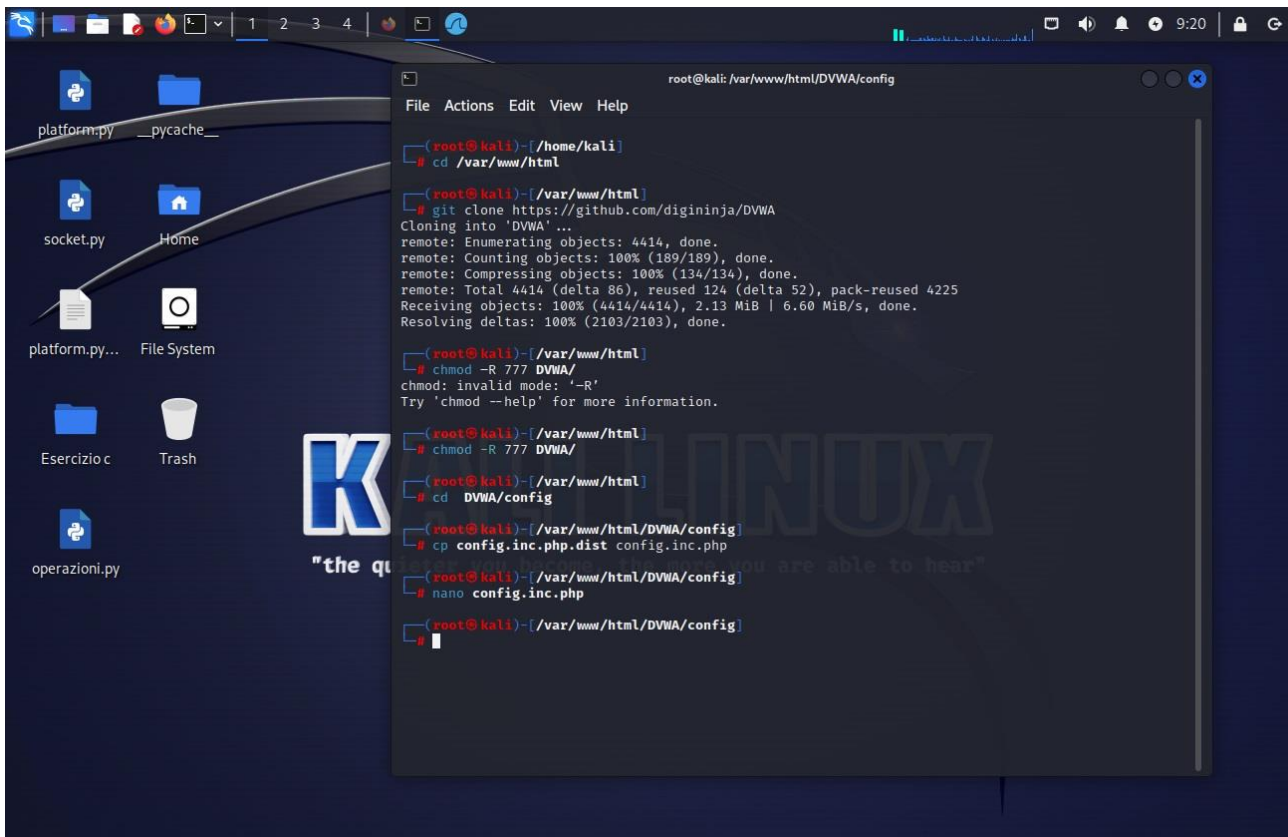


Esercizio 11/10/2023

1 – Installazione Database MySQL e Web Server Apache secondo le indicazioni



```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help

(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: 4414, done.
remote: Counting objects: 100% (189/189), done.
remote: Compressing objects: 100% (134/134), done.
remote: Total 4414 (delta 86), reused 124 (delta 52), pack-reused 4225
Receiving objects: 100% (4414/4414), 2.13 MiB | 6.60 MiB/s, done.
Resolving deltas: 100% (2103/2103), done.

(root@kali)~/var/www/html
# chmod -R 777 DVWA/
chmod: invalid mode: '-R'
Try 'chmod --help' for more information.

