Report on (LFI - 15.7.1 -15)

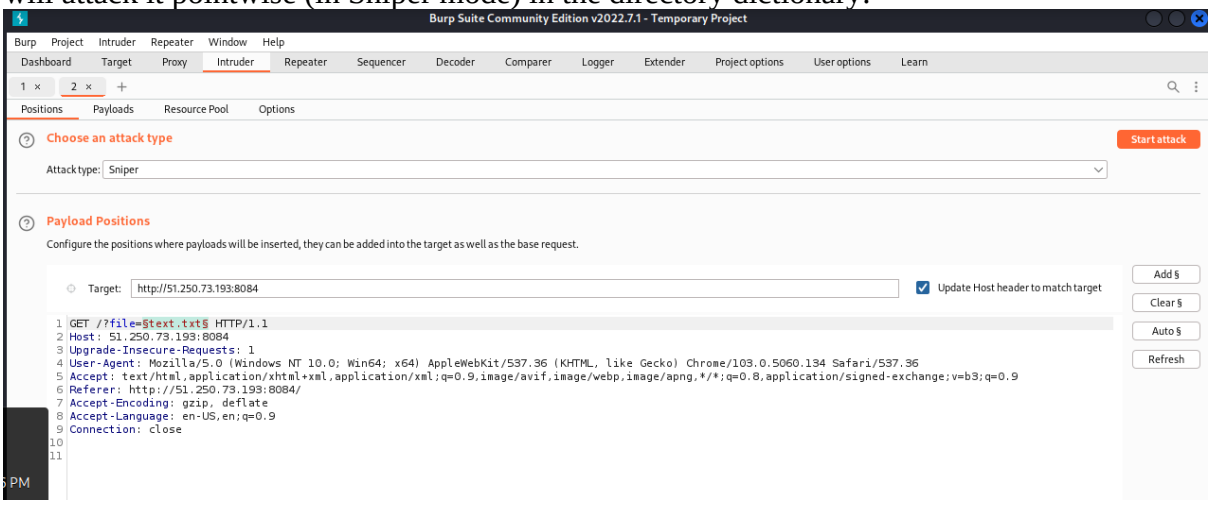
Tester's name: Stanley Ford

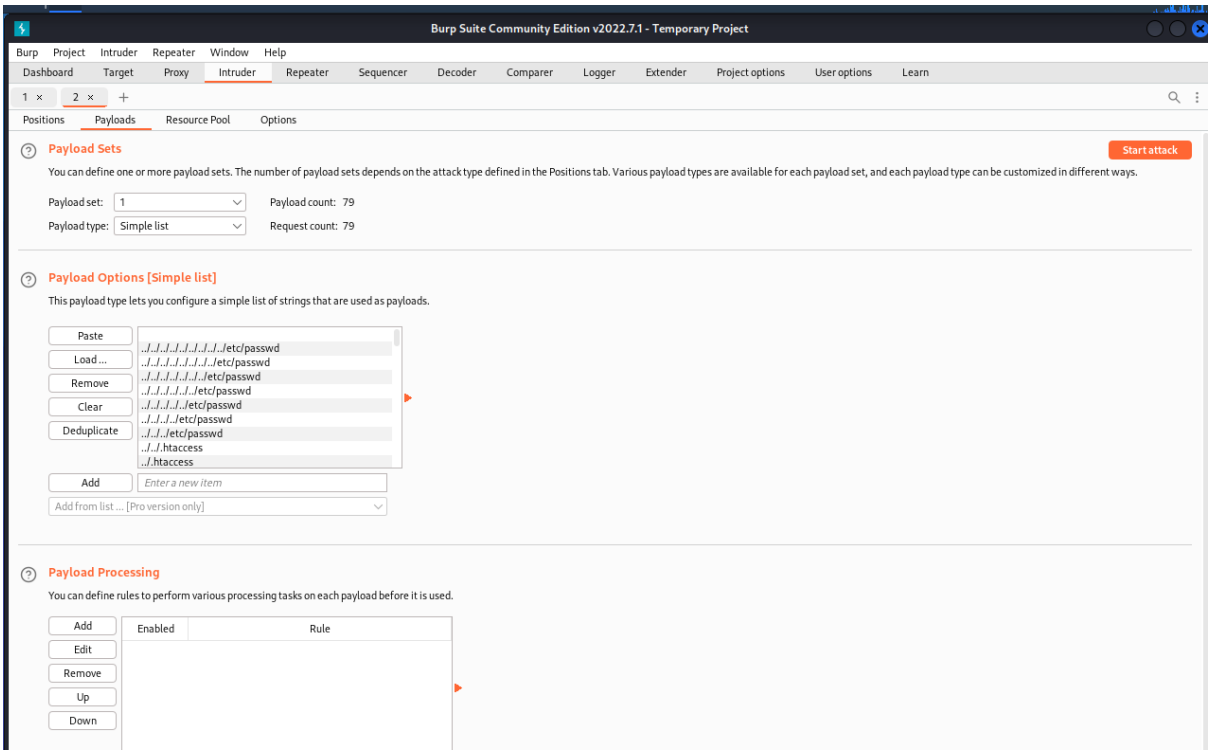
Lab No. "15.7.1 LFI" :

