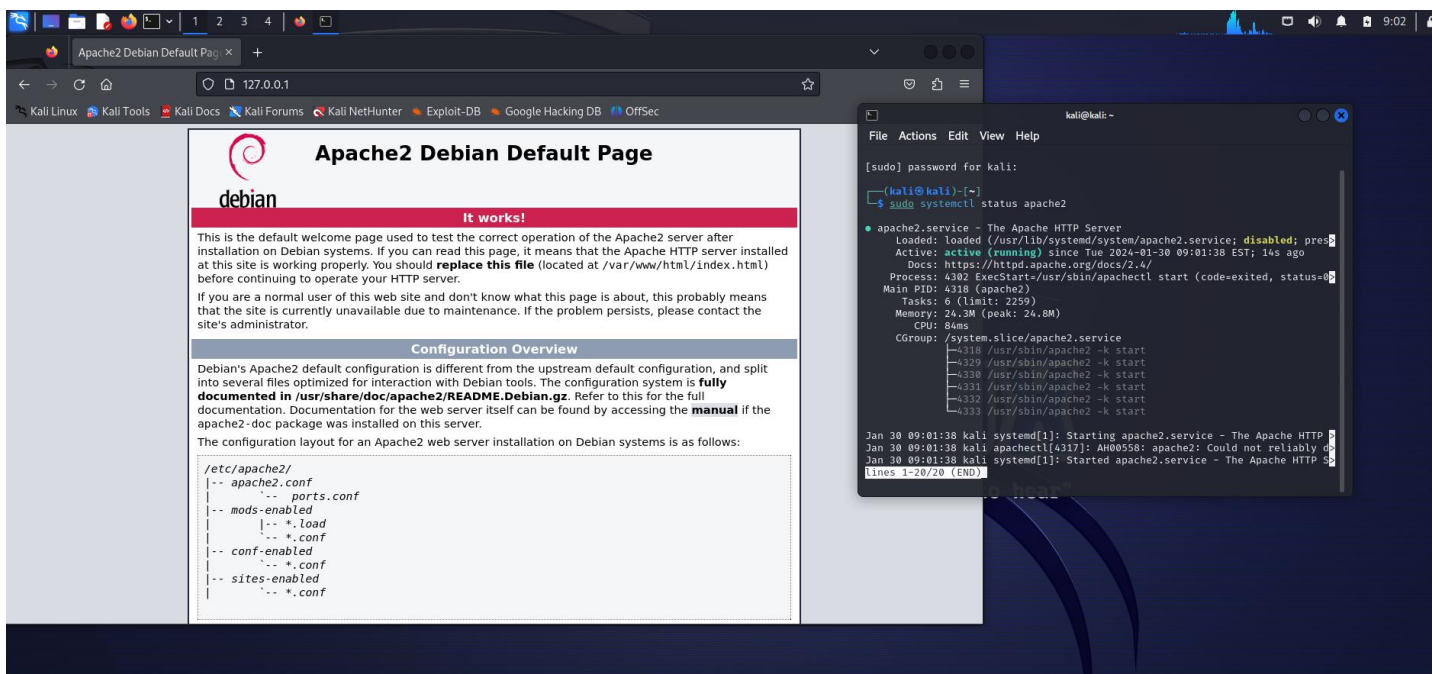


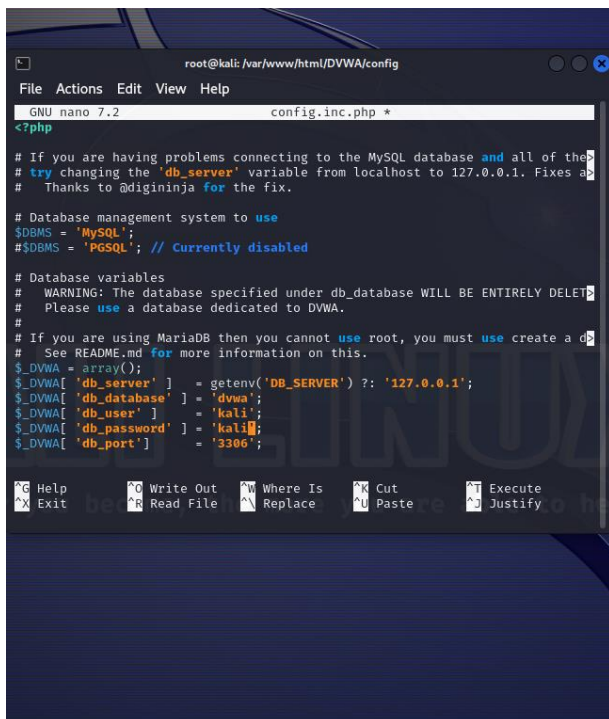
ESERCIZIO W8D1 pratica 1

Introduzione:

L'obiettivo di questo esercizio era praticare il testing delle vulnerabilità delle web application utilizzando Damn Vulnerable Web Application (DVWA) e il tool Burp Suite su Kali Linux. Durante l'esercizio, sono state eseguite diverse attività, tra cui l'installazione e la configurazione di DVWA, l'intercettazione e la modifica delle richieste HTTP con Burp Suite, e l'esplorazione delle risposte dell'applicazione a diverse manipolazioni dei parametri.

Dopo aver installato mysql e apache, procedo con l'esercizio:





```
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
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
# Thanks to @digininja for the fix.

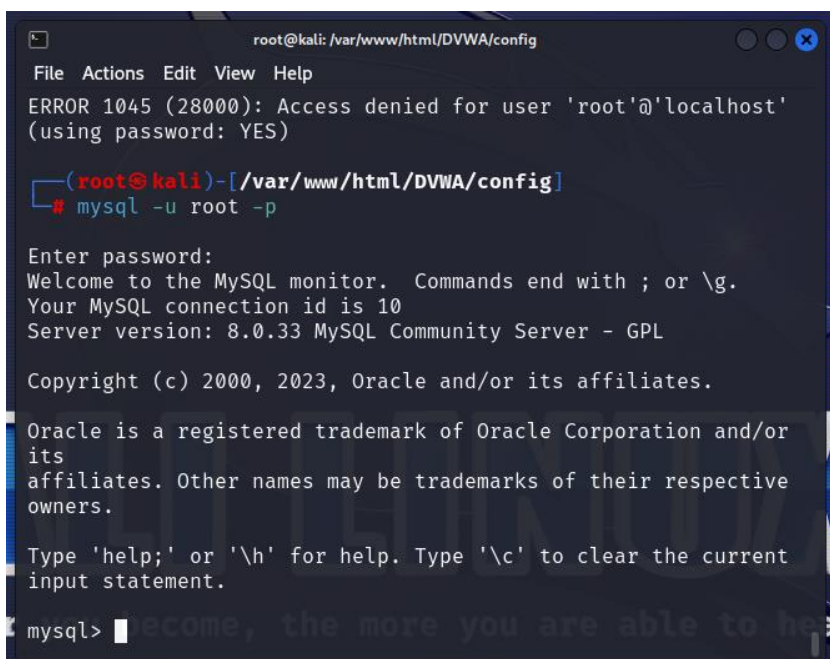
# Database management system to use
$dbms = 'MySQL';
#$dbms = 'PgSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must create a db
# 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';

^C Help      ^O Write Out  ^W Where Is   ^C Cut        ^T Execute
^X Exit      ^R Read File  ^M Replace    ^U Paste      ^J Justify
```

Da terminale su Kali, utilizzo l'utenza di root, eseguendo il comando «sudo su» e poi eseguite i comandi seguenti-cd /var/www/html-git clone https://github.com/digininja/DVWA-chmod -R 777 DVWA/-cd DVWA/config-cp config.inc.php.dist config.inc.php-nano config.inc.php.

All'interno del file config.inc.php cambio utente e password di default come da figura a lato (inserendo, user:kali, password:kali)



```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
ERROR 1045 (28000): Access denied for user 'root'@'localhost'
(using password: YES)

(root@kali)-[/var/www/html/DVWA/config]
# mysql -u root -p

Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.33 MySQL Community Server - GPL

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or
its affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current
input statement.

mysql>
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ mysql -u root -p  
  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 11  
Server version: 8.0.33 MySQL Community Server - GPL  
  
Copyright (c) 2000, 2023, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement  
.  
  
mysql> CREATE USER 'kali'@'127.0.0.1';  
ERROR 1396 (HY000): Operation CREATE USER failed for 'kali'@'127.0.0.1'  
mysql> ALTER USER 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';  
Query OK, 0 rows affected (0.01 sec)  
  
mysql> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1';  
Query OK, 0 rows affected (0.01 sec)  
  
mysql> exit
```

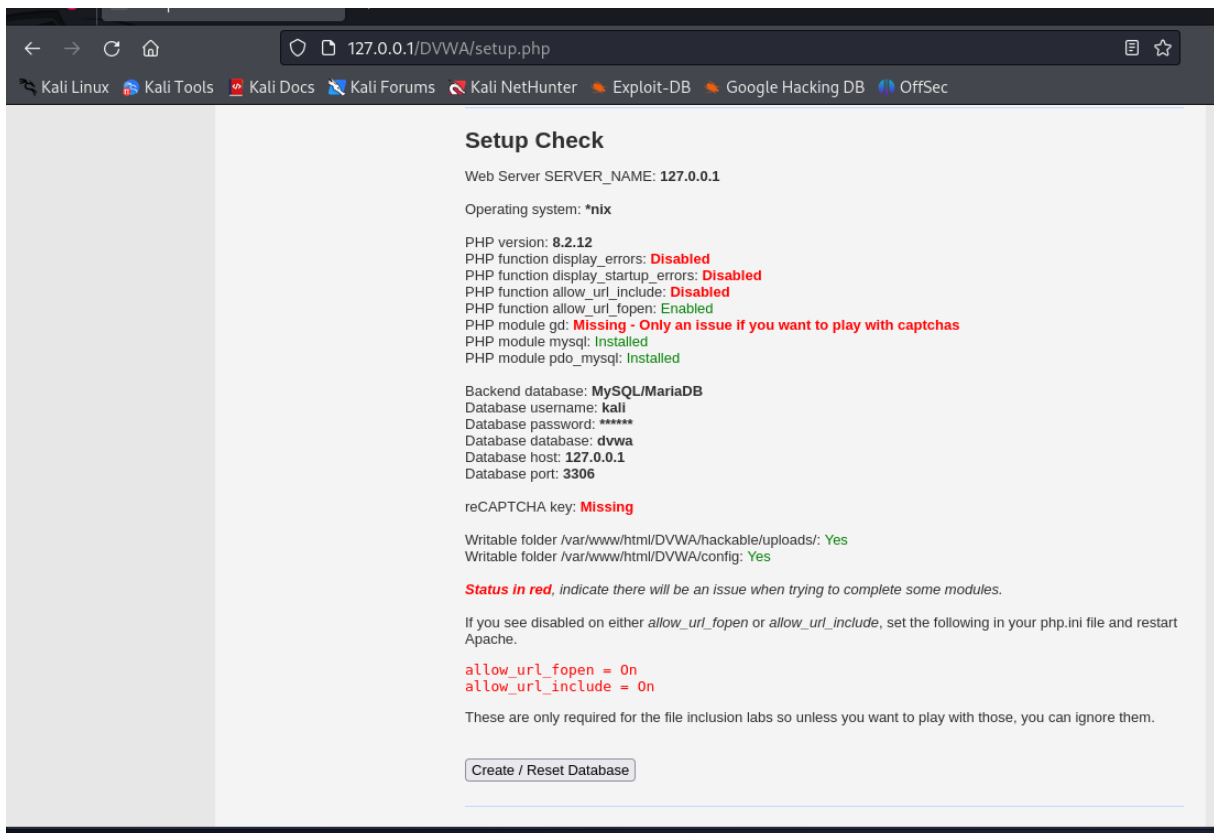
creiamo un'utenza sul db

con il seguente comando create user 'kali'@'127.0.0.1' identified by 'kali' ; successivamente assegniamo i privilegi all'utente kali con il seguente comando: grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ; ed usciamo utilizzando "exit"

