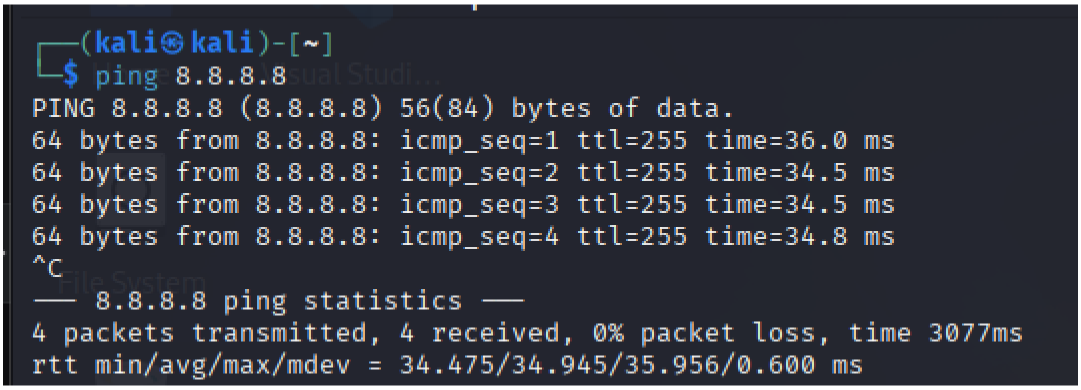
W8D1

DVWA e Burp Suite

Ho iniziato testando la connesione della Kali da terminale digitando
ping 8.8.8.8

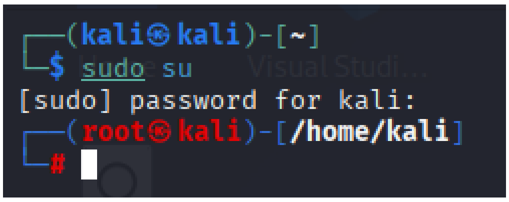


```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=36.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=34.8 ms
^C
── 8.8.8.8 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 34.475/34.945/35.956/0.600 ms
```

Dopo aver verificato la connessione attiva ho proseguito con l'installazione di DVWA

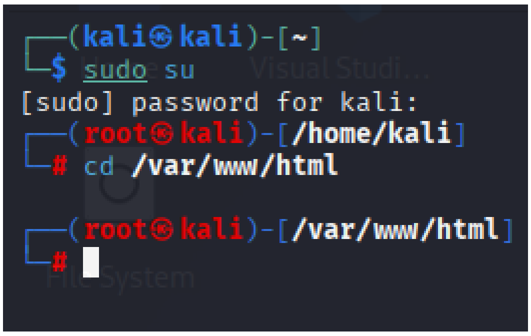
INSTALLAZIONE DVWA

Ho aperto il terminale sulla Kali e ho eseguito il comando sudo sudo su, ho inserito la password di default di Kali



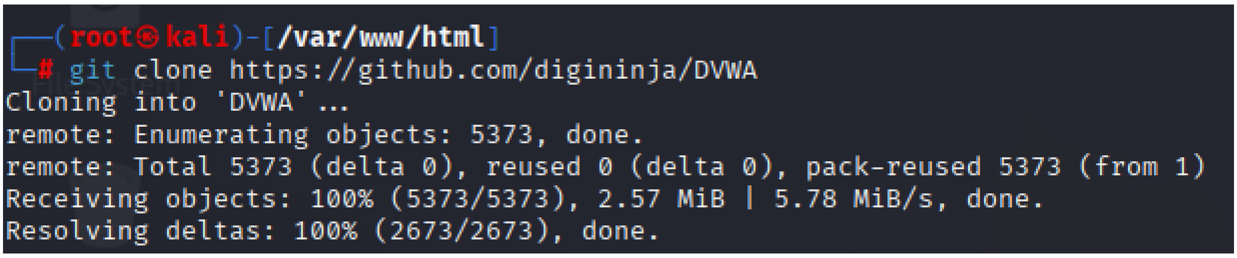
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# 
```

Ho navigato nella directory del web server spostandomi nella cartella dove risiedonoi file di DVWA digitando cd /var/www/html



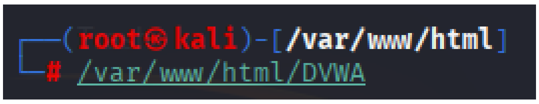
```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# cd /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# 
```

Ho proseguito clonando il repository DVWAscaricando DVWA da GitHub digitando
git clone https://github.com/digininja/DVWA



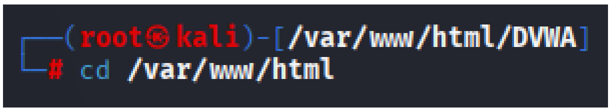
```
┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.57 MiB | 5.78 MiB/s, done.
Resolving deltas: 100% (2673/2673), done.
```

Poi ho digitato il comando /var/www/html/DVWA scaricando l’intera applicazione nella directory



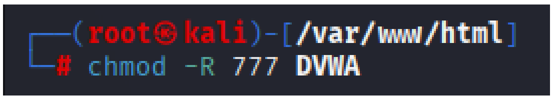
```
┌──(root㉿kali)-[/var/www/html]
└─# /var/www/html/DVWA
```

Mi sono spostato nella directory superiore cd /var/www/html



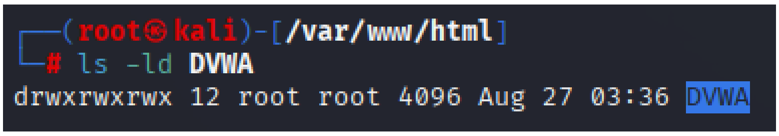
```
┌──(root㉿kali)-[/var/www/html/DVWA]
└─# cd /var/www/html
```

Ho applicato i permessi eseguendo il comando chmod -R 777 DVWA per impostare i permessi sulla directory DVWA
In questo modo imposterò i permessi di lettura , scrittura ed esecuzione per tutti gli utenti sualla directory DVWA e i suoi contenuti.
Il permesso 777 è un permesso molto permissivo, ho scelto di usalro propio per il fatto che il contesto dell’esercizio e didattico ed è stato svolto in un ambiente controllato



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

Ho verificato che i permessi siano stati applicati correttamente digitando
ls -ld DVWA

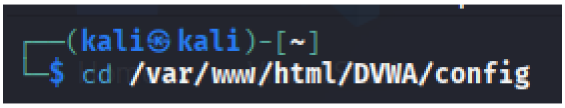


```
┌──(root㉿kali)-[/var/www/html]
└─# ls -ld DVWA
drwxrwxrwx 12 root root 4096 Aug 27 03:36 DVWA
```

Il drwxrwxrwx mi da conferma che i permessi sono stati impostati correttamente

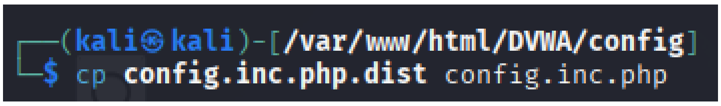
Configurazione di DVWA

Ho configurato il file spostandomi nella directory di configurazione
cd /var/www/html/DVWA/config



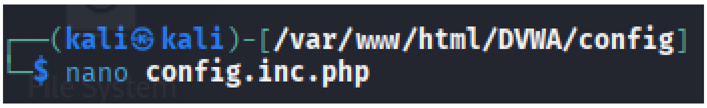
```
┌──(kali㉿kali)-[~]
└─$ cd /var/www/html/DVWA/config
```

Ho creato una copia del file di configurazione cp config.inc.php.dist config.inc.php



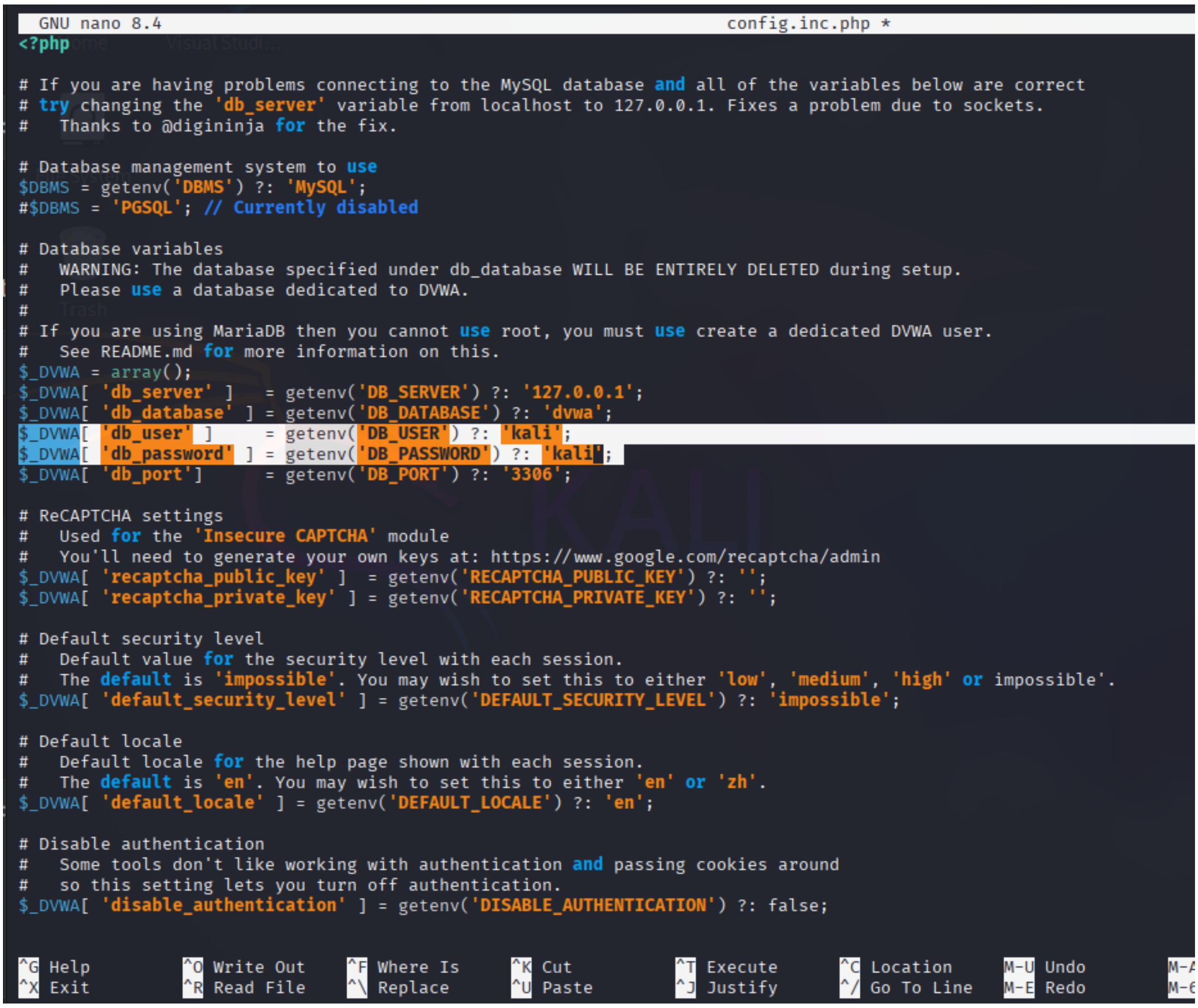
```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ cp config.inc.php.dist config.inc.php
```

Ho modificato il file config.inc.php digitando nano config.inc.php



