

ESERCIZIO S3/L2

TRACCIA:

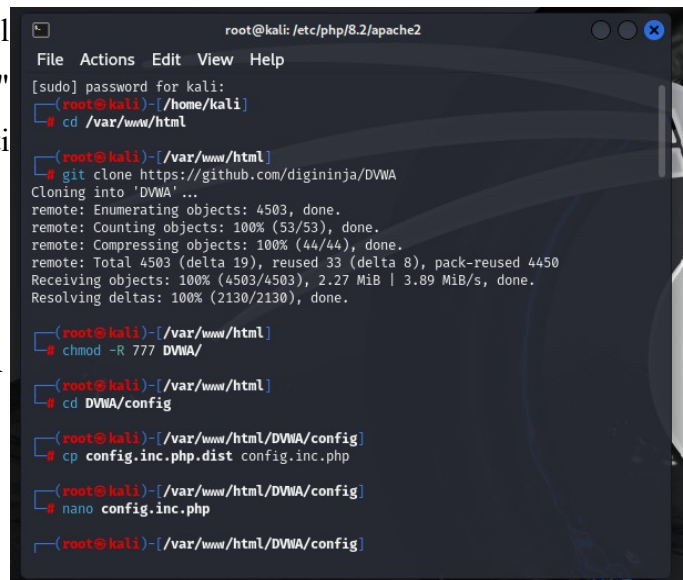
Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero "damn vulnerable web application" in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Per installare la DVWA abbiamo bisogno di 4 componenti:

- OS: Kali Linux
- Database MySQL
- Web Server Apache
- Web Server Mariadb

In questi passaggi siamo andati ad aprire il terminale di Kali e con il comando "sudo su" usiamo l'utenza di root. Si eseguono i seguenti comandi:

- `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`



```
root@kali: /etc/php/8.2/apache2
File Actions Edit View Help
[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: 4503, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (44/44), done.
remote: Total 4503 (delta 19), reused 33 (delta 8), pack-reused 4450
Receiving objects: 100% (4503/4503), 2.27 MiB | 3.89 MiB/s, done.
Resolving deltas: 100% (2130/2130), 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

root@kali: ~ - [/var/www/html/DVWA/config]
```

Con il comando `cd` siamo nella directory `html` e da qui abbiamo clonato la repository di github nella quale siamo andati a modificare i permessi. Spostatoci in seguito nella cartella `DVWA/config`, abbiamo copiato il modello del file di configurazione `config.inc.php.dist` nel nuovo file `config.inc.php` che verrà modificato come evidenziato in figura con il comando `nano config.inc.php`.



```
GNU nano 7.2
#php
# If you are having problems connecting to the MySQL database and 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 = 'PQSQL'; // 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' : 'localhost';
$DVWA['db_database'] = 'dvwa';
$DVWA['db_user'] = 'dvwa';
$DVWA['db_password'] = 'password';
$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 'impossible'.
$DVWA['default_security_level'] = 'impossible';

# Default locale
# 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.
# This does not affect the backend for any other services, just these two labs.
# If you do not understand what this means, do not change it.
$DVWA['SQLI_DB'] = MYSQL;
$DVWA['SQLI_DB'] = SQLITE;
$DVWA['SQLITE_DB'] = 'sqlite.db';

?>
```

Sempre con l'utenza root su Kali abbiamo fatto partire il servizio mysql con il comando:

```
service mysql start
```

in seguito ci siamo connessi al db con il seguente comando:

```
mysql -u root -p
```

```
(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 31
Server version: 10.11.6-MariaDB-2 Debian n/a

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)]> █
```

Andiamo a creare una nuova utenza sul db con il seguente comando:

```
create user 'kali'@'127.0.0.1' identified by 'kali' ;
```

assegnando successivamente i privilegi con il comando:

```
grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
```

```
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit
Bye
```

Dopo di ciò, facciamo partire Apache2 e spostatoci nella cartella .../8.2/apache2, abbiamo utilizzato un editor di testo per modificare il file php.ini come di seguito.

