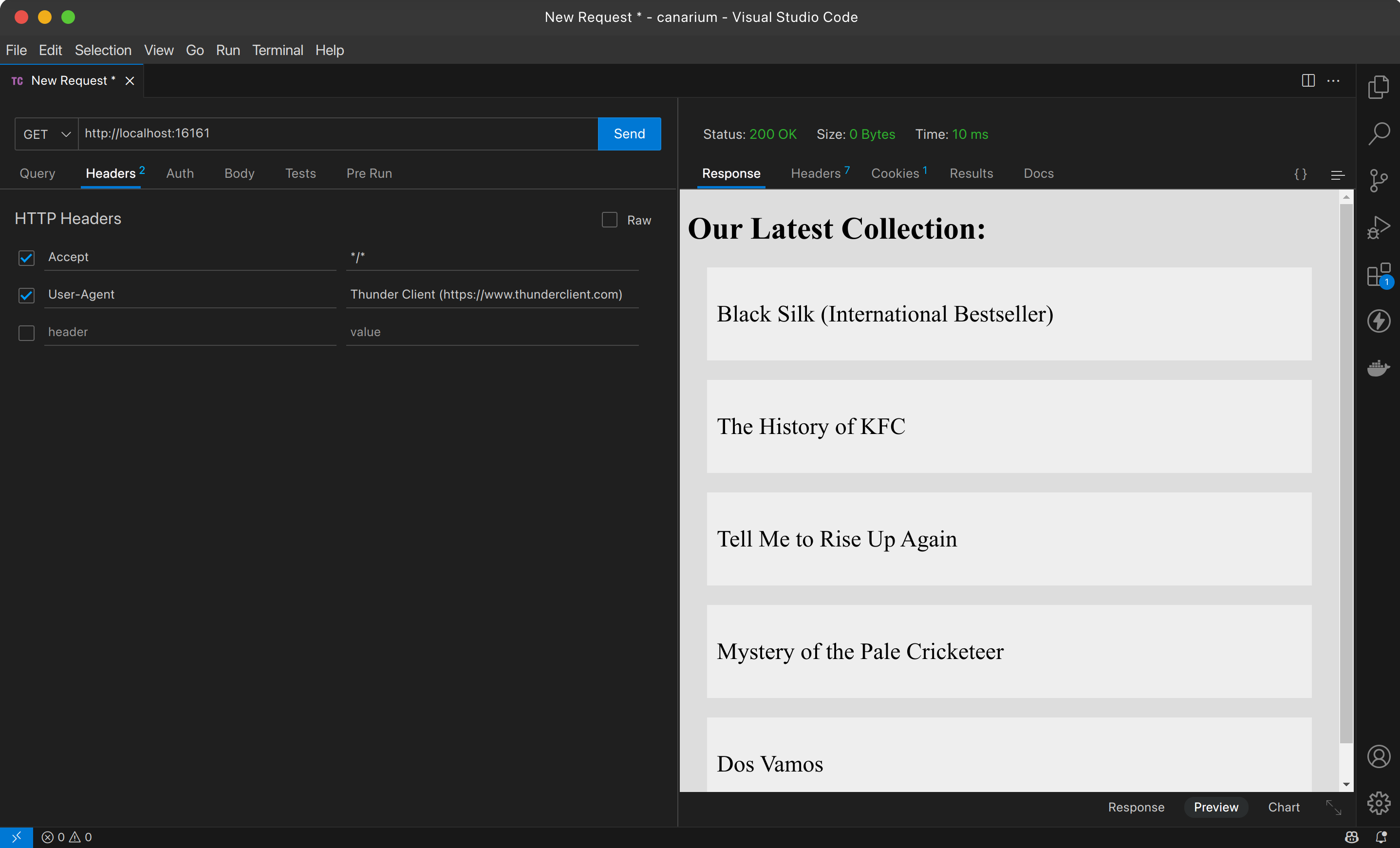
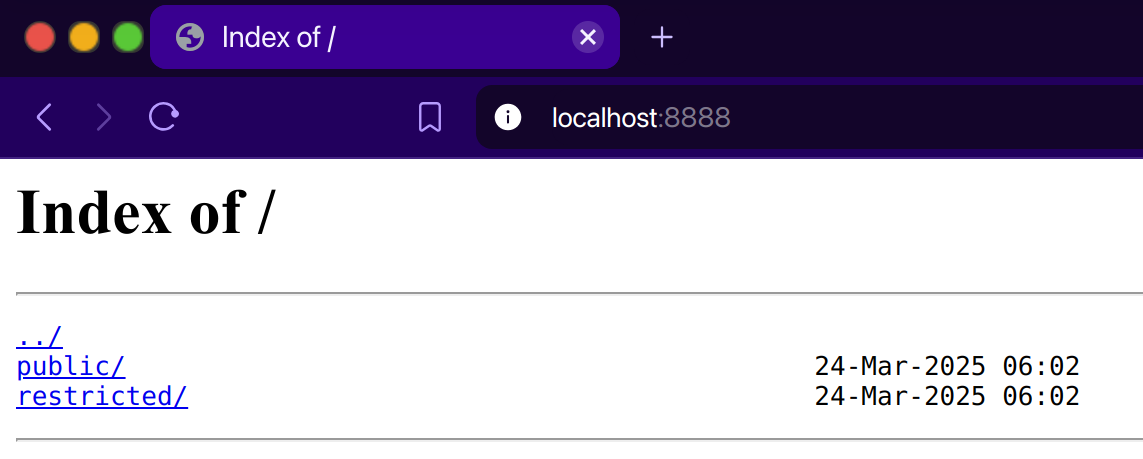
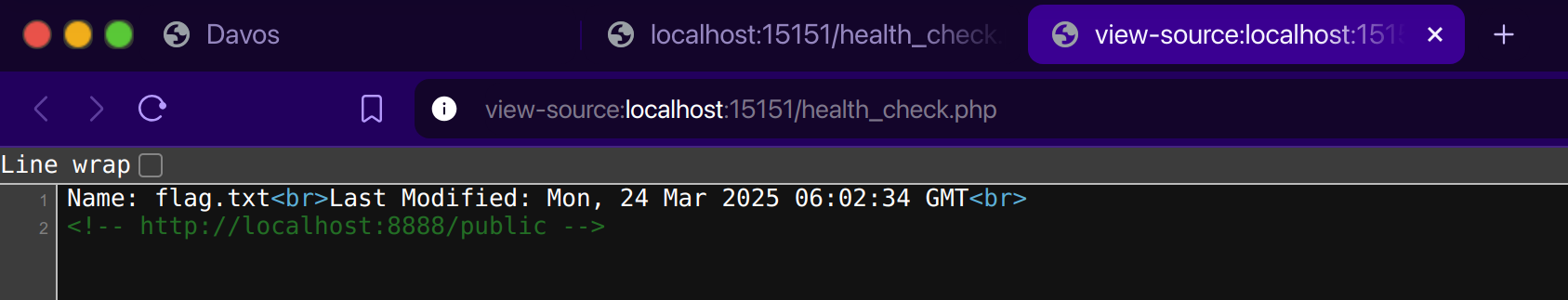
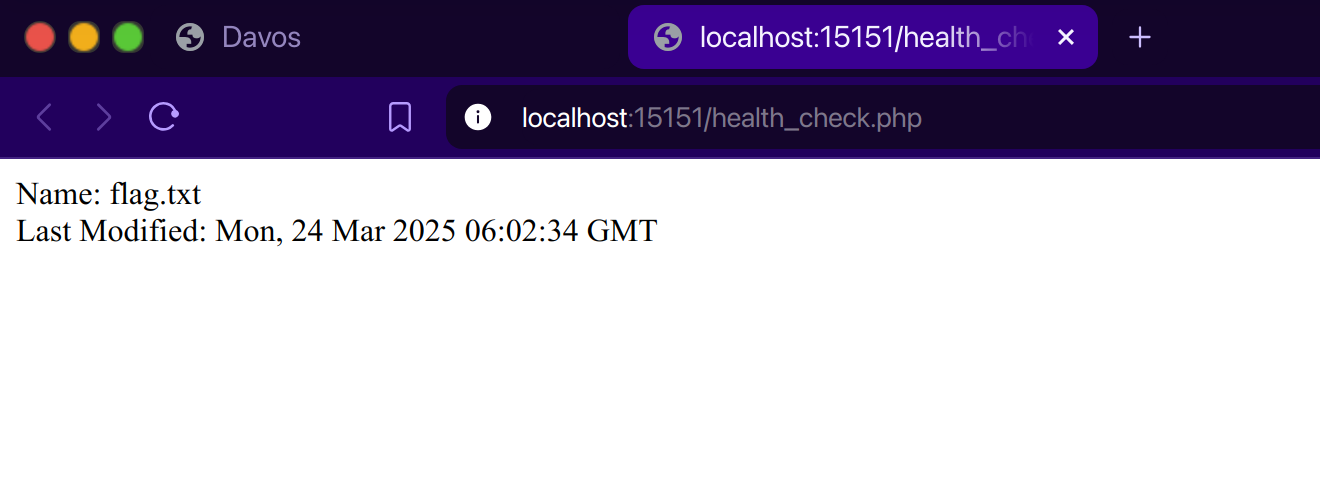
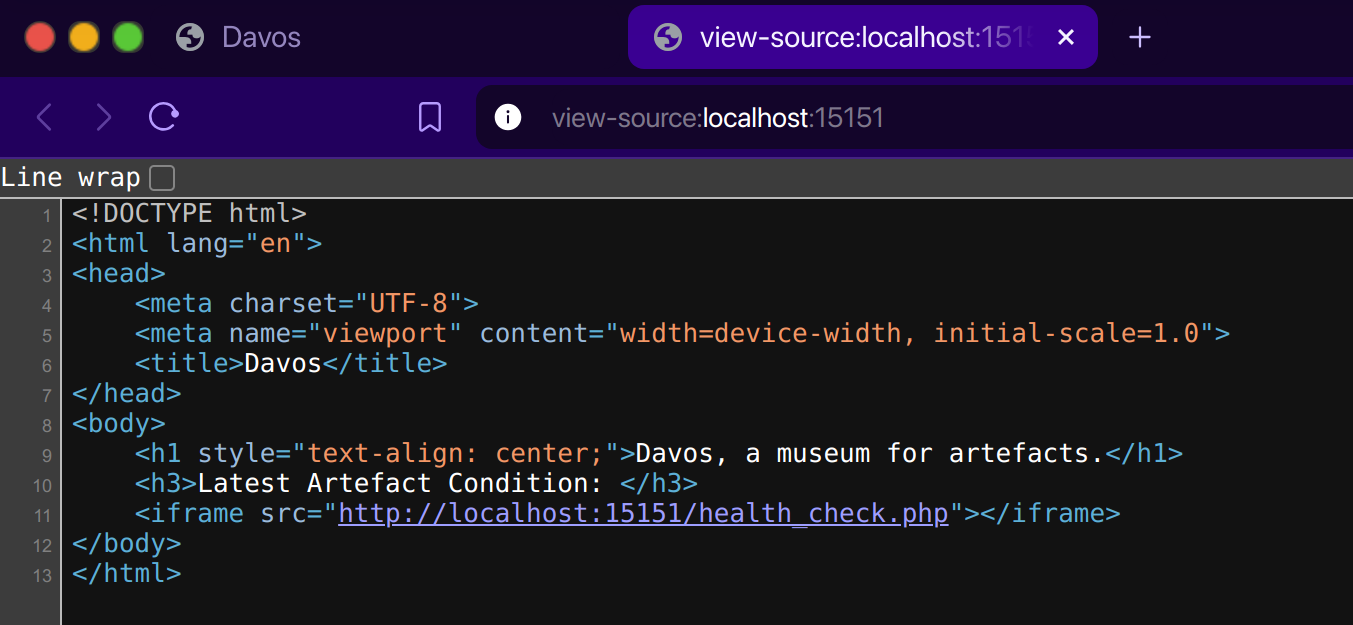
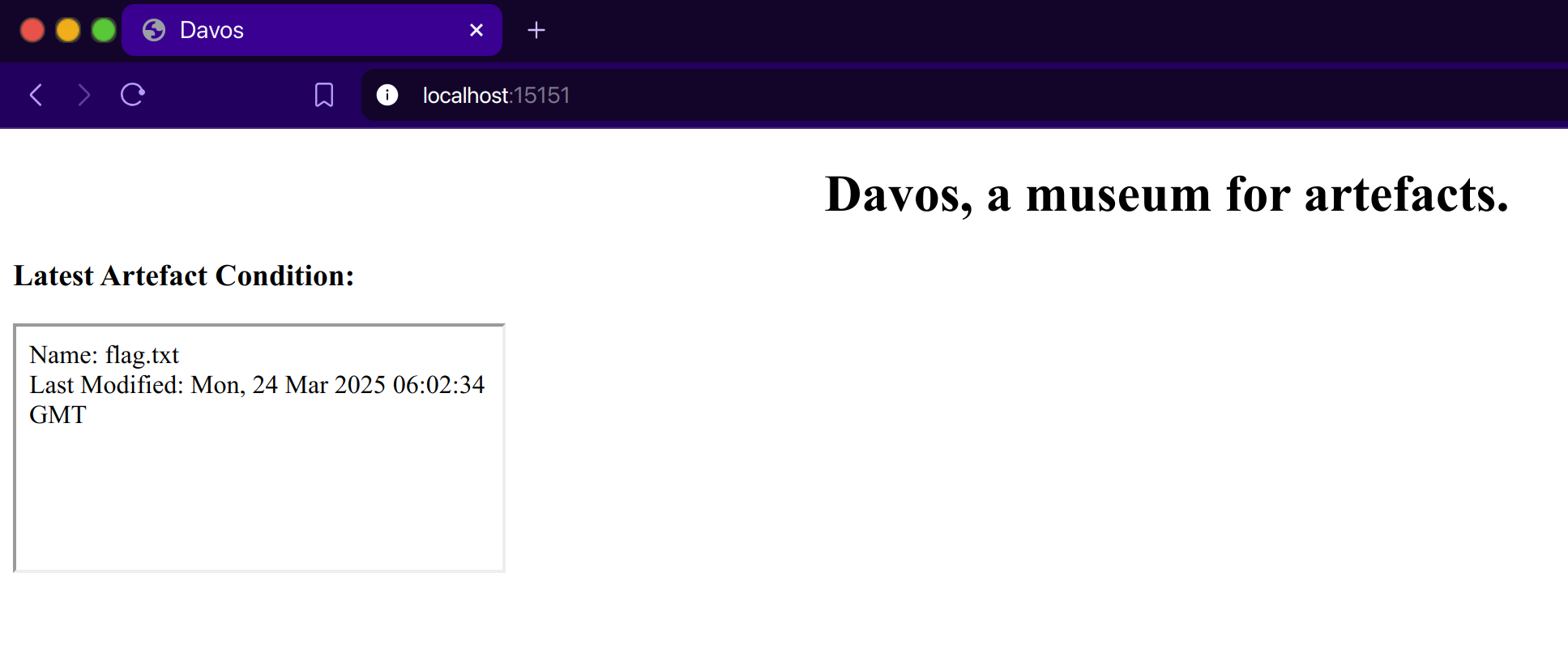
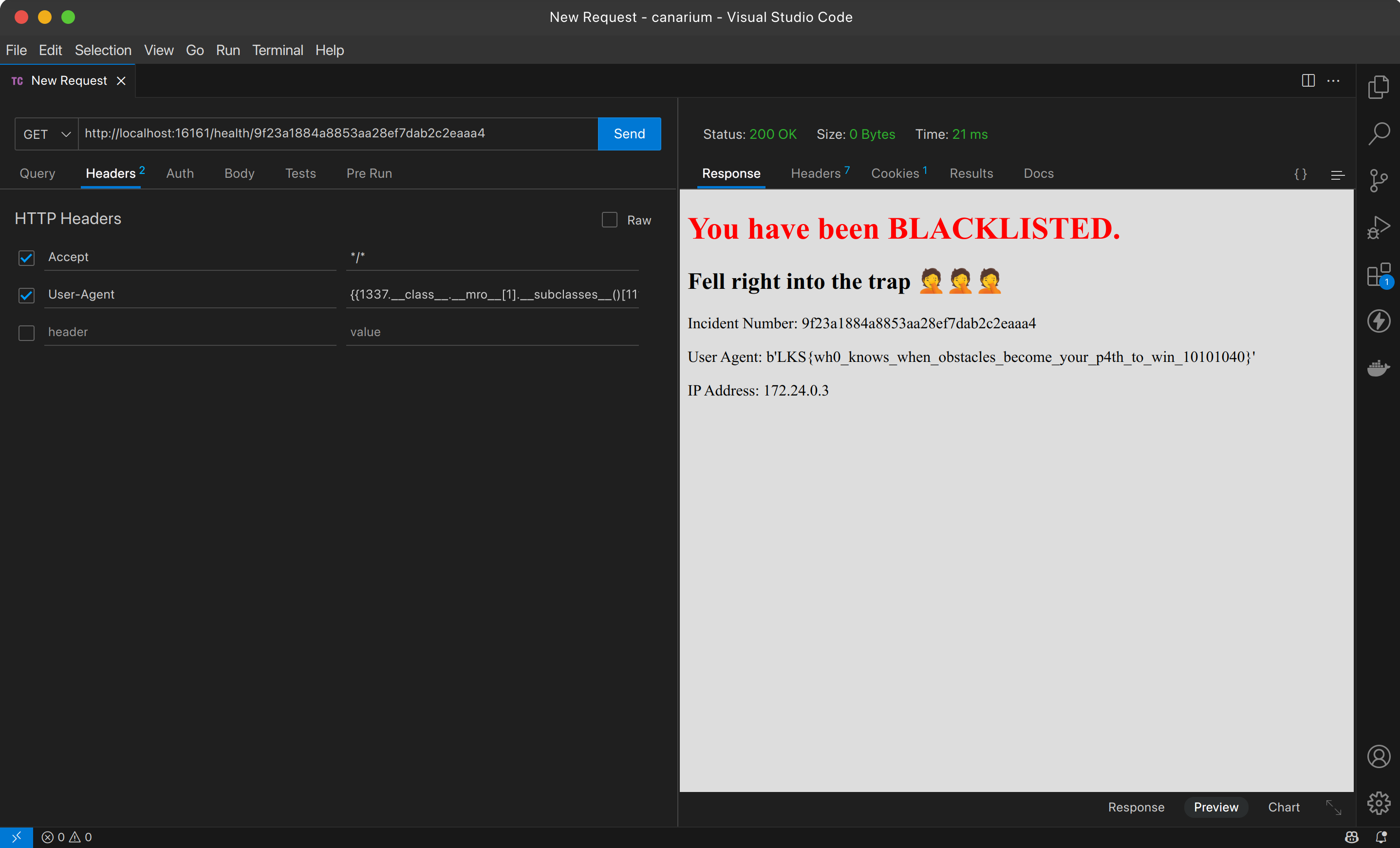
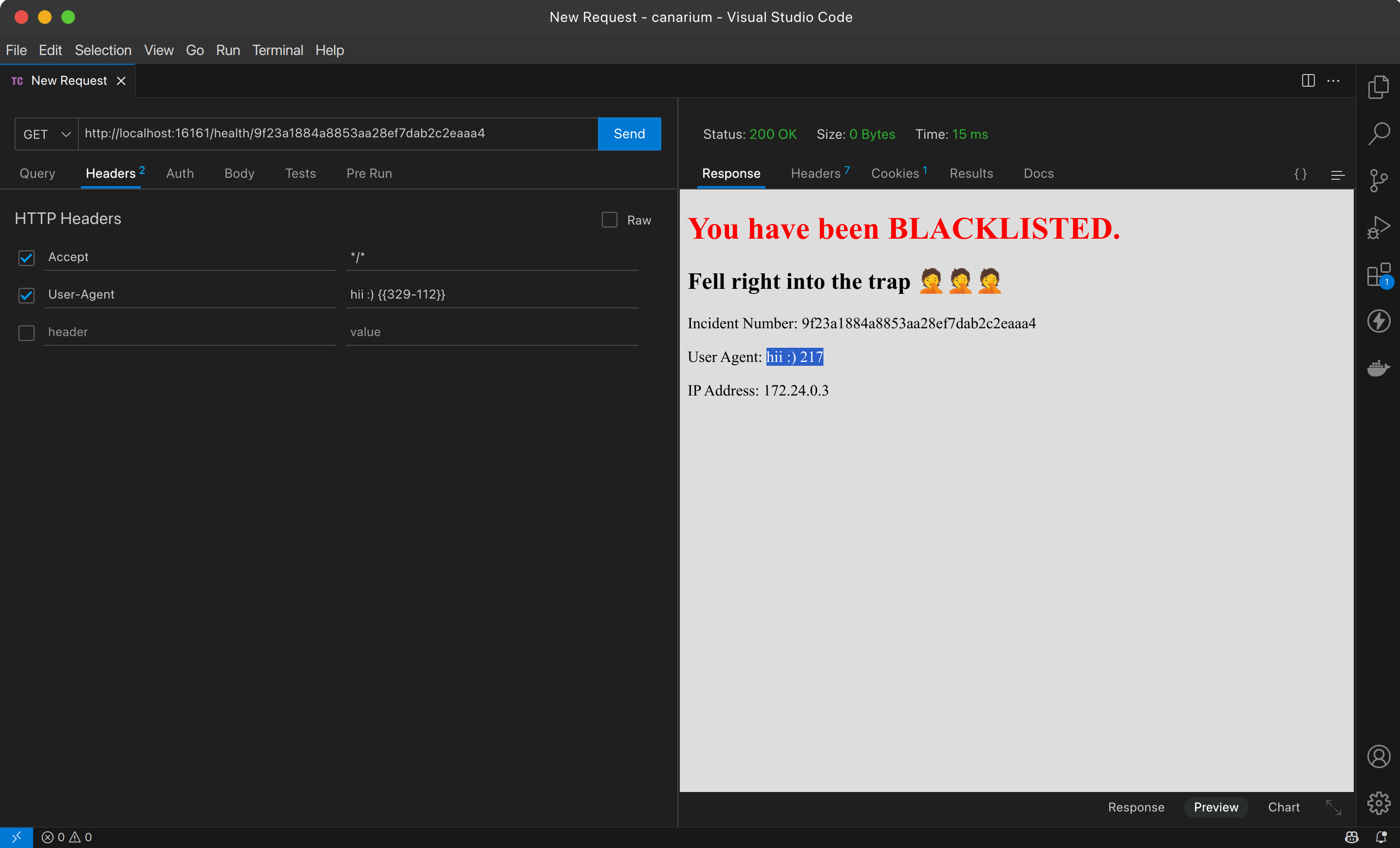
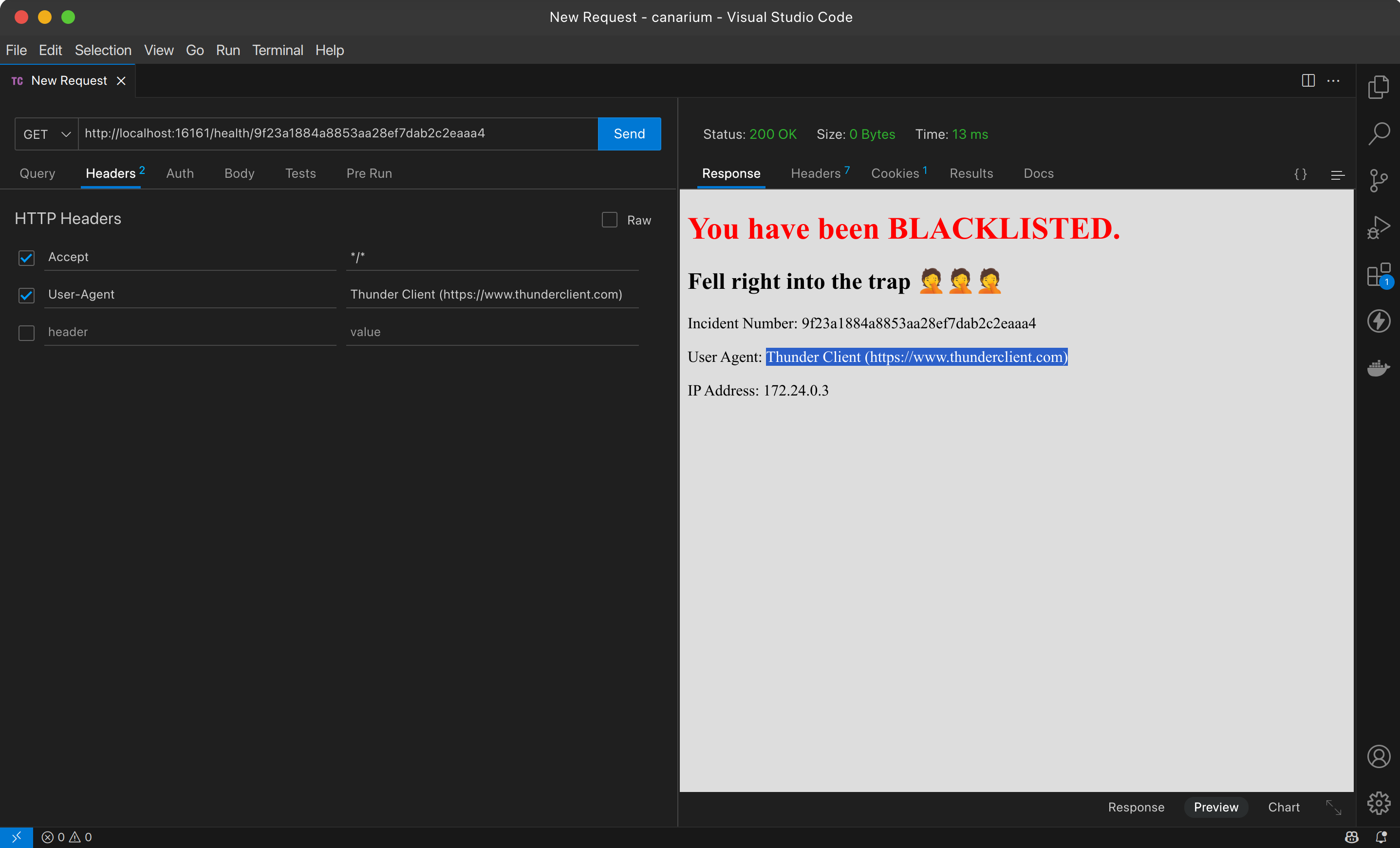
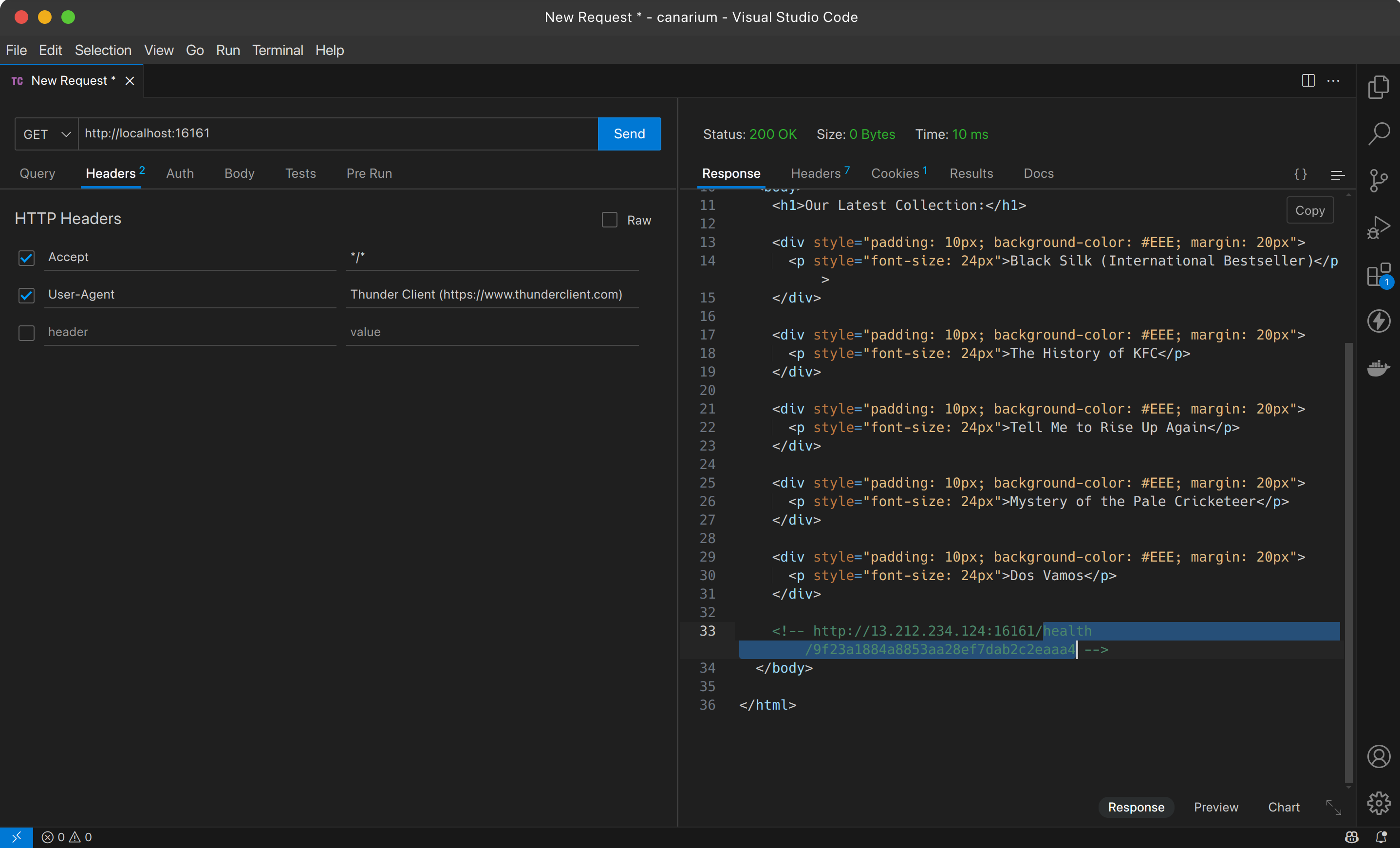
**WRITE UP  
JEOPARDY LKS 2023  
~ Jhuanes Septinus ~**

