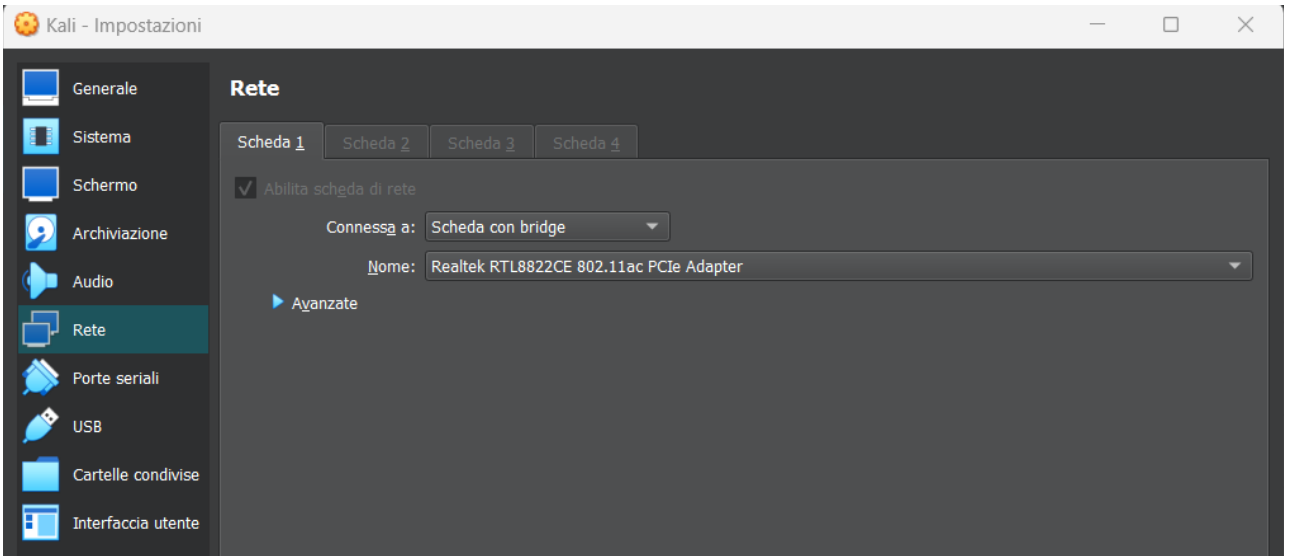
APPLICAZIONI WEB
Preparazione ambiente

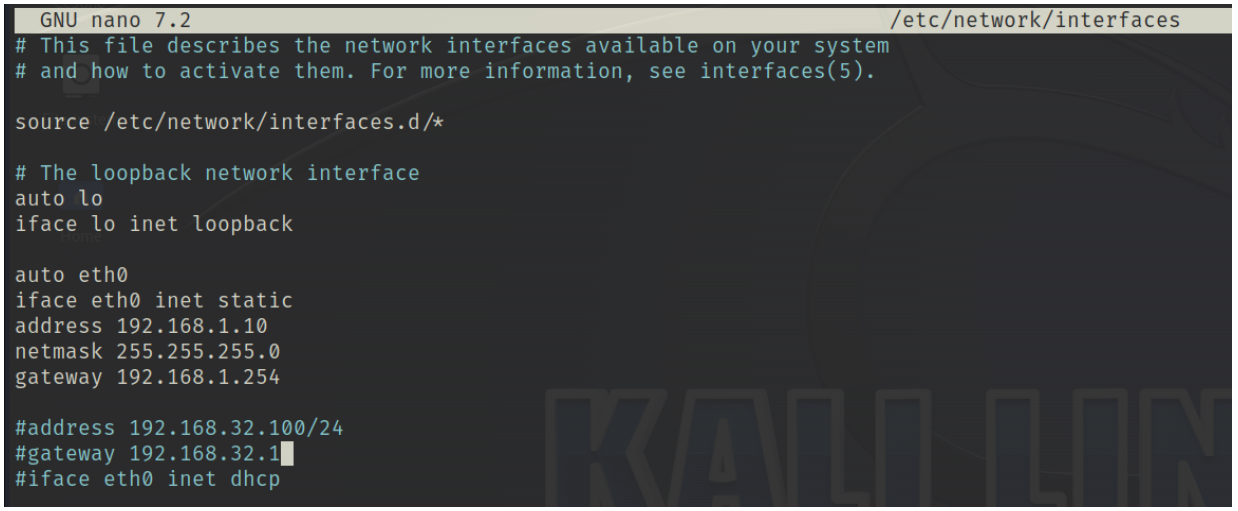
CONFIGURAZIONE DVWA = Damn Vulnerable Web Application

Vedremo come configurare una DVWA - ovvero una Damn Vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i build test

1) Abilito la connettività ad internet dalle impostazioni di rete di Kali Linux



2) Configuro il network con il comando `'sudo nano /etc/newtork/interfaces'`



3) Accedere con utenza 'root' tramite il comando `"sudo su"`

Ed eseguire i comandi:

```
┌──(root㉿kali)-[/home/jessica]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# sudo git clone htpps://github.com/digininja/DVWA
```