(root@kali)~/var/www/html
# chmod -R 777 DVWA/

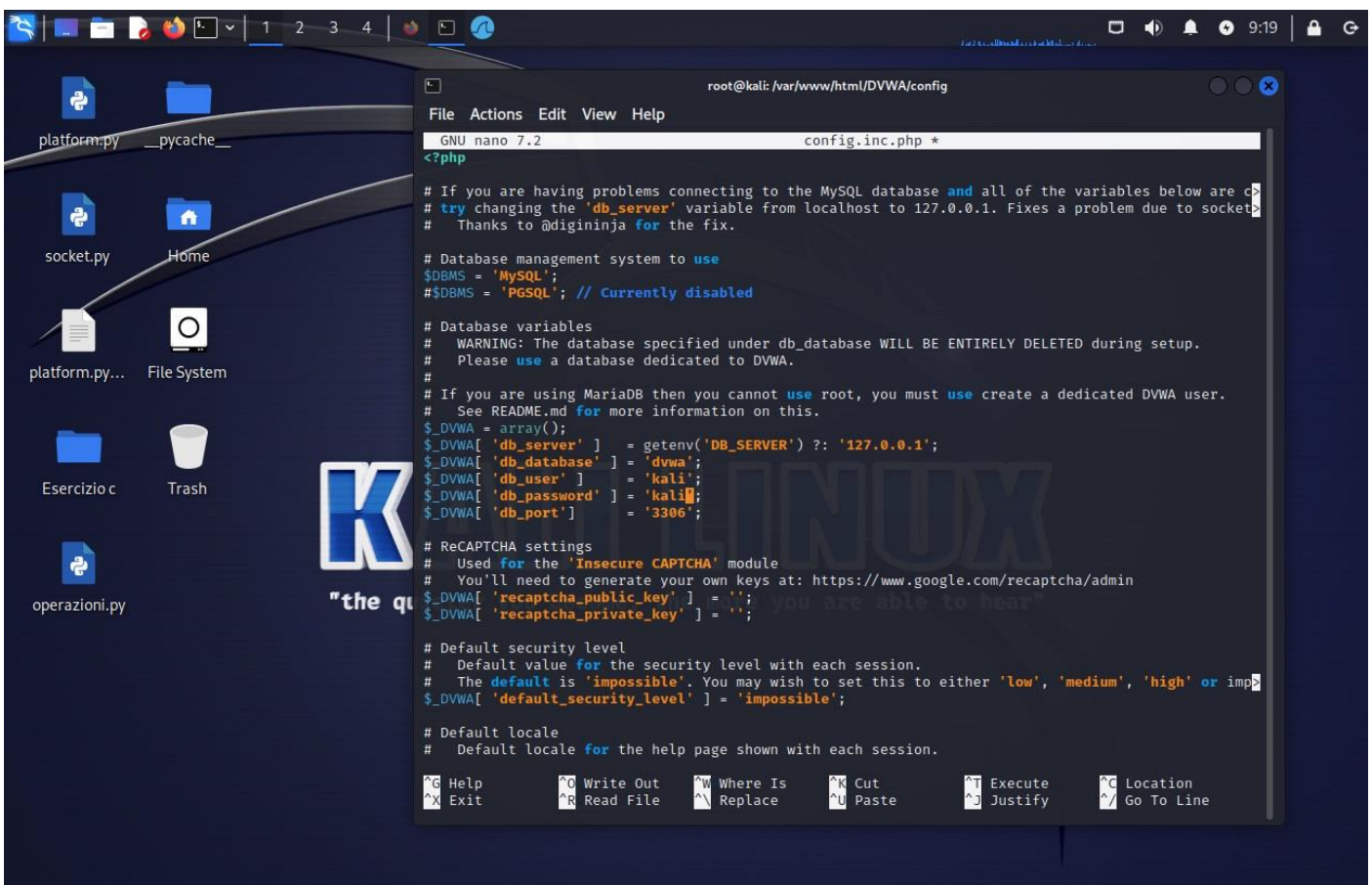
(root@kali)~/var/www/html
# cd DVWA/config

(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

(root@kali)~/var/www/html/DVWA/config
#
```

2 – Cambiati user e password all'interno del file



```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help

GNU nano 7.2 config.inc.php *
