

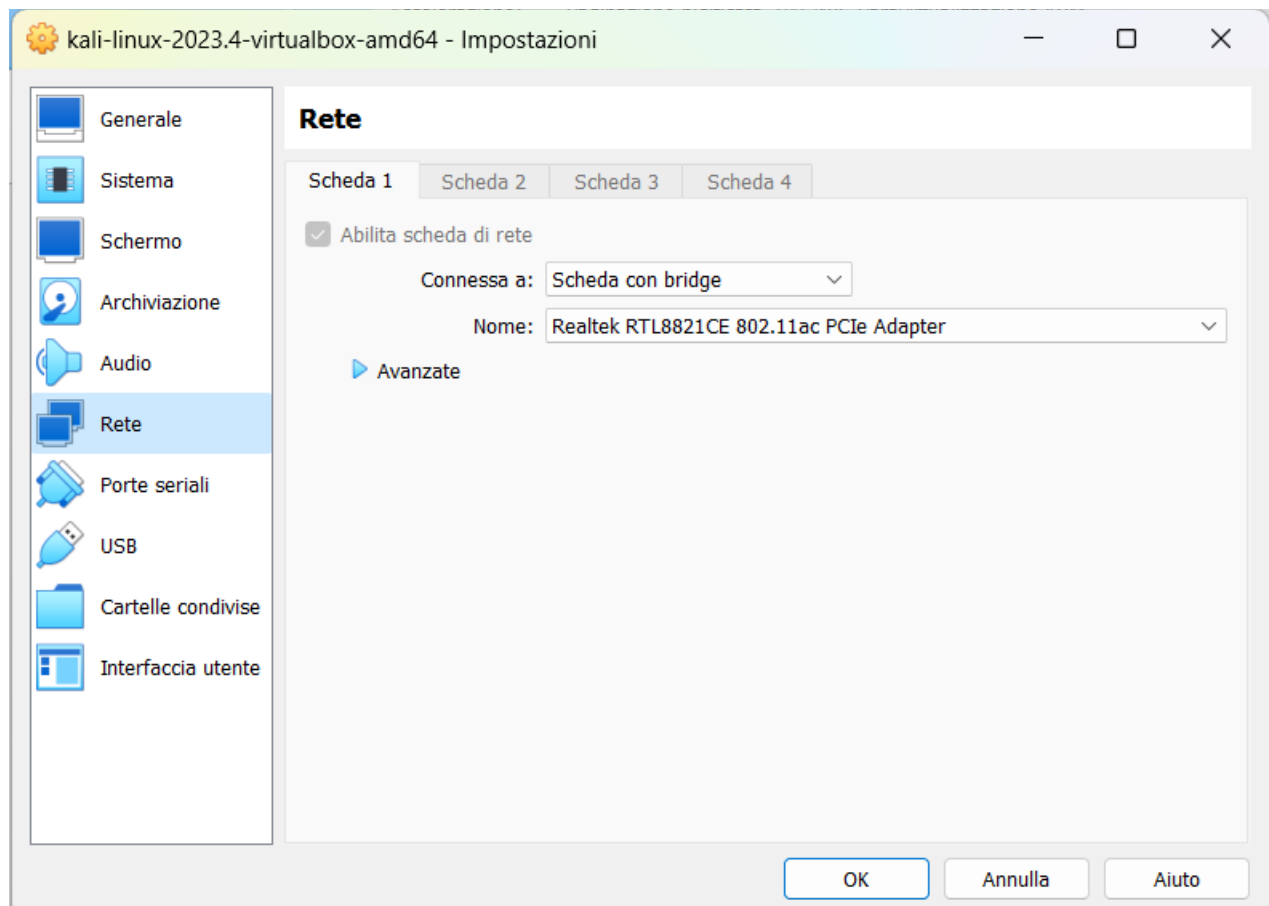
S3L2

BENVENUTI LUIGI, 06/02/2024

Traccia:

Nella lezione pratica di oggi vedremo come configurare una DMWA.

1- Collegamento la kali ad internet:



2 – Setting utente e password:

```
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 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 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

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^_ Replace    ^U Paste      ^J Justify    ^_/ Go To Line  M-E Redo      M-6 Copy
```

3 – servizio mysql

```
MariaDB [(none)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
Query OK, 0 rows affected (0.017 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identi
fied by 'kali';
^C
> Ctrl-C -- exit!
Aborted

(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 33
Server version: 10.11.5-MariaDB-3 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)]> create user 'kali'@'127.0.0.1' identified by 'kali' ;
ERROR 1396 (HY000): Operation CREATE USER failed for 'kali'@'127.0.0.1'
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.013 sec)

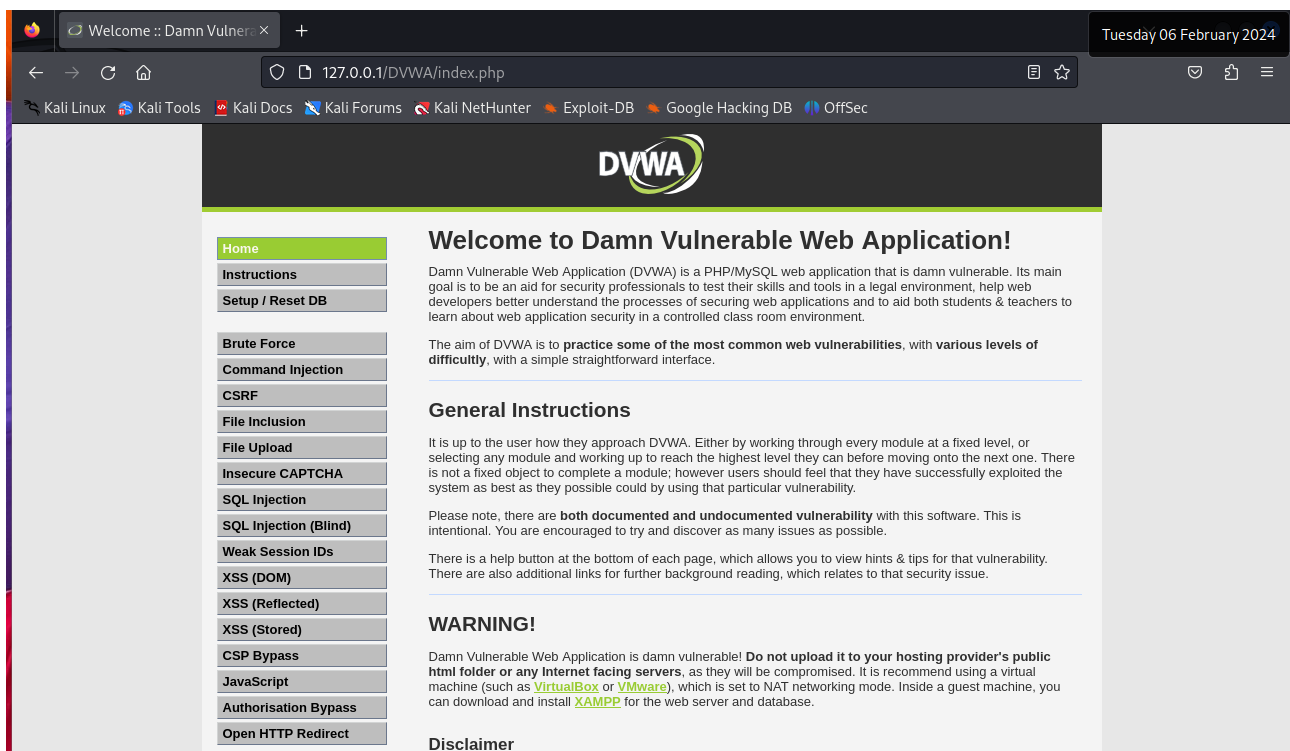
MariaDB [(none)]> exit
Bye
```

4 – editing php.ini:

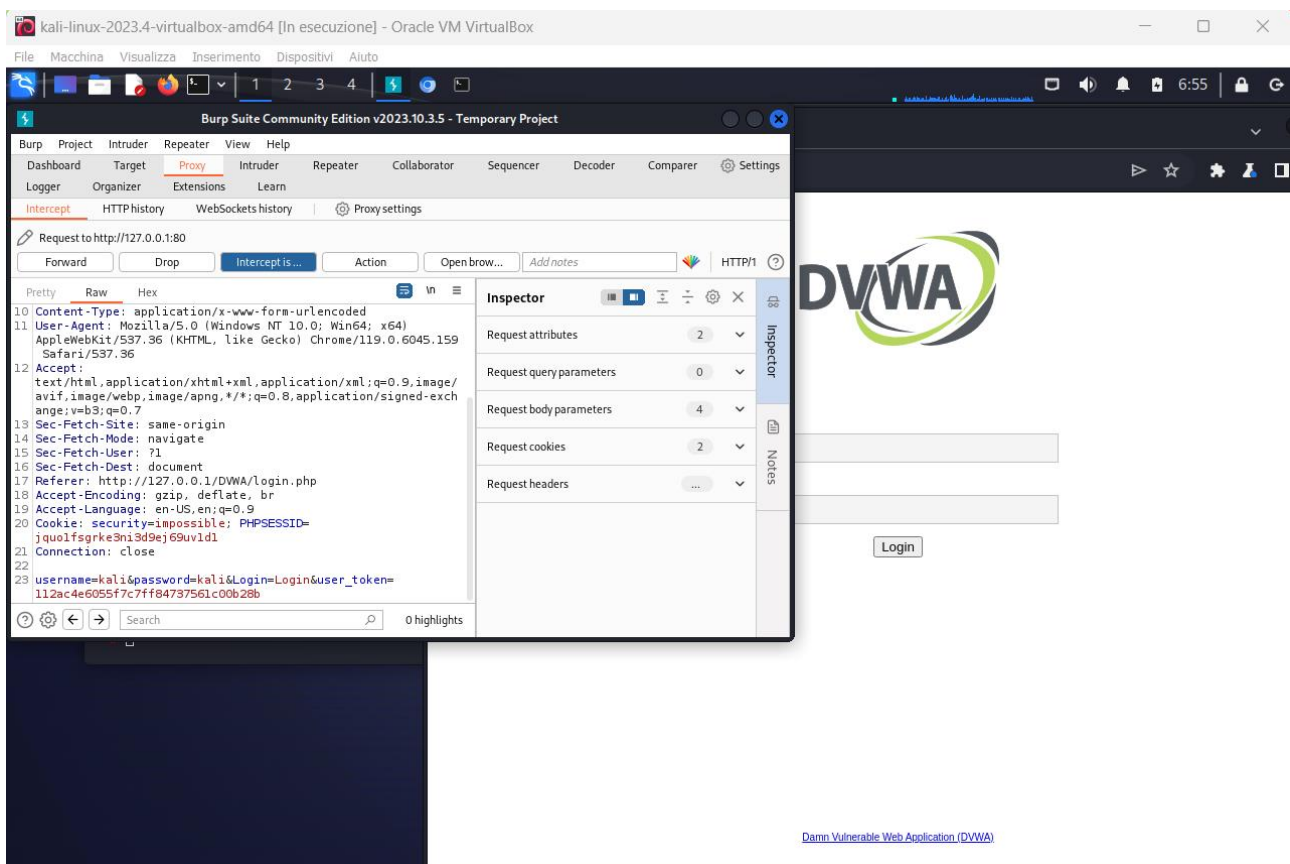
```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

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

5 – dvwa homepage



6 – burpsuite (login visualizzato in chiaro)



7 – burpsuite (attempted login failed)

File Macchina Visualizza Inserimento Dispositivi Aiuto

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Cache-Control: max-age=0
4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 Origin: http://127.0.0.1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
10 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
  application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: http://127.0.0.1/DVWA/login.php
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: security=impossible; PHPSESSID=jqu0lfsgrke3ni3d9ej69uv1dl
19 Connection: close
20
21
```

Response

Pretty Raw Hex

```
47 <br />
48
49 <label for="pass">
  Password
</label>
<input type="
password" class="
loginInput"
AUTOCOMPLETE="off"
size="20" name="
password">
50 <br />
51
52 <br />
53 <p class="submit">
  <input type="
submit" value="
Login" name="Login"
">
</p>
54
55 </fieldset>
56
57 <input type='hidden'
name='user_token'
value='
a280a9c6bbb230675bb407
ed85060bf0' />
58
59 </form>
60
61 <br />
62
```

0 highlights