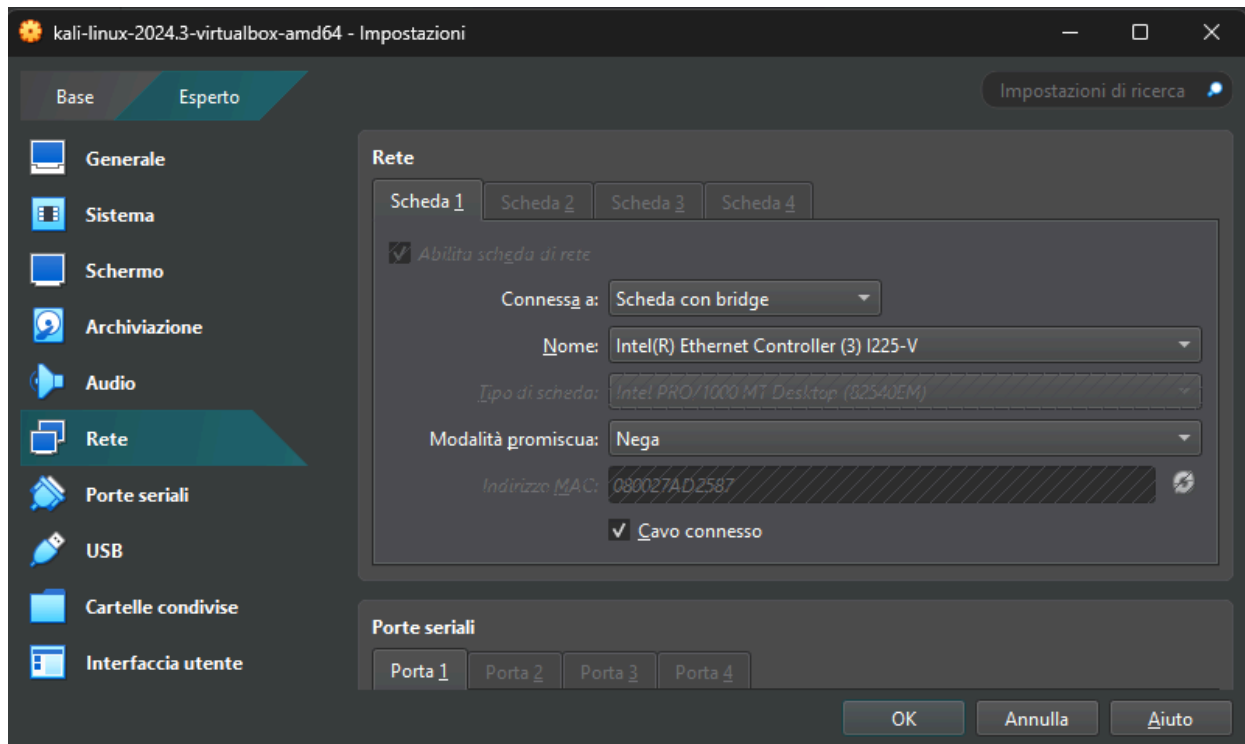


PRATICA S3L3

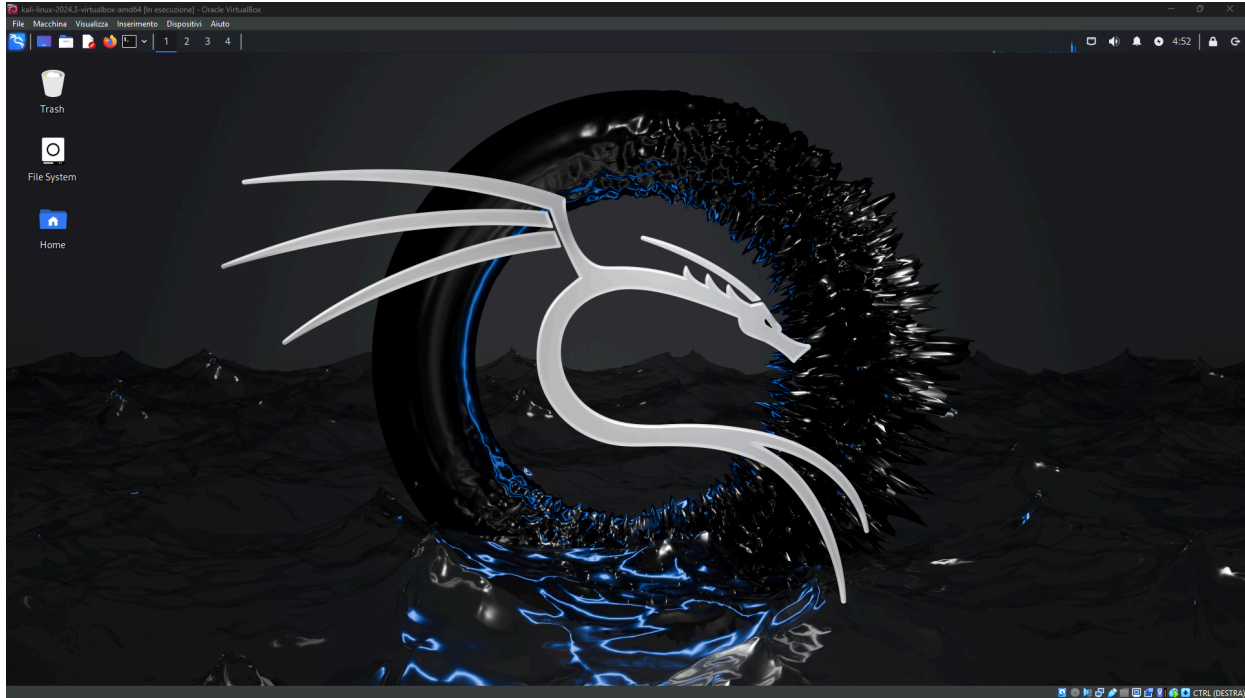
Nella lezione pratica di oggi si deve configurare una DVWA – ovvero damn vulnerable web application in Kali Linux.

1. Prerequisiti

Come prima cosa modifico la connettività ad internet dalle impostazioni macchina selezionando scheda con bridge:



Avvio la macchina per assicurarmi che la connettività sia attiva:



2. Installazione Database MySQL

Apri il terminale ed esegui "sudo su" per utilizzare l'utenza di root:

```
root@kali: /home/kali

File Actions Edit View Help

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
#
```

Poi esegui in ordine i seguenti comandi:

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

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

1. cd /var/www/html

2. 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: 4954, done.
remote: Counting objects: 100% (114/114), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 4954 (delta 69), reused 100 (delta 60), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.42 MiB | 4.89 MiB/s, done.
Resolving deltas: 100% (2421/2421), done.
```

3. chmod -R 777 DVWA/

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

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

4. cd DVWA/config

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

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

5. cp config.inc.php.dist config.inc.php

```
(root@kali)-[/var/www/html/DVWA/config]
# cp config.inc.php.dist config.inc.php

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

6. nano config.inc.php, e ottengo questa schermata

```
root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
GNU nano 8.1 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 = 'PostgreSQL'; // 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') ?: '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
# The 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';

[ Read 56 lines (converted from DOS format) ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^E Execute   ^_ Location  ^U Undo     ^-A Set Mark ^] To Bracket ^-P Previous ^_ Back
^X Exit      ^R Read File ^J Replace   ^N Paste     ^I Justify   ^G Go To Line ^-R Redo     ^-C Copy     ^_ Where Was ^-N Next     ^_ Forward
```

- 7.