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are c
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to socke
# 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';

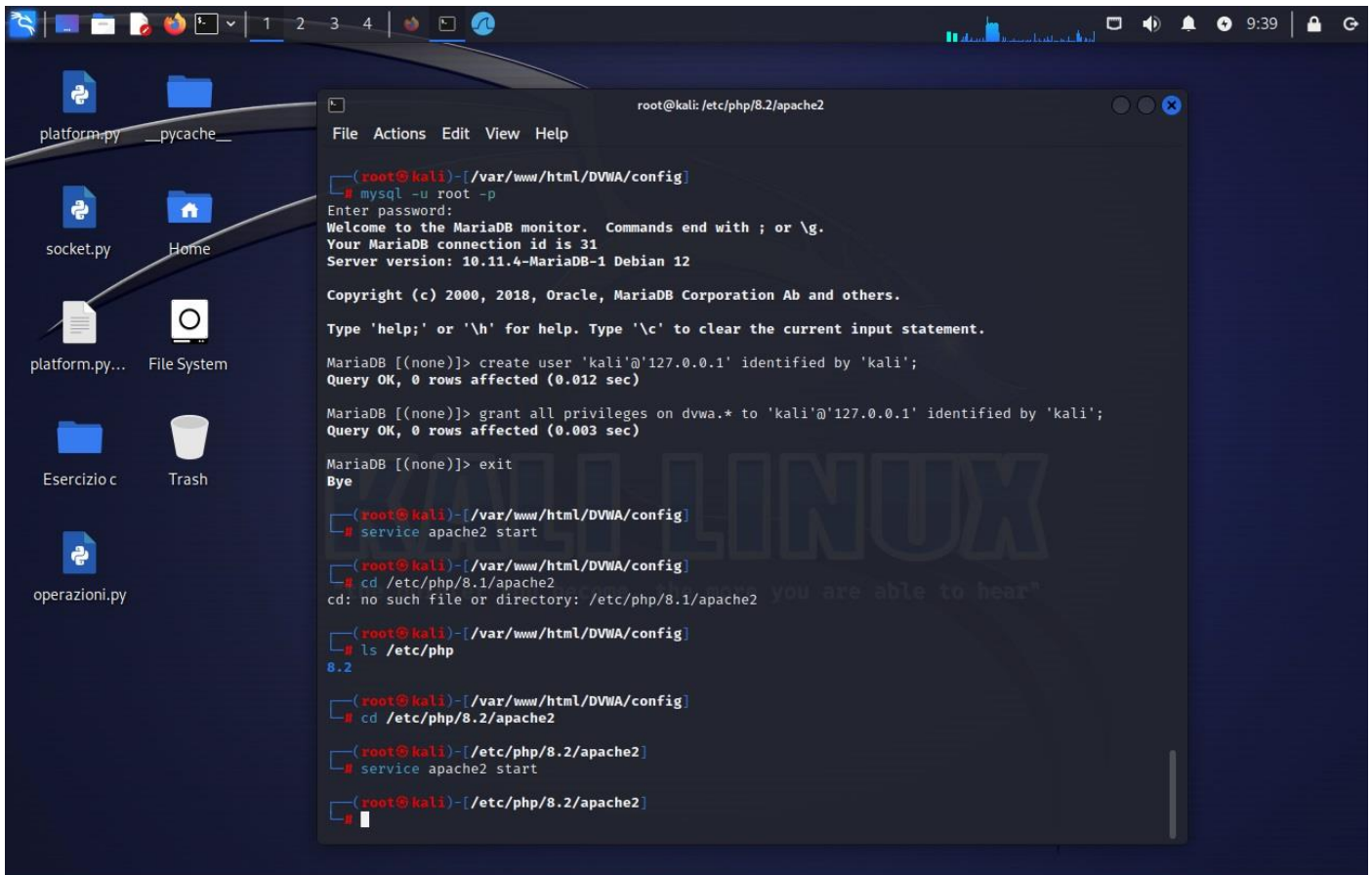
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = '';
$_DVWA['recaptcha_private_key'] = '';

# 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 imp
$_DVWA['default_security_level'] = 'impossible';