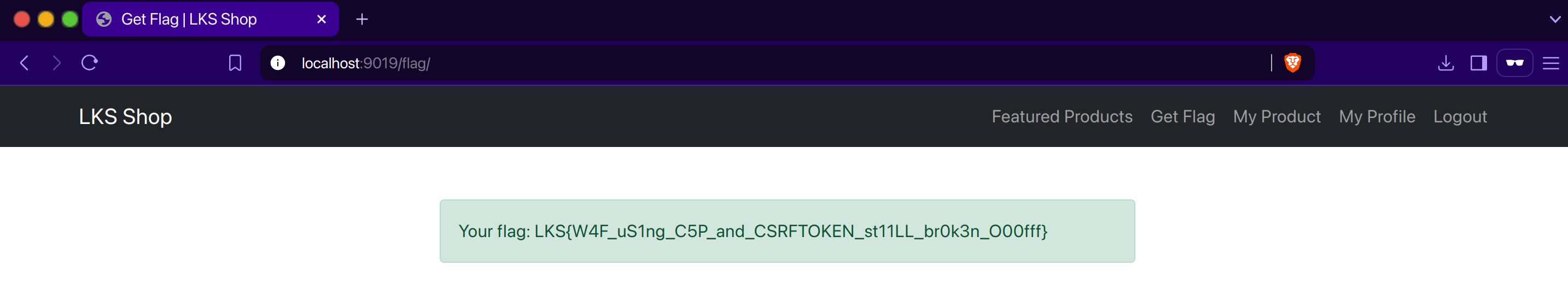
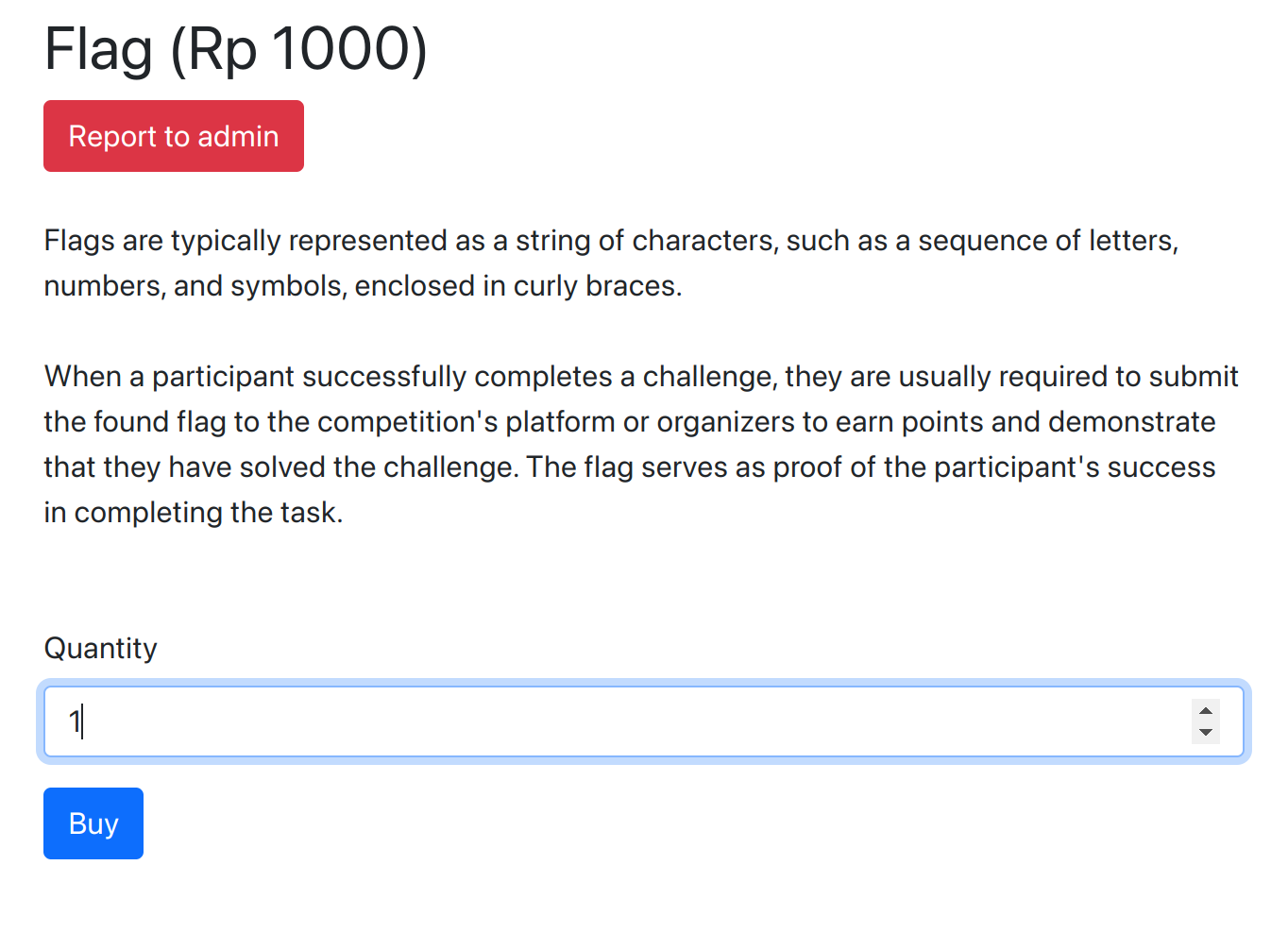
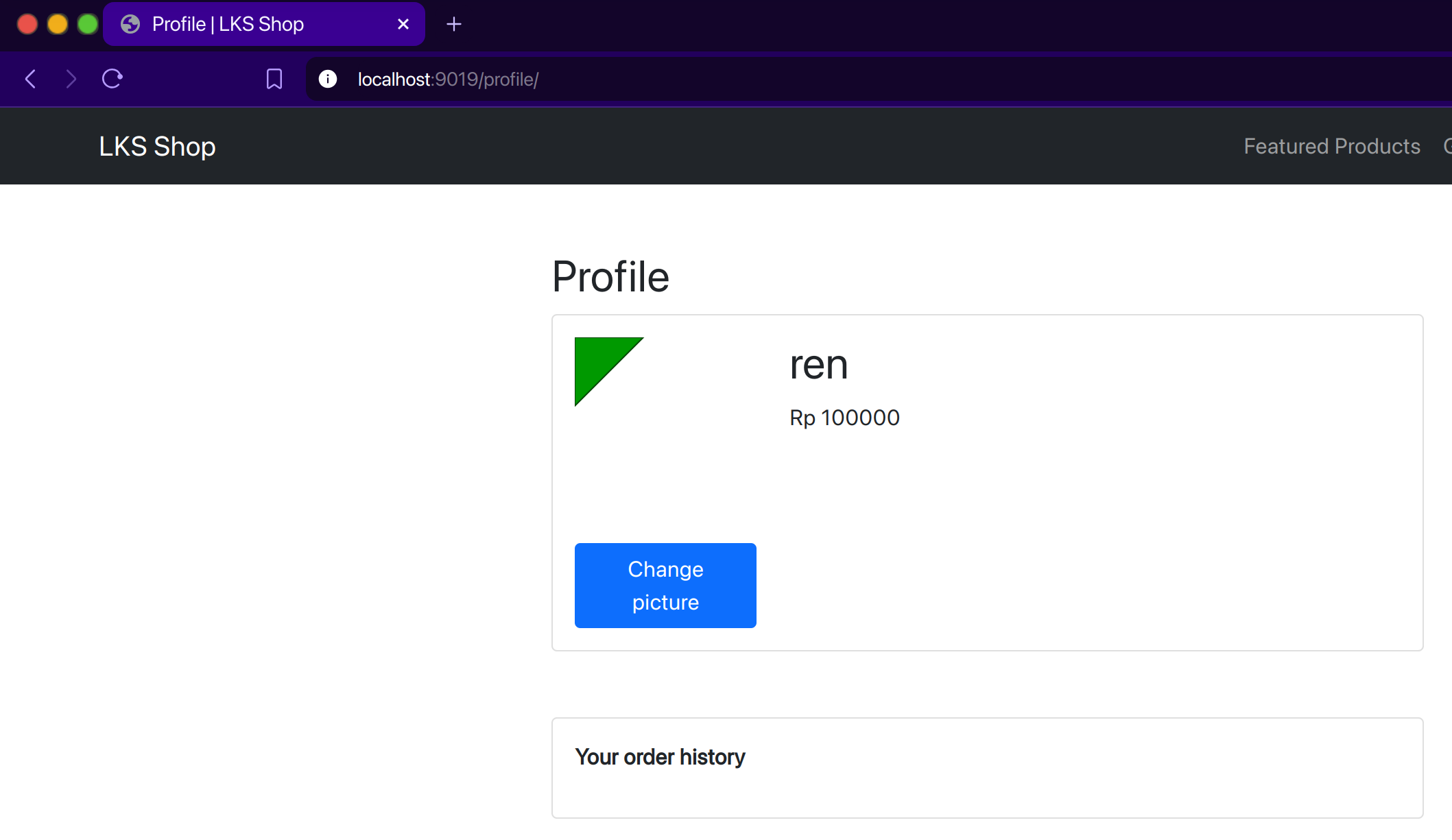
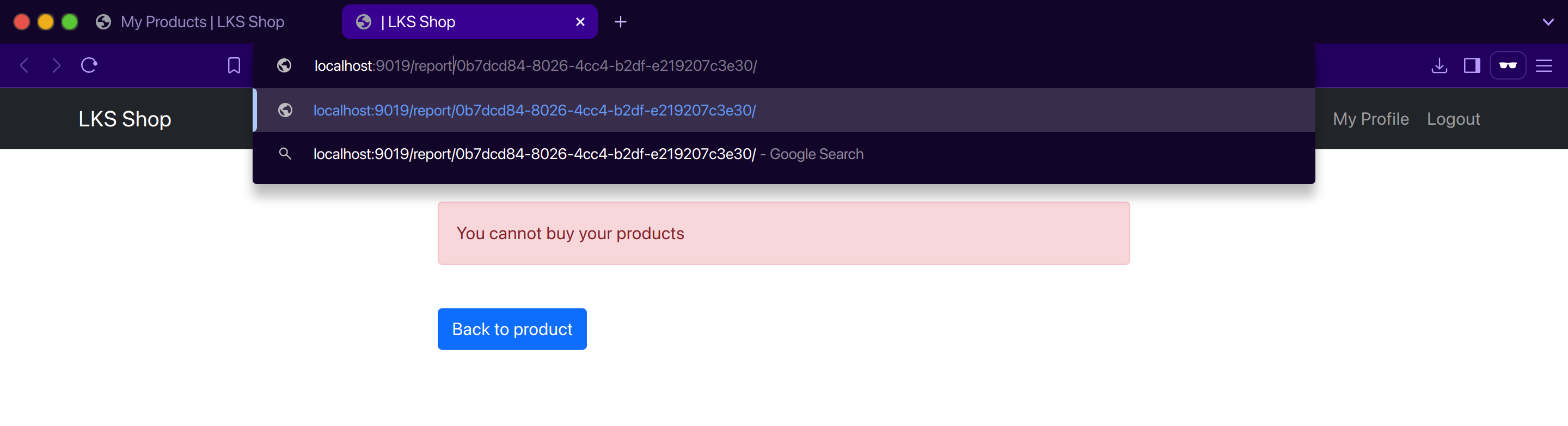
