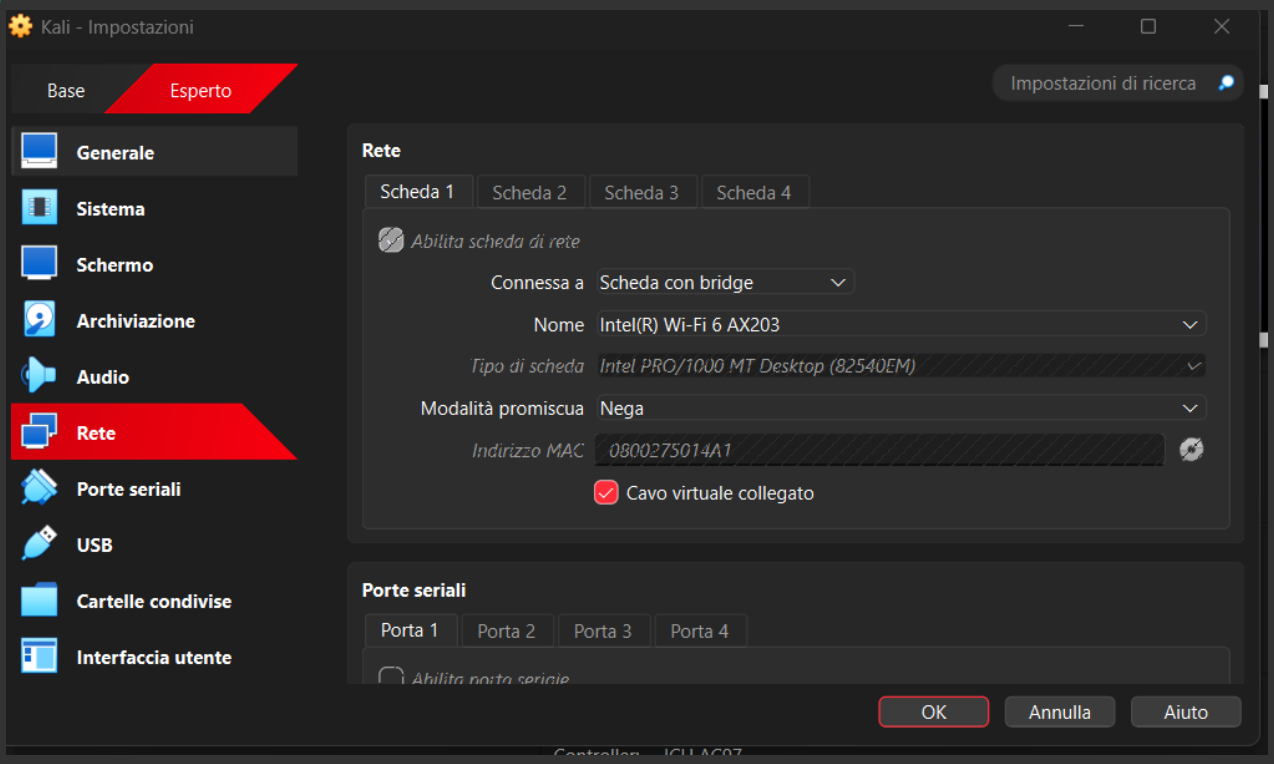