# Default locale
# Default locale for the help page shown with each session.

^G Help      ^O Write Out  ^W Where Is   ^R Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_ Go To Line
```

3 – Fatto partire il servizio mysql, connessa con l'utenza di root, assegnato i privilegi, fatto partire Apache e spostata nella cartella (ho controllato la versione di php con il comando ls e sostituito nella stringa 8.2 a 8.1)



A terminal window on a Kali Linux desktop. The window title is 'root@kali: /etc/php/8.2/apache2'. The terminal shows the following commands and output:

```
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 (0.012 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> exit
Bye

root@kali)~[/var/www/html/DVWA/config]
# service apache2 start

root@kali)~[/var/www/html/DVWA/config]
# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

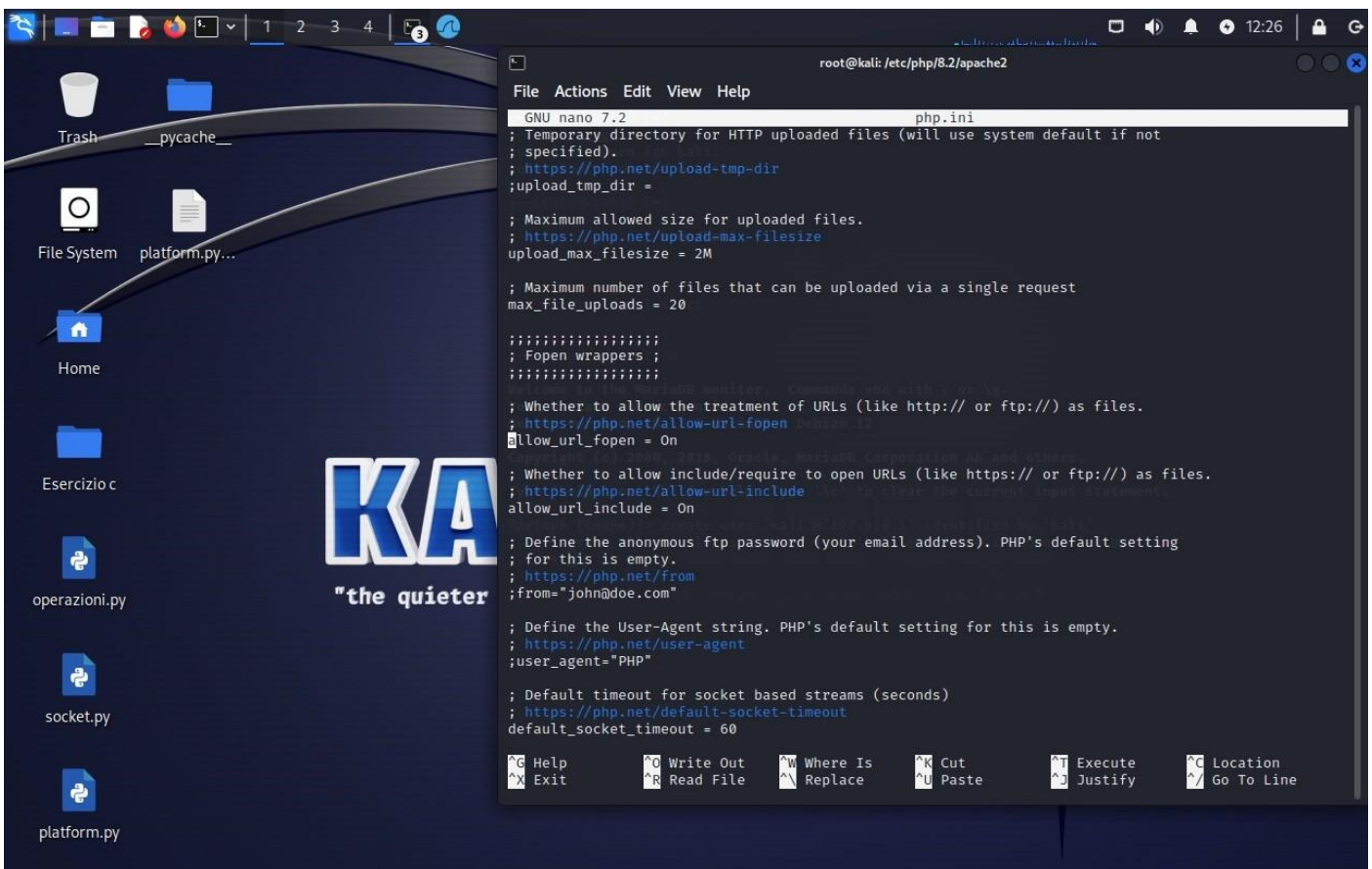
root@kali)~[/var/www/html/DVWA/config]
# ls /etc/php
8.2

root@kali)~[/var/www/html/DVWA/config]
# cd /etc/php/8.2/apache2

root@kali)~[/etc/php/8.2/apache2]
# service apache2 start

root@kali)~[/etc/php/8.2/apache2]
#
```