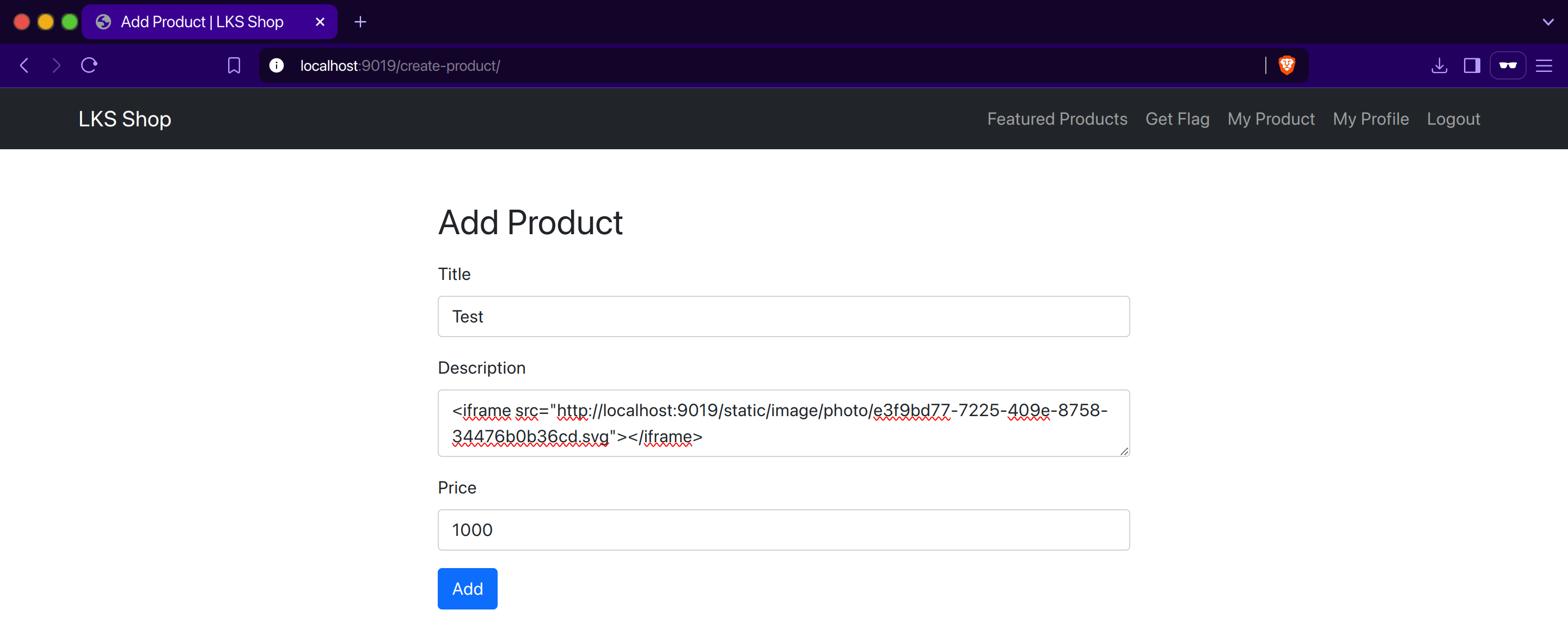
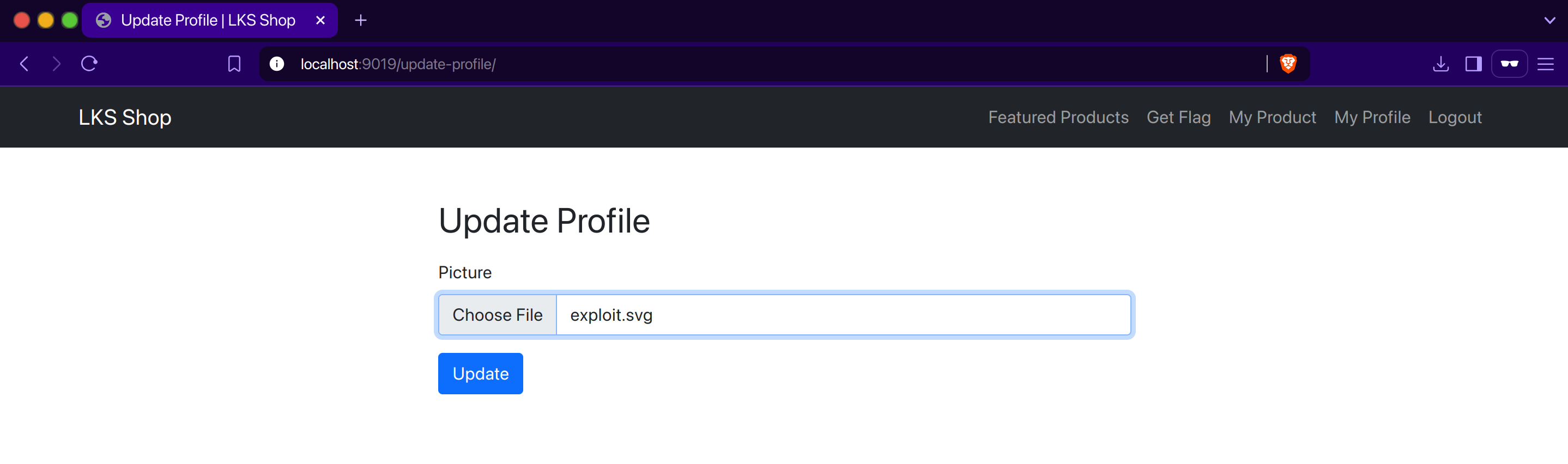
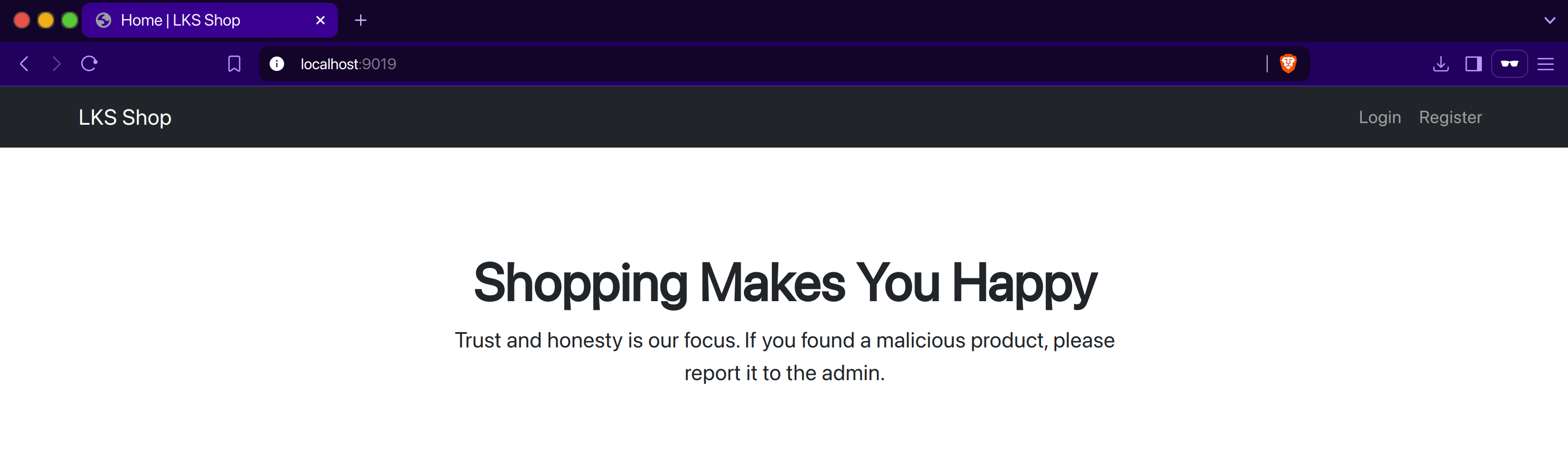
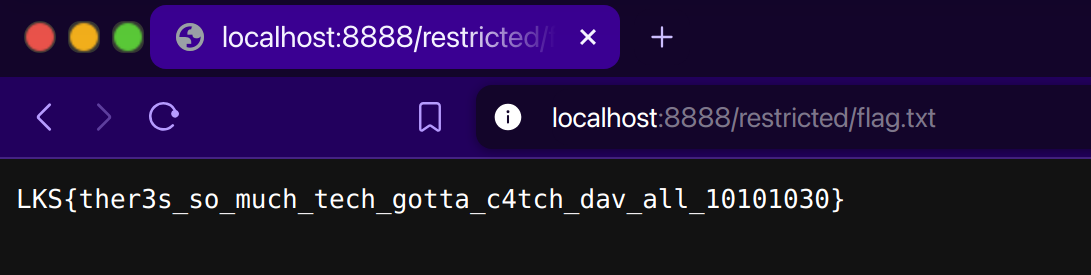
