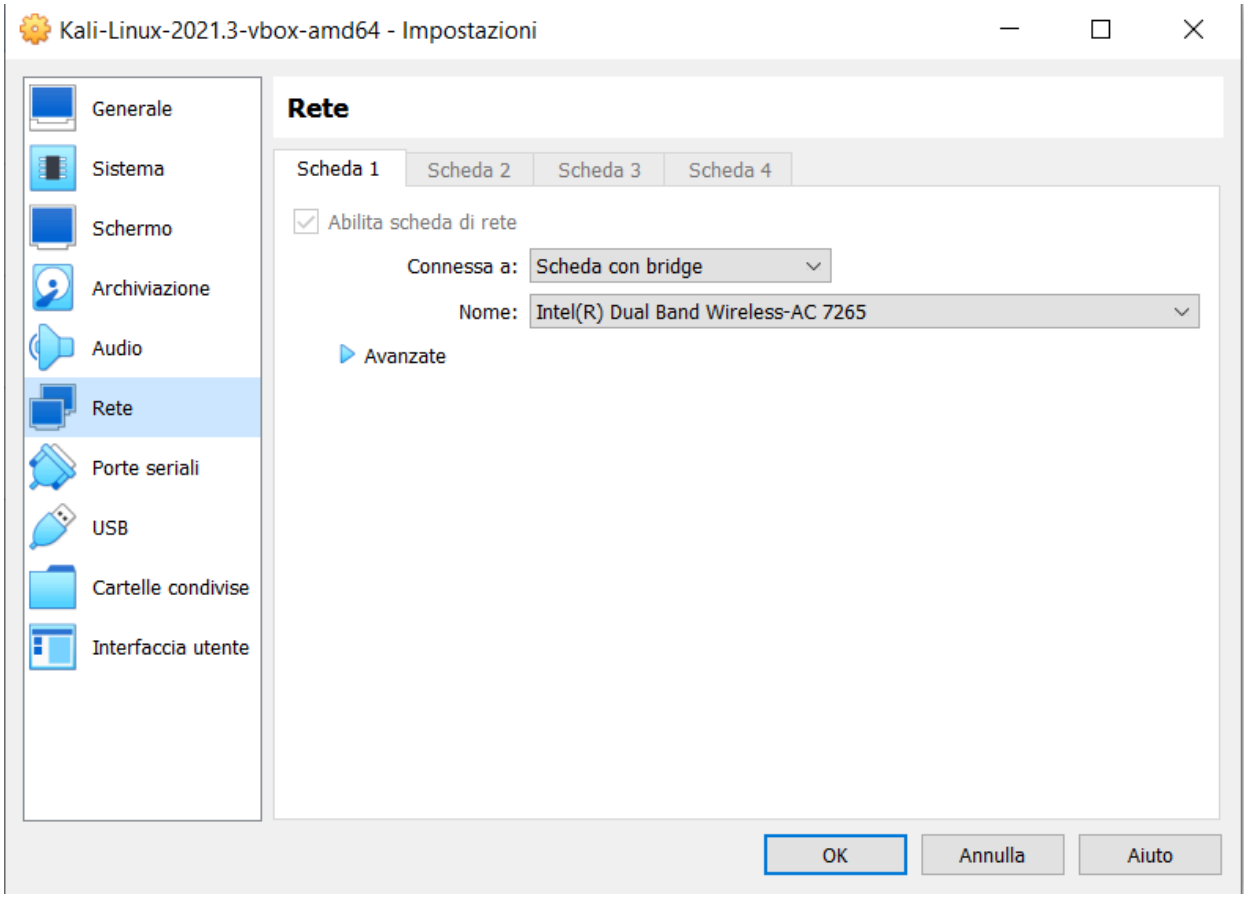
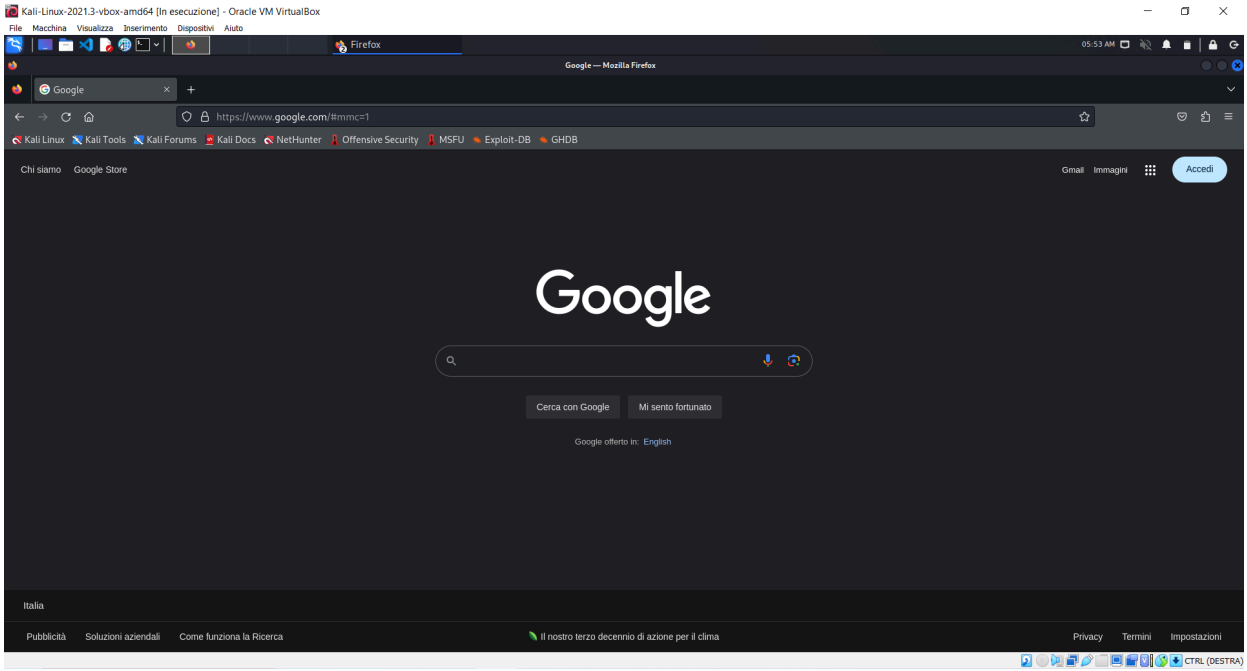
Verifica scheda di rete macchina Kali



