Obiettivo esercitazione:

- 1. Installare mysql e apache sulla nostra macchina virtuale
- 2. Creare un nuovo database impostando come user "Admin" e come password "password"
- 3. Fare login e usare burpsuite per guardare tutti i parametri che vengono passati tra client e server

Scarichiamo la DVWA dal repository

```
(1007 Mail) - /var/www/html | mg tic clone https://github.com/digininja/DVWA cloning into 'DVWA'... remote: Enumerating objects: 3986, done. remote: Total 3986 (delta 0), reused 0 (delta 0), pack-reused 3986 Receiving objects: 100% (3986/3986), 1.77 MiB | 3.25 MiB/s, done. Resolving deltas: 100% (1867/1867), done.
               pot@kali)-[/var/www/html
hmod -R 777 DVWA/
             root@kali)-[/var/www/html]
cd DVWA/config
          root@ kali)-[/var/www/html/DVWA/config
cp config.inc.php.dist config.inc.php
                       (6 kali)-[/var/www/html/DVWA/config)
config.inc.php
```

Dopodiché si passa alla configurazione del file config all'interno per impostare come user e password "kali"

```
$_DVWA = array();
$_DVWA[ 'db_server'
                           = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]
        'db_password'
                        ] = 'kali
  _DVWA[
 DVWA[ 'db_port'] = '3306';
```

Successivamente ci colleghiamo al servizio di mysql creando un'utenza kali associandogli un indirizzo identificativo, in questo caso 127.0.0.1

E facciamo partire anche il servizio di web server apache con il comando "service apache2 start" che ci servirà per raggiungere la pagina internet dove creeremo il database

```
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.006 sec)
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.008 sec)
MariaDB [(none)]> exit
```

Cercando sul browser di kali "127.0.0.1/DVWA/setup.php" uscirà il setup di apache

```
Setup Check
Web Server SERVER_NAME: 127.0.0.1
Operating system: *nix
PHP version: 8.1.5
PHP function display_errors: Disabled
PHP function safe mode: Disabled
PHP function allow url include: Enabled
PHP function allow url fopen: Enabled
PHP function magic quotes gpc: Disabled
```

In fondo alla pagina cliccando sul pulsante "Create/Reset database" verremo reindirizzati alla pagina login dove entreremo con le nostre credenziali



username: admin / / password: password

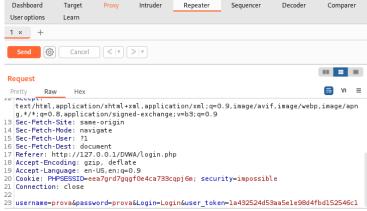
Una volta entrati possiamo impostare il livello di sicurezza e configurare il tutto a nostro piacimento

3

Riprovando a fare il login ma con il browser di Burpsuite vediamo i pacchetti che si scambiano

```
1 POST /DWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";y="103", ".Not/A)Brand";y="99"
6 sec-ch-ua-mbbile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Sec-Fetch-User: ?1
16 Sec-Fetch-User: ?1
17 Referer: http://127.0.0.1/DWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Encoding: gzip, deflate
19 Accept-Encoding: gzip, deflate
19 Accept-Encoding: gzip, deflate
20 Cookie: PHPSESSID=eea7grd7gqgf0e4ca733cqpj6m; security=impossible
21 Connection: close
22 username=admin&password=password&Login=Login&user_token=
1a432524d53aa5ele98d4fbd152546c1
```

Se provo a cambiare le credenziali di accesso con prova e prova e mando il testo con il send del repeater



Giustamente il sito non mi riconosce. E dalla schermata del response mi fa vedere che non mi fa entrare

```
<div class="message">
  Login failed
</div>
```