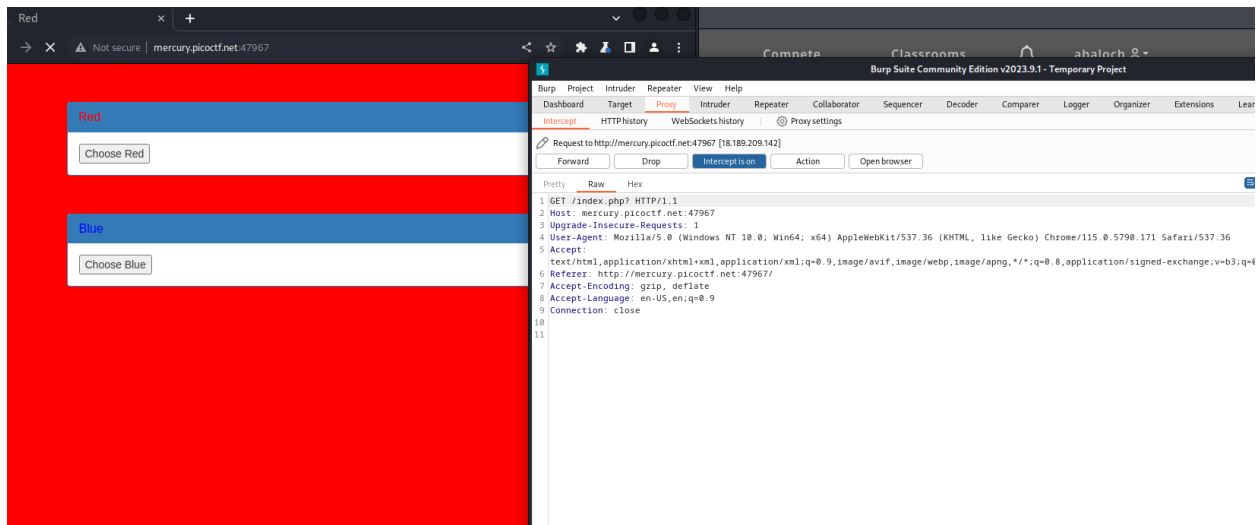
I am doing all ctf's on a kali linux machine.



To start I recognized that the title mentioned GET and HEAD requests so I had a feeling that the CTF would have to do something with that. Upon opening up the links I saw that we were presented with 2 options that changed the screen color from red to blue.



I then went to the page source and saw that there were get and post requests being made, but I did not know where to go from there. I then used the hints and saw that I could use Burpsuite which I pulled up and opened the link in the proxy tab.



I copied the link into a browser window within the proxy view. View history to see how requests are being handled. I then clicked on one of the requests and sent it to the repeater to see how it would react if I changed the request to HEAD instead of POST.

This gave me the flag.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	HEAD	/index.php	HTTP/1.1	1	HTTP/1.1	200	OK
2	Host:	mercury.picoctf.net:47967		2	flag:	picoCTF{x3j3ct_th3_du411ty_cca66bd3}	
3	Content-Length:	0		3	Content-type:	text/html; charset=UTF-8	
4	Cache-Control:	max-age=0		4			
5	Upgrade-Insecure-Requests:	1		5			
6	Origin:	http://mercury.picoctf.net:47967					
7	Content-Type:	application/x-www-form-urlencoded					
8	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36					
9	Accept:						

I then entered the flag into picoCTF and it worked!