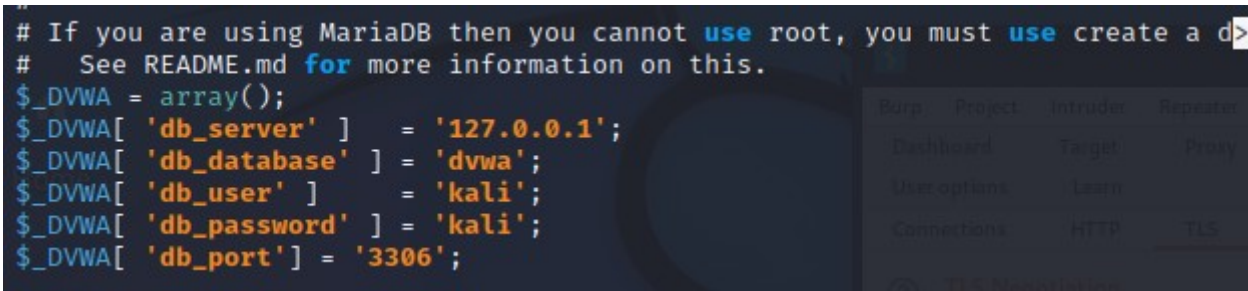


## Installazione di MySQL, APACHE2, DVWA e BurpSuite

Come prima operazione usiamo il comando “sudo su” per avere i privilegi di root ed andiamo nella cartella `/var/www/html` ed usiamo il comando `git clone https://github.com/digininja/DVWA` impostiamo tutti i privilegi con il comando `chmod` ed entriamo nella sua directory ed andiamo a configurare il file nel seguente modo:

```
# If you are using MariaDB then you cannot use root, you must use create a d>
# See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ] = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port' ] = '3306';
```



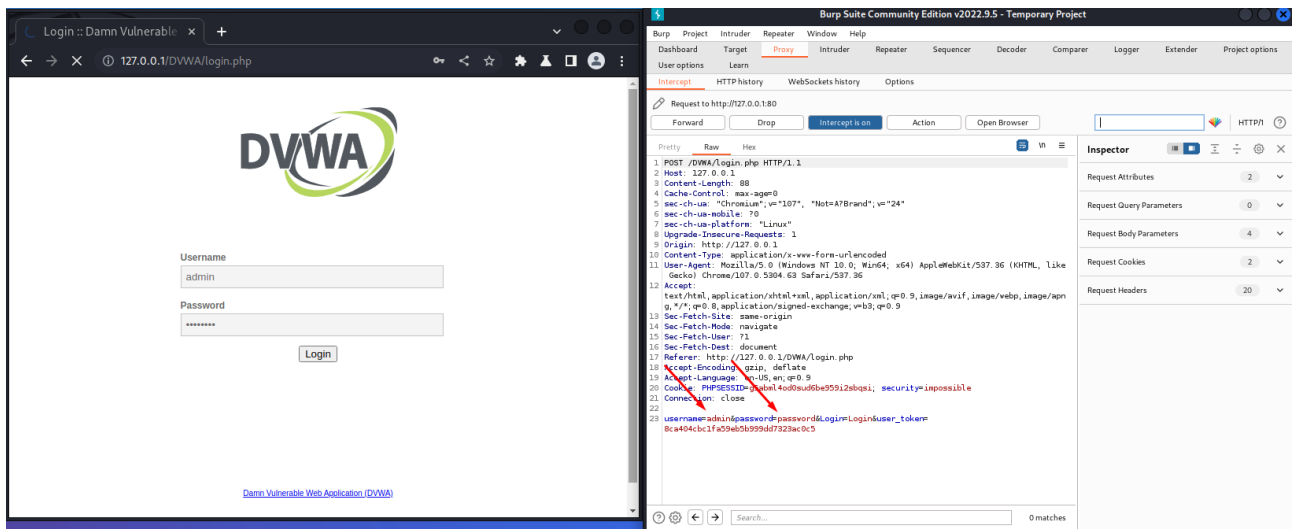
Dopodiché avviamo il servizio mysql (`service mysql start`) ed andiamo a creare un nuovo utente ed a garantirgli tutti i privilegi con i seguenti comandi:

1. `mysql -u root -p`
2. `create user 'kali'@'127.0.0.1' identified by 'kali';`
3. `grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';`