- General information:
  - Testing period: 02.02.2023
  - Test object: http://51.250.73.193:8084/
- Description of actions:

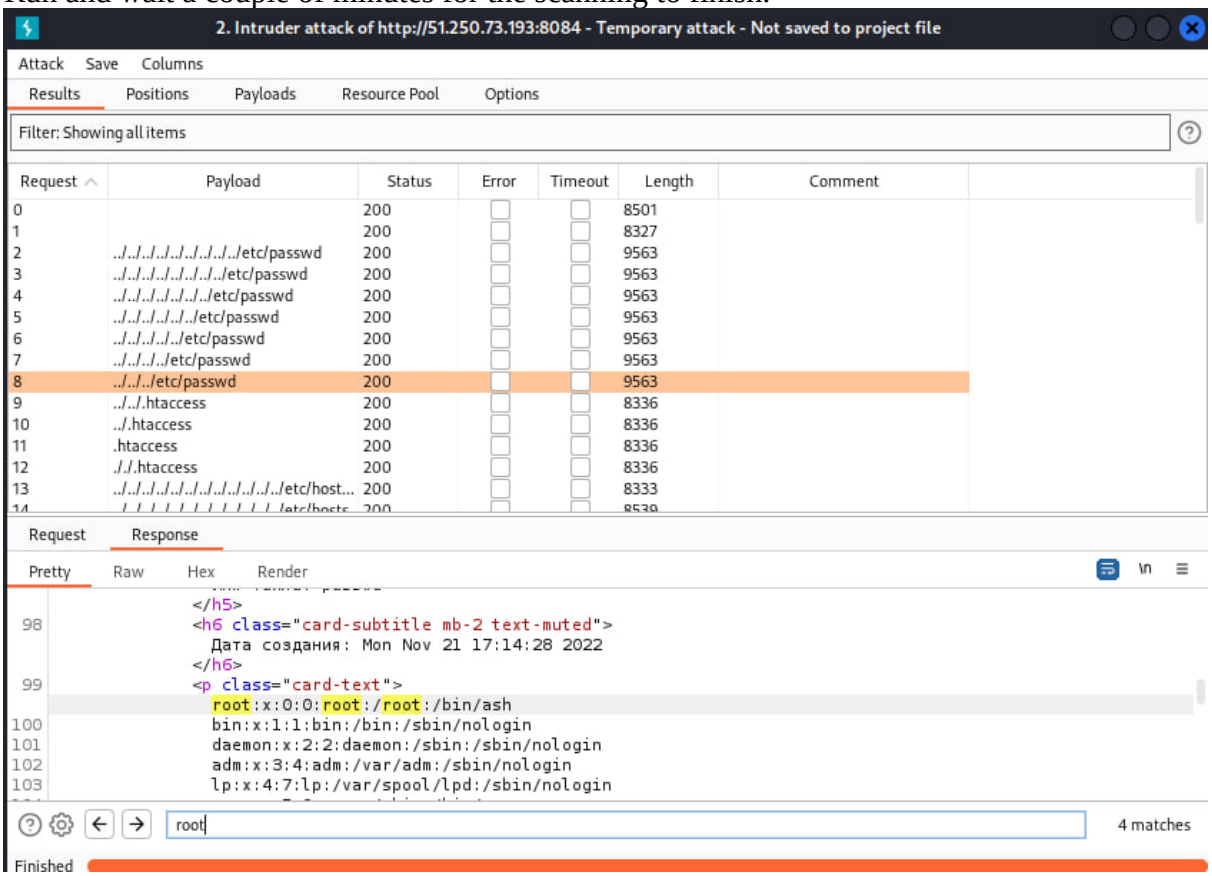
  When I went to the site, I saw an example of a file that could be found. I wrote text.txt to the search bar and noticed how the URL of the page changed to http://51.250.73.193:8084/?file=text.txt#projects. The part after the slash indirectly indicates the presence of an LFI vulnerability. That's what I'll check in the next step.