4 – Settata la voce allow_url_include su On



A terminal window on a Kali Linux desktop. The window title is 'root@kali: /etc/php/8.2/apache2'. The terminal shows the GNU nano 7.2 editor editing the file 'php.ini'. The configuration is as follows:

```
GNU nano 7.2 php.ini
; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;;;;;;;;
; 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

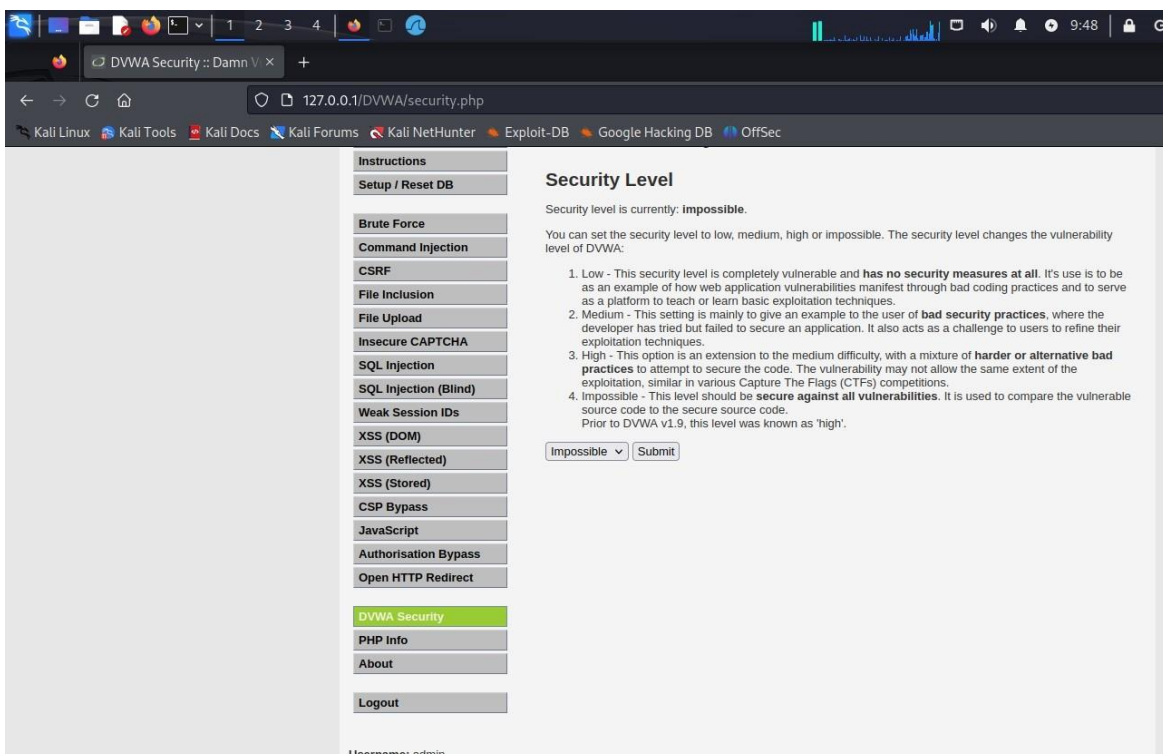
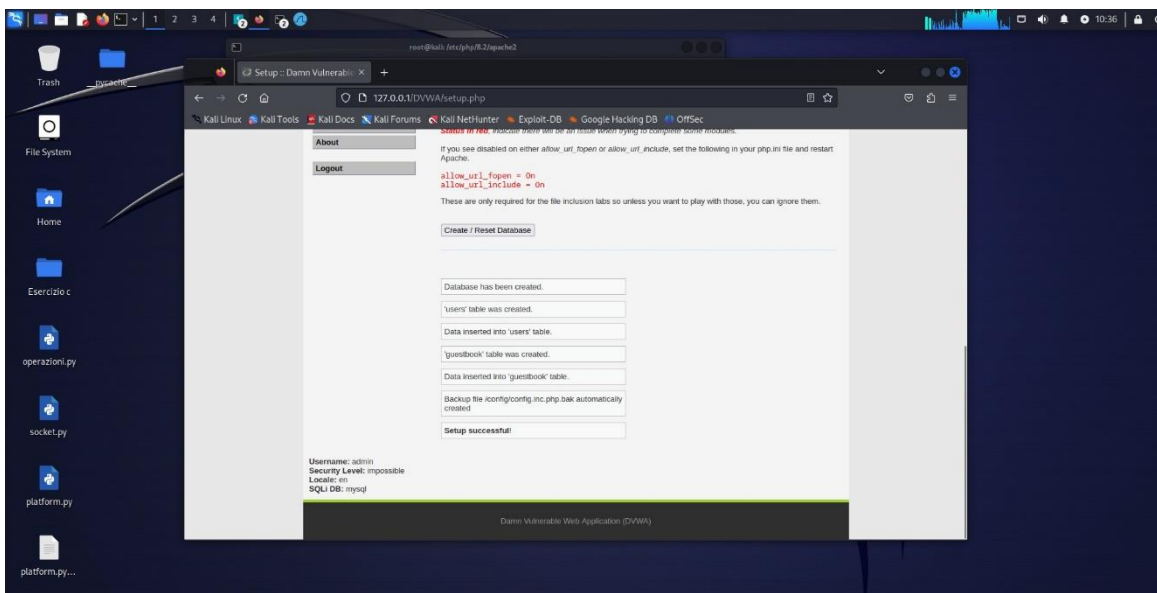
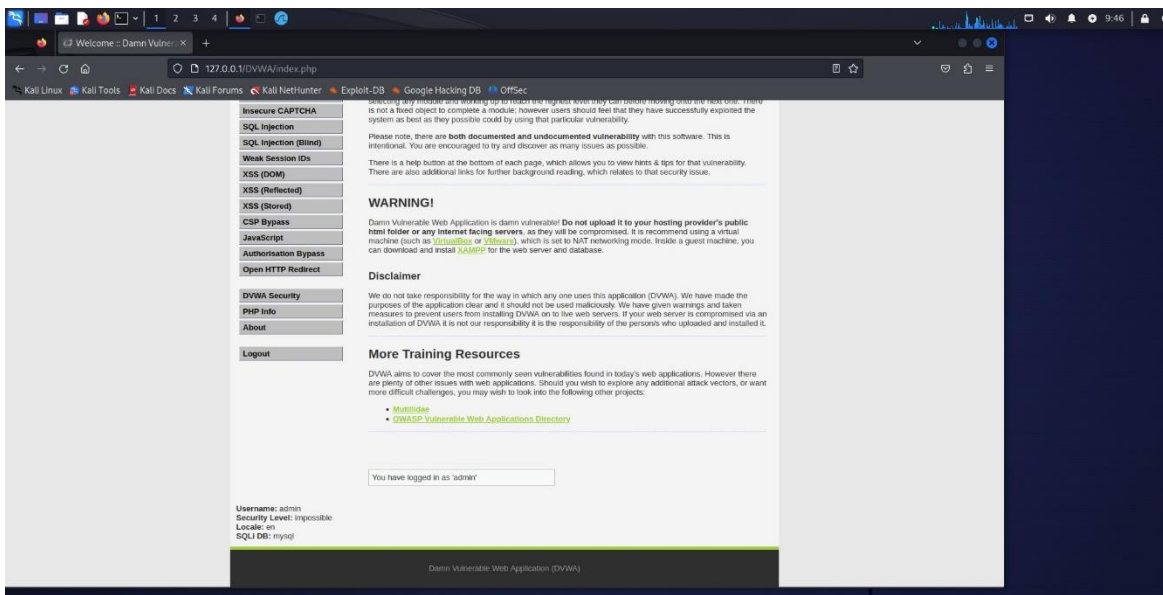
; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"

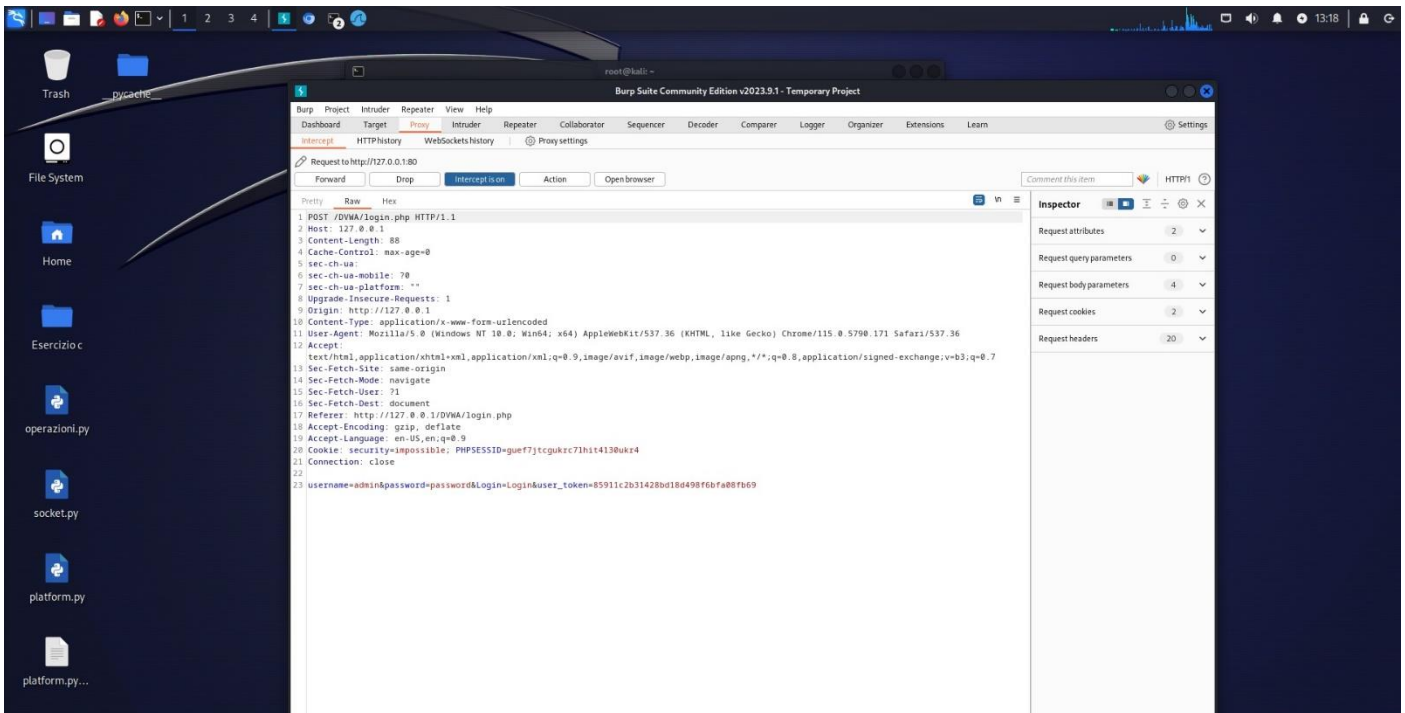
; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify
^_ Go To Line
```

5 – Aperto il browser e cliccato su «Create / Reset Database» e impostato livello di sicurezza su Low



6 – Dopo vari tentativi sono finalmente entrata nella pagina corretta (prima non riuscivo a visualizzare l'ultima riga con user e password nonostante avessi fatto correttamente tutti i passaggi)



7 – Modificati user e password ho riprovato con il login che riporta a questo punto la dicitura “CFRS token is incorrect” ed effettuato la controprova con dicitura “Login failed”

