

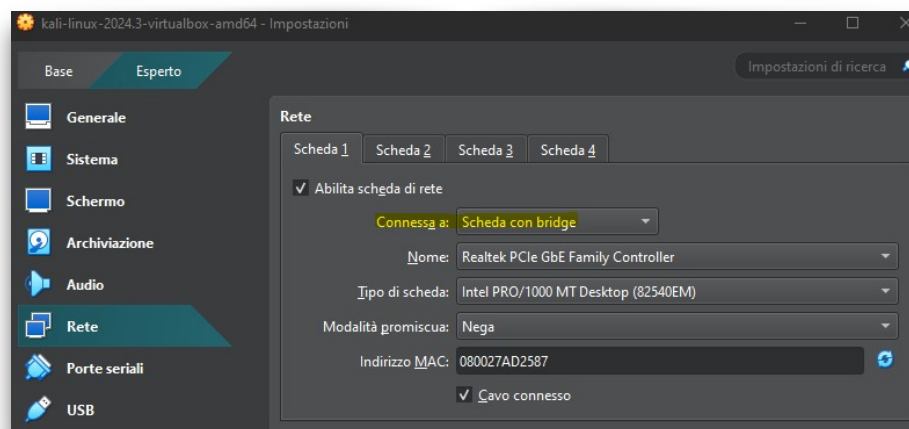
mercoledì 11 dicembre 2024

S3/L3

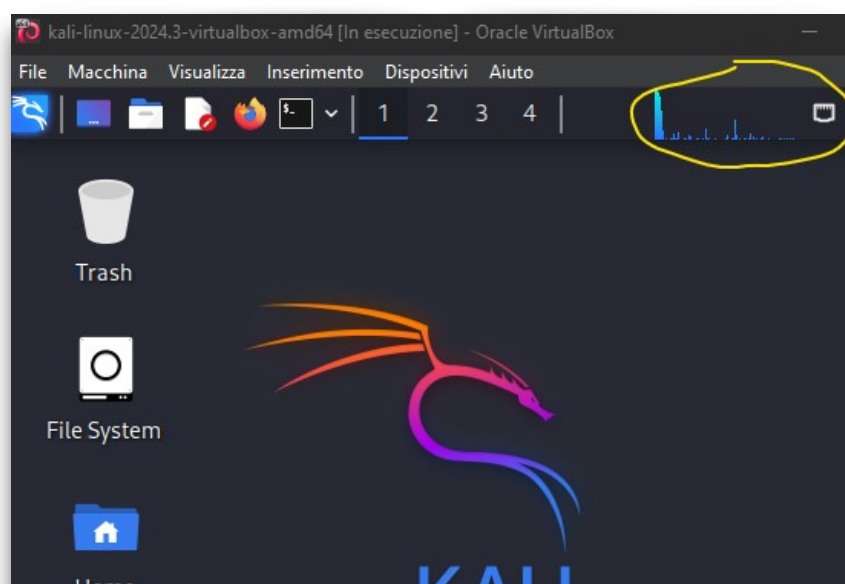
L'esercizio di oggi vedremo la configurazione di una DVWA, ovvero damn vulnerable web application in Kali Linux.

1. PRE-REQUISITI

- Prima di tutto devo modificare la connettività ad internet dalle impostazioni macchina selezionando scheda con bridge:



- A questo punto avvio la macchina per assicurarmi che la connettività sia attiva:



- Come si nota la connessione è attiva

2. INSTALLAZIONE - Database MySQL

- Apro il terminale ed eseguo “**sudo su**” per utilizzare l’utenza di root:

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
#
```

- Poi eseguo in ordine i seguenti comandi:

- **cd /var/www/html.**

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# cd /var/www/html
```

- **git clone <https://github.com/digininja/DVWA>.**

```
File Actions Edit View Help
(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: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.45 MiB | 1.41 MiB/s, done.
Resolving deltas: 100% (2405/2405), done.
```

- **chmod -R 777 DVWA/.**

```
File Actions Edit View Help
(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: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.45 MiB | 1.41 MiB/s, done.
Resolving deltas: 100% (2405/2405), done.

(root@kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
```

- **cd DVWA/config.**

```
File Actions Edit View Help
(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: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.45 MiB | 1.41 MiB/s, done.
Resolving deltas: 100% (2405/2405), done.

(root@kali)-[/var/www/html]
└─# chmod -R 777 DVWA/

(root@kali)-[/var/www/html]
└─# cd DVWA/config
```

- **cp config.inc.php.dist config.inc.php**

```
File Actions Edit View Help
(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: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.45 MiB | 1.41 MiB/s, done.
Resolving deltas: 100% (2405/2405), 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
```

- **nano config.inc.php**

```
File Actions Edit View Help
GNU nano 8.2 config.inc.php
$?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 = 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['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_database'] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA['db_user'] = getenv('DB_USER') ?: 'dvwa';
$_DVWA['db_password'] = getenv('DB_PASSWORD') ?: 'password';
$_DVWA['db_port'] = getenv('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 impossible'.
$_DVWA['default_security_level'] = getenv('DEFAULT_SECURITY_LEVEL') ?: 'impossible';

# Default locale
```

- All'interno di questo file vado a modificare utente e password, inserendo kali-kali:

```
$_DVWA = array();
$_DVWA[ 'db_server' ] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ] = getenv('DB_USER') ?: 'kali';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'kali';
$_DVWA[ 'db_port' ] = getenv('DB_PORT') ?: '3306';
```

- Salvo le modifiche del file con [Ctrl + o] + Enter.
- Ora faccio partire il servizio mysql con il comando, “**service mysql start**”; poi mi connetto al db con il 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: 11.4.2-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)]>
```

- Creo un'utenza sul db con il comando “**create user 'Kali'@'127.0.0.1' identified by 'kali' ;**”; poi assegnamo i privilegi all'utente Kali con il comando “**grant all privilegio on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;**”:

```
(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: 11.4.2-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)]> 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
```

3. INSTALLAZIONE - Web Server Apache

- Faccio partire il servizio con il comando “**service apache2 start**”, poi mi sposto nella cartella “**/etc/php/8.2/apache2**”:

```
(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php

(root@kali)-[/etc/php]
# ls
8.2

(root@kali)-[/etc/php]
# cd -
/var/www/html/DVWA/config

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

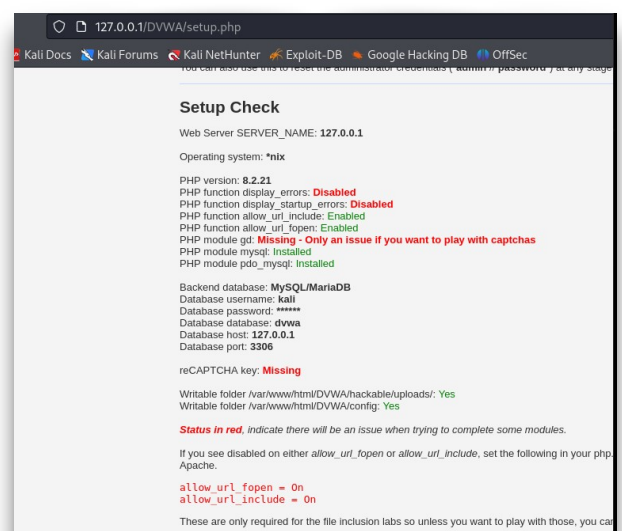
(root@kali)-[/etc/php/8.2/apache2]
# ls
conf.d  php.ini
```

- Con l’editor di testo modifico il file **php.ini** alle voci **allow_url_fopen** e **allow_url_include** mettendo “**On**”, poi eseguo di nuovo il comando “**service apache2 start**”:

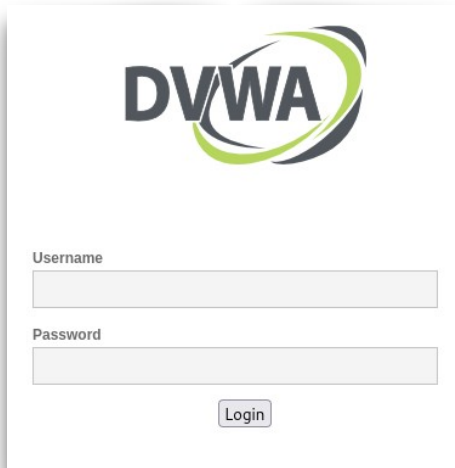
```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

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

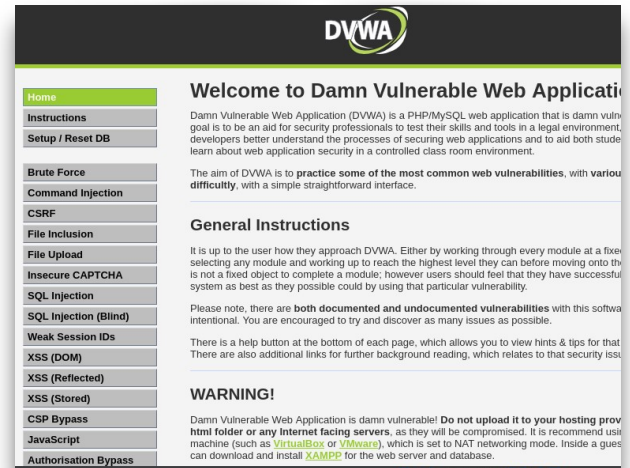
- Ora nel browser inserisco l’indirizzo “**127.0.0.1/DVWA/setup.php**”:



- Clicco su create/reset database e vengo indirizzato su una pagina di login dove inserisco username e password:

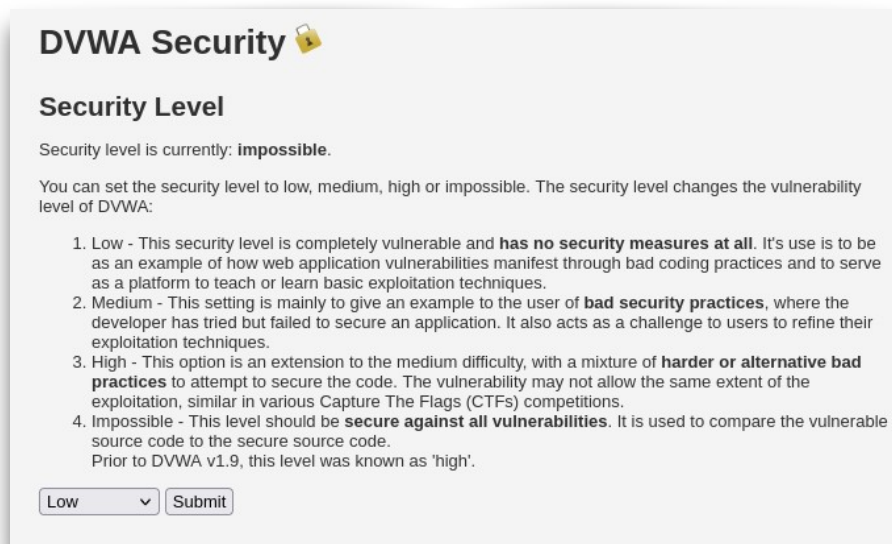


The image shows the DVWA login page. At the top is the DVWA logo. Below it are two input fields: 'Username' and 'Password'. At the bottom is a 'Login' button.



The image shows the DVWA home page. At the top is the DVWA logo. Below it is a 'Welcome to Damn Vulnerable Web Application' message. On the left is a sidebar with a list of links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript, and Authorisation Bypass. The main content area contains 'General Instructions' and a 'WARNING!' section.

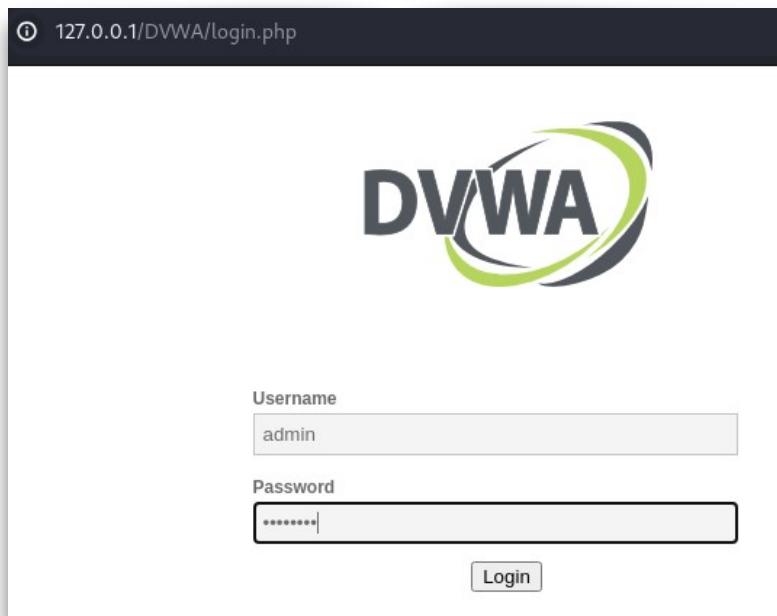
- Clicco sulla scheda (DVWA Security) dove posso scegliere il livello di sicurezza dell'app:



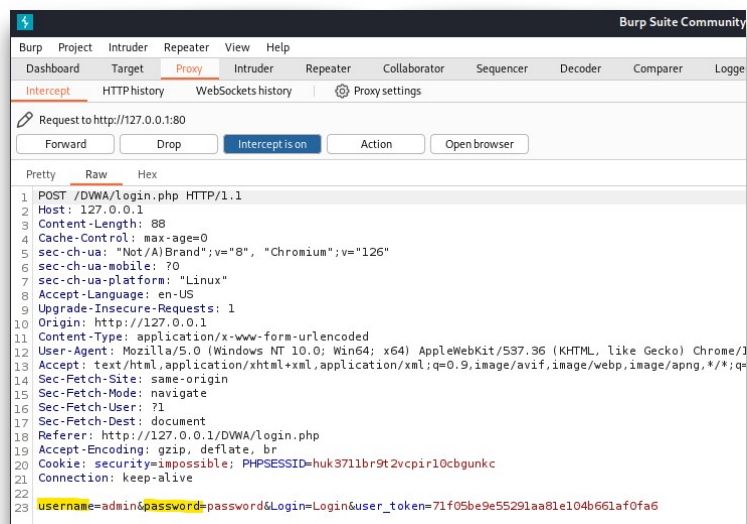
The image shows the DVWA Security page. At the top is the title 'DVWA Security' with a lock icon. Below it is the section 'Security Level'. The text says 'Security level is currently: impossible.' and 'You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:'. There is a list of four security levels: 1. Low, 2. Medium, 3. High, and 4. Impossible. At the bottom is a dropdown menu with 'Low' selected and a 'Submit' button.

4. PRATICA CON BURPSUITE

- Lancio Burpsuite, apro un browser e inserisco l'indirizzo della mia DVWA: 127.0.0.1/DVWA, poi inserisco admin e password per entrare:



- Intercettiamo il traffico con burpsuite e vediamo di modificarla:

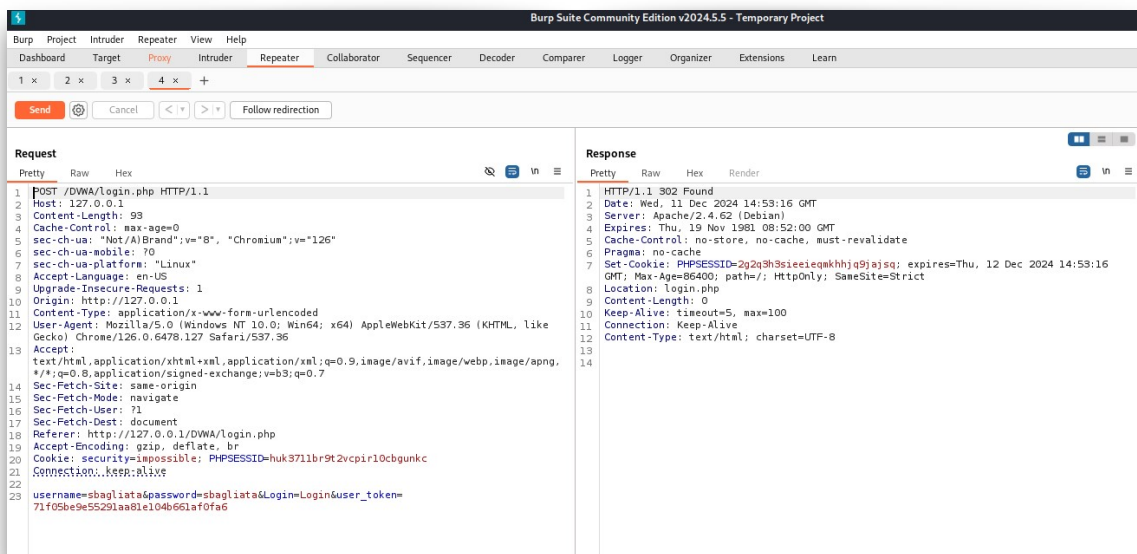


- Come si vede possiamo modificare i parametri di login prima di inviare la richiesta!

- Provo a modificare i campi inserendo delle credenziali sbagliate:

```
username=sbagliata&password=sbagliata&Login=Login&user_token=71f05be9e55291aa81e104b661af0fa6
```

- Prima di inviare la richiesta clicco su “send to repeater”, poi mando la richiesta e guardo la risposta:



- Clicco su follow redirection per seguire il reindirizzamento.
- Come ci aspettavamo, non riusciamo ad entrare con queste credenziali sbagliate, non abbiamo nessuna controprova visiva, questo potrebbe essere dovuto al fatto che il cookie security è impostato su impossibile nonostante io l'abbia impostato precedentemente su low:

