

CP6 CYBER

Nome: Rafael Afonso Benbassato

RM: 85321

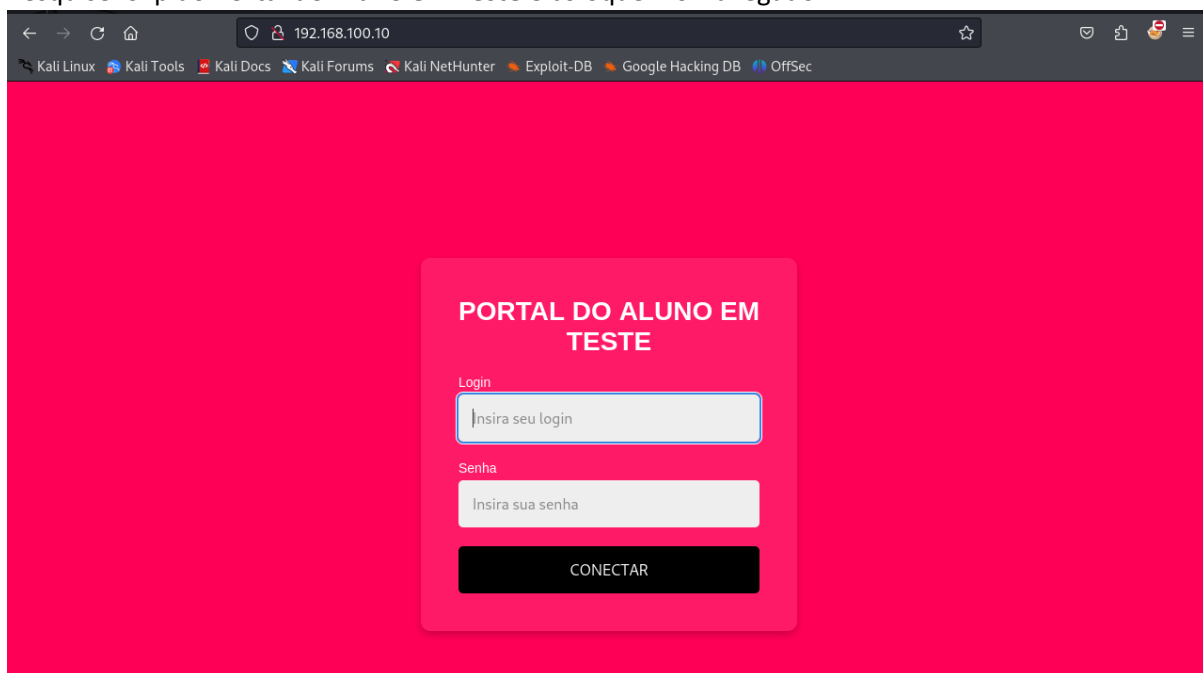
Primeiramente configurei a rede no Kali para poder se conectar ao servidor:

```
(root@kali)-[/etc/network]
# ifup eth1

(root@kali)-[/etc/network]
# ip -br -c a
lo                UNKNOWN    127.0.0.1/8 ::1/128
eth0              UP        10.0.2.15/24 fe80::829:7a13:8834:fb25/64
eth1              UP        192.168.100.70/24 fe80::a00:27ff:feaf:3e3d/64
eth2              UP        10.20.23.85/24 fe80::de1e:8a45:a920:2962/64

(root@kali)-[/etc/network]
# ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=2.95 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=2.40 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=3.10 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=64 time=2.87 ms
^S64 bytes from 192.168.100.10: icmp_seq=5 ttl=64 time=2.94 ms
^C
— 192.168.100.10 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4082ms
rtt min/avg/max/mdev = 2.401/2.852/3.098/0.237 ms
```

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

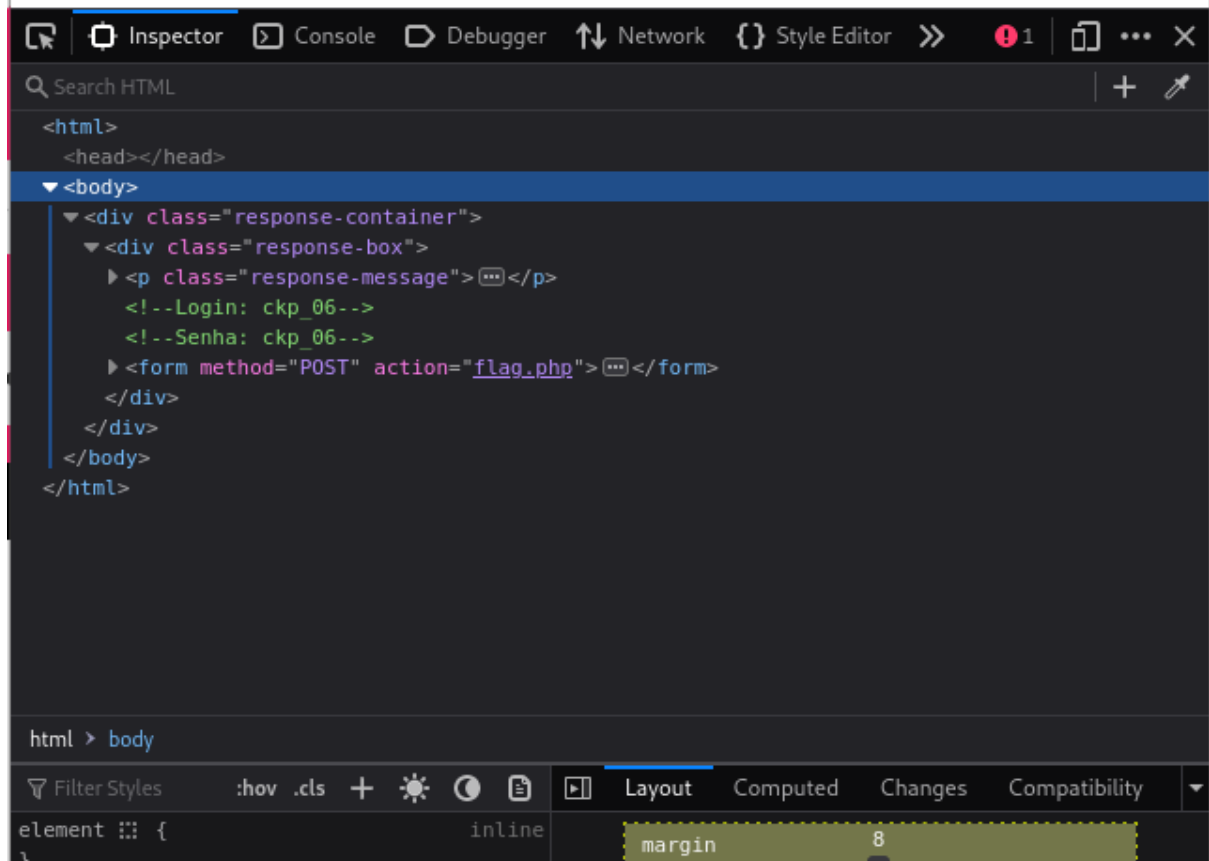


A partir do Sql Injection, utilizei os códigos:

[illegible]

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

Login bem-sucedido!
Senha do usuário:



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

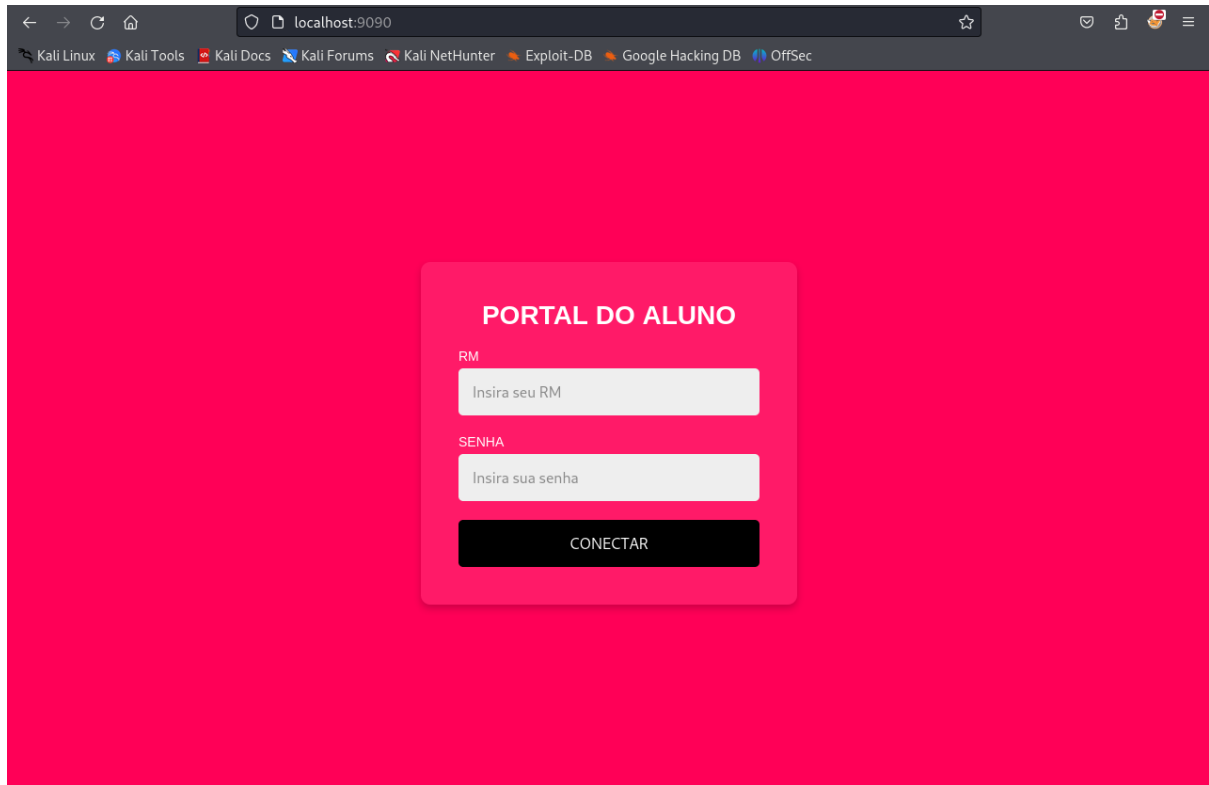
The programs included with the Debian GNU/Linux system are fr
ee software;
the exact distribution terms for each program are described i
n the
individual files in /usr/share/doc/*/copyright.

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:

Intercept

Request to http://localhost:9090 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

Add notes HTTP/1

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 2

Request cookies 1

Request headers 16

Scan

- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer Ctrl+O
- Insert Collaborator payload
- Request in browser
- Engagement tools [Pro version only]
- Change request method
- Change body encoding
- Copy Ctrl+C
- Copy URL
- Copy as curl command (bash)
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut Ctrl+X
- Copy Ctrl+C
- Paste Ctrl+V
- Message editor documentation
- Proxy interception documentation

Event log (1) All issues

Memory: 99.7MB

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

Intruder

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:9090

Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

```
1 POST /login.php HTTP/1.1
2 Host: localhost:9090
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 25
9 Origin: http://localhost:9090
10 Connection: close
11 Referer: http://localhost:9090/
12 Cookie: PHPSESSID=d7vpnjjeah22lqac217a8pqgh6
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 login=$ckp_06$senha=$ckp_06$
```

2 payload positions

2 highlights

Length: 656

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

The screenshot shows the Burp Suite interface with the Intruder tab selected. The top navigation bar includes Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the navigation bar, there are tabs for Positions, Payloads, Resource pool, and Settings. The main area is divided into three sections: Payload sets, Payload settings [Simple list], and Payload processing.

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 52
Payload type: Simple list Request count: 728

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Buttons: Paste, Load..., Remove, Clear, Deduplicate, Add, Add from list... [Pro version only]

Input field: Enter a new item

List of items: admin, manager, root, cisco, apc, pass, security, user, system, sys

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Buttons: Add, Edit, Remove, Up, Down

Rule list: .. Rule

Payload encoding

This setting can be used to URL encode selected characters within the final payload, for safe transmission within HTTP requests.

Buttons: Encode, All issues

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

The screenshot shows the Burp Suite interface with the Intruder tab selected. The top navigation bar includes Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. Below the navigation bar, there are tabs for Positions, Payloads, Resource pool, and Settings. The main area is divided into three sections: Results, Positions, Payloads, Resource pool, and Settings.

Results

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Incorrect	Comment
69	xampp-dav-unsecure	apc	0	✓					
70	vagrant	apc	0	✓					
71	admin	pass	0	✓					
72	manager	pass	0	✓					
73	root	pass	0	✓					
74	cisco	pass	0	✓					
75	apc	pass	0	✓					
76	pass	pass	0	✓					
77	security	pass	0	✓					
78	user	pass	0	✓					