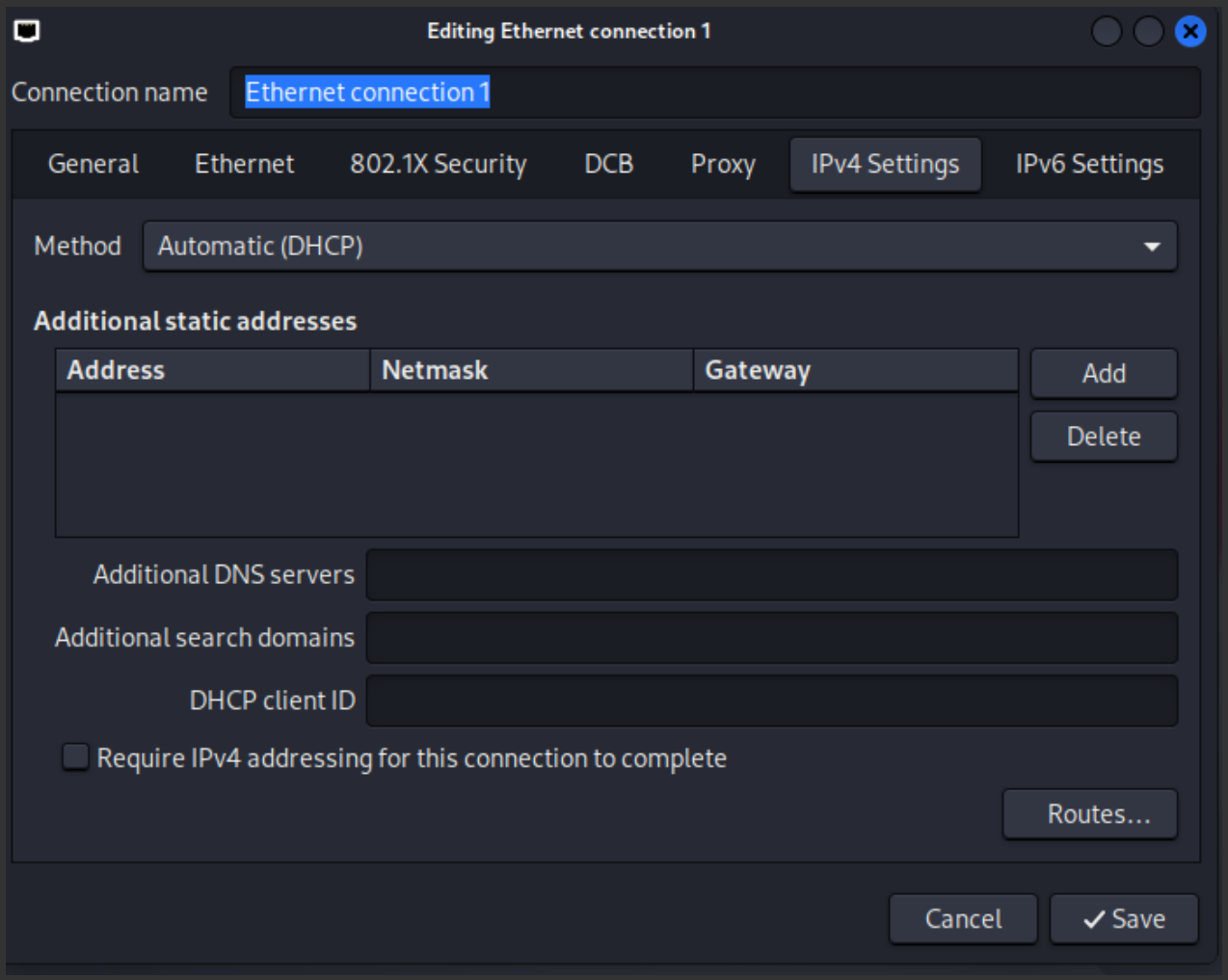
Installazione DVWA

Per prima cosa sono andato ad impostare la macchina con connessione a Scheda con bridge, in modo da poter comunicare con la rete esterna





Poi si andrà a scaricare ed installare la DVWA

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 5611, done.
remote: Counting objects: 100% (76/76), done.
remote: Compressing objects: 100% (39/39), done.
remote: Total 5611 (delta 59), reused 37 (delta 37), pack-reused 5535 (from 3)
Receiving objects: 100% (5611/5611), 2.65 MiB | 24.00 KiB/s, done.
Resolving deltas: 100% (2784/2784), 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
```

```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are corr>
# 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
$DBMS = getenv('DBMS') ?: 'MySQL';
#$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' ]   = '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' ]  = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('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 imposs>

^G Help      ^O Write Out  ^F Where Is   ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify   ^/ Go To Line M-E Redo
```

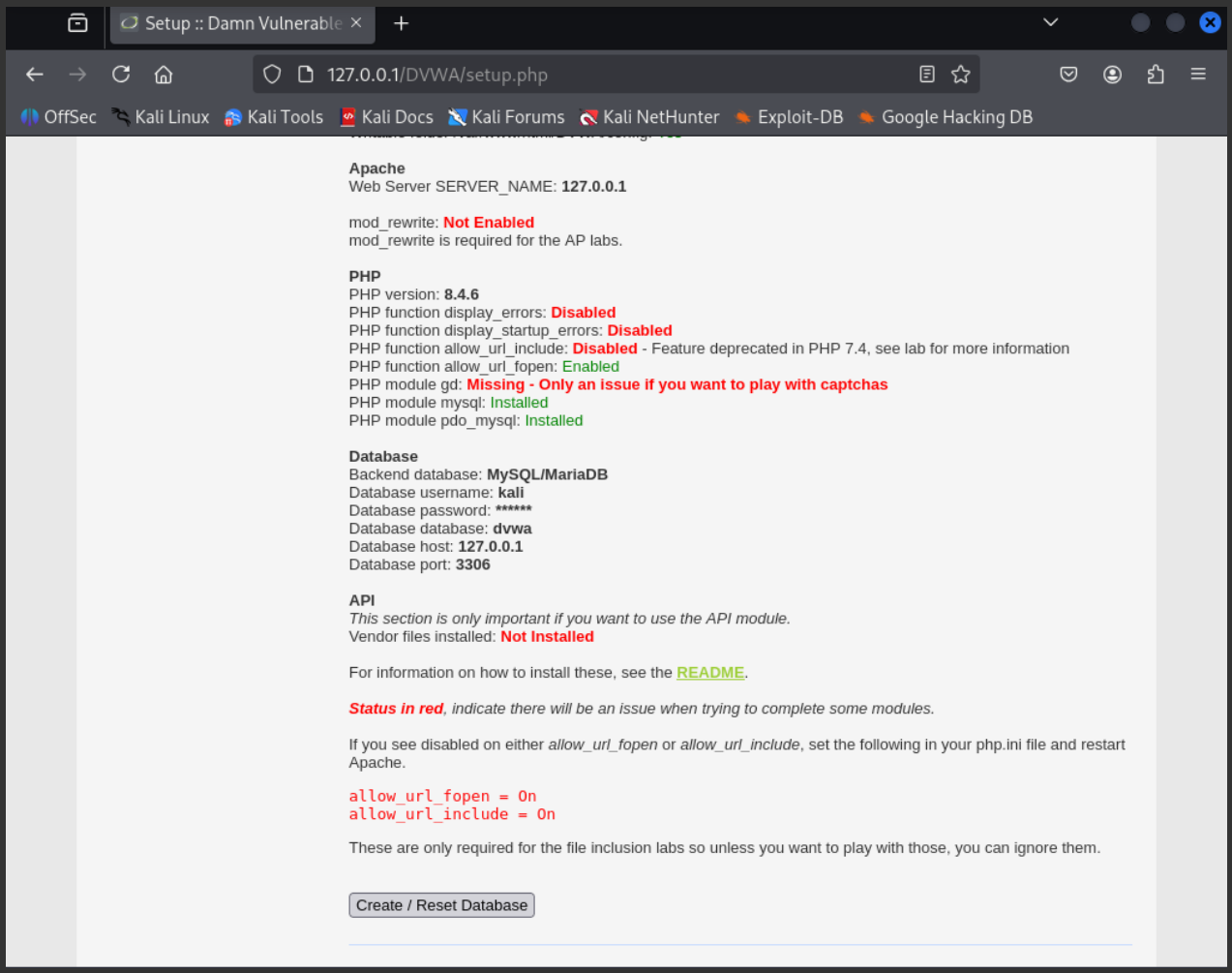
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# service mysql start