```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ nano config.inc.php
```

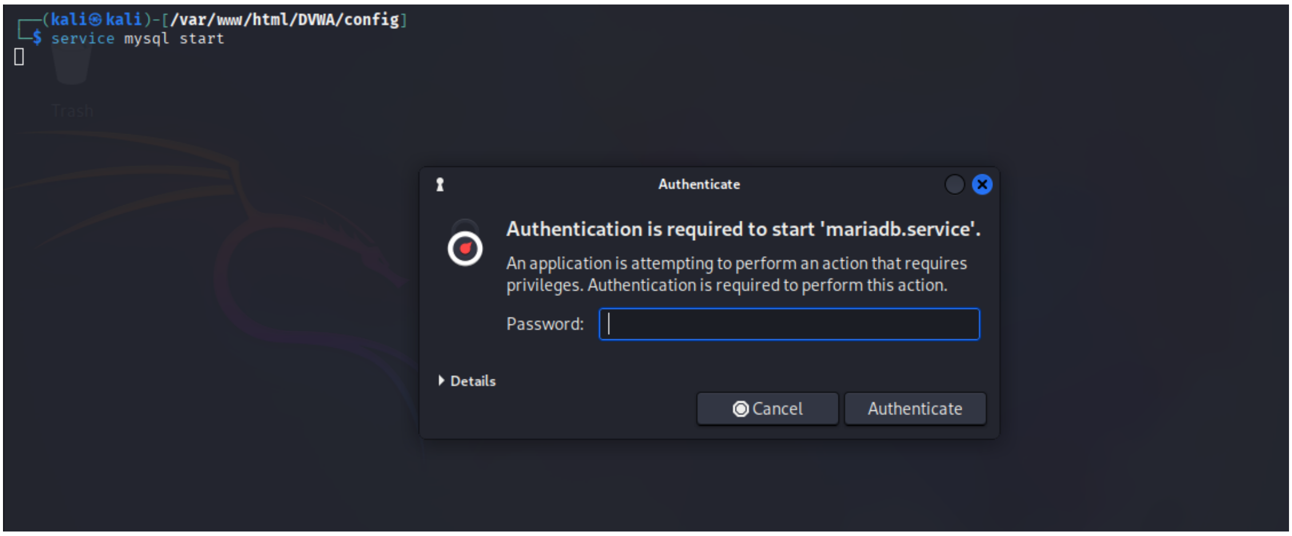
Dopo aver certato le righe di mio interesse ho proseguito nella modifica delle credenziali del database impostandole in questo modo
$_DVWA['db_user'] = 'kali';
$_DVWA['db_password'] = 'kali';



```
  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 @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 = 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') ?: '';

# 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
#   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' ] = getenv('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' ] = getenv('DISABLE_AUTHENTICATION') ?: false;


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

Ho salvato il tutto

Avvio e configuro MySQL con service mysql start



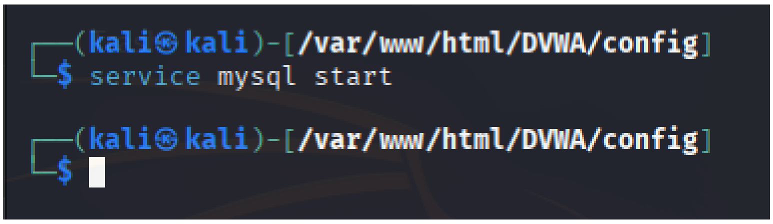
```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ service mysql start
▯
```

Authenticate

Authentication is required to start 'mariadb.service'.

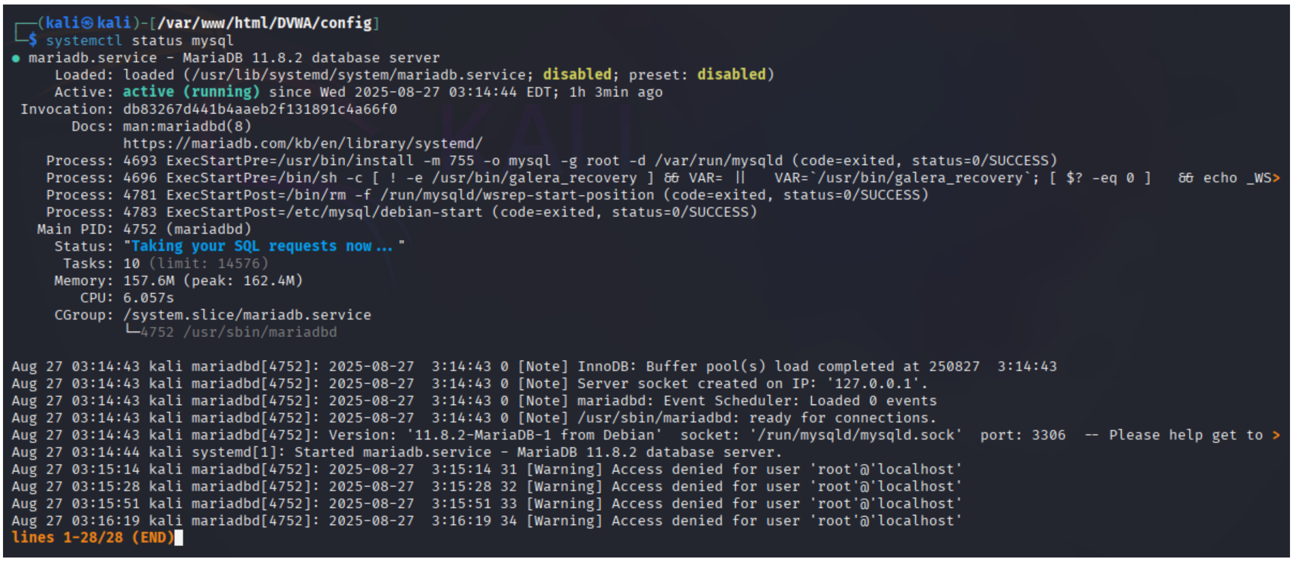
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

Password:



```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ service mysql start

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ █
```

Ho inserito la password e verificato che il servizio sia attivo con systemctl status mysql

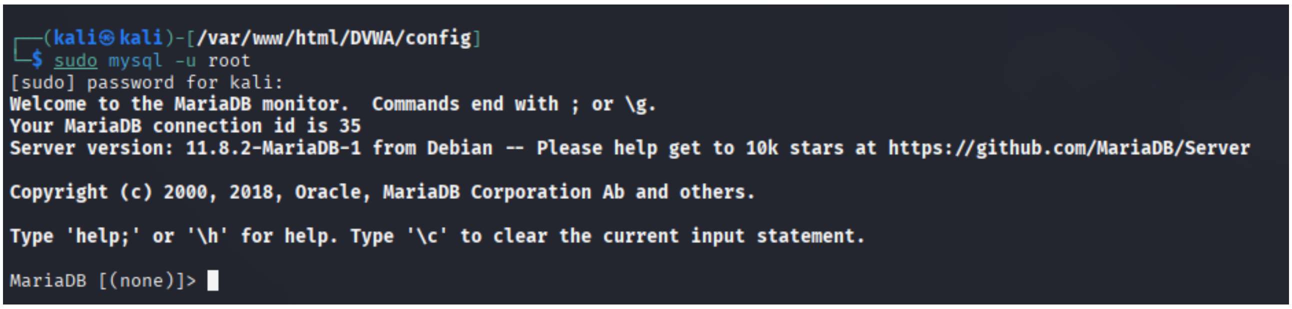


```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ systemctl status mysql
● mariadb.service - MariaDB 11.8.2 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
     Active: active (running) since Wed 2025-08-27 03:14:44 EDT; 1h 3min ago
 Invocation: db83267d441b4aaeb2f131891c4a66f0
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
    Process: 4693 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
    Process: 4696 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= ||   VAR=`/usr/bin/galera_recovery`; [ $? -eq 0 ]   && echo _WS>
    Process: 4781 ExecStartPost=/bin/rm -f /run/mysqld/wsrep-start-position (code=exited, status=0/SUCCESS)
    Process: 4783 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
   Main PID: 4752 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 10 (limit: 14576)
     Memory: 157.6M (peak: 162.4M)
        CPU: 6.057s
     CGroup: /system.slice/mariadb.service
             └─4752 /usr/sbin/mariadbd

Aug 27 03:14:43 kali mariadbd[4752]: 2025-08-27  3:14:43 0 [Note] InnoDB: Buffer pool(s) load completed at 250827  3:14:43
Aug 27 03:14:43 kali mariadbd[4752]: 2025-08-27  3:14:43 0 [Note] Server socket created on IP: '127.0.0.1'.
Aug 27 03:14:43 kali mariadbd[4752]: 2025-08-27  3:14:43 0 [Note] mariadbd: Event Scheduler: Loaded 0 events
Aug 27 03:14:43 kali mariadbd[4752]: 2025-08-27  3:14:43 0 [Note] /usr/sbin/mariadbd: ready for connections.
Aug 27 03:14:43 kali mariadbd[4752]: Version: '11.8.2-MariaDB-1 from Debian'  socket: '/run/mysqld/mysqld.sock'  port: 3306  -- Please help get to >
Aug 27 03:14:44 kali systemd[1]: Started mariadb.service - MariaDB 11.8.2 database server.
Aug 27 03:15:14 kali mariadbd[4752]: 2025-08-27  3:15:14 31 [Warning] Access denied for user 'root'@'localhost'
Aug 27 03:15:28 kali mariadbd[4752]: 2025-08-27  3:15:28 32 [Warning] Access denied for user 'root'@'localhost'
Aug 27 03:15:51 kali mariadbd[4752]: 2025-08-27  3:15:51 33 [Warning] Access denied for user 'root'@'localhost'
Aug 27 03:16:19 kali mariadbd[4752]: 2025-08-27  3:16:19 34 [Warning] Access denied for user 'root'@'localhost'
lines 1-28/28 (END)█
```

Ho riscontrato dei problemi riguardo l’accesso con utente root e la password kali

Ho proseguito in questo modo per risolverlo

Ho provato ad accedere senza password con sudo mysql -u root

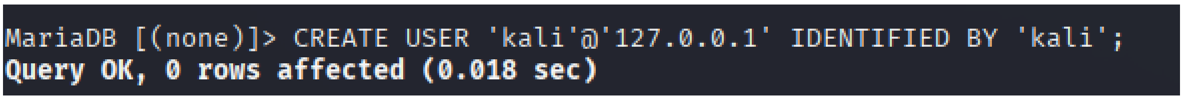


```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo mysql -u root
[sudo] password for kali:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 11.8.2-MariaDB-1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

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)]> 
```

Dopo essere entrato nella shell di MariaDB ho eseguito i comandi per configurare l’utente kali e i permessi per il database DVWA in questo modo

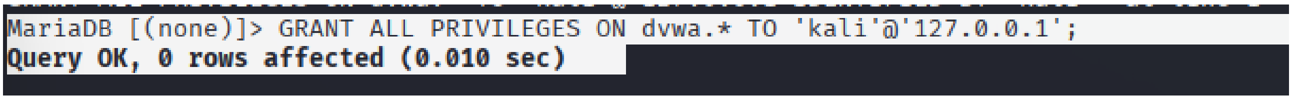
Creazione dell’utente Kali

Eseguo nella shell di MariaDB CREATE USER 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';



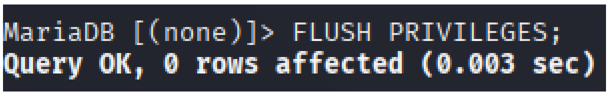
```
MariaDB [(none)]> CREATE USER 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.018 sec)
```

Assegno i privilegi facendo si che l’utente Kali abbia tutti i privilegi sul database DVWA GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';



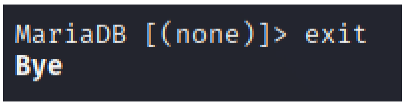
```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1';
Query OK, 0 rows affected (0.010 sec)
```

Applico le modifiche in modo da garantire che tutti i privilegi siano aggiornati con FLUSH PRIVILEGES;



```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.003 sec)
```

Infine esco da MariaDB con exit



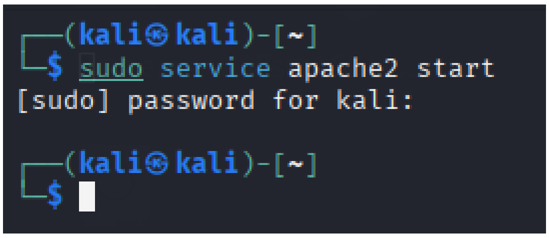
```
MariaDB [(none)]> exit
Bye
```

Adesso ho proseguito con la verifica dei file di configurazione di DVWA

Ho aperto il file e verificato che tutto fosse confermato correttamente e ho proseguito con la configurazione Apache2

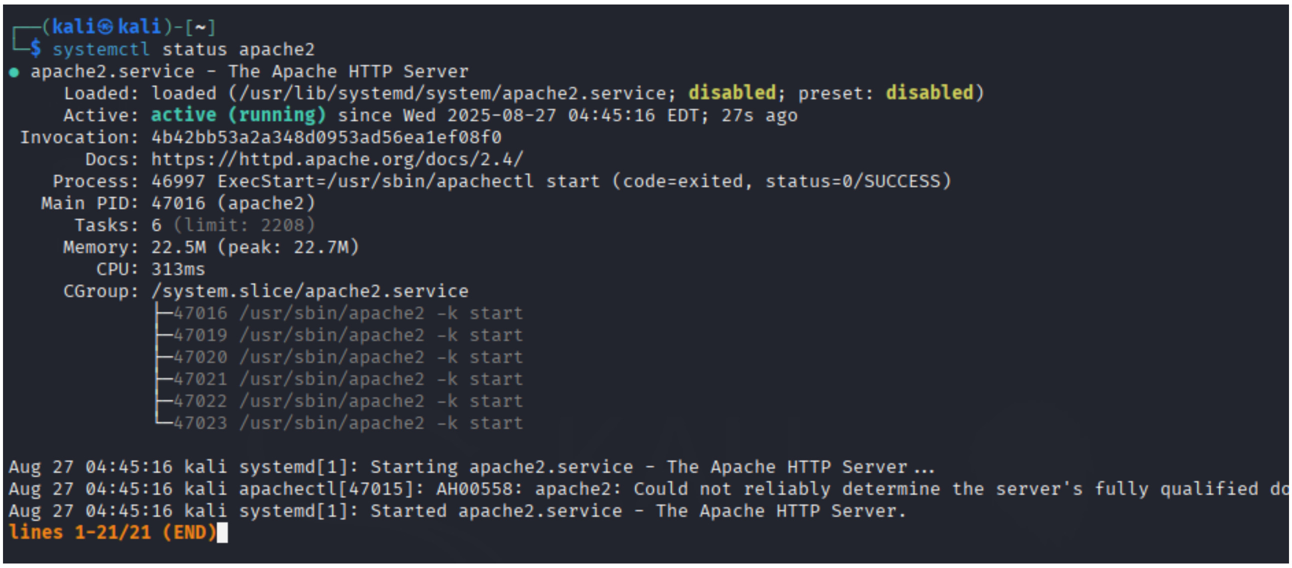
CONFIGURAZIONE APACHE2

Avvio Apache2 con sudo service apache2 start



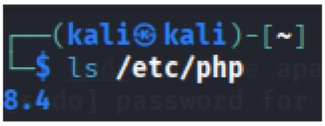
```
┌──(kali㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ 
```

Verifico che Apache2 sia in esecuzione con systemctl status apache2



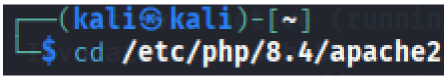
```
┌──(kali㉿kali)-[~]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Wed 2025-08-27 04:45:16 EDT; 27s ago
 Invocation: 4b42bb53a2a348d0953ad56ea1ef08f0
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 46997 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 47016 (apache2)
      Tasks: 6 (limit: 2208)
     Memory: 22.5M (peak: 22.7M)
        CPU: 313ms
     CGroup: /system.slice/apache2.service
             ├─47016 /usr/sbin/apache2 -k start
             ├─47019 /usr/sbin/apache2 -k start
             ├─47020 /usr/sbin/apache2 -k start
             ├─47021 /usr/sbin/apache2 -k start
             ├─47022 /usr/sbin/apache2 -k start
             └─47023 /usr/sbin/apache2 -k start

Aug 27 04:45:16 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 27 04:45:16 kali apachectl[47015]: AH00558: apache2: Could not reliably determine the server's fully qualified do
Aug 27 04:45:16 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

Ho proseguito con la modifica dei file php.ini verificando la versione di PHP con ls /etc/php



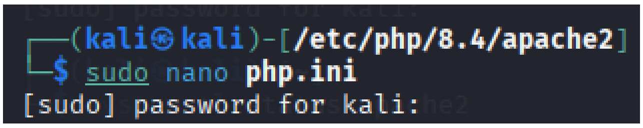
```
┌──(kali㉿kali)-[~]
└─$ ls /etc/php
8.4
```

Ho proseguito andando alla directory di configurazione di PHP 8.4 con
cd /etc/php/8.4/apache2



```
┌──(kali㉿kali)-[~]
└─$ cd /etc/php/8.4/apache2
```

Ho aperto il file php.in con l'editor nano: sudo nano php.ini

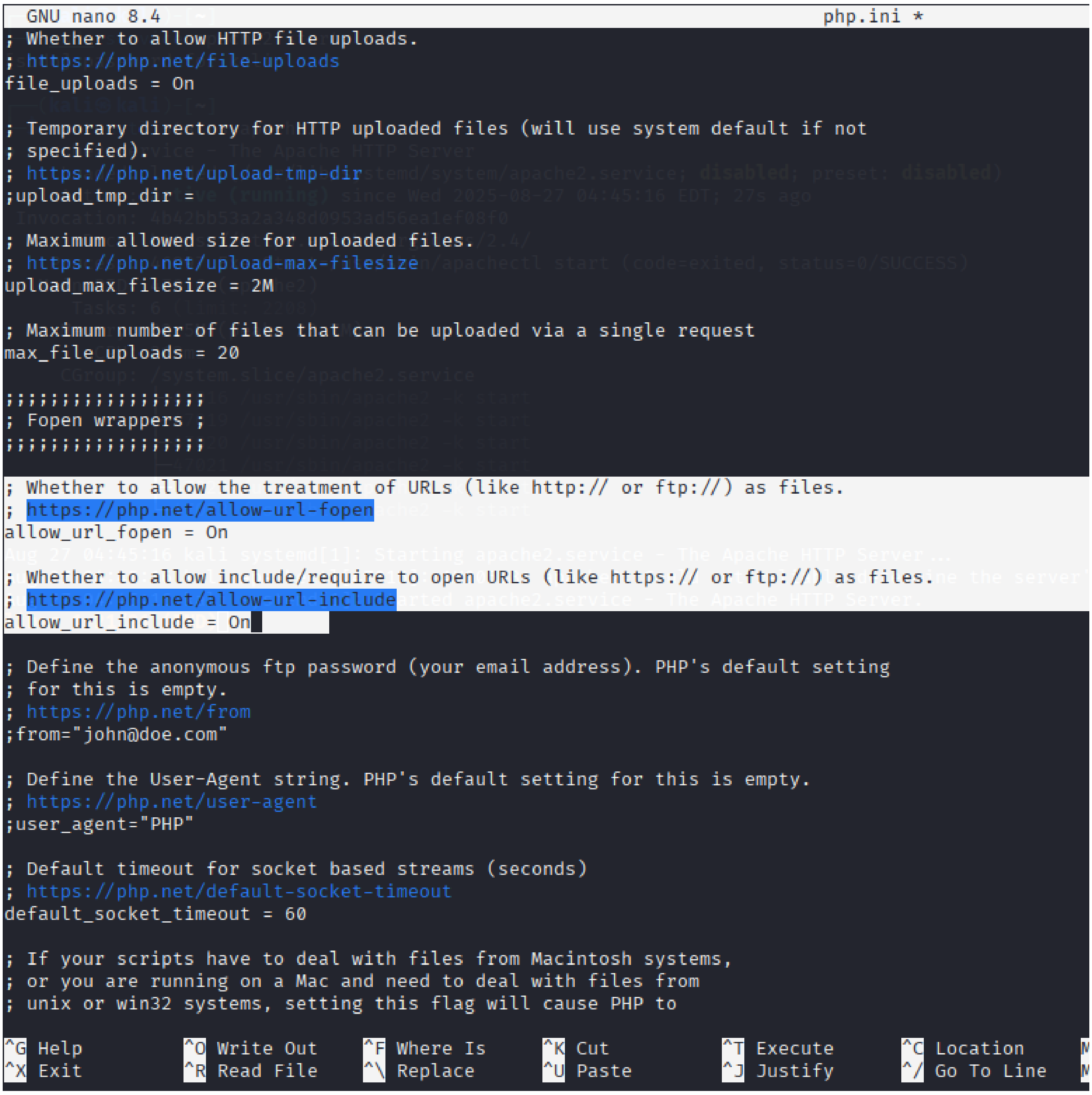


```
┌──(kali㉿kali)-[/etc/php/8.4/apache2]
└─$ sudo nano php.ini
[sudo] password for kali:
```

Modificando le 2 righe

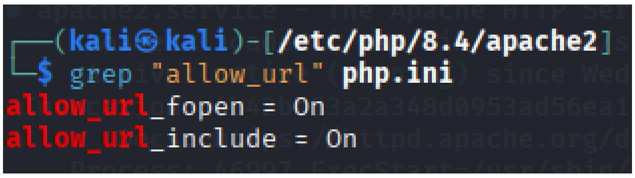
allow_url_fopen
allow_url_include

Impostandole entrambe in On come ho evidenziato nella foto di seguito in binco



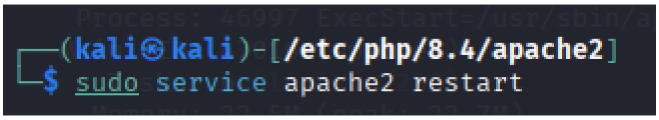
```
  GNU nano 8.4                                                    php.ini *
; Whether to allow HTTP file uploads.
; https://php.net/file-uploads
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
;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"

; Default timeout for socket based streams (seconds)
; https://php.net/default-socket-timeout
default_socket_timeout = 60

; If your scripts have to deal with files from Macintosh systems,
; or you are running on a Mac and need to deal with files from
; unix or win32 systems, setting this flag will cause PHP to

^G Help         ^O Write Out    ^F Where Is     ^K Cut          ^T Execute      ^C Location     M
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To Line   M
```

Ho verificato le modifiche con grep "allow_url" php.ini



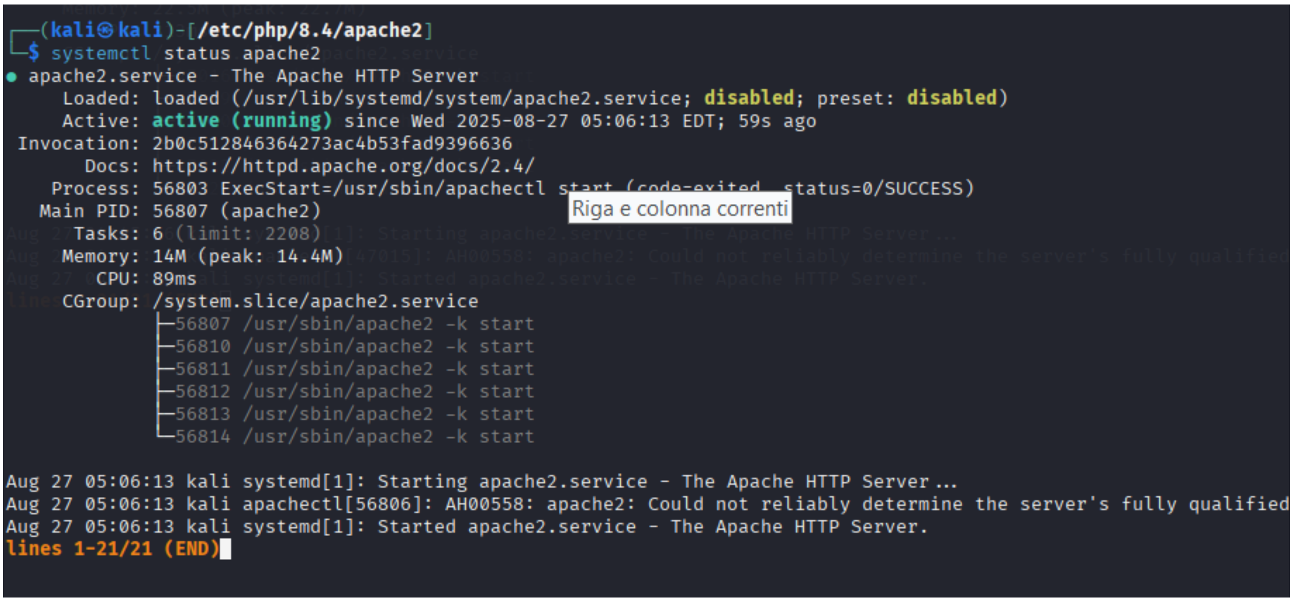
```
┌──(kali㉿kali)-[/etc/php/8.4/apache2]
└─$ grep "allow_url" php.ini
allow_url_fopen = On
allow_url_include = On
```

E riavviato Apache2 con sudo service apache2 restart



```
┌──(kali㉿kali)-[/etc/php/8.4/apache2]
└─$ sudo service apache2 restart
```

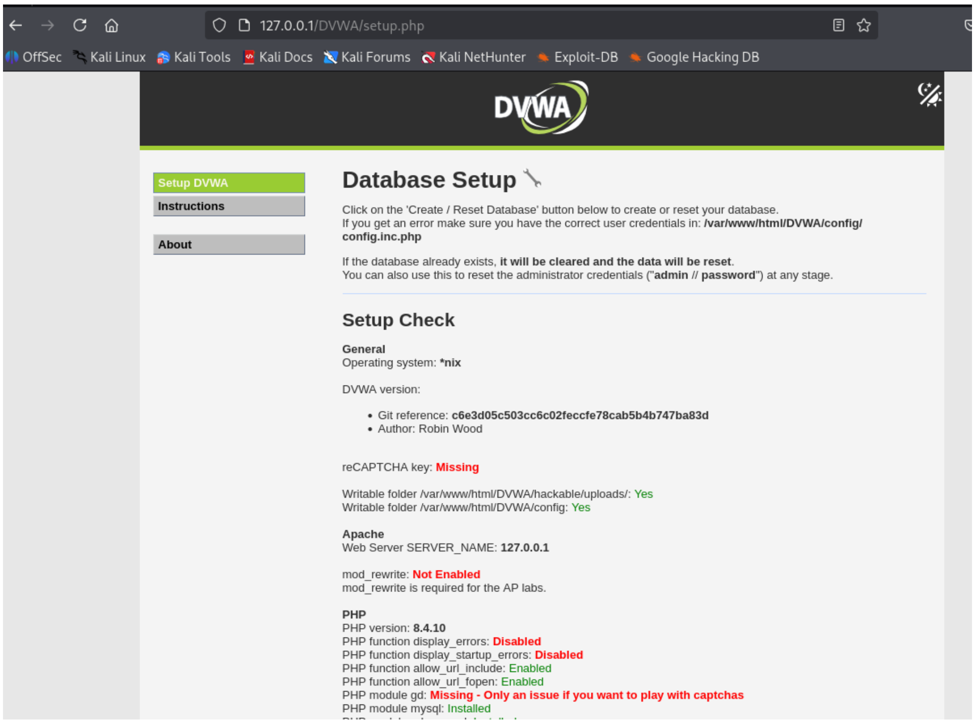
Adesso verifico che Apache2 sia in esecuzione con systemctl status apache2



```
┌──(kali㉿kali)-[/etc/php/8.4/apache2]
└─$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Wed 2025-08-27 05:06:13 EDT; 59s ago
 Invocation: 2b0c512846364273ac4b53fad9396636
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 56803 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 56807 (apache2)
      Tasks: 6 (limit: 2208)
     Memory: 14M (peak: 14.4M)
        CPU: 89ms
     CGroup: /system.slice/apache2.service
             ├─56807 /usr/sbin/apache2 -k start
             ├─56810 /usr/sbin/apache2 -k start
             ├─56811 /usr/sbin/apache2 -k start
             ├─56812 /usr/sbin/apache2 -k start
             ├─56813 /usr/sbin/apache2 -k start
             └─56814 /usr/sbin/apache2 -k start

Aug 27 05:06:13 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Aug 27 05:06:13 kali apachectl[56806]: AH00558: apache2: Could not reliably determine the server's fully qualified
Aug 27 05:06:13 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-21/21 (END)
```

CONFIGURAZIONE DVWA

Dopo aver già configurato il database MariaDB accedo alla pagina di setup di DVWA aprendo il browser su Kali con http://127.0.0.1/DVWA/setup.php



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

General
Operating system: ***nix**

DVWA version:

- Git reference: **c6e3d05c503cc6c02feccfe78cab5b4b747ba83d**
- Author: Robin Wood

reCAPTCHA key: **Missing**

Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

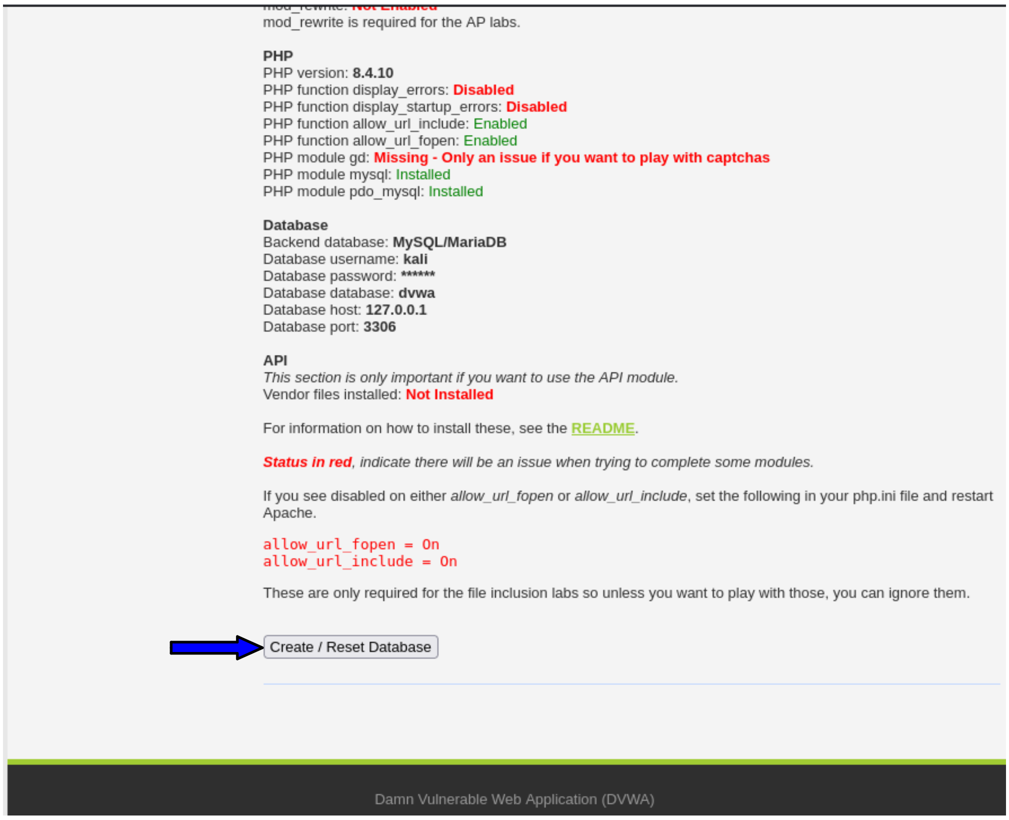
Apache
Web Server SERVER_NAME: **127.0.0.1**

mod_rewrite: **Not Enabled**
mod_rewrite is required for the AP labs.

PHP
PHP version: **8.4.10**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed

Nella pagina setup.php ho cliccato su Create / Reset Database

In questo modo popolerà il database DVWA con le tabelle necessarie usando le credenziali kali/kali che ho specificato in config.inc.php



mod_rewrite is required for the AP labs.

PHP
PHP version: **8.4.10**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Database
Backend database: **MySQL/MariaDB**
Database username: **kali**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

API
This section is only important if you want to use the API module.
Vendor files installed: **Not Installed**

For information on how to install these, see the README.

Status in red*, indicate there will be an issue when trying to complete some modules.*

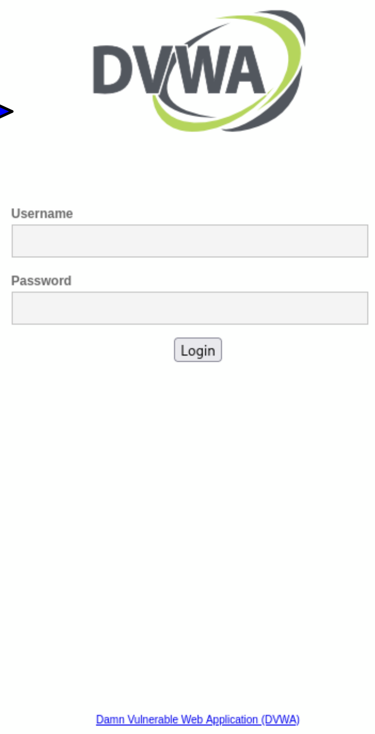
If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

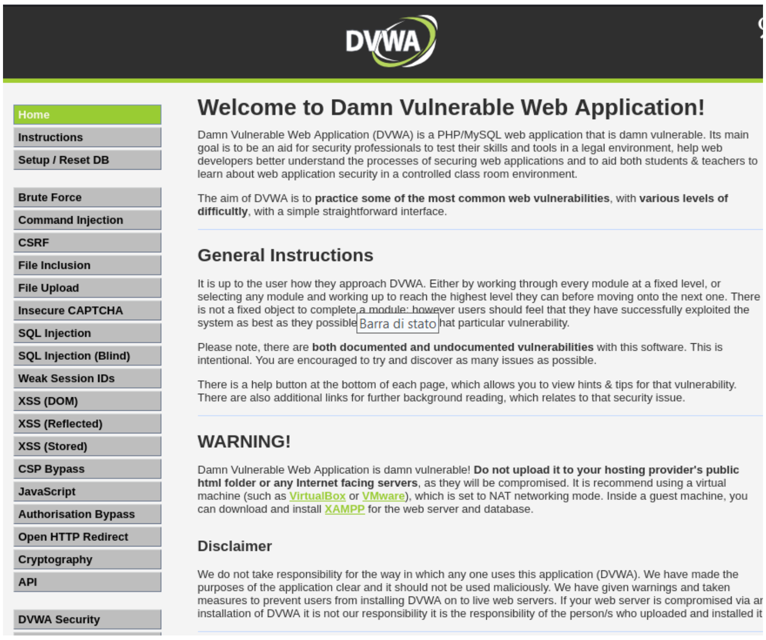
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Sulla destra la pagina che compare dopo il clik

Di seguito effettuo l’accesso a DVWA con le credeziali di default :



Username admin
Password password



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible Barra di stato hat particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

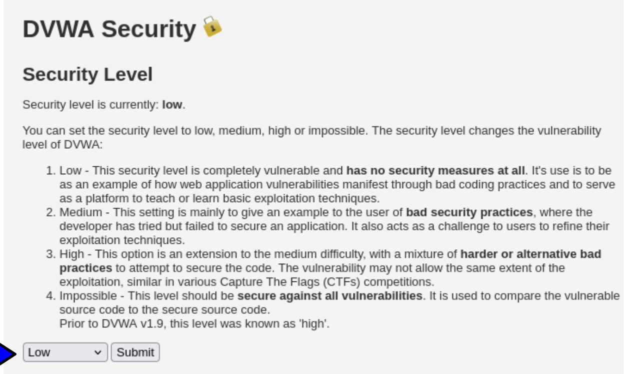
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via ar installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it

Imposto il livello di sicurezza della scheda DVWA Security in Low per specificare i test di vulnerabilità



DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low

Verifico che i servizi di Base siano Attivi prima di avviare **Burb Suite**

Terminale 1
Controllo Apache2 service apache2 status

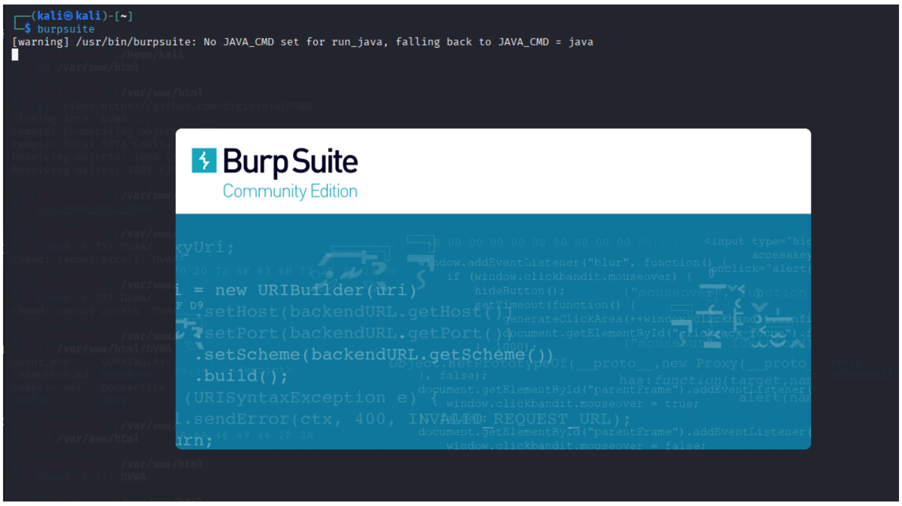
Se non active, avvia: service apache2 start

Terminale 2
Controllo MySQL service mysql status

Se non active, avvia service mysql start

BURP SUITE

Apro Burp Suite eseguendo il comando su terminale burpsuite



```
┌──(kali㉿kali)-[~]
└─$ burpsuite
[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to JAVA_CMD = java
```

Non ho configurto il proxy nel browser perchè ho utilizzato direttamente il browser di Burp Suit

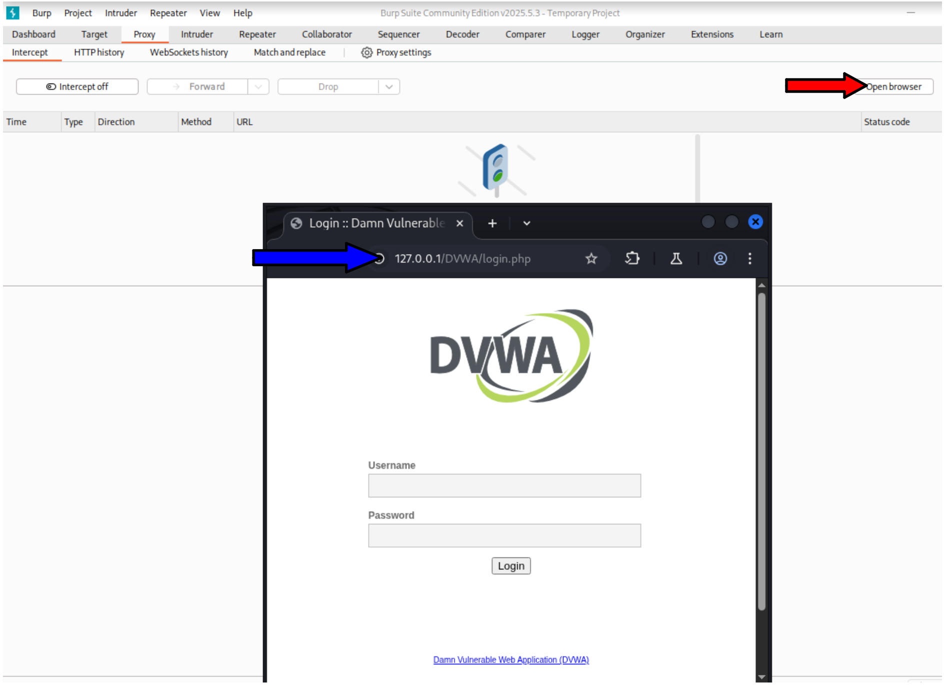
Altrimeti se era esterno avrei dovuto configurarlo cosi:

Impostazioni>rete>Proxy manuale

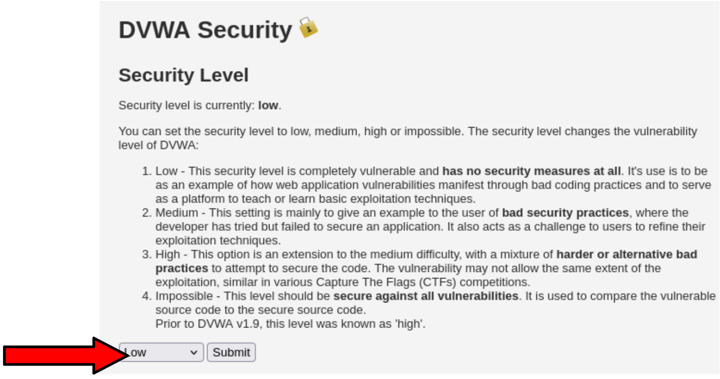
Host: 127.0.0.1
Porta: 8080

Ho aperto il browser con Open browser

Ho digitato nel browser http://127.0.0.1/DVWA



Ho inserito le credenziali e sono entrato e impostato il livello di sicurezza su Low



DVWA Security

Security Level

Security level is currently: **low**.

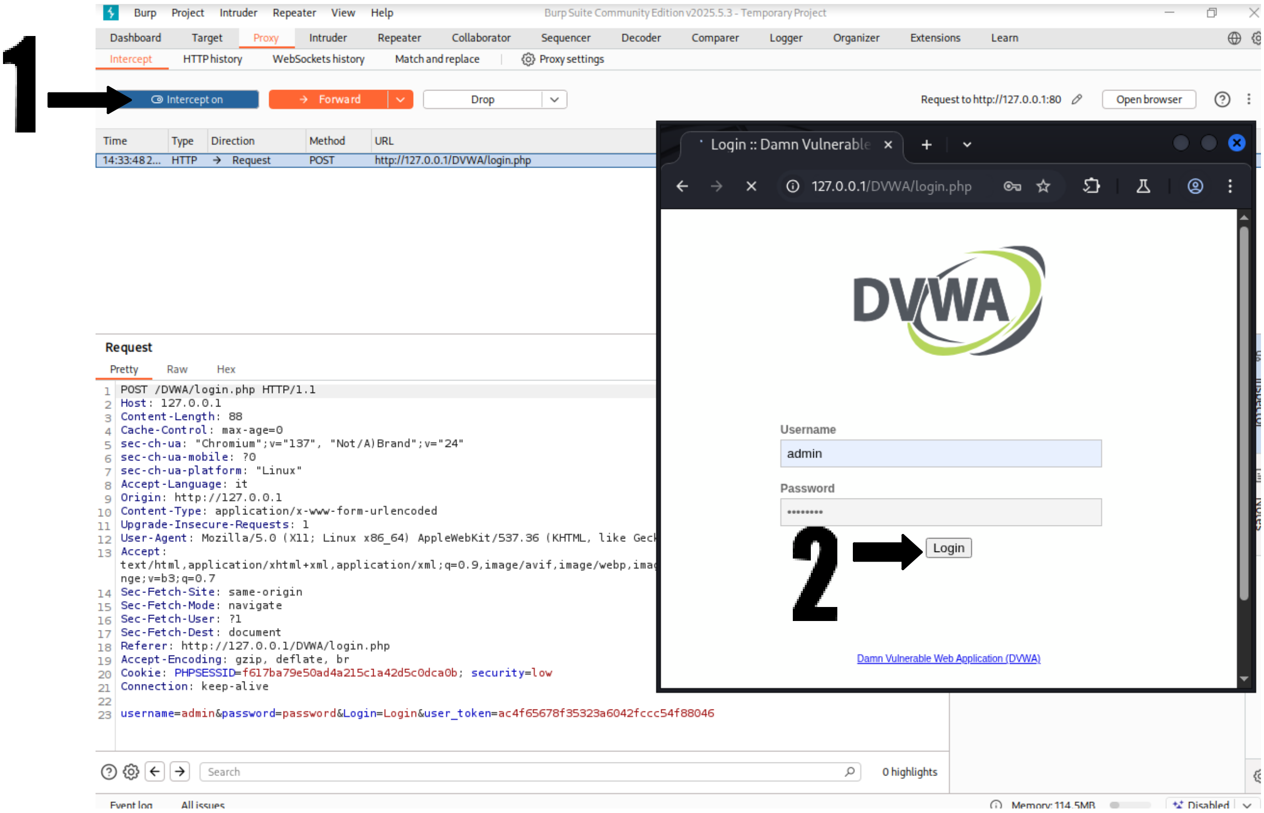
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
   Prior to DVWA v1.9, this level was known as 'high'.

Low

Sono tornato alla schermata login e inserito le credenziali originali (admin) admin e (password) password senza premere invio

Dopo ho attivto Intercept in on e avviato il login sul browers


1
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://127.0.0.1:80
Open browser
Login :: Damn Vulnerable
DVWA
2
Login
Request
Pretty Raw Hex
Search
0 highlights
Event log All issues
Memory: 114.5MB
Disabled

Time	Type	Direction	Method	URL
14:33:48 2...	HTTP	→ Request	POST	http://127.0.0.1/DVWA/login.php

127.0.0.1/DVWA/login.php

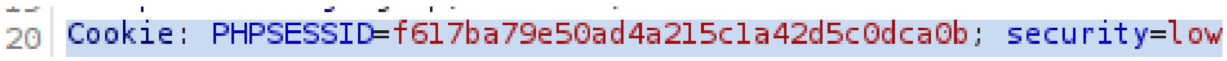
Username: admin

Password: ••••••••

Damn Vulnerable Web Application (DVWA)

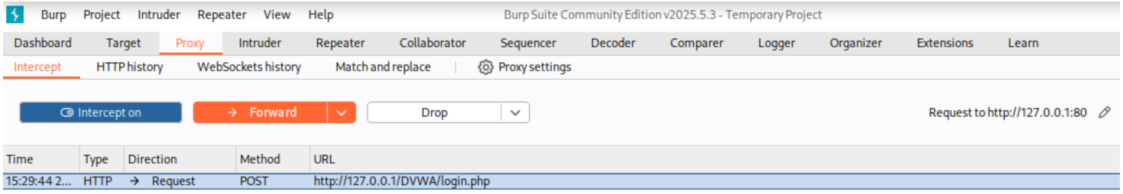
```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: it
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Geck
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
nge;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b; security=low
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=ac4f65678f35323a6042fccc54f88046
```

Nella sezione Raw ho verificato il cambio dei cookie in Burp Suite riattivando Intercept in On, ho
ricaricato la pagina DVWA in Firefox, controllando nel tex la riga Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b; security=low come ho evidenziato nella foto di seguito

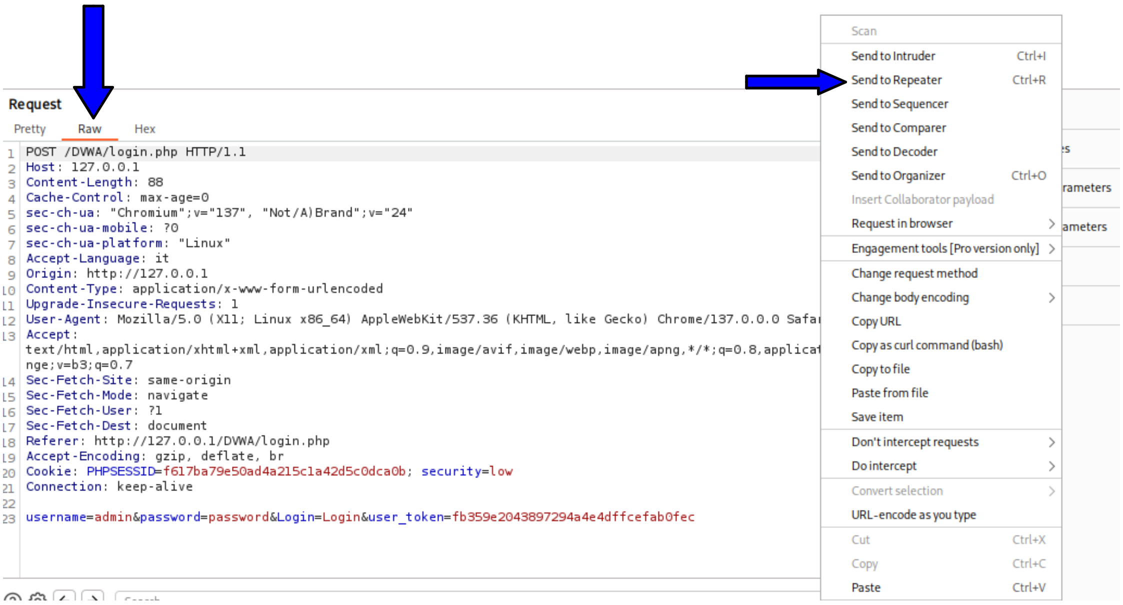


```
Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b; security=low
```

Adesso intercetto la richiesta di login assicurandomi che Intercetp sia in On e clicco sul login

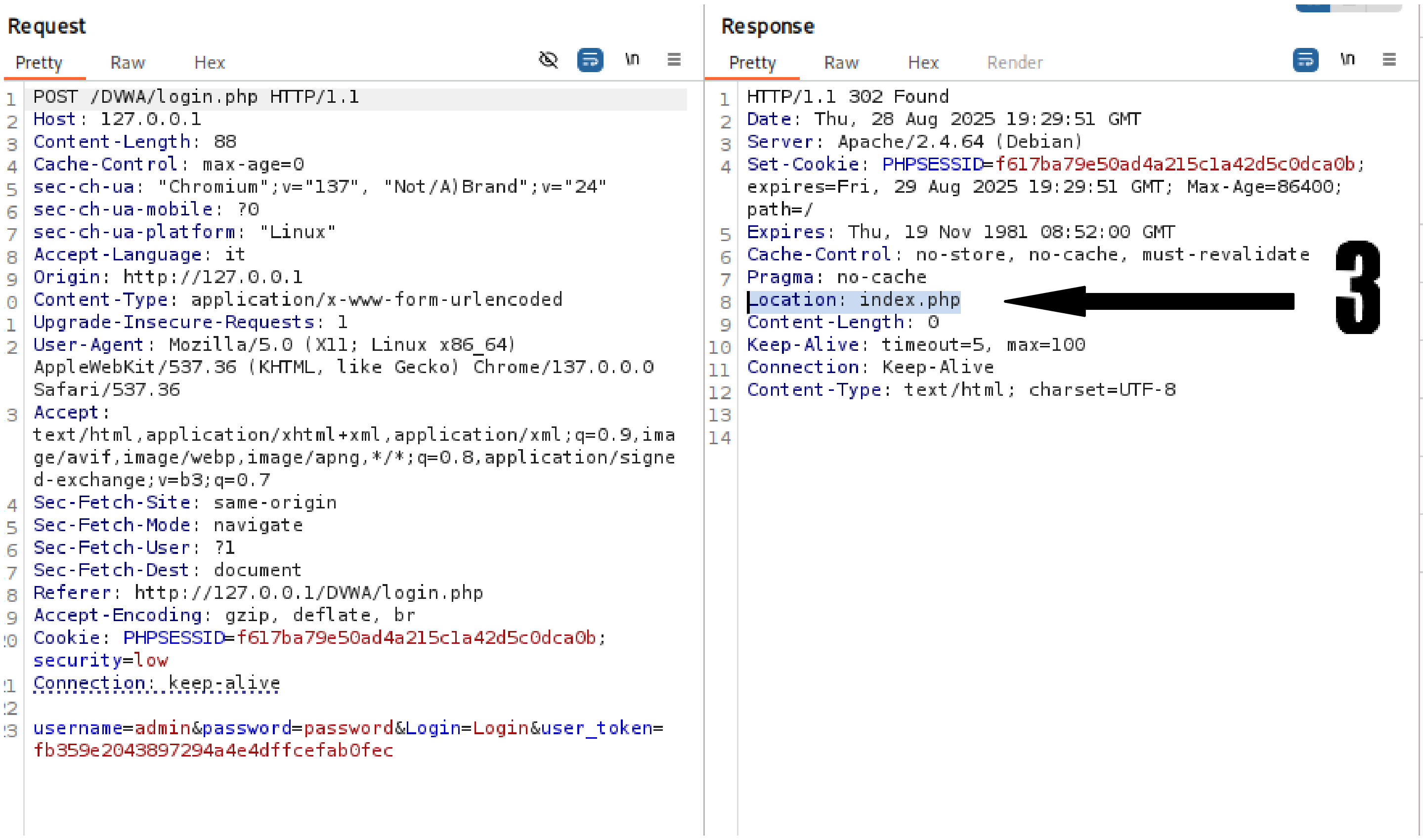


Time	Type	Direction	Method	URL
15:29:44 2...	HTTP	→ Request	POST	http://127.0.0.1/DVWA/login.php