Inserisco kali-kali nelle linee di codice db_user e db_password e salvo con Ctrl+o

```
root@kali: /var/www/html/DVWA
File Actions Edit View Help
GNU nano 8.1 config.inc.php
<?php
# If you are having problems connecting to the MySQL database and all of the variables below are c
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to socket
# 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';
```

Ora faccio partire il servizio mysql con il comando "service mysql start"; poi mi connetto al database con il comando "sudo mysql -u root".

```
(kali@kali)-[~]
$ sudo mysql -u root
[sudo] password for kali:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 36
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 assegniamo i privilegi all'utente Kali con il comando "grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;";

```
(kali㉿kali)-[~]
└─$ sudo mysql -u root
[sudo] password for kali:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
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 (0.003 sec)

MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by '
kali' ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corres
ponds to your MariaDB server version for the right syntax to use near ''kali'' at line
 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by '
kali' ;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> █
```

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":

```
kali@kali: /etc/
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ service apache2 start

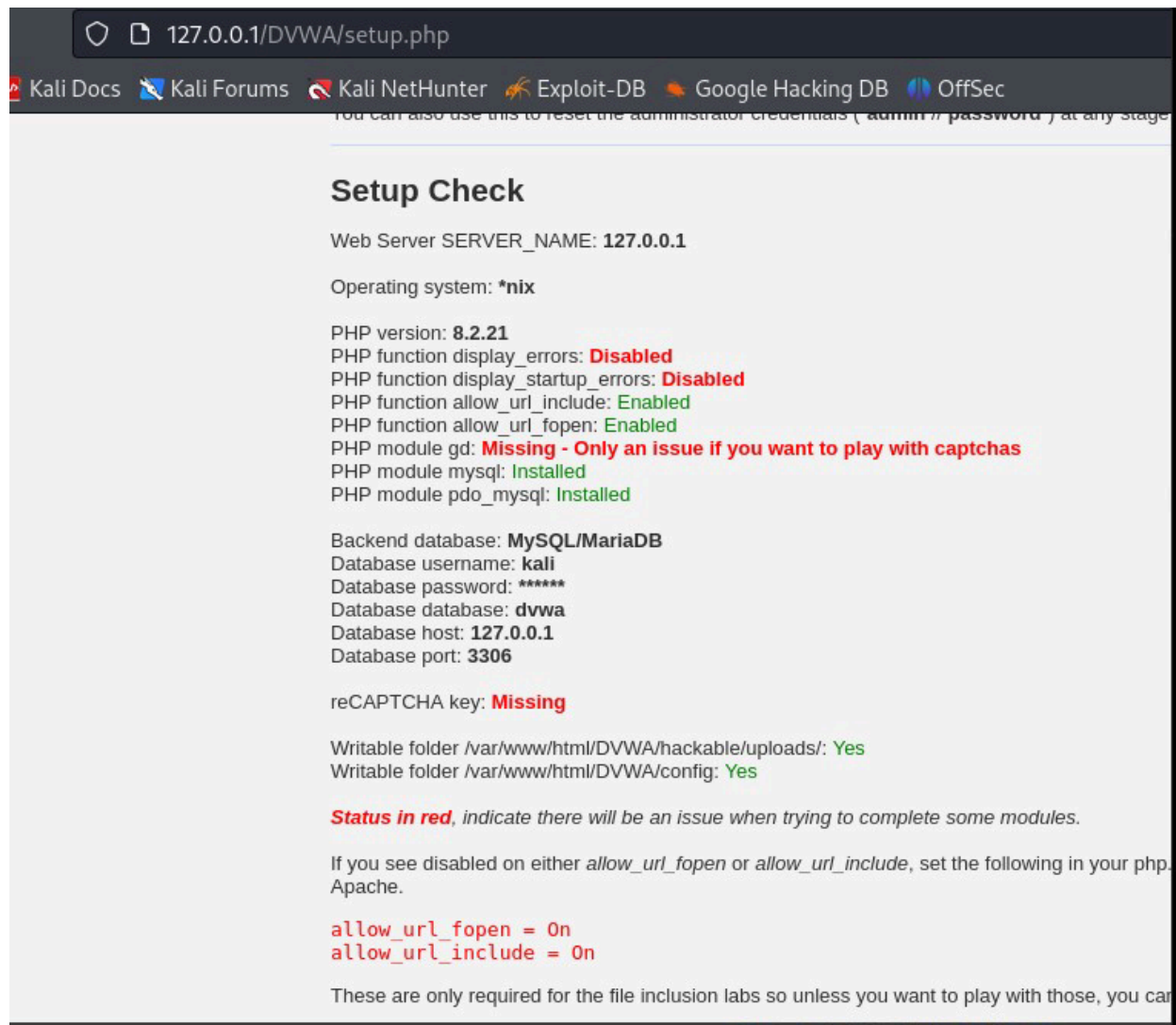
(kali㉿kali)-[~]
└─$ cd /etc/php/8.2/apache2