Verifica accesso internet



Installazione DVWA

```
┌──(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: 4590, done.
remote: Counting objects: 100% (140/140), done.
remote: Compressing objects: 100% (103/103), done.
remote: Total 4590 (delta 58), reused 101 (delta 36), pack-reused 4450
Receiving objects: 100% (4590/4590), 2.34 MiB | 6.09 MiB/s, done.
Resolving deltas: 100% (2153/2153), done.

┌──(root💀kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
chmod: invalid mode: '-R'
Try 'chmod --help' for more information.

┌──(root💀kali)-[/var/www/html]
└─# chmod -r 777 DVWA/
chmod: invalid mode: '-r'
Try 'chmod --help' for more information.

┌──(root💀kali)-[/var/www/html]
└─# chmod --help
Usage: chmod [OPTION]... MODE[,MODE]... FILE...
  or:  chmod [OPTION]... OCTAL-MODE FILE...
  or:  chmod [OPTION]... --reference=RFILE FILE...
Change the mode of each FILE to MODE.
With --reference, change the mode of each FILE to that of RFILE.

  -c, --changes          like verbose but report only when a change is made
  -f, --silent, --quiet  suppress most error messages
  -v, --verbose          output a diagnostic for every file processed
      --no-preserve-root  do not treat '/' specially (the default)
      --preserve-root    fail to operate recursively on '/'
      --reference=RFILE  use RFILE's mode instead of specifying MODE values.
                         RFILE is always dereferenced if a symbolic link.
  -R, --recursive        change files and directories recursively
      --help        display this help and exit
      --version     output version information and exit

Each MODE is of the form '[ugoa]*([-+=]([rwxXst]*|[ugo]))+|[-+=][0-7]+'.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/chmod>
or available locally via: info '(coreutils) chmod invocation'
```