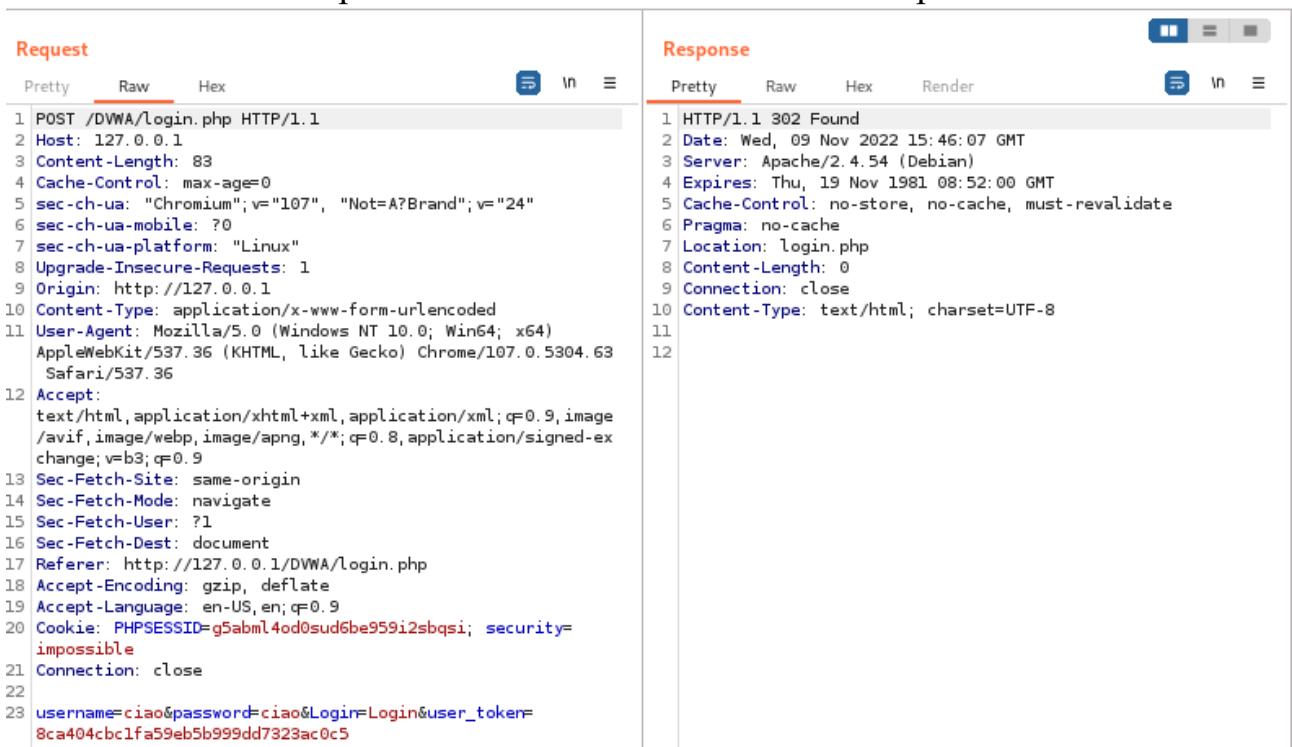
Fatto ciò scriviamo ed inviamo exit per poi avviare il servizio apache2 (`service apache2 start`) per poi spostarci nella directory `/etc/php/8.1/apache2` e poi cliccando F6 andiamo a cercare le seguenti frasi mettendoli entrambi su On:

- `allow_url_fopen`
- `allow_url_include`

Dopodiché eseguire di nuovo il comando `service apache2 start` e finalmente possiamo andare sul sito `127.0.0.1/DVWA/setup.php` per poi cliccare su Create/Reset Database. Fatto ciò apparirà sulla sinistra un menù ed andando a cliccare su DVWA Security possiamo notare che ci sono più livelli di sicurezza (Low, Medium High, Impossible) e sarà impostato di default Impossible. Fatto ciò possiamo cliccare su Logout e provare ad inserire le credenziali intercettando i pacchetti con BurpSuite come di seguito:



Ora andiamo a modificare le credenziali inserendo “ciao” ad entrambi e poi con tasto destro mandiamo al repeater dove andremo a cliccare send e poi follow redirection:



```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium"; v="107", "Not=A?Brand"; v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.63
  Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image
  /avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
  change;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: PHPSESSID=g5abml4od0sud6be959i2sbqsi; security=
  impossible
19 Connection: close
20
21
```

```

  Login">
    </p>
54
55    </fieldset>
56
57    <input type='hidden' name='user_token' value='
      2b89e02fe59f68db3f93eae5200dae65' />
58
59    </form>
60
61    <br />
62
63    <div class="message">
      Login failed
    </div>
64
65    <br />
66    <br />
67    <br />
68    <br />
69    <br />
70    <br />
71    <br />
72    <br />
73
74    <!--  -->
75  </div>
76    <!--<div id="content">-->
77
78    <div id="footer">
```