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

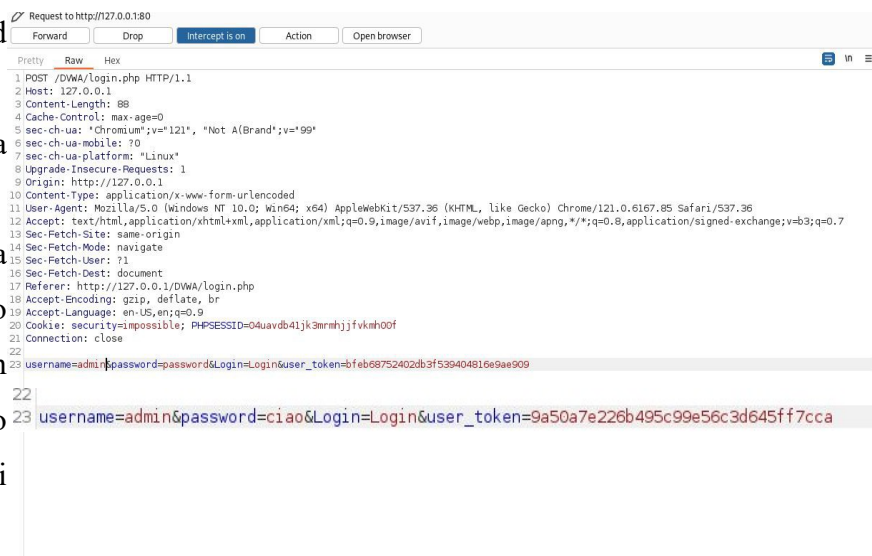
; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On█
```

Andando su un Browser abbiamo effettuato il log-in nella pagina di DVWA tramite l'indirizzo 127.0.0.1/DVWA/setup.php.

Ora che l'ambiente è creato, andiamo ad effettuare delle prove con Burpsuite.

Come primo passaggio andiamo nella sezione proxy e attiviamo intercept is on.

Apriamo il Browser del programma inseriamo l'indirizzo IP di DVWA, ovvero 127.0.0.1/DVWA ed effettuiamo il login con username e password che verranno intercettate da Burpsuite, permettendoci di visualizzarle e modificarle.

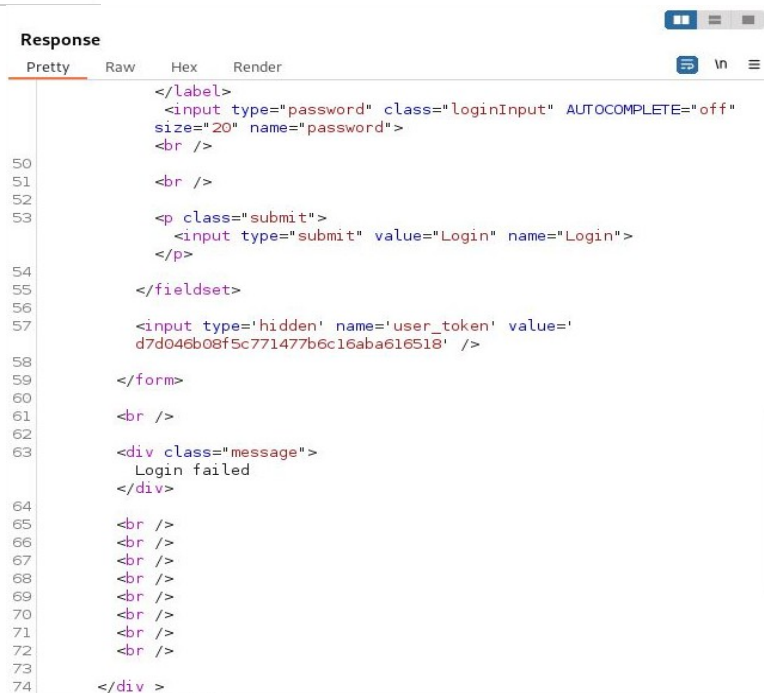


Username

Password

Login failed

Una volta apportati i cambiamenti, effettuando il login noteremo che la password sarà sbagliata e che quindi ci darà "login failed" nella sezione Response del repeater.



Team 2:

Alberto Guimp

Gabriele Arcelli

Michael Andreoli

Donato Tralli

Zhongshi Liu

Valerio Zampone