

# Report Esercizio 11/12/2024

## Configurazione DVWA Leonardo Catalano

“La traccia di oggi ci chiedeva di fare una configurazione di una DVWA ovvero una damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i test.

Bisogna andare ad installare il Database MySql e il Web Server Apache.

I comandi sono i seguenti

```
root@kali: /var/www/html/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), 2.42 MiB | 4.27 MiB/s, done.
Resolving deltas: 100% (2420/2420), done.

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

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

All'interno del file config.inc.php si deve cambiare la password utente e password con 'kali'.

```
root@kali: /var/www/html/DVWA/config
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 = 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';

[ Wrote 56 lines ]
Help Write Out Where Is Cut Execute Location M-U Undo M-A Set Mark M-B To Bracket
Exit Read File Replace Paste Justify Go To Line M-B Redo M-G Copy M-B Where Was
```

Poi bisogna far partire il servizio mysql sempre in root quindi con i privilegi dell'amministratore, e poi ci andiamo a connettere al database.

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

(root@kali)-[~]
# service mysql start

(root@kali)-[~]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 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)]>
```

Ora creiamo un'utenza sul database e gli assegniamo i privilegi d'amministratore.

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

(root@kali)-[~]
# service mysql start

(root@kali)-[~]
# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 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 (0.008 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali';
Query OK, 0 rows affected (0.003 sec)

MariaDB [(none)]> exit
Bye

(root@kali)-[~]
```

Dopo bisogna configurare il servizio apache il web server andando a modificare dei

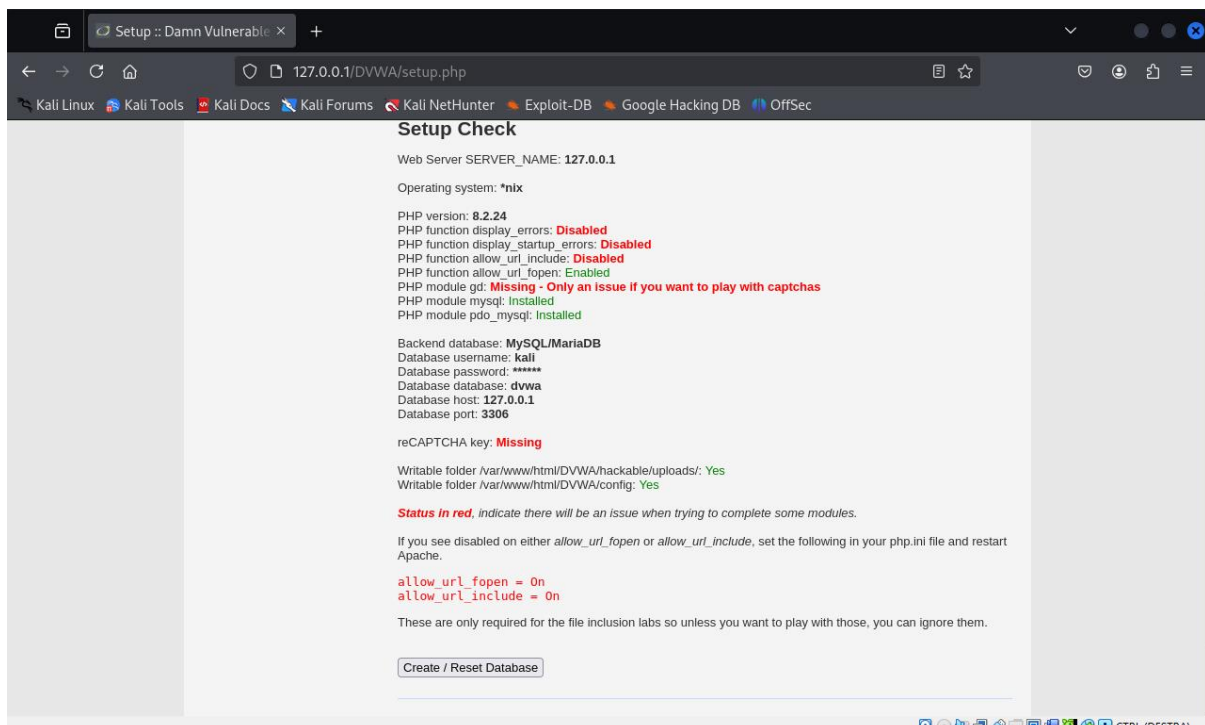
parametri interni. e dopo lo si avvia.

```
(root@kali)~# service apache2 start
(root@kali)~# cd /etc/php/
(root@kali)~/etc/php# ls
8.2
(root@kali)~/etc/php# cd /8.2/apache2
cd: no such file or directory: /8.2/apache2
(root@kali)~/etc/php# cd 8.2/apache2
(root@kali)~/etc/php/8.2/apache2# ls
conf.d  php.ini
(root@kali)~/etc/php/8.2/apache2# nano php.ini
(root@kali)~/etc/php/8.2/apache2# service apache2 start
apache: unrecognized service
(root@kali)~/etc/php/8.2/apache2# cd
(root@kali)~# service apache2 start
(root@kali)~#
```

```
; 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
```

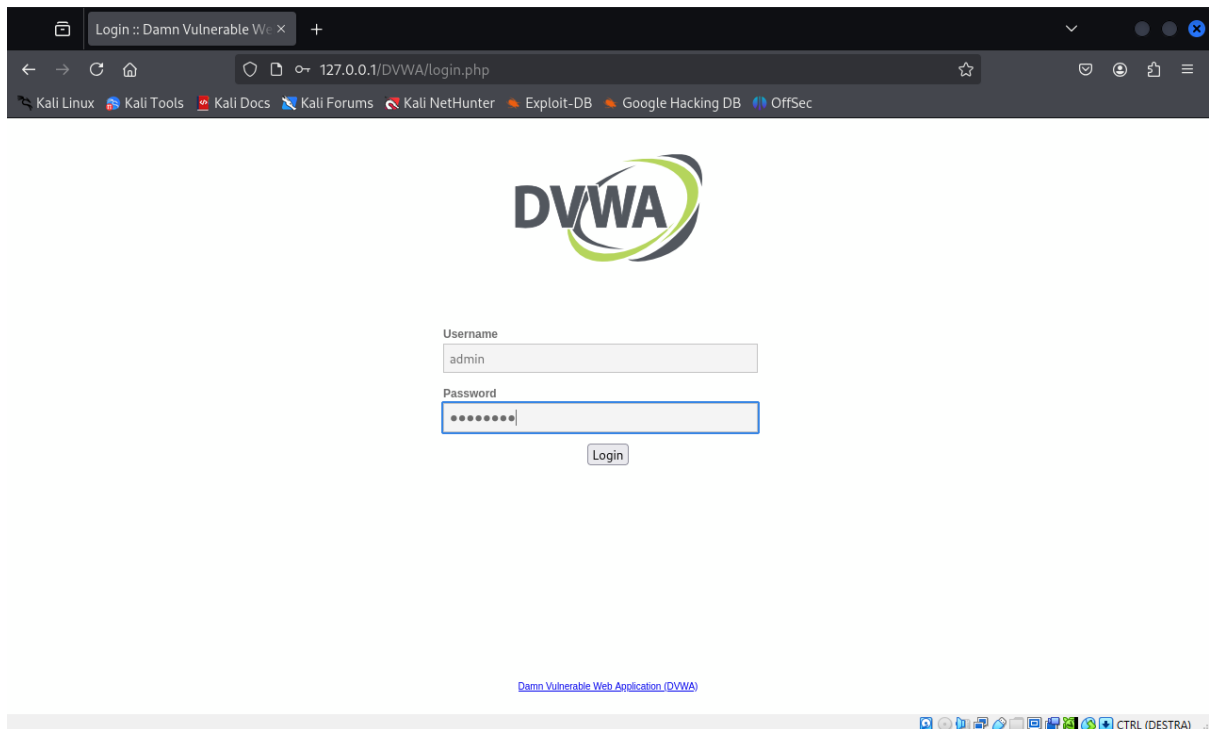
A questo punto che il server è aperto dal browser si va ad aprire una sessione con il seguente comando 127.0.0.1/DVWA/setup.php



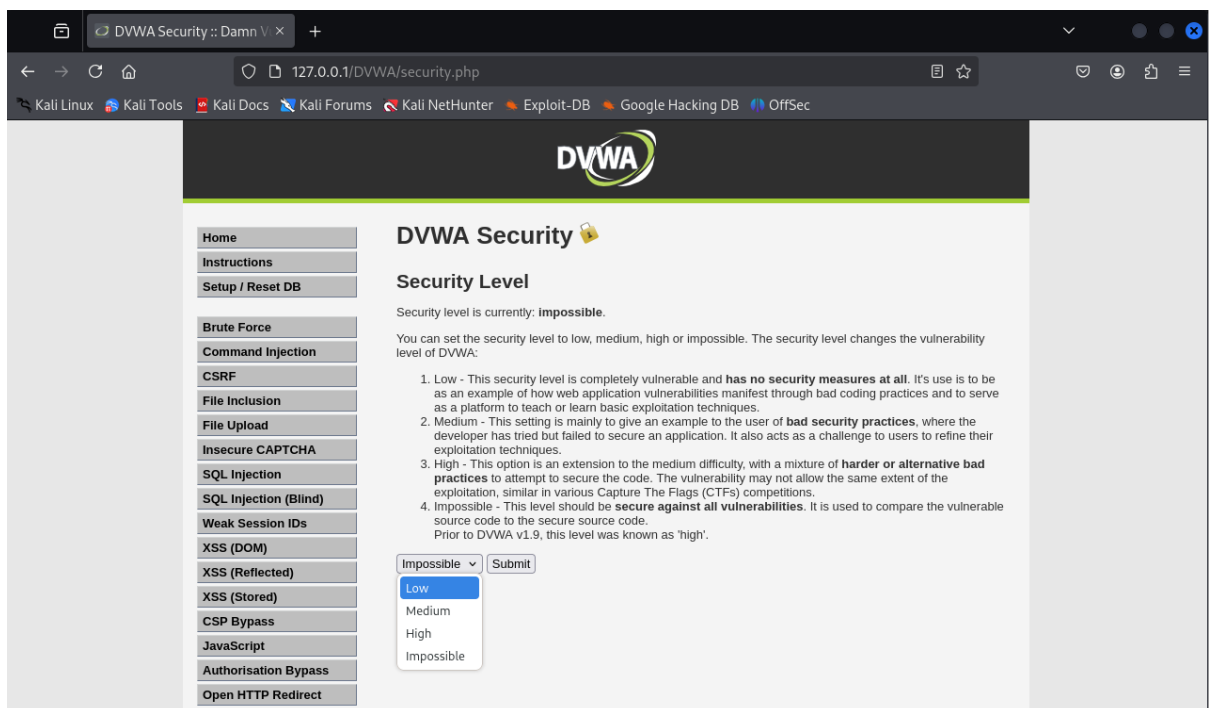
Bisogna andare a Creare/Resettare il Database, cliccando in basso Create/Reset Database.

Fatto ciò ci uscirà una finestra di login dove andremo ad inserire nome utente: admin e