(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ █
```

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
```

Nel browser inserisco l'indirizzo "127.0.0.1/DVWA/setup.php":



127.0.0.1/DVWA/setup.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.2.21
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

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

reCAPTCHA key: Missing

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

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.
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

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



Username

Password

Login

[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](#)[Authorisation Bypass](#)

Welcome to Damn Vulnerable Web Application

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its goal is to be an aid for security professionals to test their skills and tools in a legal environment, to help developers better understand the processes of securing web applications and to aid both students and professionals 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 difficulty**, 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 pace, or by selecting any module and working up to reach the highest level they can before moving onto the next. It is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possibly could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. Some are 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 module. 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 or any Internet facing servers**, as they will be compromised. It is recommended to use a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest OS you can download and install [XAMPP](#) for the web server and database.

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

DVWA Security

Security Level

Security level is currently: **impossible**.

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 

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:

127.0.0.1/DVWA/login.php



Username

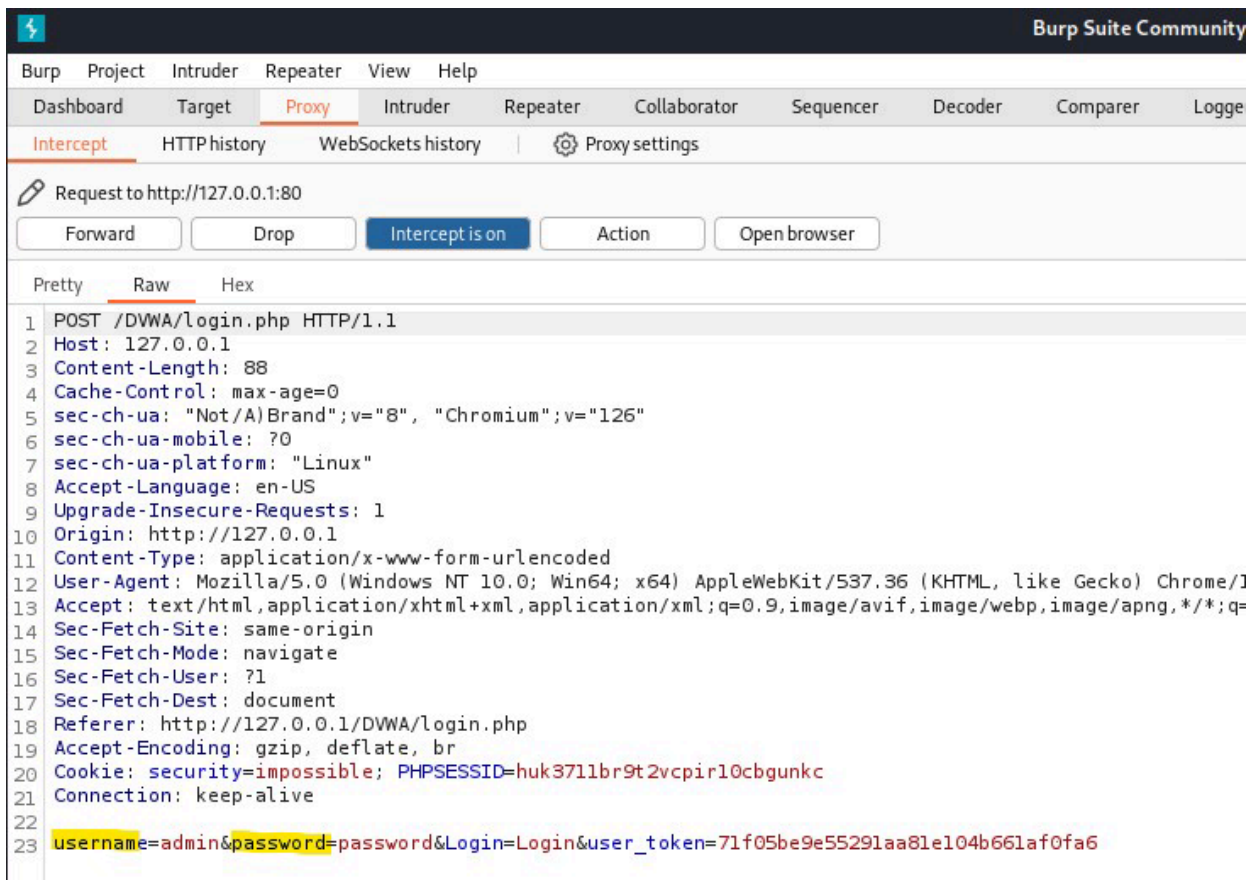
admin

Password

.....

Login

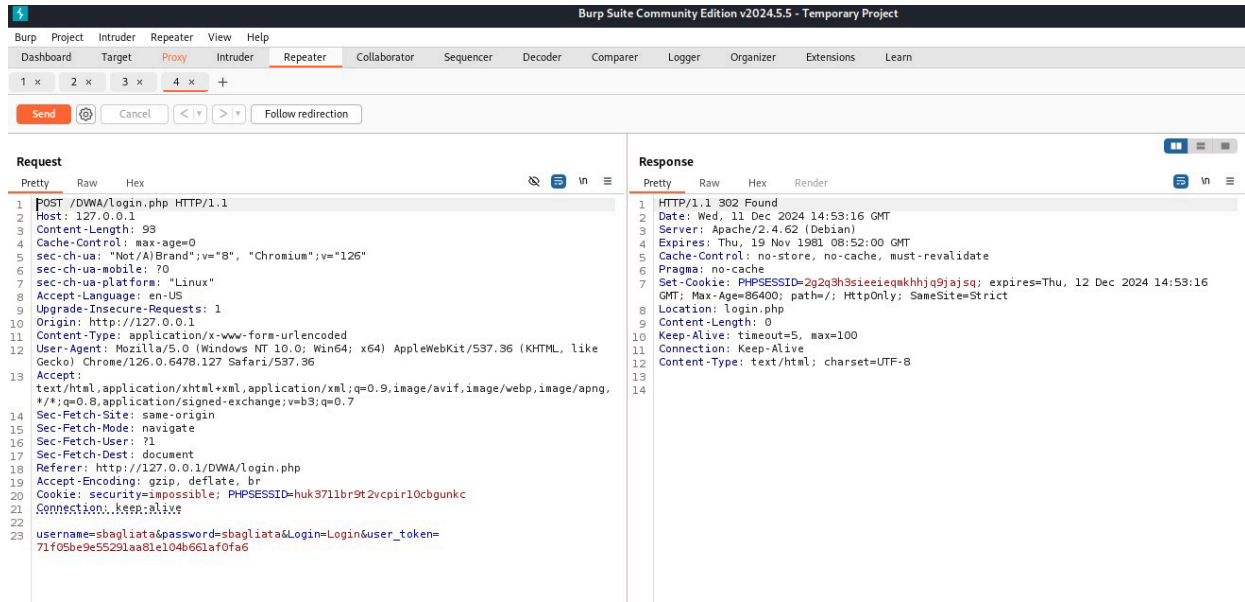
Intercettiamo il traffico con burpsuite e vediamo di modificarla:



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:

