REPORT ESERCIZIO BURPSUITE

FRANCESCO PERSICHETTI

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

1

Scarichiamo la DVWA dal repository

```
┌──(root㉿kali)-[/var/www/html]
└─# git 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.

┌──(root㉿kali)-[/var/www/html]
└─# chmod -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

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# nano 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' ]     = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_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
```

2

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

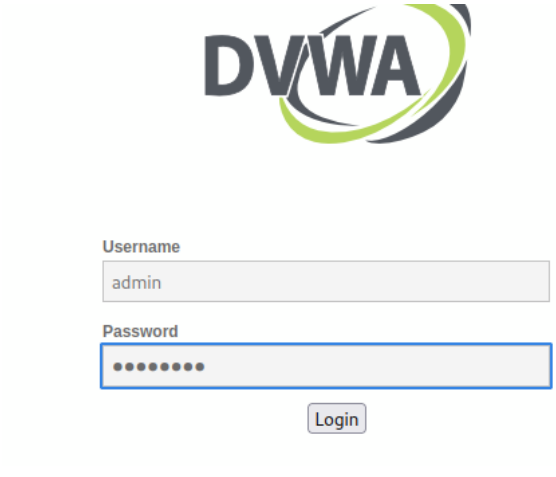
Setup Check

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

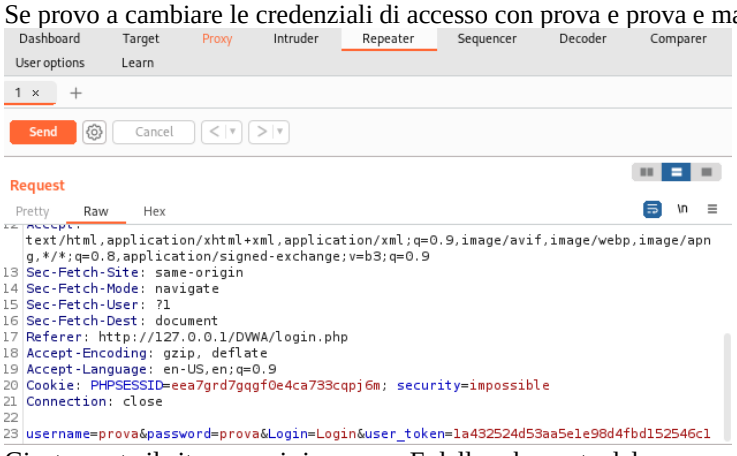
Una volta entrati possiamo impostare il livello di sicurezza e configurare il tutto a nostro piacimento

3
Riprovando a fare il login ma con il browser di Burpsuite vediamo i parametri che si scambiano

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="103", ".Not/A)Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=eea7grd7gqgf0e4ca733cqpj6m; security=impossible
Connection: close

username=admin&password=password&Login=Login&user_token=
1a432524d53aa5e1e98d4fbd152546c1
```

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




```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=eea7grd7gqgf0e4ca733cqpj6m; security=impossible
Connection: close

username=prova&password=prova&Login=Login&user_token=1a432524d53aa5e1e98d4fbd152546c1
```

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>
```