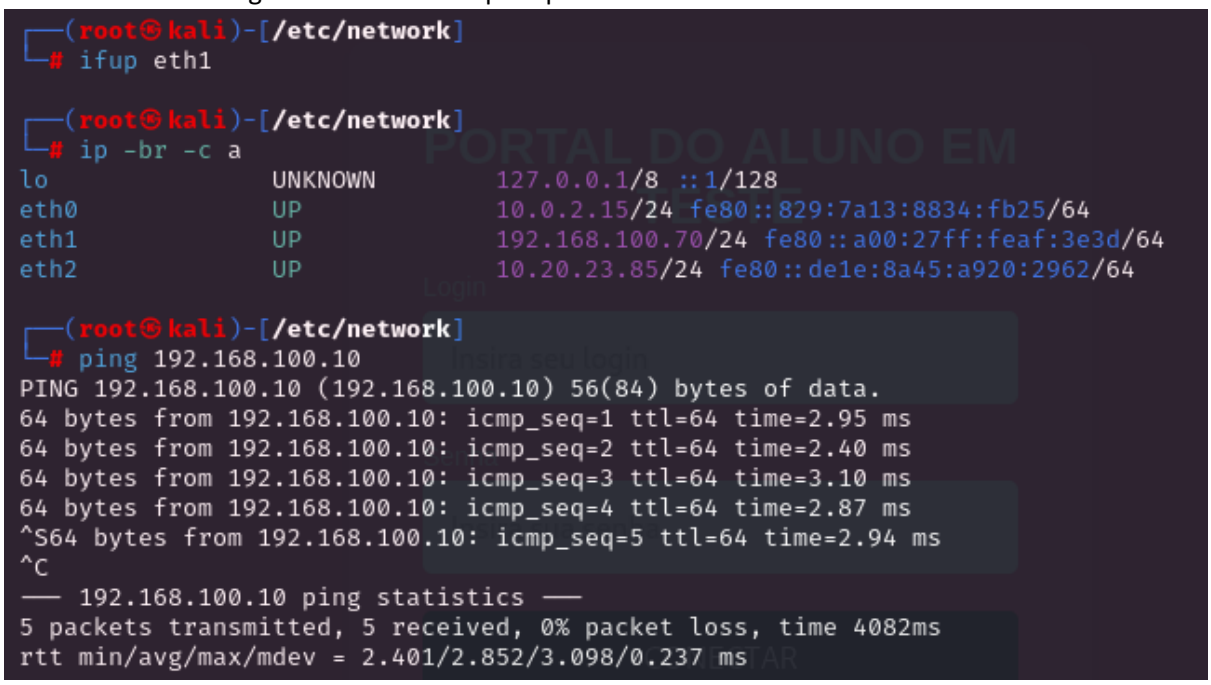
CP6 CYBER

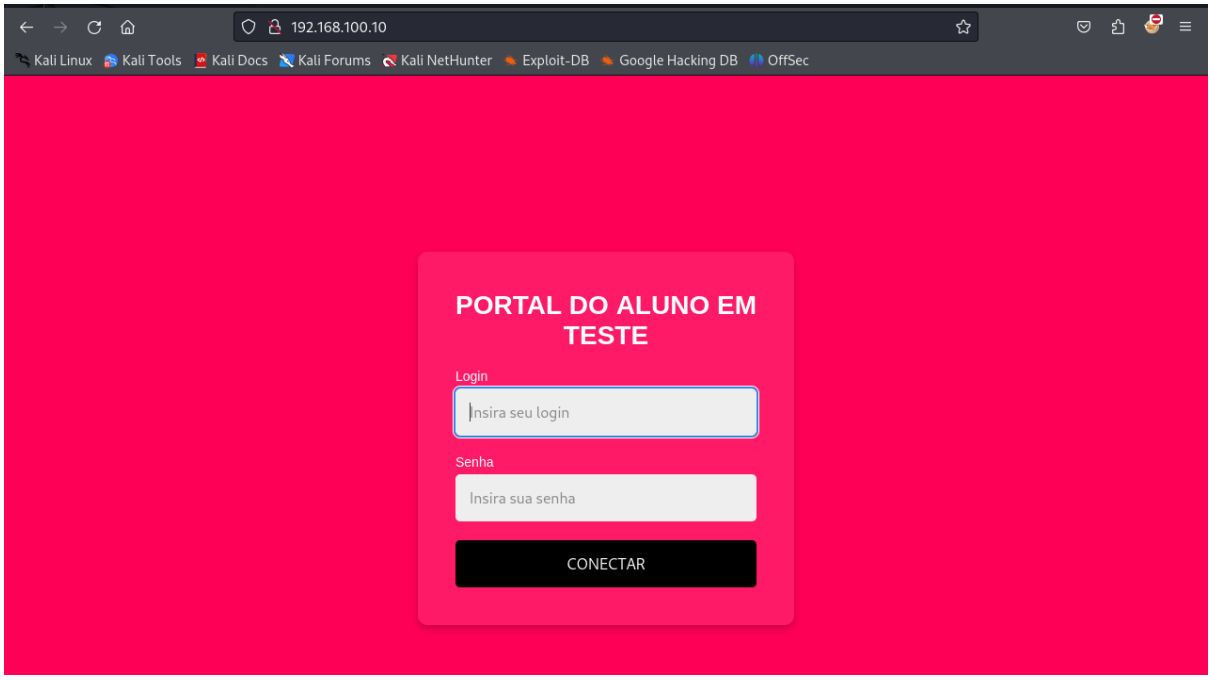
Nome: Rafael Afonso Benbassato

RM: 85321

Primeiramente configurei a rede no Kali para poder se conectar ao servidor:

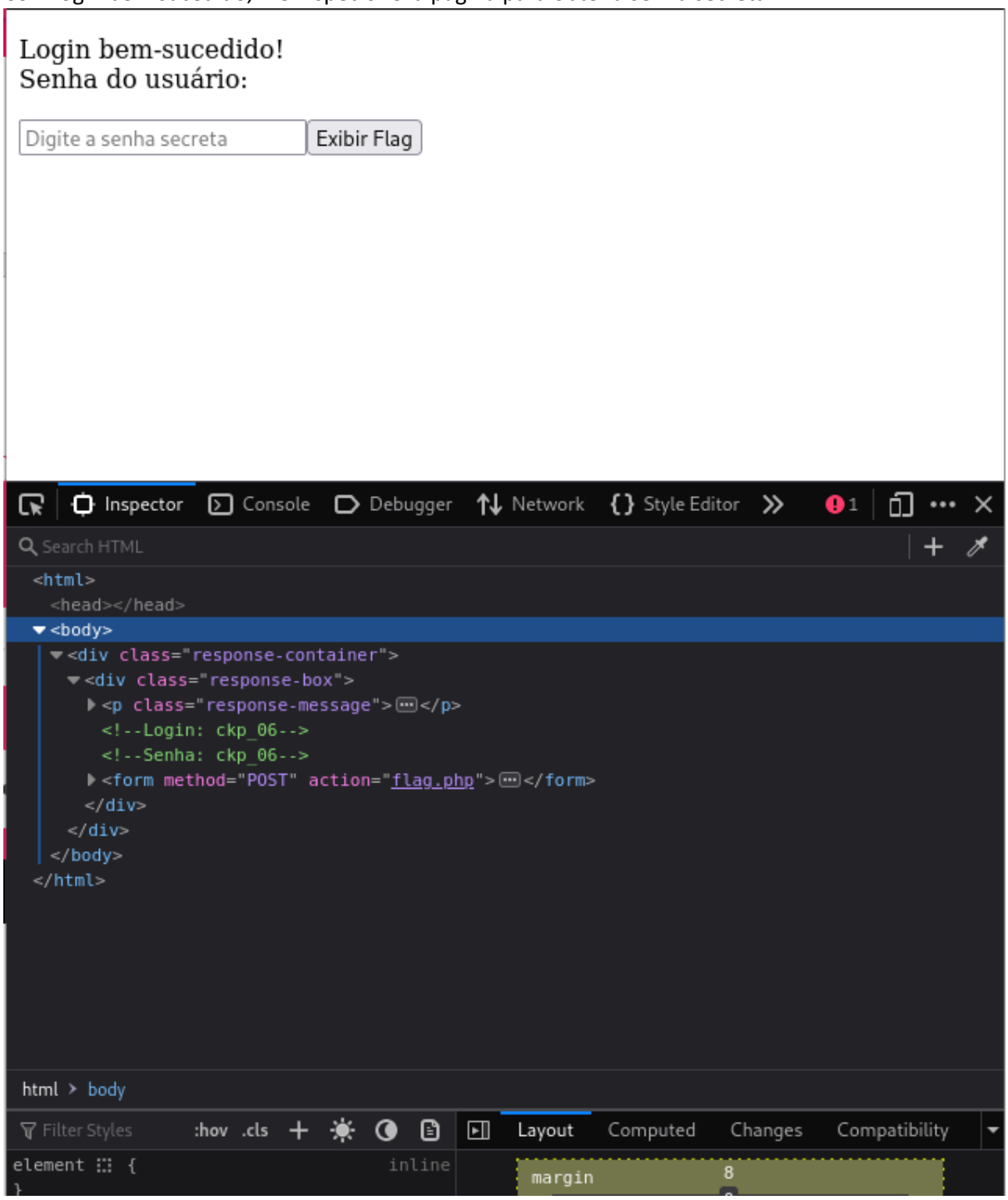


Pesquisei o ip do **Portal do Aluno em Teste** e coloquei no Navegador:



A partir do Sql Injection, utilizei os códigos:

Com login bem sucedido, me inspecionei a pagina para obter a senha secreta:



Utilizando a senha secreta, me conectei e obtive a primeira Flag:

Flag: FIAP_SQLI{6716e1333e7cd}

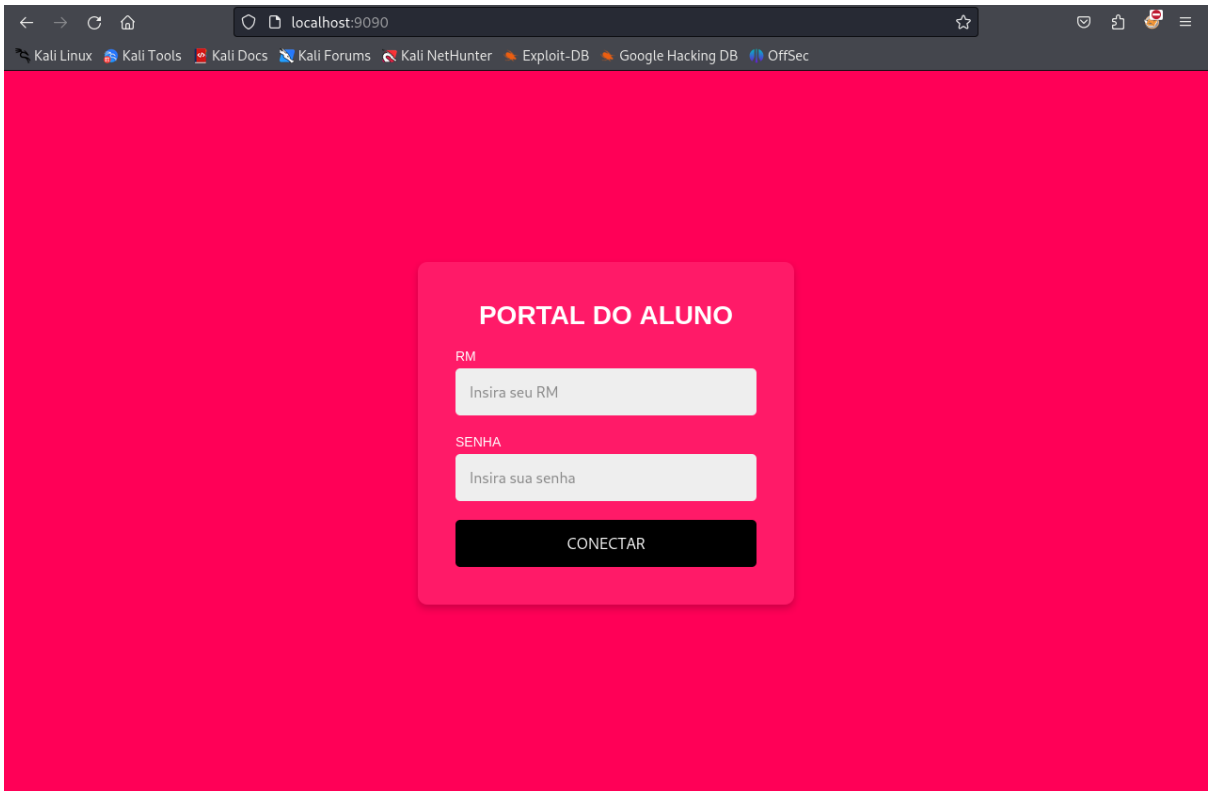
Conexão SSH no usuário ckp_06:

```
┌──(root㉿kali)-[~]
└─# ssh ckp_06@192.168.100.10
The authenticity of host '192.168.100.10 (192.168.100.10)' ca
n't be established.
ED25519 key fingerprint is SHA256:HXhrA8QYF6+aAdX6DXLn9JPGa5w
1kiz18cEZmmWGaGQ.
This host key is known by the following other names/addresses
:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerp
rint])? yes
Warning: Permanently added '192.168.100.10' (ED25519) to the
list of known hosts.
ckp_06@192.168.100.10's password:
Linux debian 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-0
1-31) x86_64

The programs included with the Debian GNU/Linux system are fr
ee software;
the exact distribution terms for each program are described i
n the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the ex
tent
permitted by applicable law.
Last login: Sun Oct 20 19:34:50 2024 from 192.168.100.20
Could not chdir to home directory /home/ckp_06: No such file
or directory
$
```