password: password

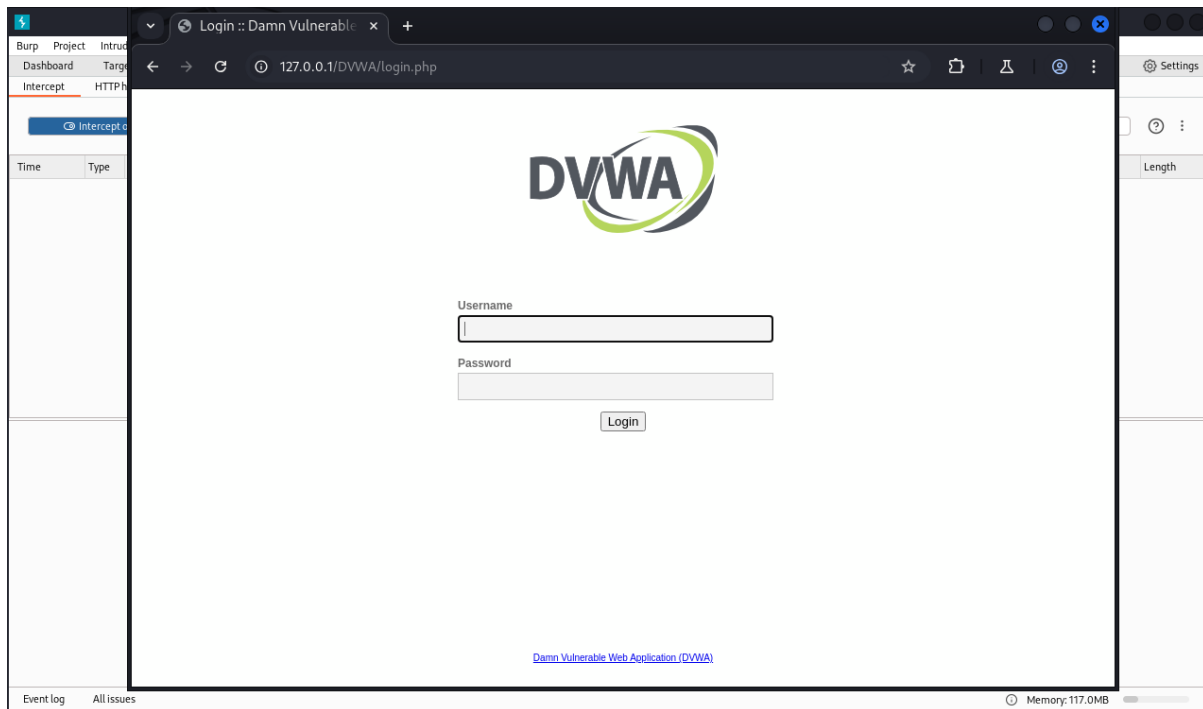


Una volta entrati su DVWA Security possiamo scegliere il livello di sicurezza dell'app.

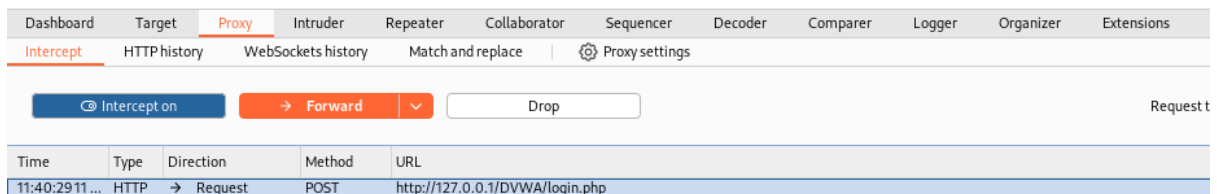


Ora che la nostra app è attiva, lanciamo Burpsuite, browser interno e inserendo l'indirizzo della nostra DVWA e inseriamo nei campi login e password i valori admin e password, intercettando la richiesta con burp andiamo a modificarla prima di inviare la

richiesta.



Apro barsuit, starto l'intercept e apro il browser, vado su 127.0.0.1, faccio un pò di volte forward finchè non mi esce la pagina di login, una volta uscita metto admin, password, login e torno su barsuit.



Qui possiamo modificare i campi inseriti di admin e password prima di inviare la richiesta all'app, per far funzionare il metodo però bisogna anche cambiare la security da impossibile a low.

Allora per far funziona il metodo sia proxy che repeater.