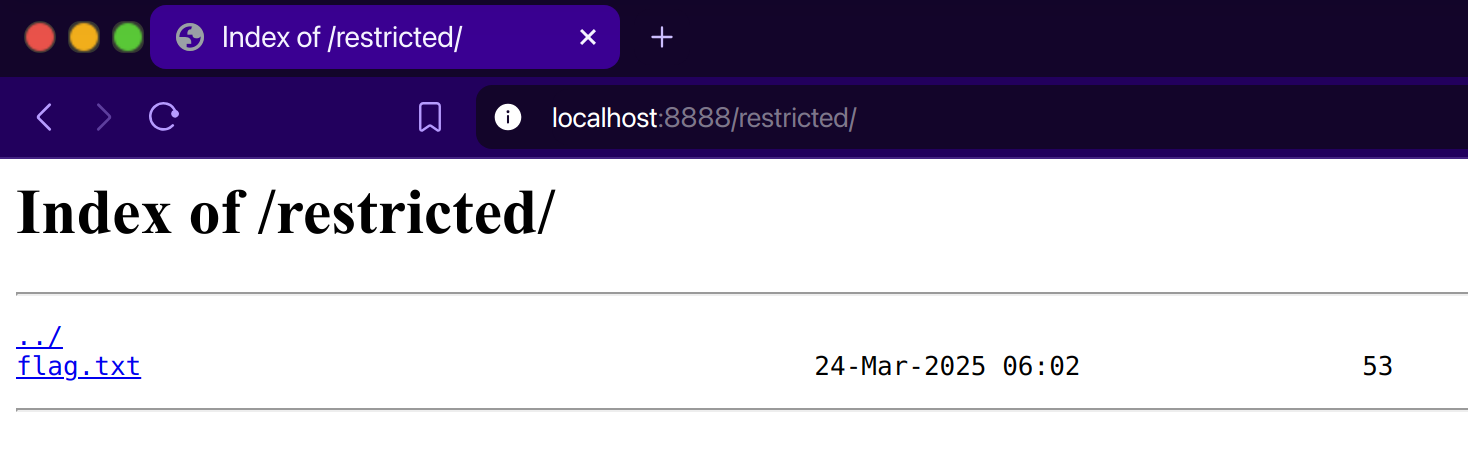
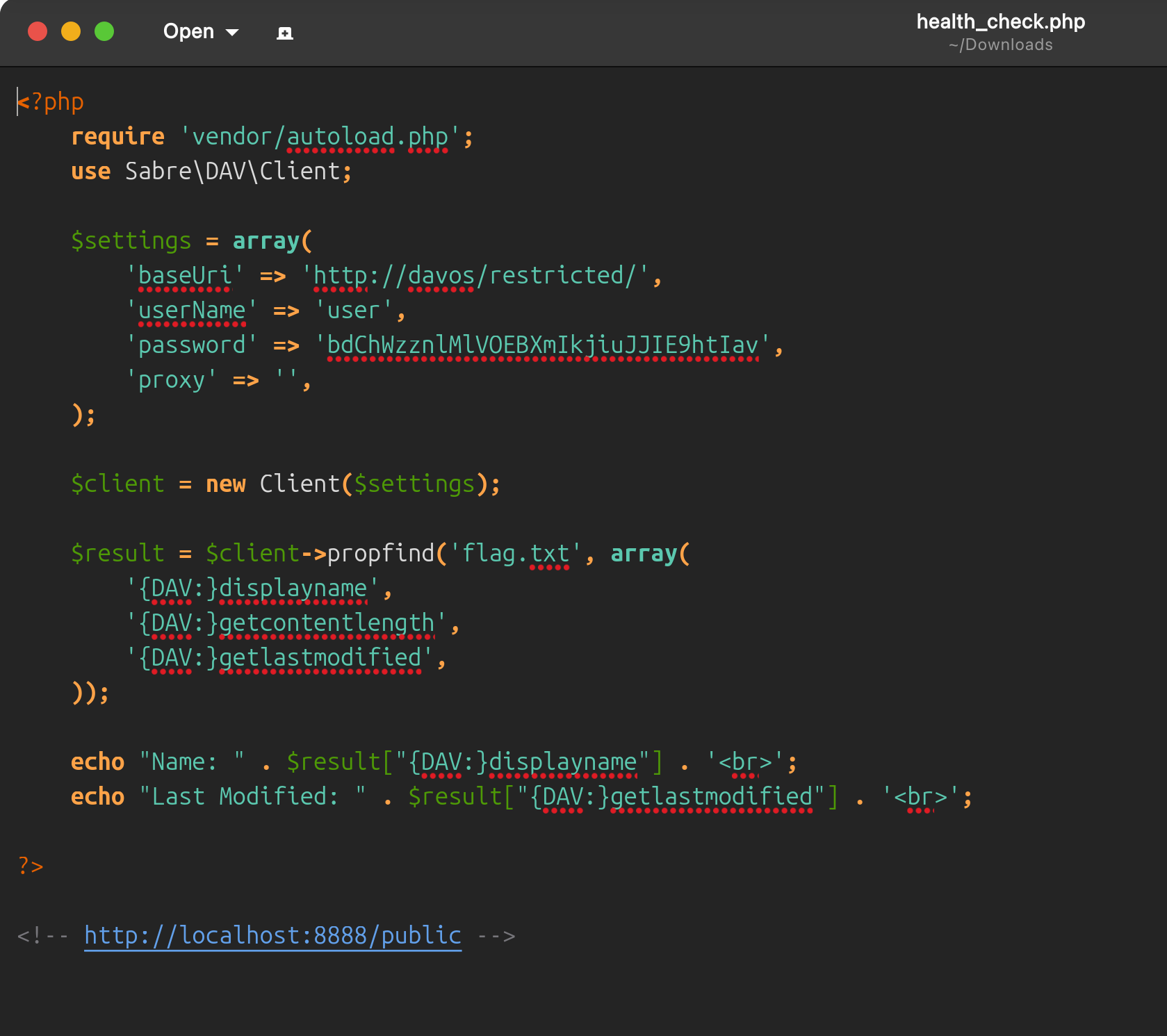
**1. WEB EXPLOITATION  
 a. canarium** 1. Tampilan awal



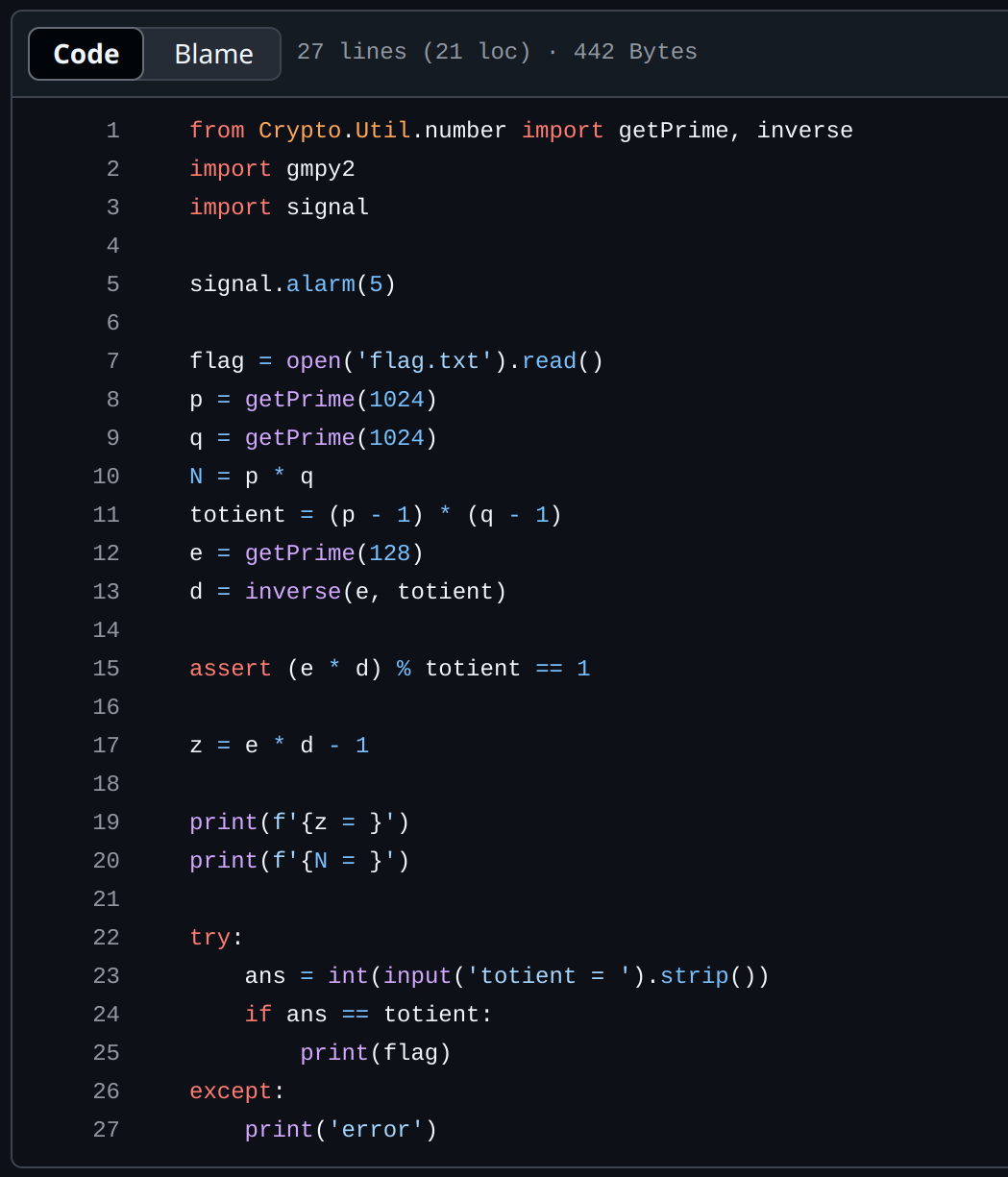
2. Cek source-code web, saya menemukan sebuah path   
   
