

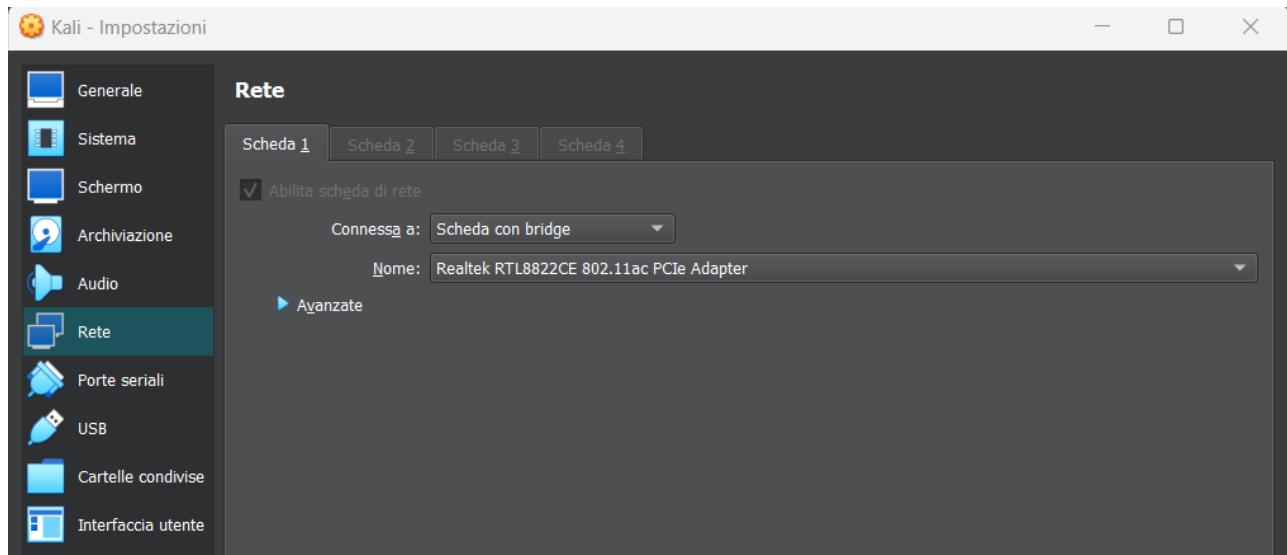
APPLICAZIONI WEB

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/network/interfaces'`

```
GNU nano 7.2
/etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.254

#address 192.168.32.100/24
#gateway 192.168.32.1
#iface eth0 inet dhcp
```

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

```
(jessica㉿kali)-[~]
$ sudo su
```

Ed eseguire i comandi:

```
[root@kali]~[~/home/jessica]
# cd /var/www/html

[root@kali]~[~/var/www/html]
# sudo git clone https://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
      Home

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 '*D64F6611CF18EA567
ED1E8E74F2243AC1EDF54C4' |
| 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’



Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.2.2
 PHP function display_errors: **Disabled**
 PHP function display_startup_errors: **Disabled**
 PHP function allow_url_include: Enabled
 PHP function allow_url_fopen: Enabled
 PHP module gd: **Missing - Only an issue if you want to play with captchas**
 PHP module mysqli: Installed
 PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
 Database username: kali
 Database password: *****
 Database database: dvwa
 Database host: 127.0.0.1
 Database port: 3306

reCAPTCHA key: **Missing**

Writable folder /var/www/html/DVWA/hackable/uploads/: **No**
 Writable folder /var/www/html/DVWA/config: **No**

Status in red, indicate there will be an issue when trying to complete some modules.

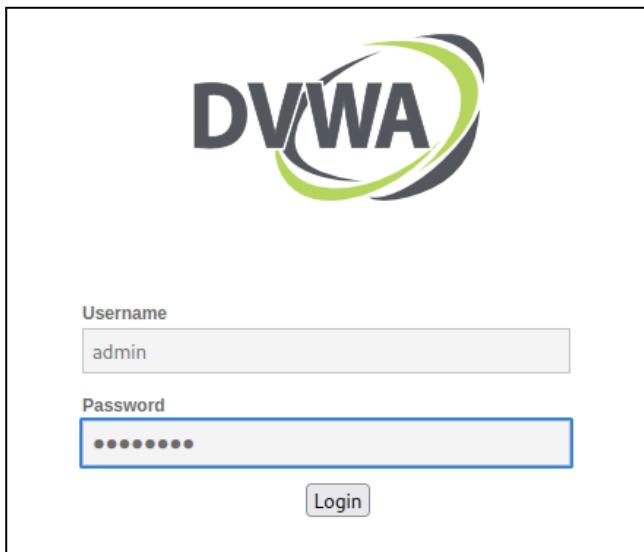
If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

[Create / Reset Database](#)

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

```

1 GET /DVWA/setup.php HTTP/1.1
2 Host: 127.0.0.1
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
8 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
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate

```