root@Kali: /var/www/html/DVWA/config

File Actions Edit View Help

GNU nano 7.2 config.inc.php *

```php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port']      = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
#   so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = false;

define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
#   This does not affect the backend for any other services, just these two labs.
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^◂ Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward ^▸ Next Word ^E End

In questo esercizio andremo a installare una DVWA (Damn Vulnerable Web Application) su Kali Linux, creare un db (database) con MySQL e setuppare un web server con Apache.

Il tutto ci permetterà di fare pratica con delle varie vulnerabilità, utilizzando un ambiente protetto completamente su Kali Linux.

Per prima cosa, ho abilitato la connessione da rete interna a connessione con bridge, per ottenere l'accesso ad internet (ho abilitato il DHCP successivamente).

In questa schermata ho sostituito "user" e "password" del db.

Questa è l'interfaccia del db. Qui ho associato l'indirizzo IP (127.0.0.1) al database e creato un utente (kali) con tutti i privilegi a disposizione.

root@Kali: /etc/php/8.2/apache2

File Actions Edit View Help

```
┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# service mysql start

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
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)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.014 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
    '>
    '> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your Ma
riaDB server version for the right syntax to use near 'kali'@'127.0.0.1' identified by 'kali'' at line
 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.020 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
└─# service apache2 start

┌──(root㉿Kali)-[/var/www/html/DVWA/config]
```

Burp Suite Community Edition v2023.9.1 - Temporary Project

Request to http://127.0.0.1:80

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua:
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=dliu0udu5819av0ub3c4nicbko
Connection: close

username=admin&password=password&Login=Login&user_token=a335ca3e5cb59563eb7bd8fa72afe5ea
```

Login :: Damn Vulnerable

127.0.0.1/DVWA/login.php

Username: admin

Password: ••••••••

Login

A sinistra si può vedere "Burp Suite". Un programma che ci permette di fare da "filtro" o "intermediario" tra noi ed un eventuale sito web. Scambiando il certificato TLS legittimo, ci dà tutte le info, ad esempio, che il sito ci va ad inviare. Tutti i passaggi che ovviamente non notiamo navigando nel web ogni giorno.
(potremmo dire che ci fa dissezionare accuratamente ogni passaggio che ci porta alla connessione e alla visualizzazione di un sito web.)

Burp Suite Community Edition v2023.9.1 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /DVWA/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:
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: ""
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/115.0.5790.171 Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl
   ication/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=dliu0udu5819av0ub3c4nicbko
21 Connection: close
22
23 username=pippo&password=pippo&Login=Login&user_token=dddac1ebc31a78a764344487c6d8b4ac
```

Inspector

- Request attributes 2
- Request query parameters 0
- Request body parameters 4
- Request cookies 2
- Request headers ...

Search... 0 highlights

Login :: Damn Vulnerable

127.0.0.1/DVWA/login.php

DVWA

Username

admin

Password

••••••••

Login

Login failed

Damn Vulnerable Web Application (DVWA)

In questa sezione ho provato a cambiare username e password con dei valori ovviamente sbagliati. Come previsto il login non avviene correttamente.

DVWA è un ambiente vulnerabile di proposito, perciò ora che il laboratorio è stato setuppato correttamente si potranno testare varie tecniche ed exploit.