  
 3. Ketika di cek pada path tersebut, saya masuk ke dalam trap. Namun disini ada 3 informasi, yaitu Incident Number, User Agent dan IP Address, dari informasi tersebut ada kemungkinan kerentanan ini adalah SSTI, dan field yang berpotensi menjadi celah kerentanan adalah field User Agent.  
   
  
 4. Test kerentanan SSTI  
   
  
 5. Eksekusi kerentanan, menggunakan payload  
 {{1337.\_\_class\_\_.\_\_mro\_\_[1].\_\_subclasses\_\_()[111].\_\_subclasses\_\_()[0].\_\_subclasses\_\_()[0](“/flag.txt").read()}}  
   
 Flag : LKS{wh0\_knows\_when\_obstacles\_become\_your\_p4th\_to\_win\_10101040} **b. davos** 1. Tampilan awal  
   
 2. Cek source-code web  
   
   
 3. Akses health\_check.php dan cek source-code nya  
   
   
  
 4. Akses [http://localhost:8888/](http://localhost:8888/public/) muncul 2 directory, public dan restricted, karena ini WebDav, maka directory public akan berisi kode program dan directory restricted akan berisi file-file yang diamankan.



5. Ketika mengakases directory restricted, akan muncul popup login. Untuk mendapatkan credentials login yang berkemungkinan ada di dalam kode program di directory public, saya akan coba akses public/.env dan public/health\_check.php. Ketika mengakses file public/health\_check.php, maka akan otomatis mendownload file tersebut, yang berisi credentials login.  
   
  
 6. Akses directory restricted dan akses file flag.txt  
   
   
  
 Flag : LKS{ther3s\_so\_much\_tech\_gotta\_c4tch\_dav\_all\_10101030}  
 **c. lks-Shop** 1. Tampilan awal  
   
 2. Buat user kemudian login. Di halaman dashboard, ada product dari user admin yaitu product flag, kemudian ada fitur add product, dan hint yang diberikan adalah admin memiliki banyak uang. Maka dapat kita akan membuat sebuah product yang nantinya akan secara otomatis dibeli oleh admin dan kita akan mendapat uang (kerentanan XSS). Namun di website LKS Shop ini ada http-equiv="Content- Security-Policy" content="default-src 'self';", untuk mencegah serangan XSS dari host lain, maka kita harus menyisipkan kode exploit dari website itu sendiri. Di sini saya melihat bahwa profile picture dapat mengupload file .svg, maka kita akan sisipkan kode javascript ke dalam file svg dan menguploadnya.  
   
   
 3. Sisipkan dalam tag iframe  
   
 4. Setelah add product, maka kita coba report product tersebut, dengan format {host}/report/{id\_product}  
   
 5. Cek profile, setelah mendapatkan uang maka kita beli product flag dan akses menu Get Flag

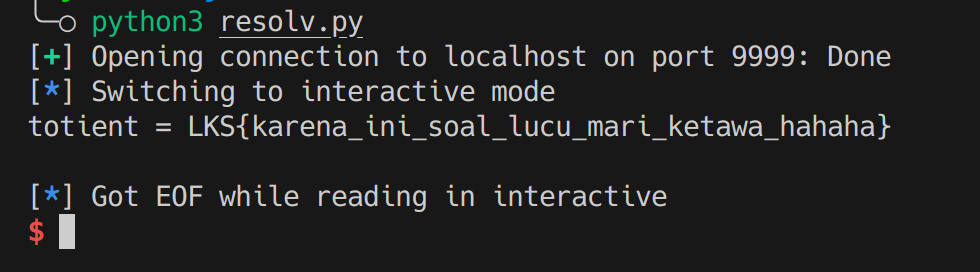


**2. CRYPTO  
 a. totient** 1. Terdapat file chall.py  
   
   
 2. Pada chall ini terdapat beberapa variabel prima yang digenerate secara random seperti p,q dan e. bisa dilihat bahwa p dan q digunakan untuk menghitung N. dari sini dapat disimpulan bahwa algoritma yang digunakan adalah RSA, kemudian terdapat variabel totient yang melakukan kalkulasi antara variabel p dan q. selanjutnya terdapat d yang berisi invers antara e dan totient tadi, dan operator assert jika e \* d mod totient sama dengan 1 maka program akan berlanjut, terakhir adalah variabel z yang berisi e \* d -1.



Untuk menyelesaikan chall ini diperlukan menghitung totient kembali menggunakan variabel z dan N, berikut solution yang sudah saya buat

3. Menghitung totient dengan z // (z // N + 1)



**3. FORENSIC**