

ESERCIZIO 2 SETTIMANA 3

Inizio dell'esercizio -> configurazione e installazione DVWA

Dopo aver aperto il terminale ho digitato i seguenti comandi in modo da poter avviare il servizio apache per poi accedere alla pagina di localhost, dove posso creare il mio db.

```
File Actions Edit View Help
(kali@kali)~[/Desktop]
$ sudo su
[sudo] password for kali:
(root@kali)~[/home/kali/Desktop]
# cd /var/www/html

(root@kali)~[/var/www/html]
# pwd
/var/www/html

(root@kali)~[/var/www/html]
# dir
DVWA index.html index.nginx-debian.html

(root@kali)~[/var/www/html]
# ll
total 20
drwxrwxrwx 12 root root 4096 Dec 12 09:44 DVWA
-rw-r--r-- 1 root root 10701 Aug 21 14:58 index.html
-rw-r--r-- 1 root root 615 Aug 21 14:57 index.nginx-debian.html

(root@kali)~[/var/www/html]
# cd DVWA

(root@kali)~[/var/www/html/DVWA]
# DIR
DIR: command not found

(root@kali)~[/var/www/html/DVWA]
# dir
about.php      docs            login.php      README.fr.md  SECURITY.md
CHANGELOG.md   dvwa            logout.php     README.id.md  security.php
compose.yml    external       phpinfo.php    README.md     security.txt
config         favicon.ico     php.ini        README.pt.md  setup.php
COPYING.txt    hackable       README.ar.md   README.tr.md  tests
database       index.php      README.es.md   README.zh.md  vulnerabilities
Dockerfile     instructions.php README.fa.md    robots.txt
```

```
(root@kali)~[/var/www/html/DVWA]
# cd 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

(root@kali)~[/var/www/html/DVWA/config]
# vi config.inc.php

(root@kali)~[/var/www/html/DVWA/config]
# pwd
/var/www/html/DVWA/config

(root@kali)~[/var/www/html/DVWA/config]
# cd /

(root@kali)~[/]
# service mysql status
o mariadb.service - MariaDB 10.11.4 database server
   loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: >
   active: inactive (dead)
   docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
... skipping ...
o mariadb.service - MariaDB 10.11.4 database server
   loaded: loaded (/lib/systemd/system/mariadb.service; disabled; preset: >
   active: inactive (dead)
   docs: man:mariadb(8)
        https://mariadb.com/kb/en/library/systemd/
```

```
(root@kali)~[/]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.11.4-MariaDB-1 Debian 12

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)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identi
fied by 'kali';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> exit
Bye

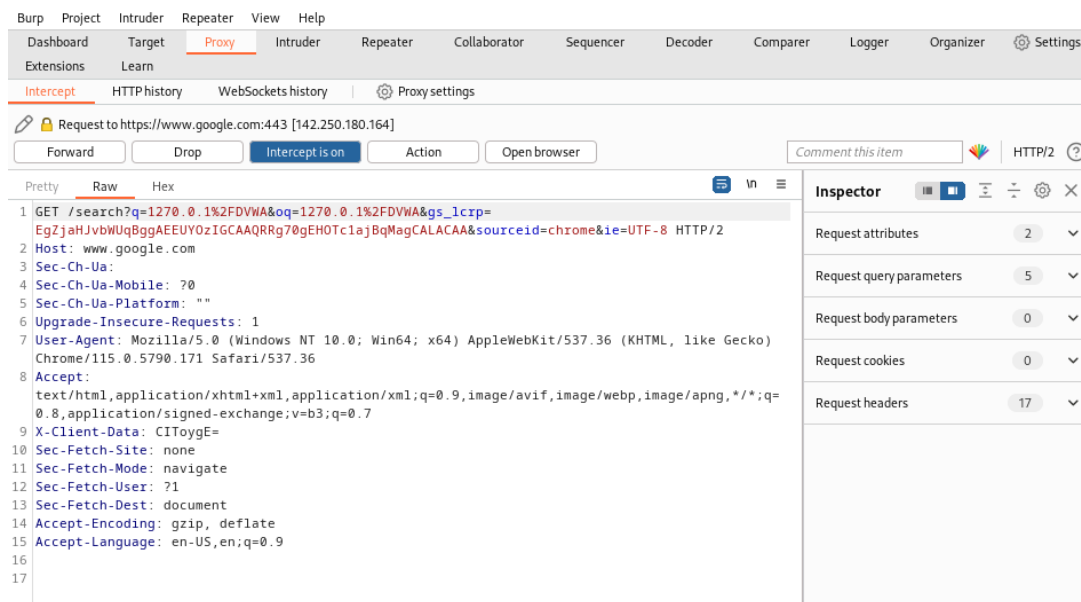
(root@kali)~[/]
# service apache2 start
```

Successivamente sono andato a modificare le voci che erano segnate Off in On.

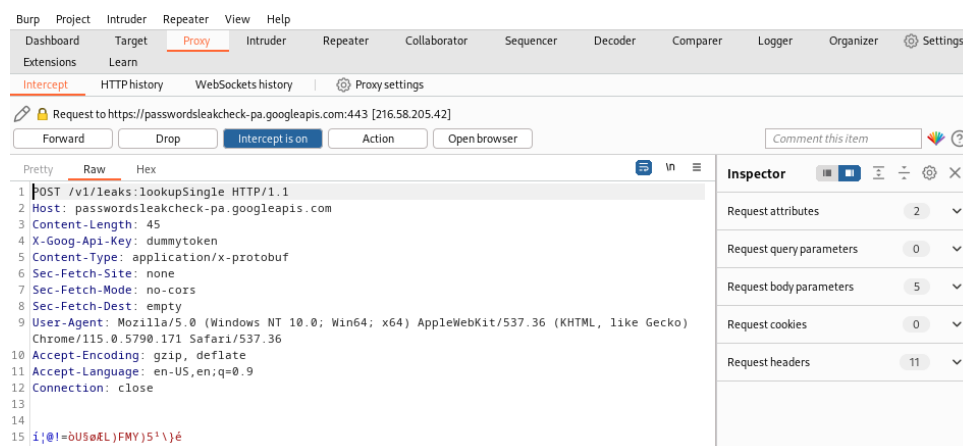
```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

Successivamente ho lanciato Burp Suite, programma che funziona da proxy e mi permette di vedere tutte le richieste e risposte tra me e il sito web al quale voglio connettermi.



Successivamente ho provato ad aprire la pagina di localhost tramite Burp, inizialmente ho fatto l'accesso inserendo le credenziali corrette e sono riuscito ad accedere tranquillamente.



Dopo, invece, ho provato ad accedere con le credenziali errate e ovviamente la connessione mi è stata bloccata

The screenshot shows the Burp Suite interface with the Proxy tab selected. A request to `http://127.0.0.1:80` is intercepted. The request is a POST to `/DVWA/login.php` with the following details:

- Host: 127.0.0.1
- Content-Length: 81
- Cache-Control: max-age=0
- sec-ch-ua: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
- sec-ch-ua-mobile: ?0
- sec-ch-ua-platform: ""
- 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/115.0.5790.171 Safari/537.36
- 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=0.7
- 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: security=impossible; PHPSESSID=kv9achlnqh72oi54evvnnsi42t
- Connection: close
- body: `username=bla&password=bla&Login=Login&user_token=bf5324f6331eefd712d60dbd2ae068d8`

The Inspector panel on the right shows the request attributes, query parameters, body parameters, cookies, and headers.

Infine, ho provato a modificare le credenziali inserite direttamente all'interno di Burp per vedere il comportamento del sito tramite "send to repeater" in modo da inviare la richiesta direttamente dall'app. Il login è fallito e lo possiamo notare visionando il codice: noteremo nel body la scritta -> Login failed.

The screenshot shows the Burp Suite interface with the Repeater tab selected. A GET request to `/DVWA/login.php` is shown. The response is an HTML page with the following details:

- Host: 127.0.0.1
- Cache-Control: max-age=0
- sec-ch-ua: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
- sec-ch-ua-mobile: ?0
- sec-ch-ua-platform: ""
- Upgrade-Insecure-Requests: 1
- Origin: http://127.0.0.1
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
- 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=0.7
- 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: security=impossible; PHPSESSID=kv9achlnqh72oi54evvnnsi42t
- Connection: close

The response body contains the following HTML code:

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