Repeater è una zona di test apparte dove puoi fare le prove che vuoi.

Puoi mandare la richiesta al repeater senza modificarla o la modifichi prima/dopo non cambia.

In questo caso l'ho modificata e l'ho mandata al repeater

The screenshot displays the Burp Suite Repeater interface. At the top, there's a navigation bar with tabs: Dashboard, Target, Proxy, Intruder, Repeater (selected), Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, and Extensions. Below this is a tab bar with tabs 1 x, 2 x, 3 x, 4 x (selected), and a plus icon. A 'Send' button is visible. The main area is split into two panels: 'Request' on the left and 'Response' on the right. The 'Request' panel has sub-tabs: Pretty (selected), Raw, and Hex. It shows an HTTP POST request to /DWWA/login.php. The request body contains a form submission with 'username=ciao&password=ciao&Login=Login&user\_token=ad7a1775b3d275953c5dcccfc25e5012'. The 'Response' panel is currently empty. At the bottom, there's a status bar showing 'Ready' and 'Event log'.

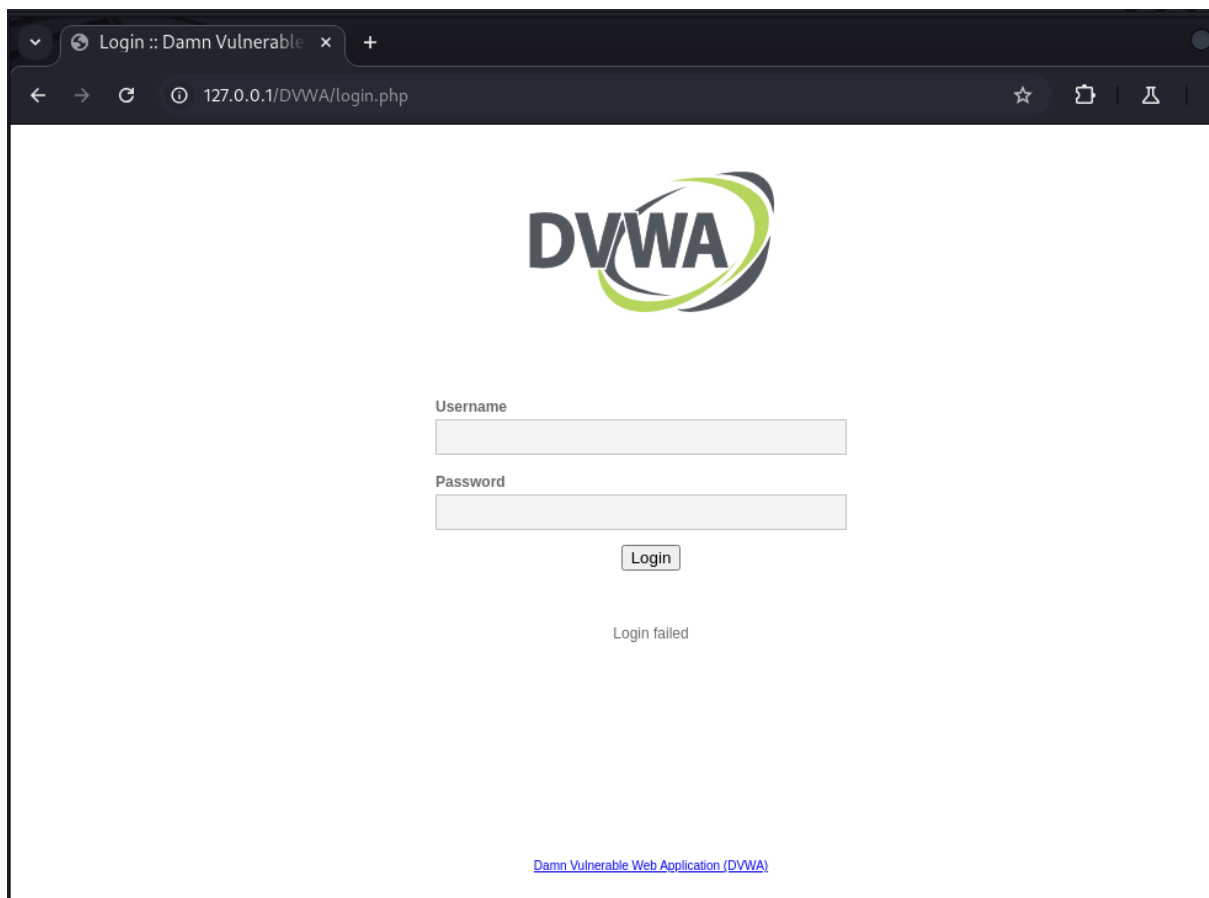
```
1 POST /DWWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not?A_Brand";v="99", "Chromium";v="130"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Accept-Language: en-US,en;q=0.9
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
  Safari/537.36
13 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DWWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: security=low; PHPSESSID=69o7rcp88p8t4nfsflat94mi0l
21 Connection:.keep-alive
22
23 username=ciao&password=ciao&Login=Login&user_token=
  ad7a1775b3d275953c5dcccfc25e5012
```

Per testare si fa Send e Follow redirection

E nel corpo (body) della risposta dell'html avremo login failed



Infine la pagina di output sarà :



Username

Password

Login

Login failed

[Damn Vulnerable Web Application \(DVWA\)](#)