

W8D1

1. Ho aggiornato Kali.

```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
$ sudo apt upgrade && sudo apt upgrade -y  
[sudo] password for kali:  
The following packages were automatically installed and are no longer required:  
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl  
Use 'sudo apt autoremove' to remove them.  
  
Upgrading:  
adwaita-icon-theme chromium-sandbox kali-desktop-base libexpat1 libnm0 python3-bitstruct python3-urllib3  
chromium fuse3 kali-themes libexpat1-dev network-manager python3-paramiko theharvester  
chromium-common gir1.2-nm-1.0 kali-themes-common libfuse3-4 network-manager-l10n python3-tk  
  
Summary:  
Upgrading: 20, Installing: 0, Removing: 0, Not Upgrading: 0  
Download size: 106 MB / 115 MB  
Space needed: 57.3 kB / 61.9 GB available
```

2. Come da guida, ho ottenuto i permessi di root con i comandi:

“sudo su”.

-Mi sono spostato nella cartella del web server (“cd /var/www/html”).

-Ho clonato la versione DVWA dal repository ufficiale (“git clone git clone <https://github.com/digininja/DVWA>”)

-Ho modificato i permessi della cartella per consentire lettura e scrittura (“chmod -R 777 DVWA/”)

-Mi sono spostato nella cartella di configurazione (“cd DVWA/config”)

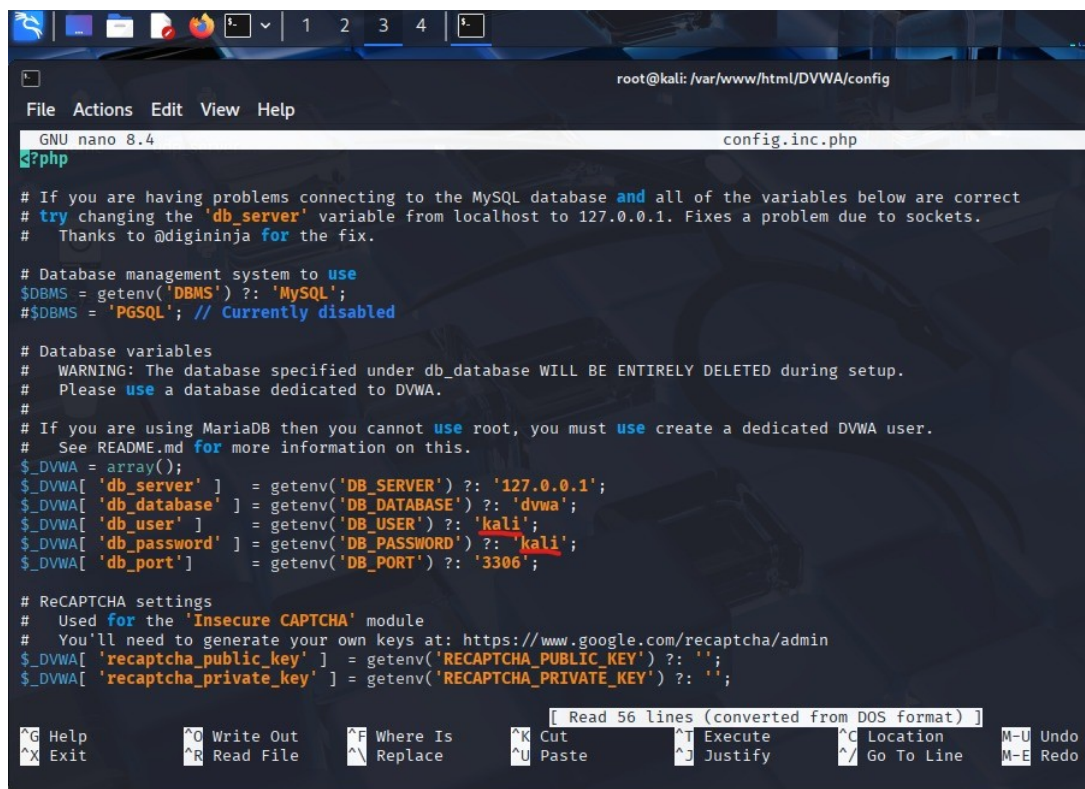
-Ho copiato il file di configurazione in esempio (“cp config.inc.php.dist config.inc.php”)

```
root@kali: /var/www/html/DVWA  
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: 5373, done.  
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)  
Receiving objects: 100% (5373/5373), 2.58 MiB | 2.54 MiB/s, done.  
Resolving deltas: 100% (2667/2667), 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
```

3. Ho modificato il file config.inc.php per impostare utente e password del DB:

“user: kali

password: kali”



```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.4 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 @diginiinja 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 = 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';

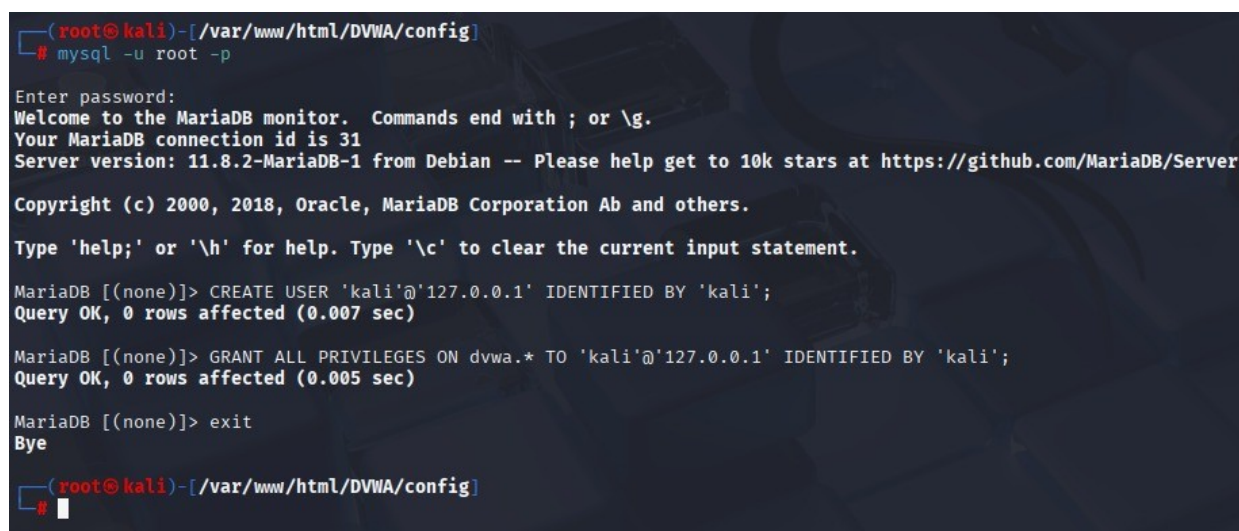
# ReCAPTCHA settings
# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA['recaptcha_public_key'] = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA['recaptcha_private_key'] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

[ Read 56 lines (converted from DOS format) ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line M-E Redo
```

4. Ho avviato il servizio MySQL (“service mysql start”),

e mi sono connesso come root (“mysql -u root -p”).

Ho creato un nuovo utente per DVWA e sono uscito da MySQL.



```
(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: 11.8.2-MariaDB-1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

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';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.005 sec)

MariaDB [(none)]> exit
Bye

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

5. Ho avviato Apache (“service apache2 start”),
mi sono spostato nella cartella di configurazione PHP (“cd /etc/php/8.1/apache2”),
Poi, ho modificato il file php.ini per abilitare, ed ho riavviato apache.

```
GNU nano 8.4 php.ini
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;;;;;;;

; 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

; Define the anonymous ftp password (your email address). PHP's default setting
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"
```

```
(root@kali)-[/var/www/html/DVWA/config]
# service apache2 start

File System: /var/www/html/DVWA/config
(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

(root@kali)-[/var/www/html/DVWA/config]
# cd /etc/php
ls
8.4

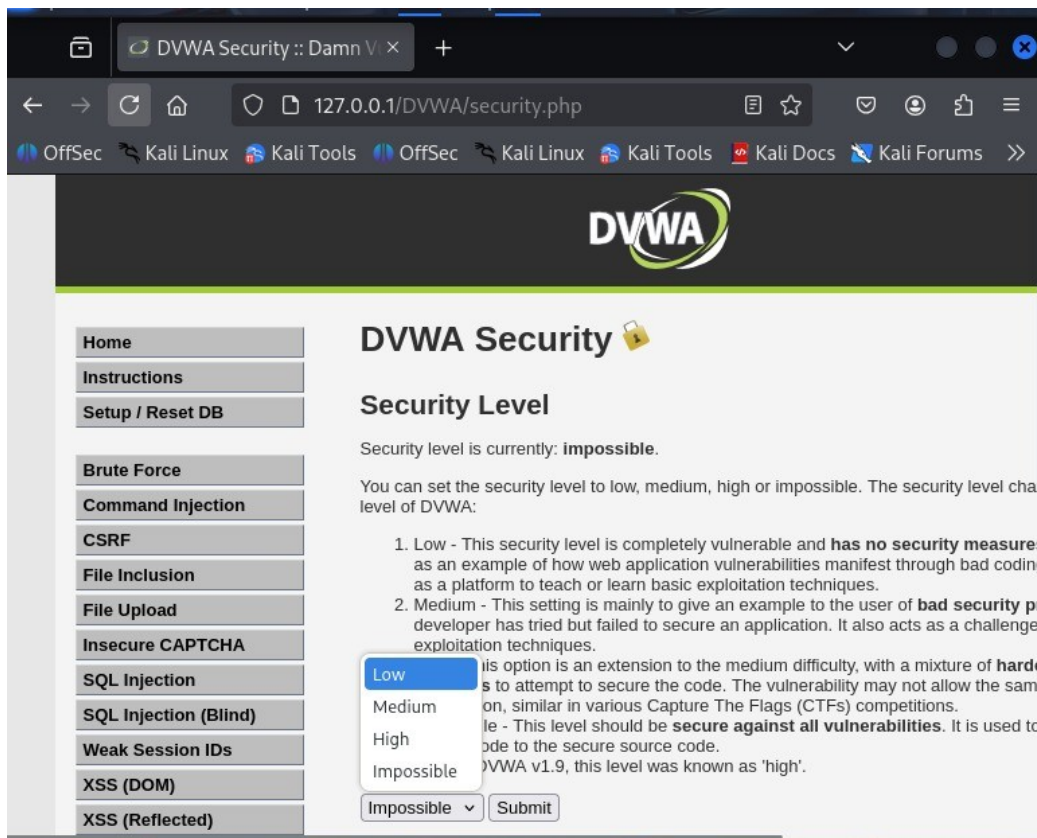
(root@kali)-[/etc/php]
# cd /etc/php/8.4/apache2

(root@kali)-[/etc/php/8.4/apache2]
# nano php.ini

(root@kali)-[/etc/php/8.4/apache2]
# service apache2 restart

(root@kali)-[/etc/php/8.4/apache2]
#
```


6. Ho settupato DVWA via browser, tramite il link “http://127.0.0.1/DVWA/setup.php”.
- Ho cliccato Create, poi Reset Database per creare il database.
- Sono stato reindirizzato alla pagina di login, in cui ho inserito come credenziali, rispettivamente: “admin” e “password”.
- Ho infine impostato il livello di sicurezza su “Low”.



7. Ho iniziato i tentativi di accesso su Burpsuite.
- Ho lanciato Burp Suite e scelto un progetto temporaneo.
- Ho configurato il browser per usare il proxy di Burp su “127.0.0.1:8080”
- Ho provato ad intercettare la richiesta di login di DVWA .

Time	Host	Request	Method	URL	Status	
13:06:1...	HT...	Request	127.0.0.1	GET	http://127.0.0.1/DVWA/	127.
13:06:1...	HT...	Request	127.0.0.1	GET	http://127.0.0.1/DVWA/	127.
13:08:1...	HT...	Request	127.0.0.1	GET	http://127.0.0.1/DVWA/	127.



8. PROBLEMA RISCONTRATO:

Come visibile dall'ultima foto, non apparivano i parametri "username" e "password".

Ho tentato con varie soluzioni:

- Ho controllato tutti i proxy listeners, assicurandomi che il browser fosse ben configurato.
- Ho modificato i listeners di burp.
- Ho verificato alcuni eventuali conflitti di porta con altri processi (questo l'ho fatto tramite il comando "lsof -i :8080").
- Ho modificato le impostazioni firefox.
- Ho provato a eseguire l'esercizio anche utilizzando Metasploitable, ma nella versione di DVWA presente sulla macchina le credenziali sono fisse e i parametri di login non vengono inviati chiaramente.

9. Alla fine ho provato ad agire modificando altri parametri della richiesta HTTP, come il cookie PHPSESSID, inviando le richieste tramite Repeater e osservando le risposte del server. In questo modo ho dimostrato la capacità di intercettare e modificare richieste, anche se i parametri di login non erano visibili nella versione corrente di DVWA.

Time	Type	Direction	Host	Method	URL
13:06:1...	HT...	→ Request	127.0.0.1	GET	http://127.0.0.1/DVWA/
13:06:...	HT...	→ Request	127.0.0.1	GET	http://127.0.0.1/DVWA/
13:08:1...	HT...	→ Request	127.0.0.1	GET	http://127.0.0.1/DVWA/

Request

Pretty Raw Hex

```
1 GET /DVWA/ HTTP/1.1
2 Host: 127.0.0.1
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;c
7 Sec-Fetch-Site: none
8 Sec-Fetch-Mode: navigate
9 Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
12 sec-ch-ua-mobile: ?0
13 sec-ch-ua-platform: "Linux"
14 Accept-Encoding: gzip, deflate, br
15 Cookie: security=low; PHPSESSID=1234567890abcdef
16 Connection: keep-alive
17
18
```

Event log (4) All issues