```
POST /DWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: it
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safa
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
nge;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b; security=low
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=fb359e2043897294a4e4dffcefab0fec
```

Effettuo il test con password corretta spostandomi su Send to Repeat e una volta andato nella sezione Repeater clicco su Send e poi follow redirection dove nella Respose trovo la conferma del login OK con index.php questo è il redirect che conferma il successo



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: it
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b;
security=low
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=
fb359e2043897294a4e4dffcefab0fec
```

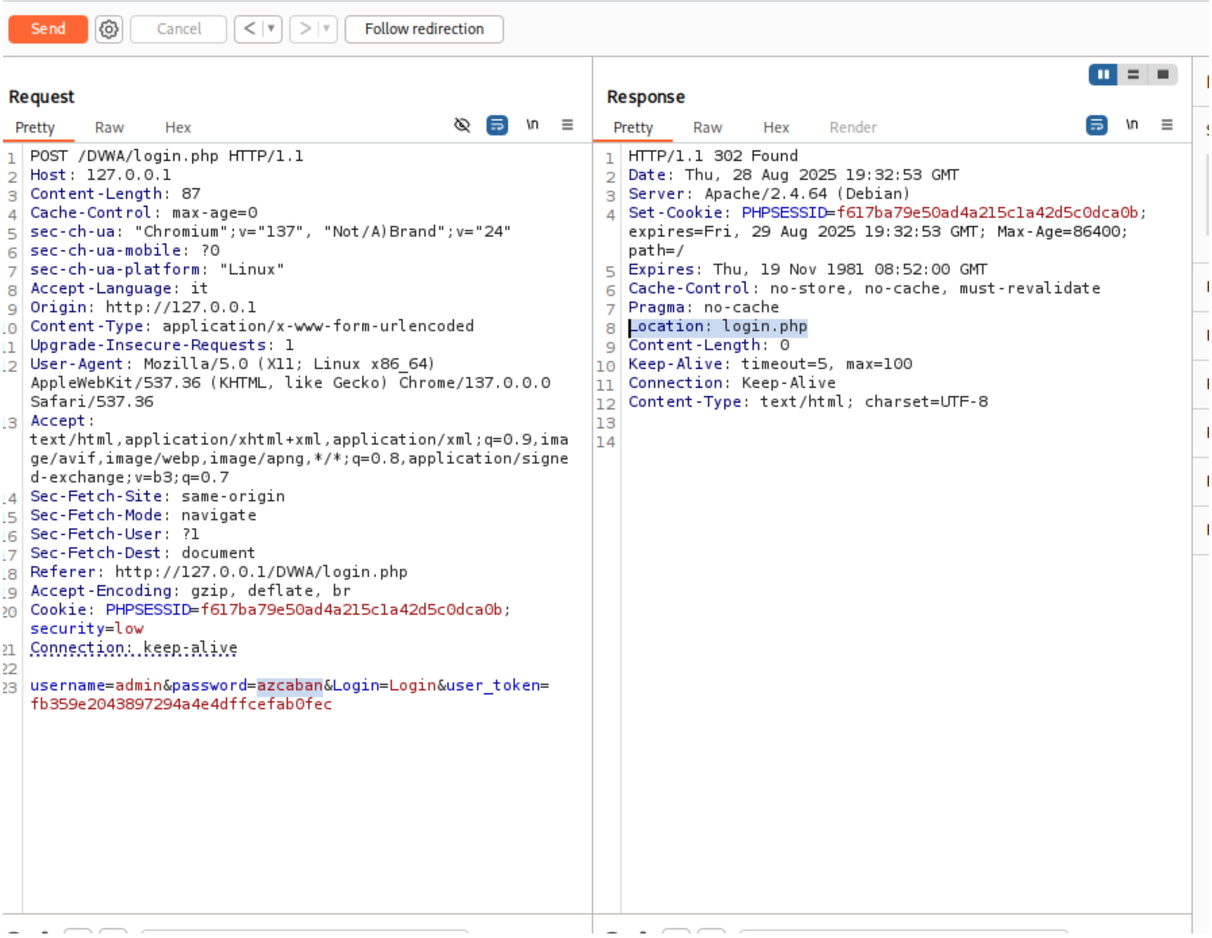
```
HTTP/1.1 302 Found
Date: Thu, 28 Aug 2025 19:29:51 GMT
Server: Apache/2.4.64 (Debian)
Set-Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b;
expires=Fri, 29 Aug 2025 19:29:51 GMT; Max-Age=86400;
path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Nella schermata Request vedo la riga nel tex
username=admin&password=password&Login=Login

Proseguo con la modifica della richiesta

username=**admin**&password=**azkaban**&Login=Login

Dopo la modifica clicco Send e piu su Follow per inviare la richiesta di modifica



```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 87
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: it
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
ge/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b;
security=low
Connection: keep-alive

username=admin&password=azcaban&Login=Login&user_token=
fb359e2043897294a4e4dffcefab0fec
```

```
HTTP/1.1 302 Found
Date: Thu, 28 Aug 2025 19:32:53 GMT
Server: Apache/2.4.64 (Debian)
Set-Cookie: PHPSESSID=f617ba79e50ad4a215c1a42d5c0dca0b;
expires=Fri, 29 Aug 2025 19:32:53 GMT; Max-Age=86400;
path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Verifico il login fallito, infatti ho conferma login.php questo è il redirect che conferma il fallimento

Nel svolgere l’esercizo confrontanto le lezioni teoriche ho notato che per rendelro piu completo avrei potuto cambiareil Content-Length, inbase alla password che ho scelto di seguito ho riportato il calcolo che ho fatto per modificarlo:

Modifico il Content-Length calcolandolo questo modo

username=admin: 14 characters (u s e r n a m e = a d m i n)
&password=azkaban: 17 characters (& p a s s w o r d = a z k a b a n)
&Login=Login: 12 characters (& L o g i n = L o g i n)
&user_token=87e1c15a6b252afd056adac7965d8aa3: 44 characters (& u s e r _ t o k e n = 32-character token)

Total: 14 + 17 + 12 + 44 = 87 bytes

Ho selezionato in giallo perchè è una spiegazione aggiuntiva che ho aggiunto dopo aver concluso l’esercizio

Facoltativo

Confronto tra livelli di sicurezza in DVWA

Dopo aver completato la configurazione della DVWA e aver eseguito i primi test con il livello di sicurezza impostato su Low nell'esercizio precedente, ho proseguito con l'esercizio facoltativo, dove mi chiedeva di ripetere gli stessi test impostando i livelli di sicurezza su Medium e High per analizzare le differenze nel comportamento dell'applicazione.

Modifico il livello di sicurezza

Ho caricato la pagina DVWA all'indirizzo 127.0.0.1/DVWA

Ho effettuato il login con le credenziali predefinite **admin / password** e sono andato nella sezione DVWA Security

Ho prima impostato il livello di sicurezza su **Medium** e svolto il test

Poi successivamente su **High**

Ricordandomi ogni volta di salvare con il pulsante **Submit** per rendere le modifiche effettive

Test con Burp Suite

Con Burp Suite ho intercettato le richieste di login effettuate al sito DVWA, come già fatto nei passaggi precedenti con il livello Low.

Ho inviato la richiesta al Repeater e ho testato le seguenti varianti:

Inserimento di credenziali errate

SQL Injection nei campi username e password

Modifica manuale dei parametri prima dell'invio

Descrizione rilevate

Livello	Comportamento dell'applicazione	Protezioni aggiuntive	Esito
Low	Nessun controllo sui dati	Nessun filtro o token	Exploit riuscito facilmente
Medium	Controlli base sui parametri	Escape su caratteri speciali, basic validation	Exploit più difficile, ma ancora possibile
High	Protezioni robuste	CSRF Token, validazione lato server, sanitizzazione avanzata	La maggior parte degli exploit fallisce

Descrizione Pratica

Con Low la SQL Injection nel corpo username permette l'accesso senza password

Con Medium la stessa iniezione non funzionava subito, il campo veniva in parte santizzato

Con High oltre alla sanitizzazione ho notato l'uso dei token CSFR nei form, mancandoli o inserendoli in modo errato, la richiesta falliva impedendo l'accesso.

Cosiderazioni finali

Dopo aver svolto gli esercizi adesso comprendo in modo pratico l'importanza dei **diversi livelli di sicurezza** in un'applicazione web.
Anche piccole modifiche nel codice o nella configurazione (come escaping, validazione o CSRF token) possono rendere molto più difficile l'exploit da parte di un attaccante.