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

4) All'interno del file 'config.inc.php' cambio utente e password inserendo rispettivamente
user:kali
password:kali.

```
# 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' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
$_DVWA[ 'db_port']      = '3306';
```

5) Creo l'utenza con le credenziali salvate nel file 'config.inc.php' ed eseguo il comando:

```
> create user 'kali'@'127.0.0.1' identified by 'kali';
```

successivamente assegno i privilegi all'utente kali:

```
> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali'
```

```
┌──(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 48
Server version: 10.11.2-MariaDB-1 Debian n/a

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)]> SHOW GRANTS for 'kali'@'127.0.0.1';
+-----------------------------------------------------------------------------------------------------------------------+
| Grants for kali@127.0.0.1                                                                                             |
+-----------------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `kali`@`127.0.0.1` IDENTIFIED BY PASSWORD '*D64F6611CF18EA567ED1E8E74F2243AC1EDF54C4' |
| GRANT ALL PRIVILEGES ON `dvwa`.* TO `kali`@`127.0.0.1`                                                                |
+-----------------------------------------------------------------------------------------------------------------------+
2 rows in set (0,001 sec)

MariaDB [(none)]>
```

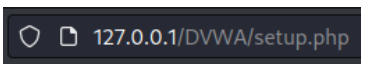
6) Eseguo il comando `'cd /etc/php'` per verificare la versione di php.

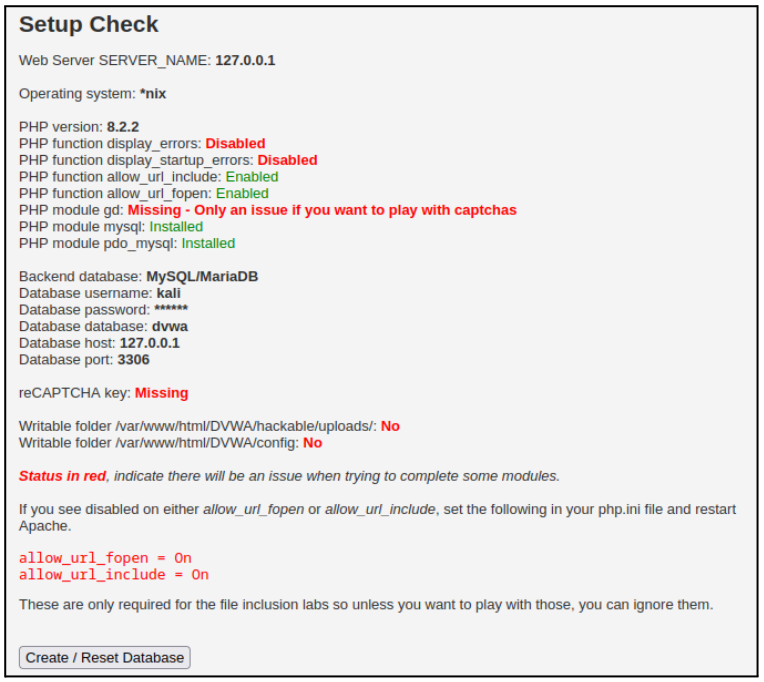
```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.2/apache2

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# sudo nano php.ini

┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# service apache2 start
```

7) Modificare il file 'php.ini' sotto la voce 'allow_url_include' configurata ad ON

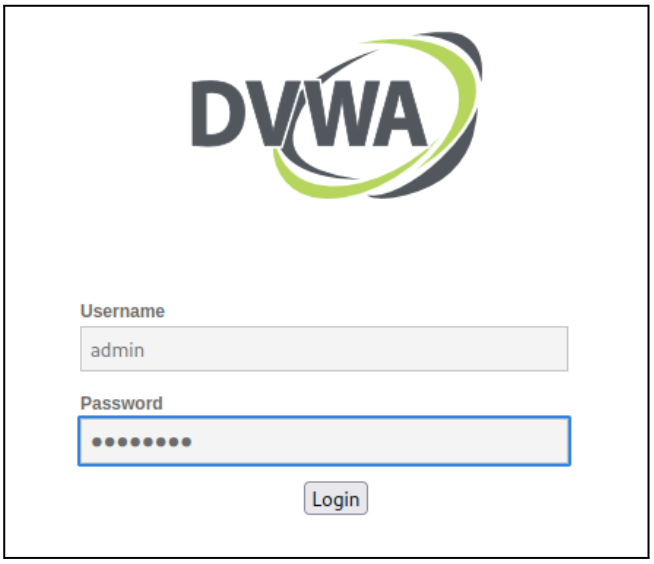
```
;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; 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
```

8) Apro la sessione nel browser digitando '127.0.0.1/DVWA/setup.php'





Ci comparirà una pagina simile alla figura a sinistra.
Clicchiamo quindi su “Create / Reset Database” nella parte in basso della pagina



9) Verremo reindirizzati ad una pagina di login dove inseriremo le seguenti credenziali:

Username: admin
Password: password

10) Apro Burpsuite e scelgo un progetto temporaneo, andando ad inserire l’indirizzo della nostra DVWA: 127.0.0.1/DVWA