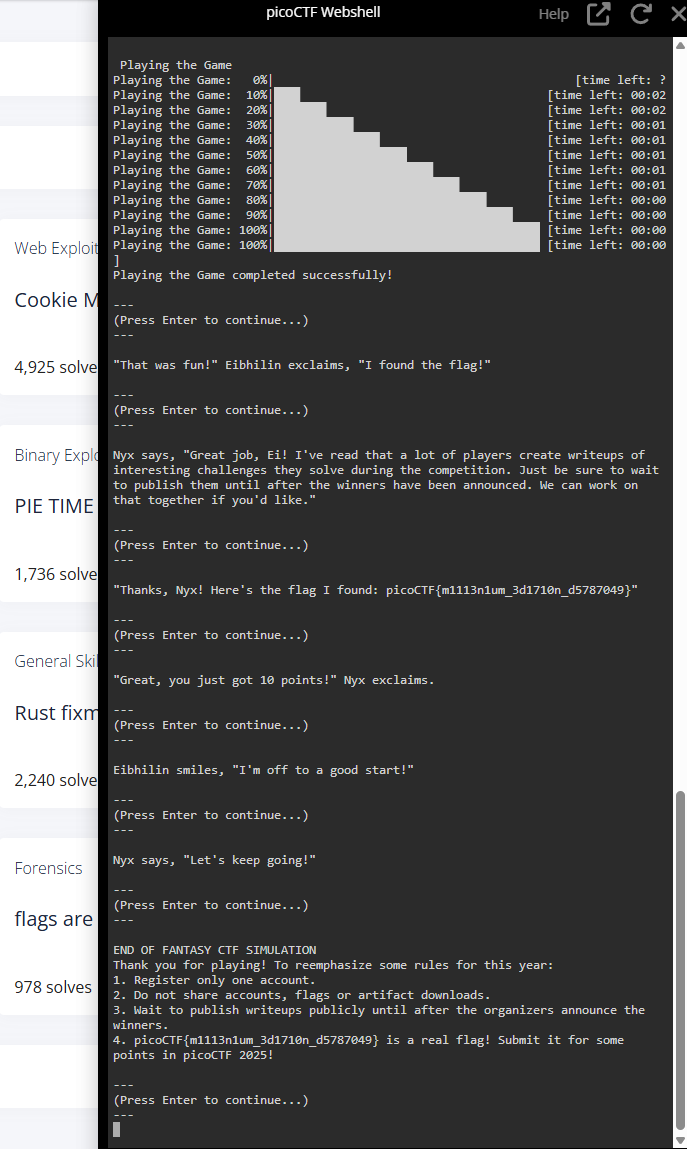
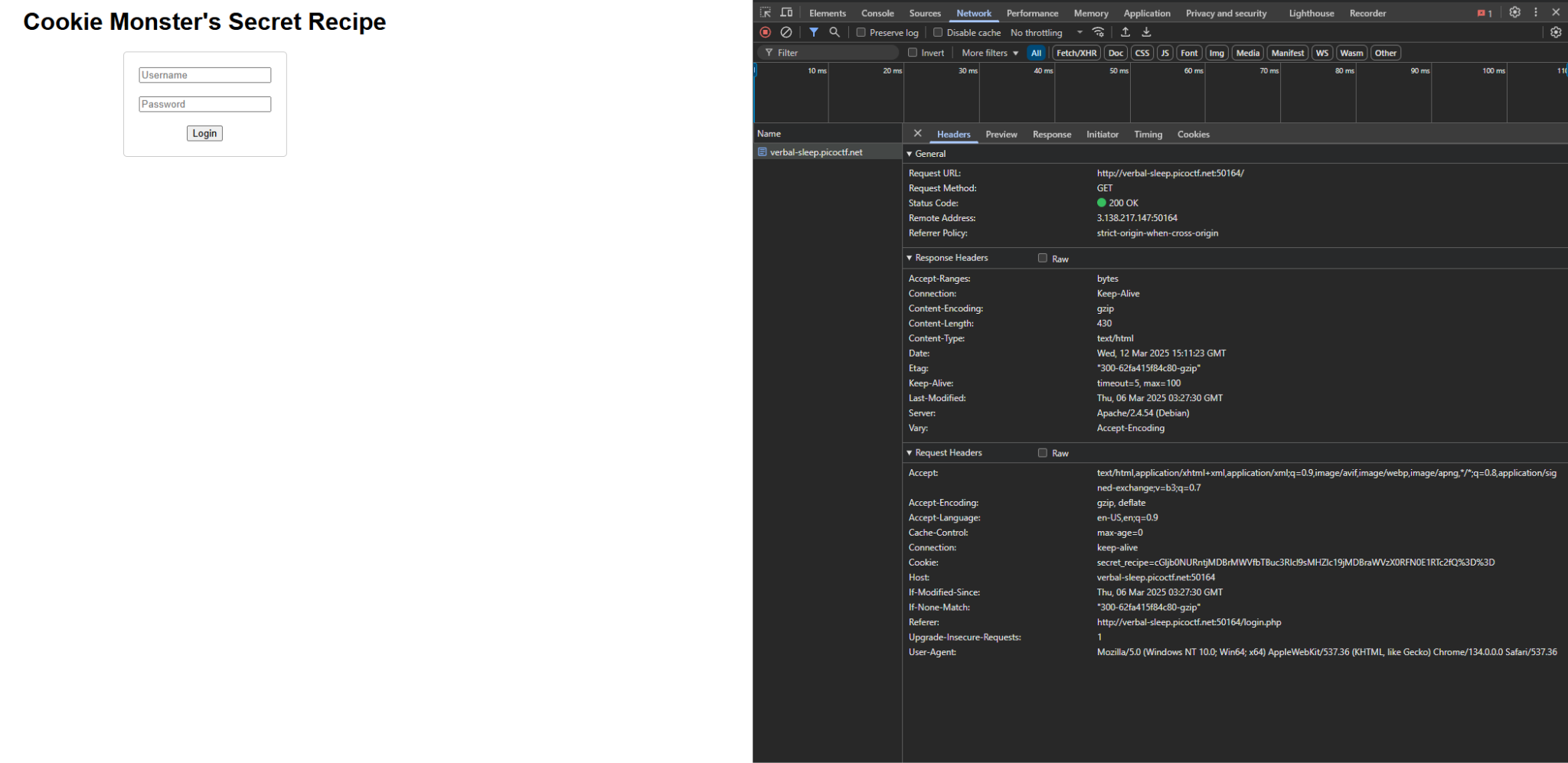
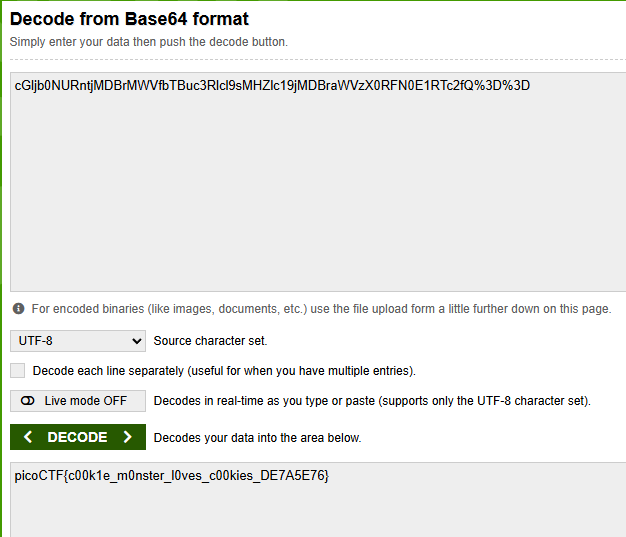
Fantasy CTF: I found the first flag by playing the game. I used the given netcat command and followed the instructions. picoCTF{m1113n1um\_3d1710n\_d5787049}

Cookie Monster Secret Recipe: Going to the website and trying a random password didn’t work, but gave me a hint talking about the cookies in plain sight. I went on to inspect the elements, searching for everything, and found the secret recipe in the network tab. It was not a standard flag and needed to be decoded. picoCTF{c00k1e\_m0nster\_l0ves\_c00kies\_DE7A5E76}





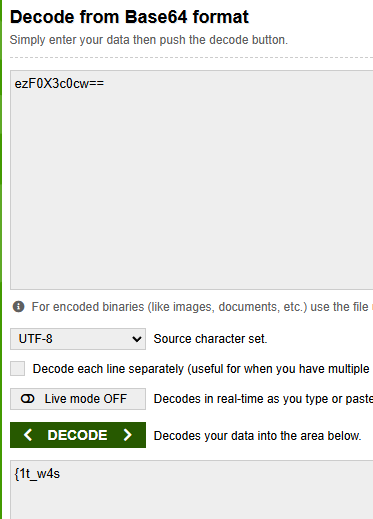
PH4ntom 1ntrud3r:

picoCTF{1t\_w4snt\_th4t\_h\_4r\_d}

ezF0X3c0cw== NgI1NzkwOQ== XzM0c3lfdA== bnRfdGg0dA== YmhfNHJfZA== cGljb0NURg==

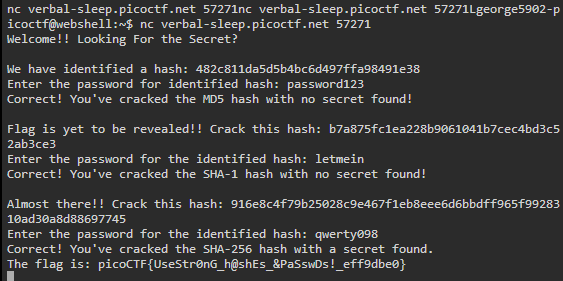
picoCTF{1t\_w4s\_34sy\_t0\_f1nd\_th4t\_bh\_4r\_d}

Took fragments from the wireshark packets and put them together. I couldn’t find the flag though as this didn’t work.

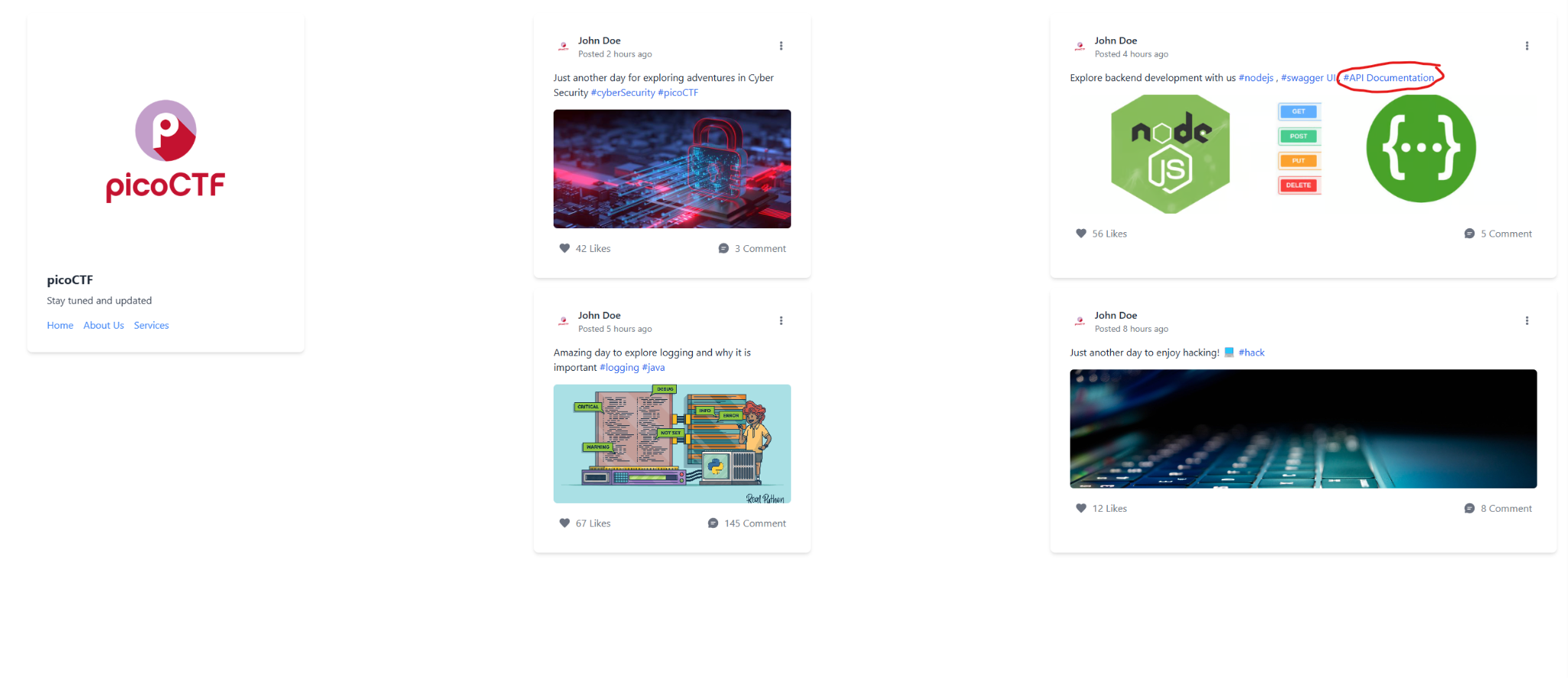
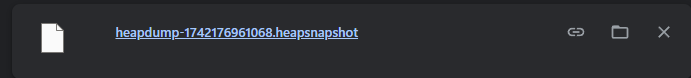
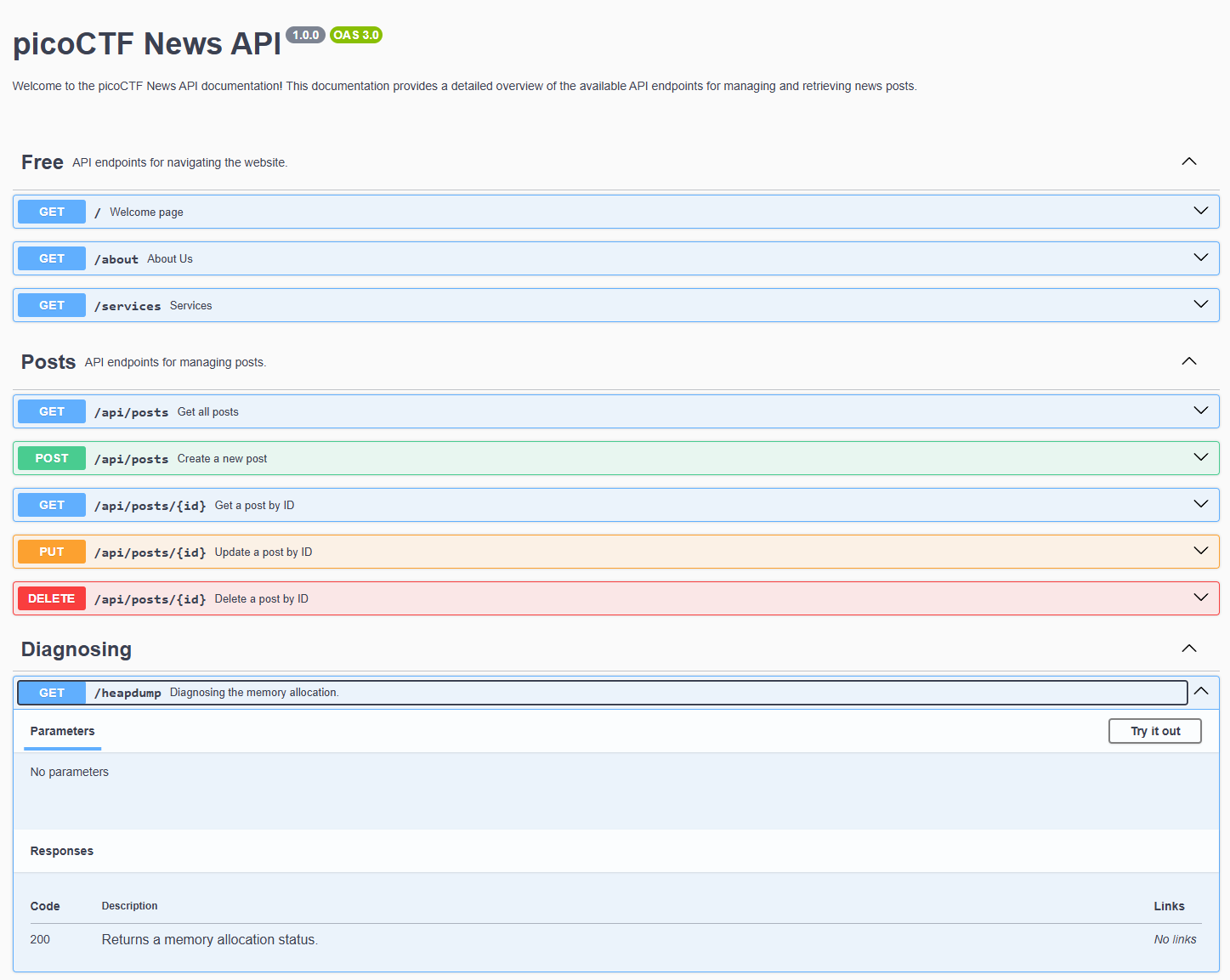


hashcrack:

I put in the given netcat command which brought up a hash and password. I used a hash identifier to identify the hash type. First one was MD5, second was SHA-1, and last was SHA 256. I then cracked each of these hashes and gave the correct password. This gave me the flag. picoCTF{UseStr0nG\_h@shEs\_&PaSswDs!\_eff9dbe0}



Head-dump:

I launched the website and looked around until I came across #API Documentation which led me to another page where the heap dump was at. You could download and analyze the file, which I believe you were supposed to do. I could not get it analyzed so I could not locate the flag.

RED:  
I downloaded the image and it’s a red square. One of the hints talked about what facebook was called now so I checked on the metadata. It has a poem in it and the first letters are CHECKLSB. I downloaded zsteg to use for png images and the flag was given after decoding. picoCTF{r3d\_1s\_th3\_ult1m4t3\_cur3\_f0r\_54dn355\_}