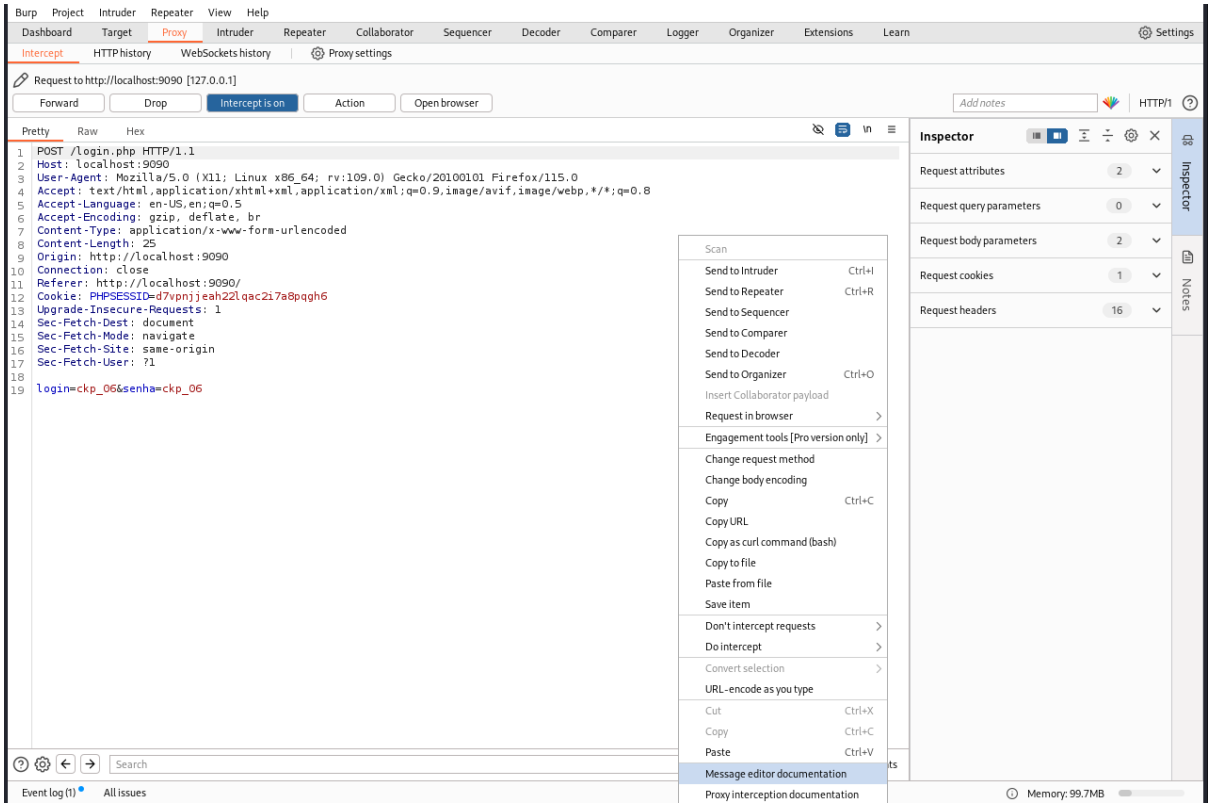
Usarei esse código para trocar a porta e consegui me conectar ao segundo site:

```
┌──(root㉿kali)-[~]
└─# ssh -p 22 -L 9090:localhost:9090 ckp_06@192.168.100.10
```

