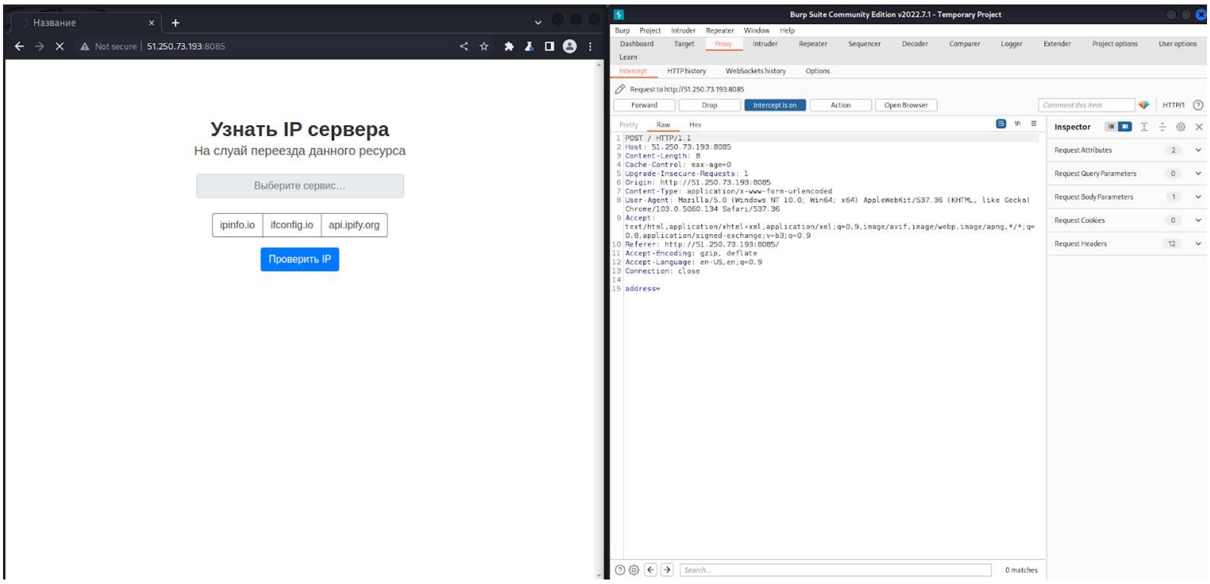
SSRF Report - 16.8.1 - 16

Tester's name: Stanley Ford

SSRF Lab No. 16.8.1

- General information:
  - Testing period: 07.02.2023
  - Test object: http://51.250.73.193:8085/
- Description:The first thing I did was to look at the code of the page element. Next, I tried how the site works and saw that somehow the IP address of the resource was returned to the screen



Узнать IP сервера

На случай переезда данного ресурса

Request to http://51.250.73.193:8085

```
POST / HTTP/1.1
Host: 51.250.73.193:8085
Content-Length: 8
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://51.250.73.193:8085
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://51.250.73.193:8085/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

address=
```

. For example, I can pass the parameter ?url=file:///etc/passwd. Note that I shouldn't be able to do this: I'm trying to find out the IP address of something, even though I didn't give any input before pressing the button. Here is the very fact of the existence of a "hole".

So, having entered in address=123, I redirected the request further and I got the flag:flag {s3rv3r_s1d3_r3qu3st_f0rd3n@ry}

Lab done!

Self-Assessment Questions:

- List the tools (programs and utilities) that you used to solve this lab:Web Browser (Google Chrome)
  Burp Suite

- List the vulnerabilities you have discovered:
  SSRF (Server-Side Request Forgery)

- Give advice on how to improve security: Create a whitelist of addresses that can be forwarded to.