  I go to BurpSuite, where I intercept this HTTP request and send it to Intruder, where I will attack it pointwise (in Sniper mode) in the directory dictionary:



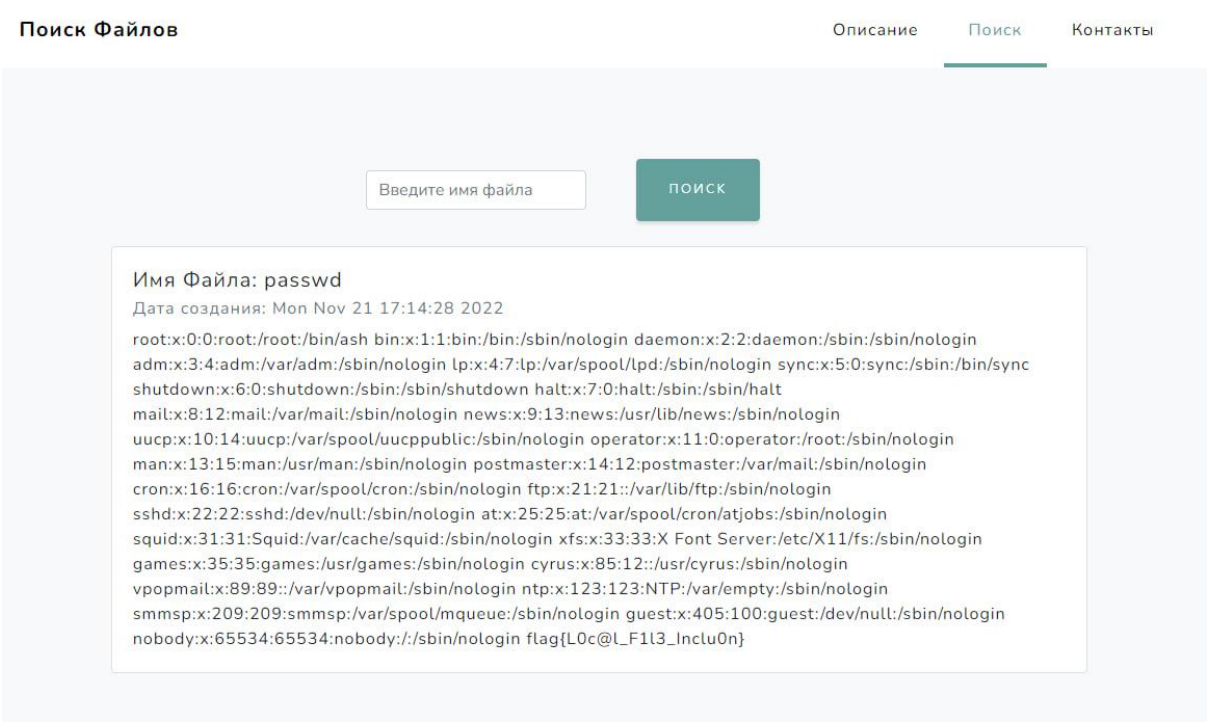


Run and wait a couple of minutes for the scanning to finish.



So, I got a set of directories that return the status of "200 OK" and filtered some of them for the word "root", which would point to the root folder with passwords. Such a one was found in .. /.. /.. /etc/passwd.

It's good news. Obviously, this is what you should try to implement in the search box and here is the result:



I got access to the folder with passwords. At the end, the flag you want to find is flag{L0c@l_F1l3_Inclu0n}. Job done.

Self-Assessment Questions:

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

- List the vulnerabilities you have discovered:LFI

- Give advice on how to improve protection:Filter the input. In particular: allow only alphanumeric and numeric characters, while special characters such as /, <, > should not be processed.