┌──(root㉿kali)-[/home/kali]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.1-MariaDB-4 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

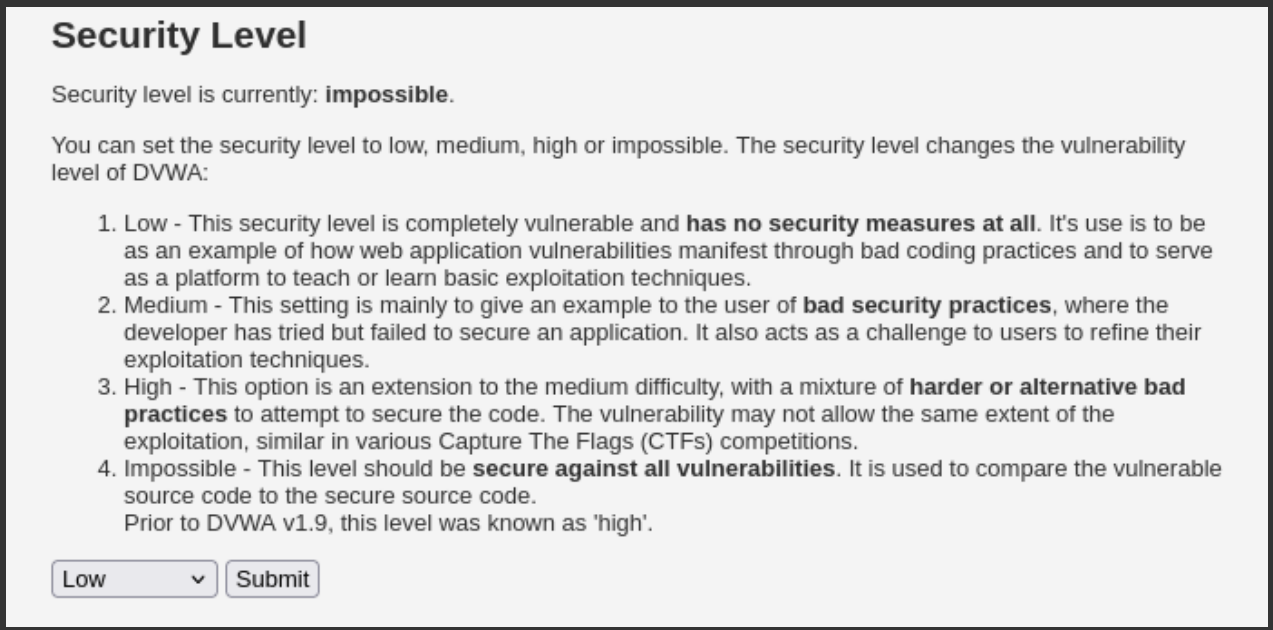
```
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali'
    -> ;
Query OK, 0 rows affected (0.054 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.044 sec)

MariaDB [(none)]> exit
Bye

┌──(root㉿kali)-[/home/kali]
└─#
```

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

┌──(root㉿kali)-[/home/kali]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

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

┌──(root㉿kali)-[/etc/php]
└─# ls
8.4

┌──(root㉿kali)-[/etc/php]
└─# cd 8.4

┌──(root㉿kali)-[/etc/php/8.4]
└─# cd apache2

┌──(root㉿kali)-[/etc/php/8.4/apache2]
└─# ls
conf.d  php.ini

┌──(root㉿kali)-[/etc/php/8.4/apache2]
└─# sudo nano php.ini
```

```
; 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
```

A questo punto cerchiamo nella barra degli indirizzi sul Browser 127.0.0.1/DVWA/setup.php e andiamo a creare u database, impostando poi la difficoltà su “low”





A questo punto apriamo Burpsuite, apriamo un browser e facciamo l'accesso sulla DVWA. In questo caso si possono intercettare le richieste, e modificarne i pacchetti con la richiesta di accesso.