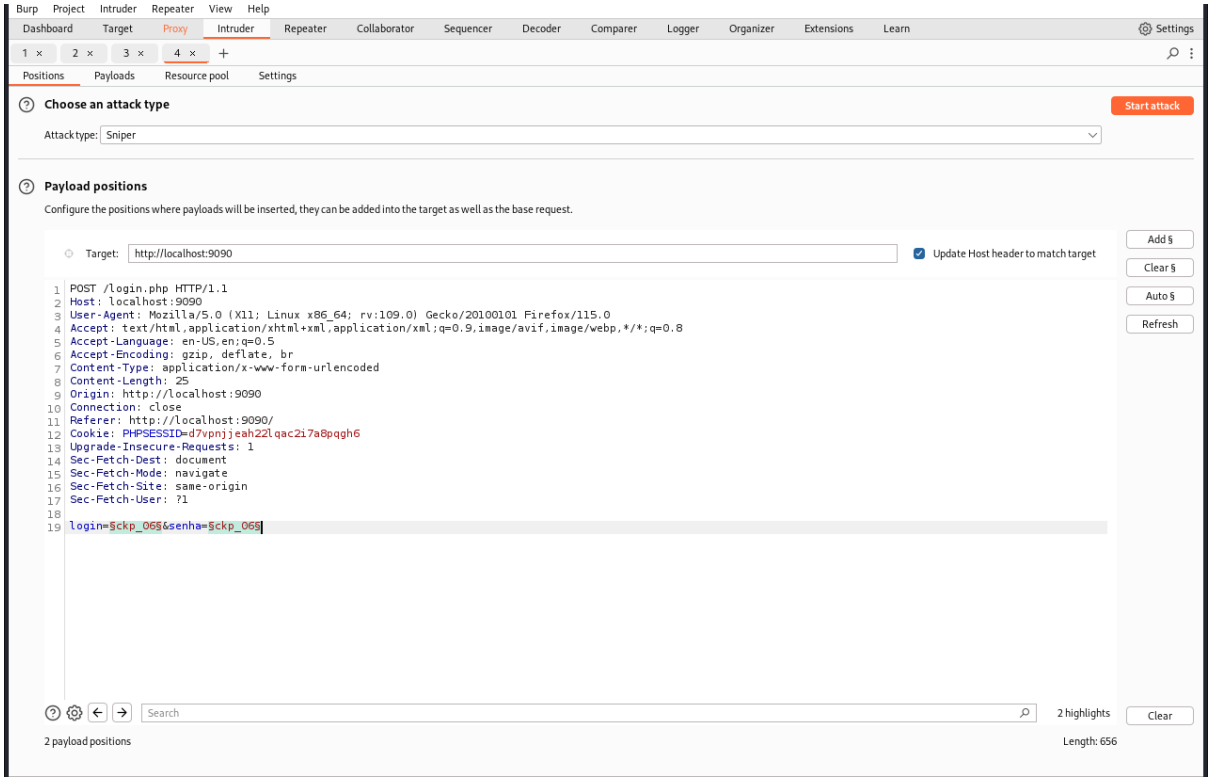
Assim consigo acessar o segundo site através do Local Host:



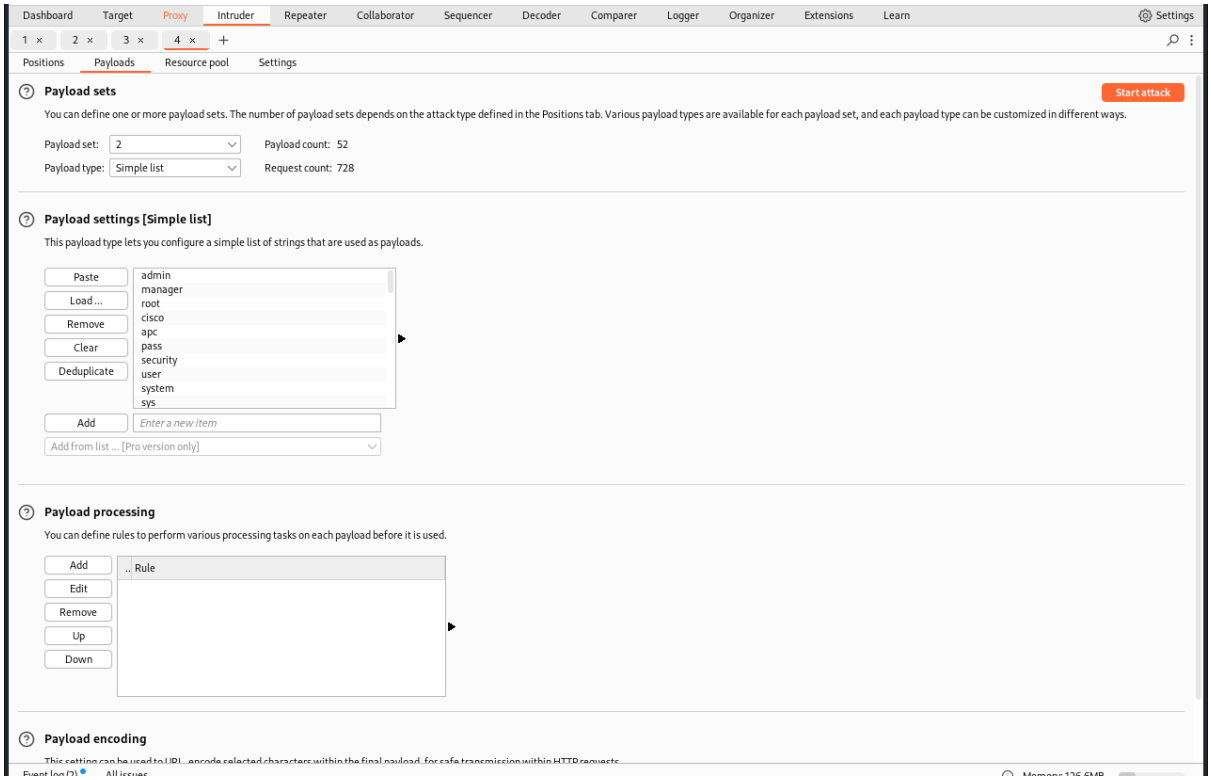
Após ligar o Burp, tento fazer uma requisição na aplicação e depois venho no Burp e Send TO intruder:



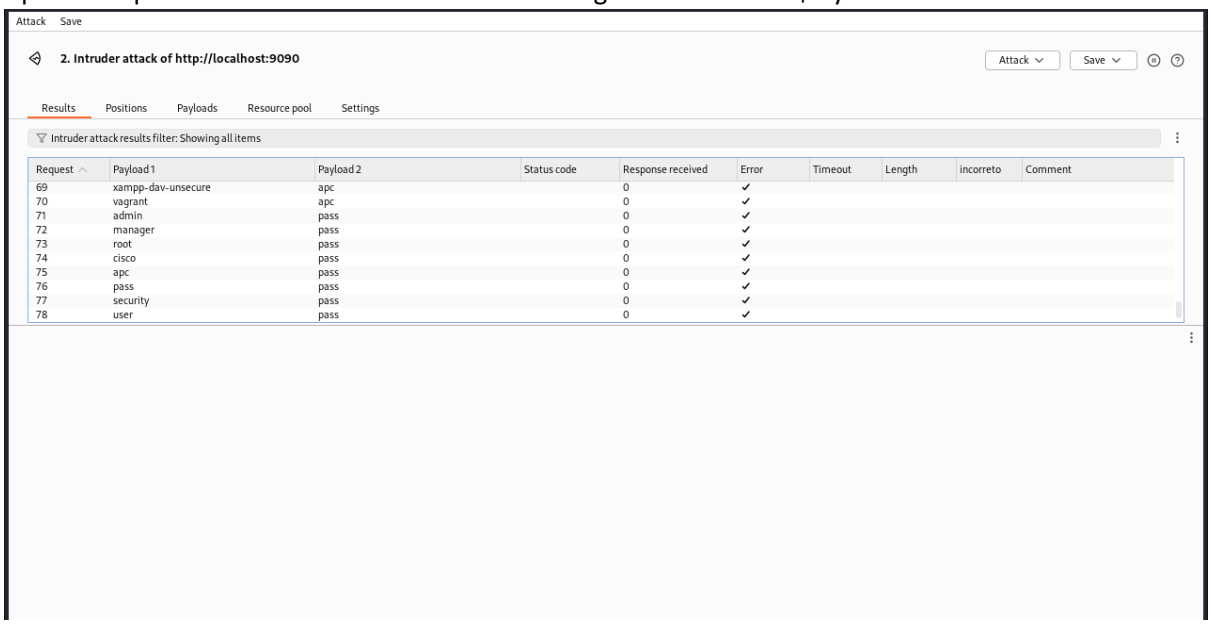
Vou dar add na senha e no login já no intruder:

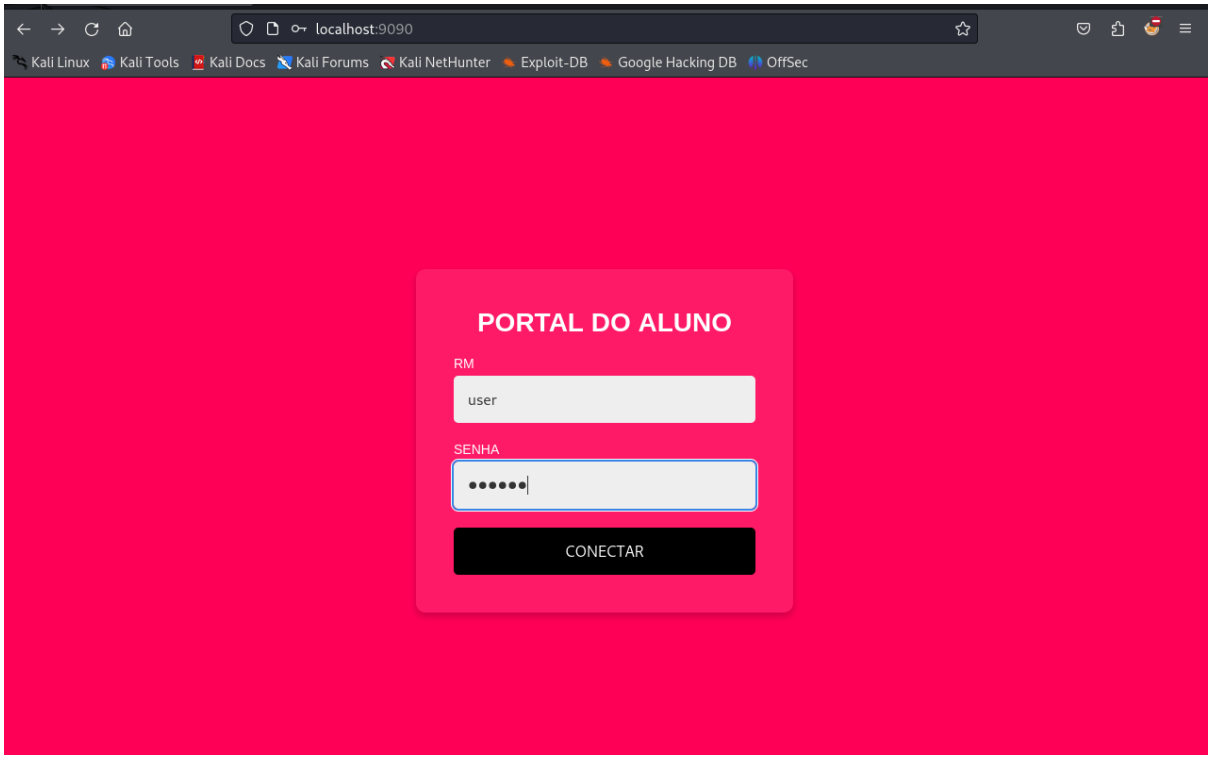


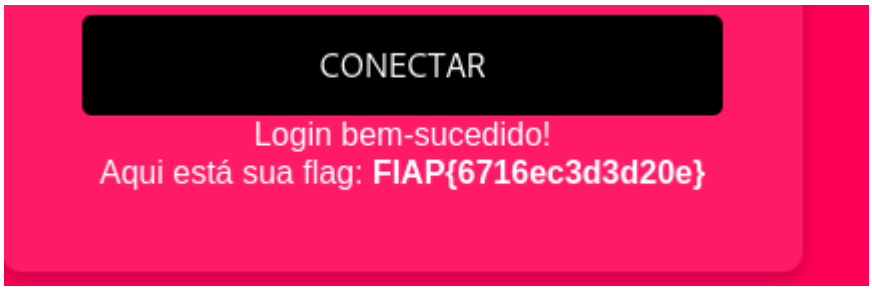
Configuerei o Payload para login e senha e iniciei o Ataque:



Após o Burp terminar de rodar você vai achar a login e senha User $ System:




localhost:9090
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PORTAL DO ALUNO
RM
user
SENHA
CONECTAR


CONECTAR
Login bem-sucedido!
Aqui está sua flag: FIAP{6716ec3d3d20e}