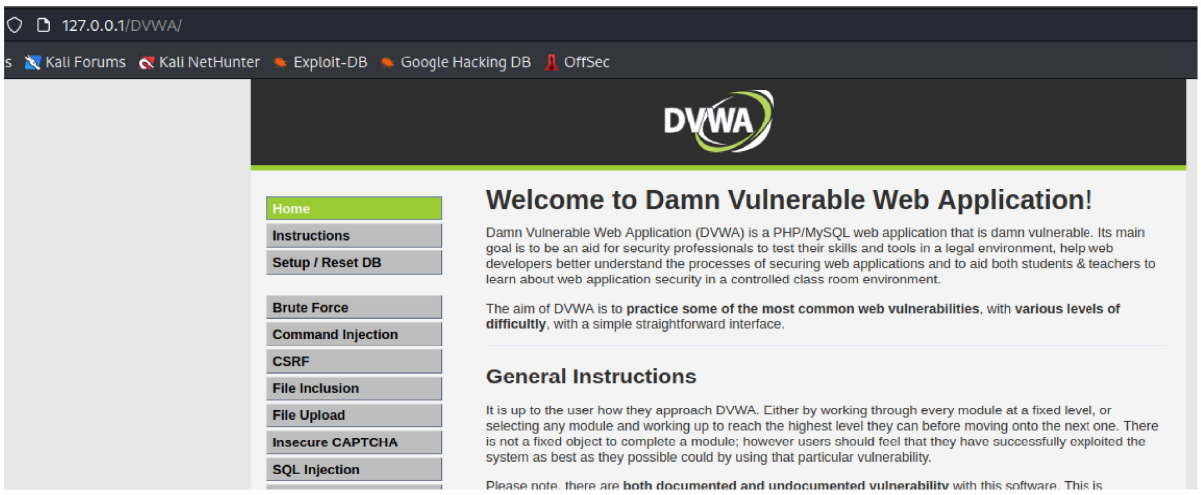
Setup apache2

```
┌──(root㉿kali)-[/home/alessio]
└─# service apache2 start

┌──(root㉿kali)-[/home/alessio]
└─# cd /etc/php/8.1/apache2

┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─# ls
conf.d  php.ini

┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─# gedit php.ini

┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─# service apache2 start
```

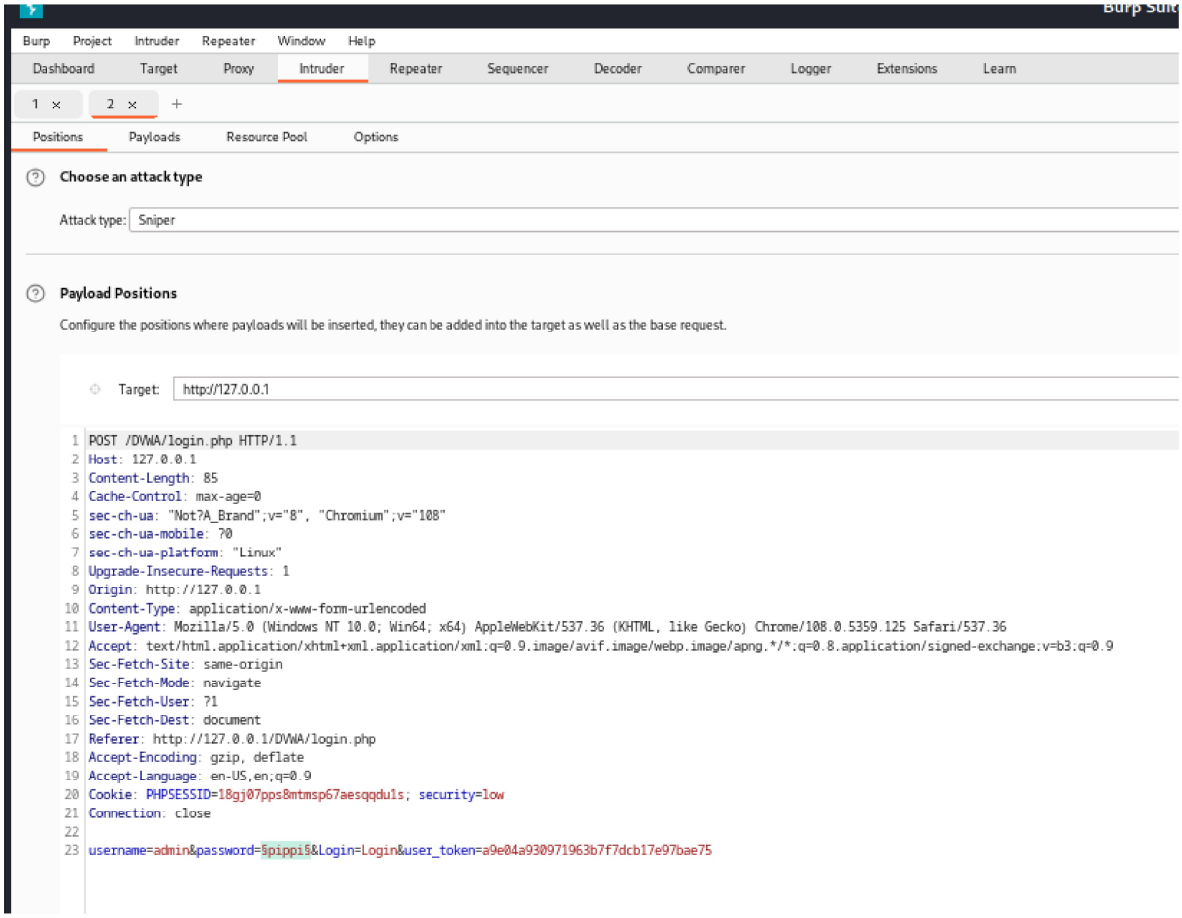
Configurazione mysql

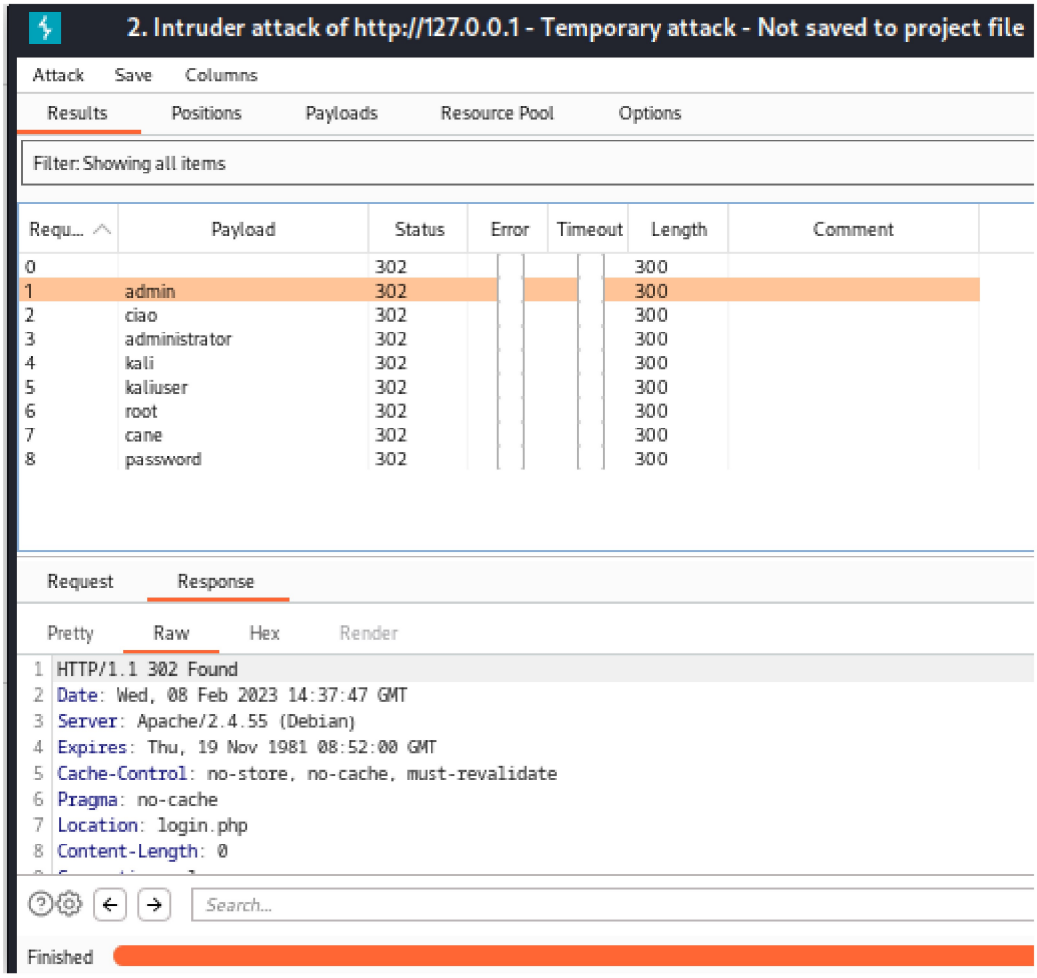
```
┌──(root㉿kali)-[/home/alessio]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.6.11-MariaDB-2 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali'
    -> create user 'kali'@'127.0.0.1' identified by 'kali'
    -> create user 'kali'@'127.0.0.1' identified by 'kali'
    -> create user 'kali'@'127.0.0.1' identified by 'kali' /g
    -> create user 'kali'@'127.0.0.1' identified by 'kali' \g
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server
version for the right syntax to use near 'create user 'kali'@'127.0.0.1' identified by 'kali'
create user 'kali'@'127.0 ... ' at line 2
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' \g
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> exit
Bye
```

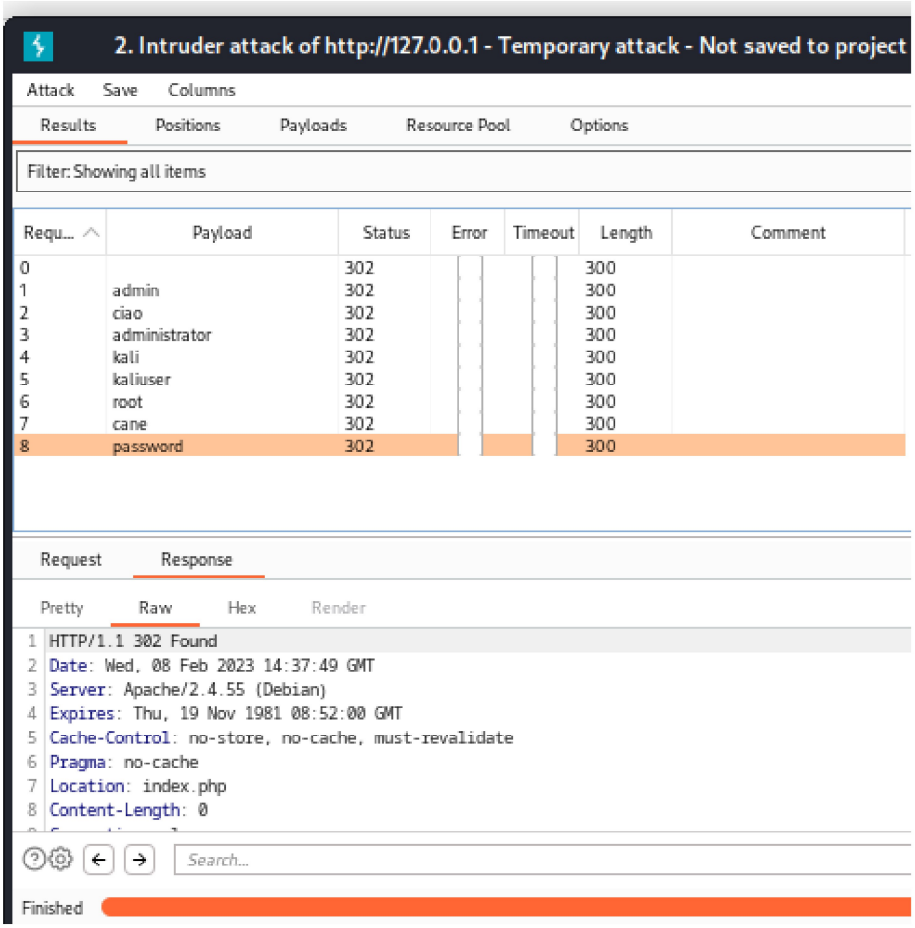
DVWA



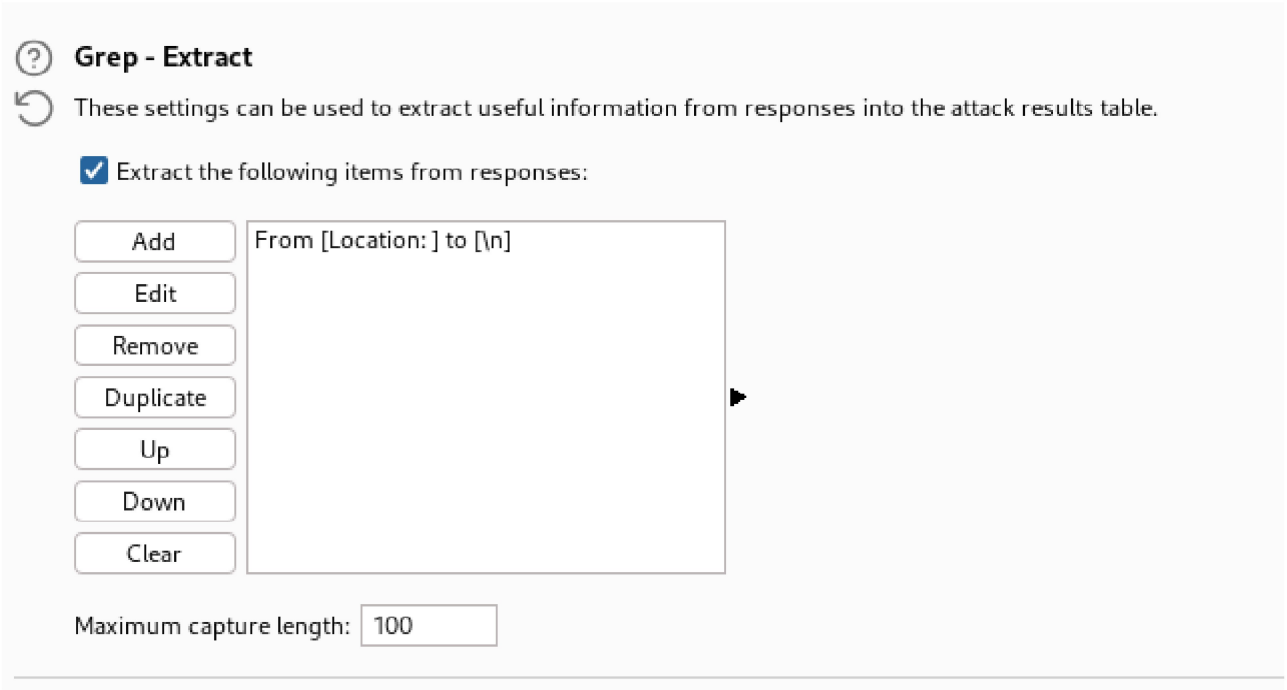
Prova di intruder




2. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource Pool
Options
Filter: Showing all items
Requ...
Payload
Status
Error
Timeout
Length
Comment
0 302 300
1 admin 302 300
2 ciao 302 300
3 administrator 302 300
4 kali 302 300
5 kaliuser 302 300
6 root 302 300
7 cane 302 300
8 password 302 300
Request
Response
Pretty
Raw
Hex
Render
1 HTTP/1.1 302 Found
2 Date: Wed, 08 Feb 2023 14:37:47 GMT
3 Server: Apache/2.4.55 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 0
Search...
Finished


2. Intruder attack of http://127.0.0.1 - Temporary attack - Not saved to project
Attack
Save
Columns
Results
Positions
Payloads
Resource Pool
Options
Filter: Showing all items
Requ...
Payload
Status
Error
Timeout
Length
Comment
0 302 300
1 admin 302 300
2 ciao 302 300
3 administrator 302 300
4 kali 302 300
5 kaliuser 302 300
6 root 302 300
7 cane 302 300
8 password 302 300
Request
Response
Pretty
Raw
Hex
Render
1 HTTP/1.1 302 Found
2 Date: Wed, 08 Feb 2023 14:37:49 GMT
3 Server: Apache/2.4.55 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: index.php
8 Content-Length: 0
Search...
Finished

Password trovata




Risultato con extract

| Request | Payload | Status | Error | Timeout | Length | Location: |
|---|---|---|---|---|---|---|
| 0 | | 302 | ☐ | ☐ | 300 | login.php |
| 1 | admin | 302 | ☐ | ☐ | 300 | login.php |
| 2 | ciao | 302 | ☐ | ☐ | 300 | login.php |
| 3 | administrator | 302 | ☐ | ☐ | 300 | login.php |
| 4 | kali | 302 | ☐ | ☐ | 300 | login.php |
| 5 | kaliuser | 302 | ☐ | ☐ | 300 | login.php |
| 6 | root | 302 | ☐ | ☐ | 300 | login.php |
| 7 | cane | 302 | ☐ | ☐ | 300 | login.php |
| 8 | password | 302 | ☐ | ☐ | 300 | index.php |

Possiamo capire più facilmente qual’è la password corretta