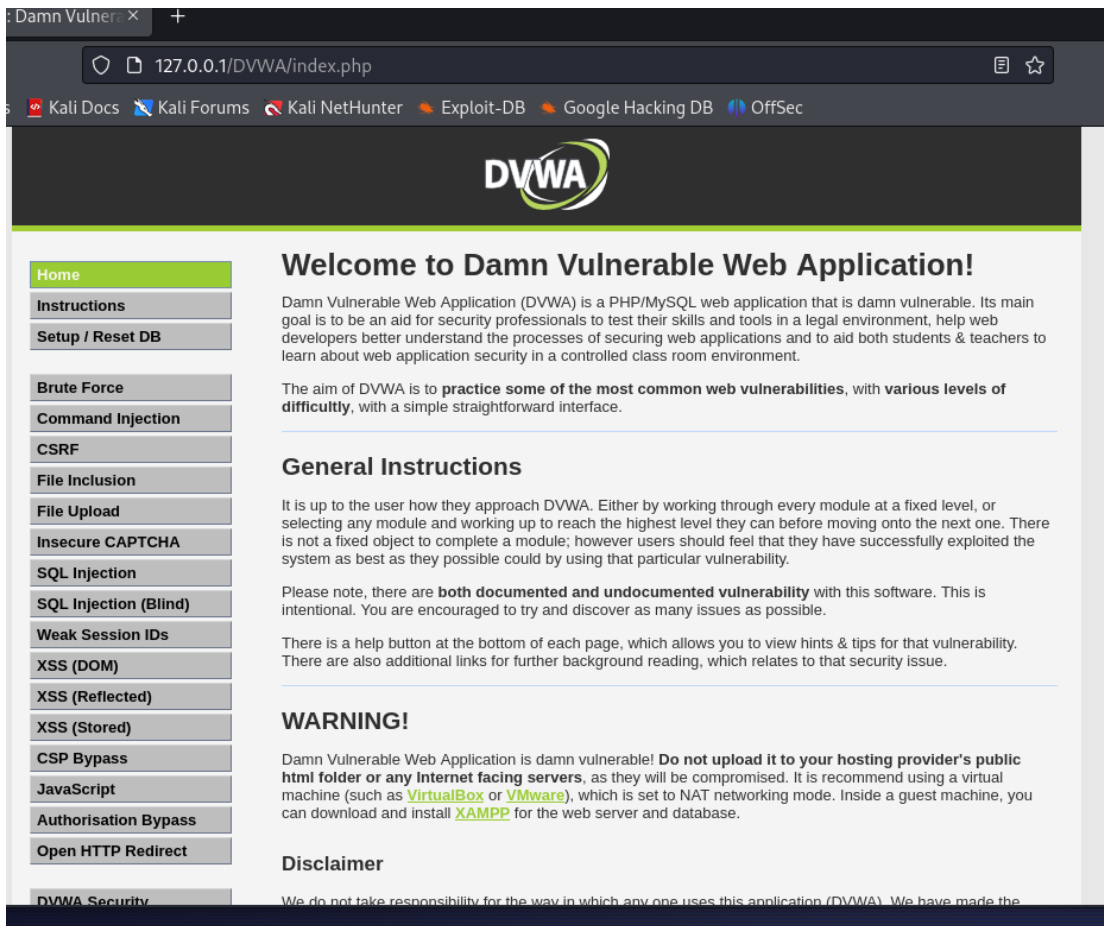
```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.  
; https://php.net/allow-url-fopen  
allow_url_fopen = On  
  
; Whether to allow include/require to open URLs (like https:// or ftp://) as files.  
; https://php.net/allow-url-include  
allow_url_include = On
```

modifico le due voci su on.

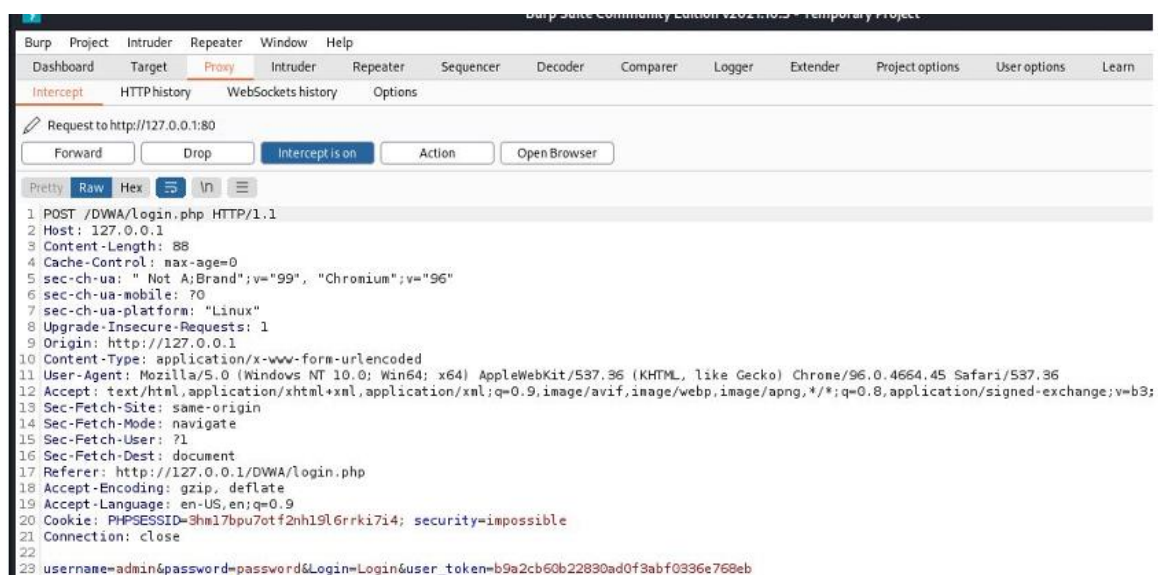
A questo punto apro una sessione del vostro browser e scrivo nella barra degli indirizzi: 127.0.0.1/DVWA/setup.php. Clicco su «Create / Reset Database» nella parte bassa della pagina



appena creato il database vengo rediretto su una pagina di login, dove posso entrare inserendo le credenziali di admin di default. Username: admin password: password. Una volta entrato nell'app, clicco sulla scheda DVWA Security. Qui posso scegliere il livello di sicurezza dell'APP.



Ora lancio burpsuite e modifico le credenziali di accesso in errate.



Invio la richiesta e come previsto non si può accedere

