GNU nano 7.2

🥞 📗 🛅 🍃 🐞 🖭 🗸 🗎 2 3 4 🕒 🕡

config.inc.php *

```
<?php
# If you are having problems connecting to the MySQL database <mark>and</mark> all of the variables below are correct
# 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
$DBMS = 'MySQL';
#$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 <mark>use</mark> root, you must <mark>use</mark> create a dedicated DVWA user.
# See README.md for more information on this.
_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
# 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 impossible'.
$_DVWA[ 'default_security_level' ] = 'impossible';
# Default locale
 Default locale for the help page shown with each session.
# The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';
# Disable authentication
 Some tools don't like working with authentication and passing cookies around
# so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = false;
define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');
# SQLi DB Backend
  Use this to switch the backend database used in the SQLi and Blind SQLi labs.
```

In questo esercizio andremo a installare una DVWA (Damn Vulnerable Web Application) su Kali Linux, creare un db (database) con MySQL e setuppare un web server con Apache.

Il tutto ci permetterà di fare pratica con delle varie vulnerabilità, utilizzando un ambiente protetto completamente su Kali Linux.

Per prima cosa, ho abilitato la connessione da rete interna a connessione con bridge, per ottenere l'accesso ad internet (ho abilitato il DHCP successivamente).

In questa schermata ho sostituito "user" e "password" del db.

^X Exit

^R Read File

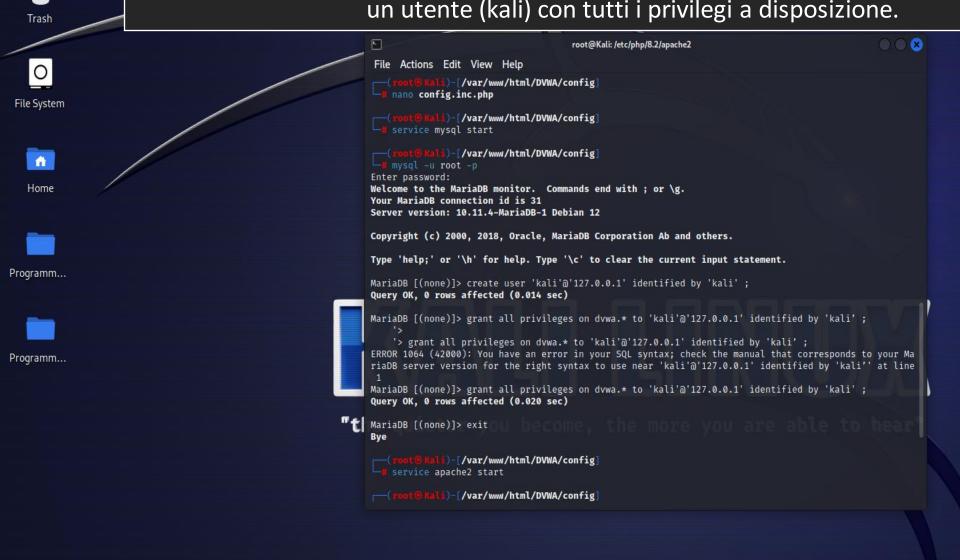
This does not affect the backend for any other services, just these two labs.

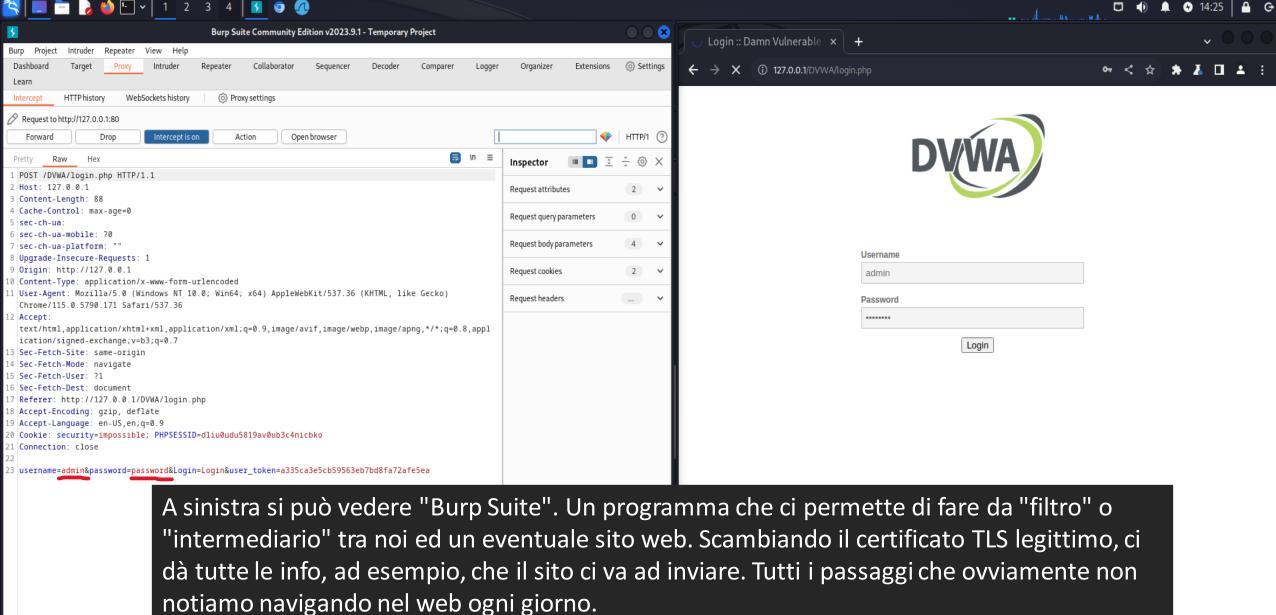
`T Execute

[^]J Justify

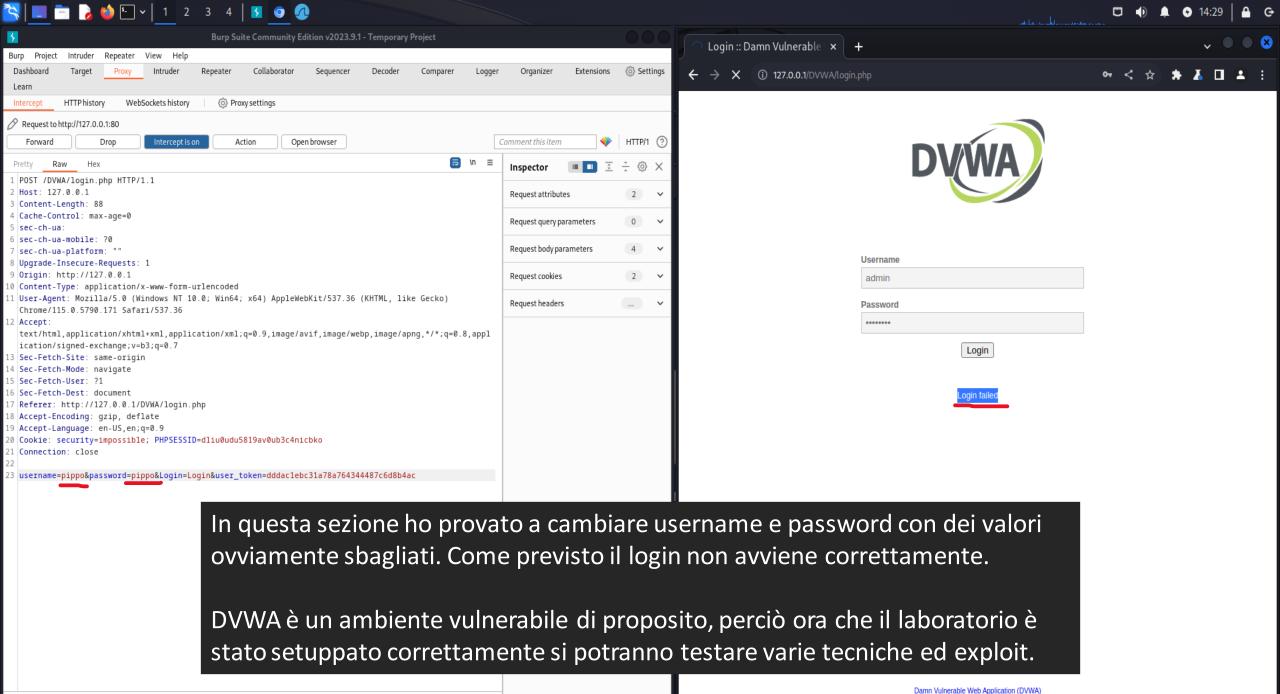
[^]F Forward







(potremmo dire che ci fa dissezionare accuratamente ogni passaggio che ci porta alla connessione e alla visualizzazione di un sito web.)



0 highlights

(?) (§) (← | → | Search.