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

```
┌──(root💀kali)-[/var/www/html]
└─# ls -alt
total 28
drwxrwxrwx 12 root root  4096 Jun 25 05:54 DVWA
drwxr-xr-x  3 root root  4096 Jun 25 05:54 .
-rw-r--r--  1 root root 10701 Sep  8  2021 index.html
-rw-r--r--  1 root root   612 Sep  8  2021 index.nginx-debian.html
drwxr-xr-x  3 root root  4096 Sep  8  2021 ..
```

```
┌──(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
```

Modifica file config.inc.php. User: kali, password: kali

```
 GNU nano 8.0                                                    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
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ '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' ] = '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' ] = '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' ] = false;

define ('MYSQL', 'mysql');
define ('SQLITE', 'sqlite');

# SQLi DB Backend
#   Use this to switch the backend database used in the SQLi and Blind SQLi labs.
```

```
┌──(root💀kali)-[/var/www/html/DVWA/config]
└─# service mysql start

┌──(root💀kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
mysql  Ver 15.1 Distrib 10.5.12-MariaDB, for debian-linux-gnu (x86_64) using  EditLine wrapper
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Usage: mysql [OPTIONS] [database]

Default options are read from the following files in the given order:
/etc/my.cnf /etc/mysql/my.cnf ~/.my.cnf
The following groups are read: mysql mariadb-client client client-server client-mariadb
The following options may be given as the first argument:
--print-defaults          Print the program argument list and exit.
--no-defaults             Don't read default options from any option file.
The following specify which files/extra groups are read (specified before remaining options):
--defaults-file=#         Only read default options from the given file #.
--defaults-extra-file=#   Read this file after the global files are read.
--defaults-group-suffix=# Additionally read default groups with # appended as a suffix.

  -?, --help          Display this help and exit.
  -I, --help          Synonym for -?
  --abort-source-on-error
                      Abort 'source filename' operations in case of errors
  --auto-rehash       Enable automatic rehashing. One doesn't need to use
                      'rehash' to get table and field completion, but startup
```

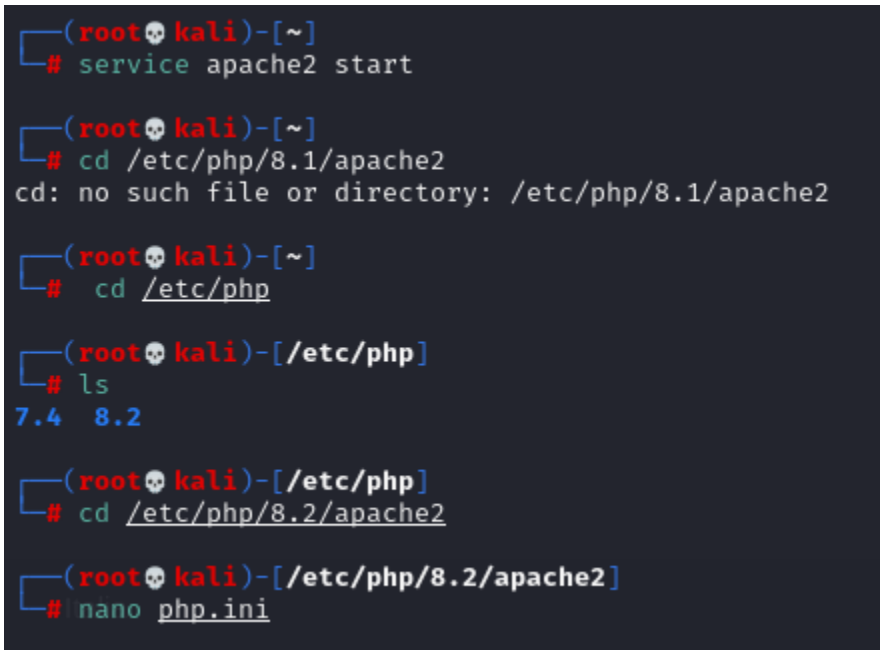
Partenza servizio db - *comando: systemctl start mariadb*

Creazione utenza e assegnazione privilegi all'utente kali

```
┌──(root💀kali)-[~]
└─# mysql -u root -p

Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 10.5.12-MariaDB-1 Debian 11

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 (0.014 sec)
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> SHOW GRANTS FOR 'kali'@'127.0.0.1';
+-----------------------------------------------------------------------------------------------------------------+
| Grants for kali@127.0.0.1                                                                                       |
+-----------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `kali`@`127.0.0.1` IDENTIFIED BY PASSWORD '*D64F6611CF18EA567ED1E8E74F2243AC1EDF54C4' |
| GRANT ALL PRIVILEGES ON `dvwa`.* TO `kali`@`127.0.0.1`                                                          |
+-----------------------------------------------------------------------------------------------------------------+
2 rows in set (0.000 sec)

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

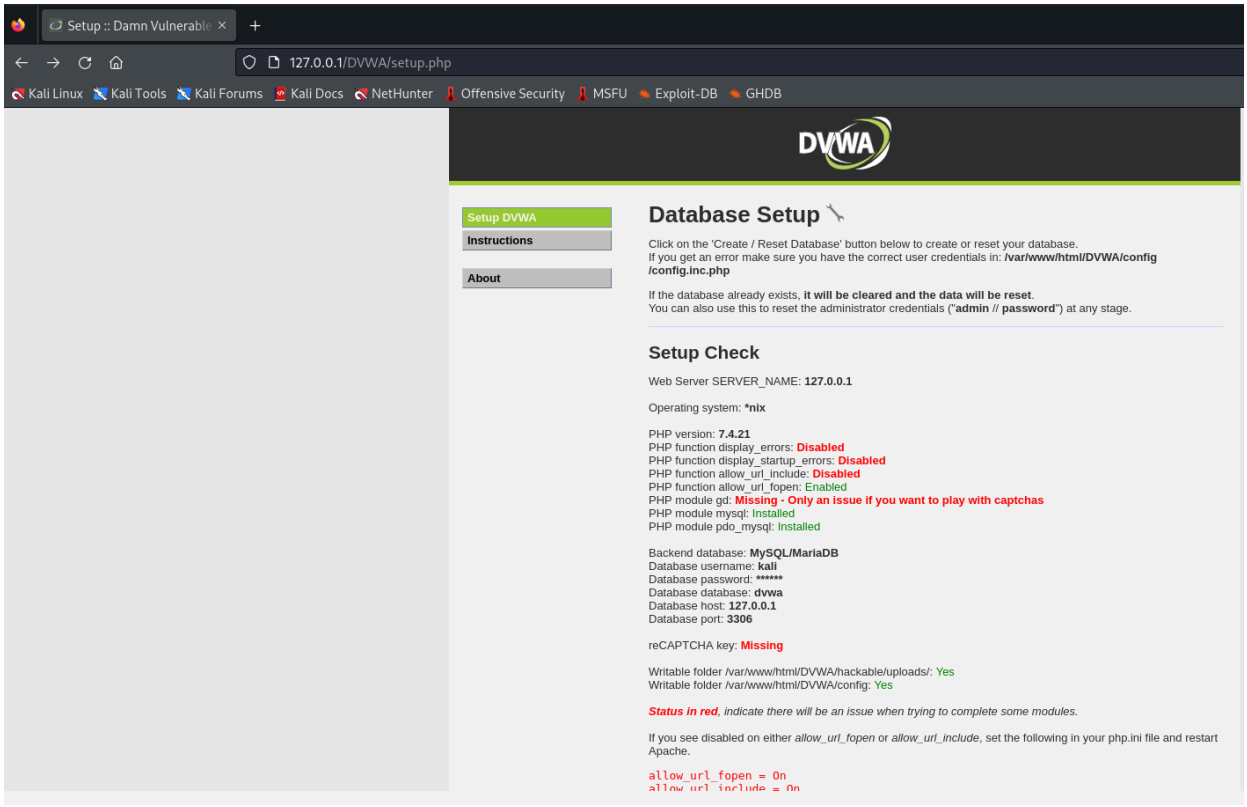
Partenza servizio apache e modifica voci *allow_url_fopen* **e** *allow_url_include* **su file php.ini**



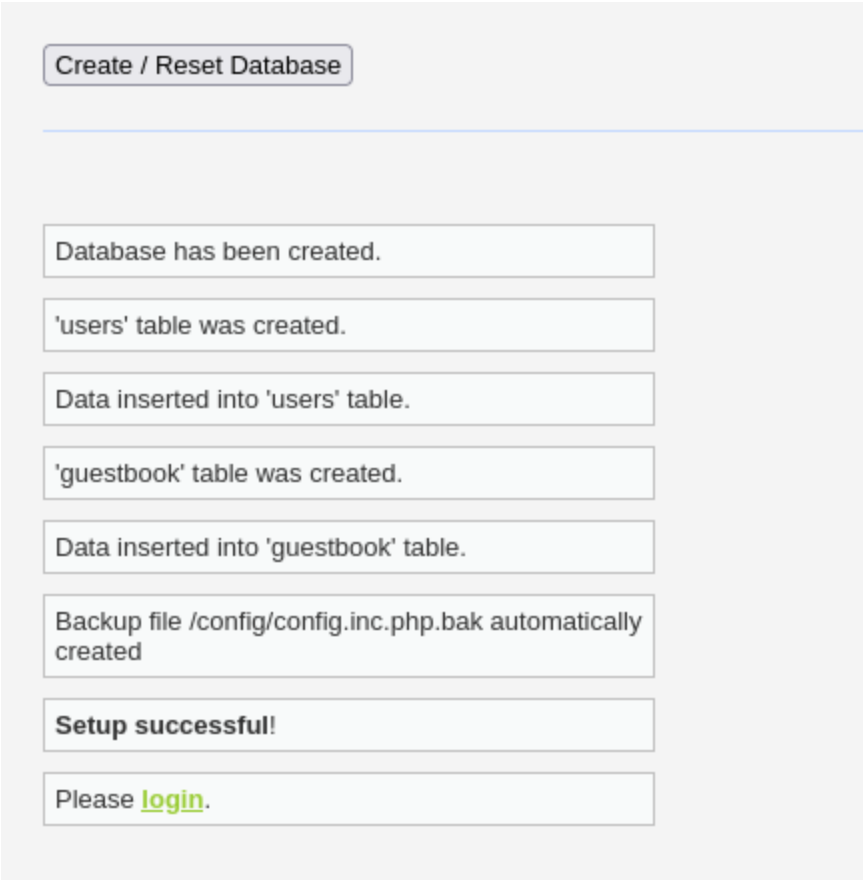
```
 GNU nano 8.0                                                    php.ini *
;cgi.rfc2616_headers = 0

; cgi.check_shebang_line controls whether CGI PHP checks for line starting with #!
; (shebang) at the top of the running script. This line might be needed if the
; script support running both as stand-alone script and via PHP CGI<. PHP in CGI
; mode skips this line and ignores its content if this directive is turned on.
; https://php.net/cgi.check-shebang-line
;cgi.check_shebang_line=1

;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;

; 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"
```

Partenza servizio apache e sessione browser su 127.0.0.1/DVWA/setup.php

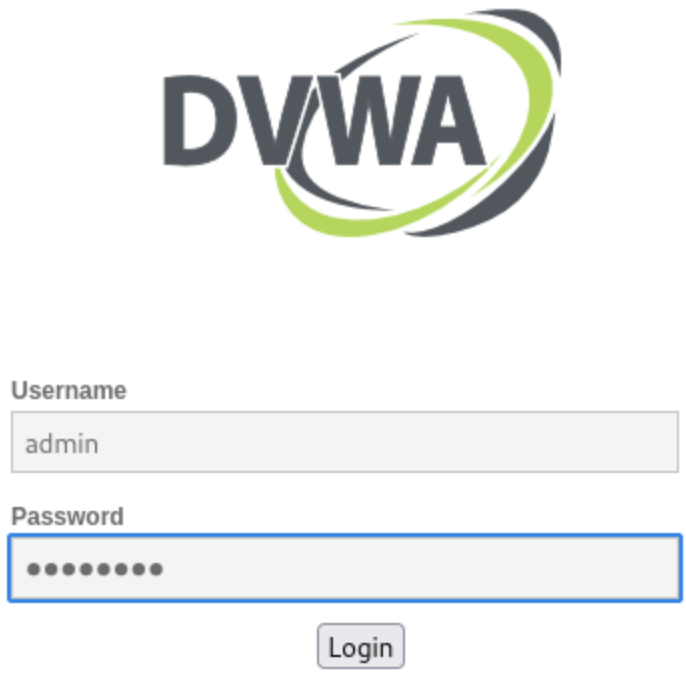
```
┌──(root💀kali)-[/etc/php/8.2/apache2]
└─# service apache2 start
```



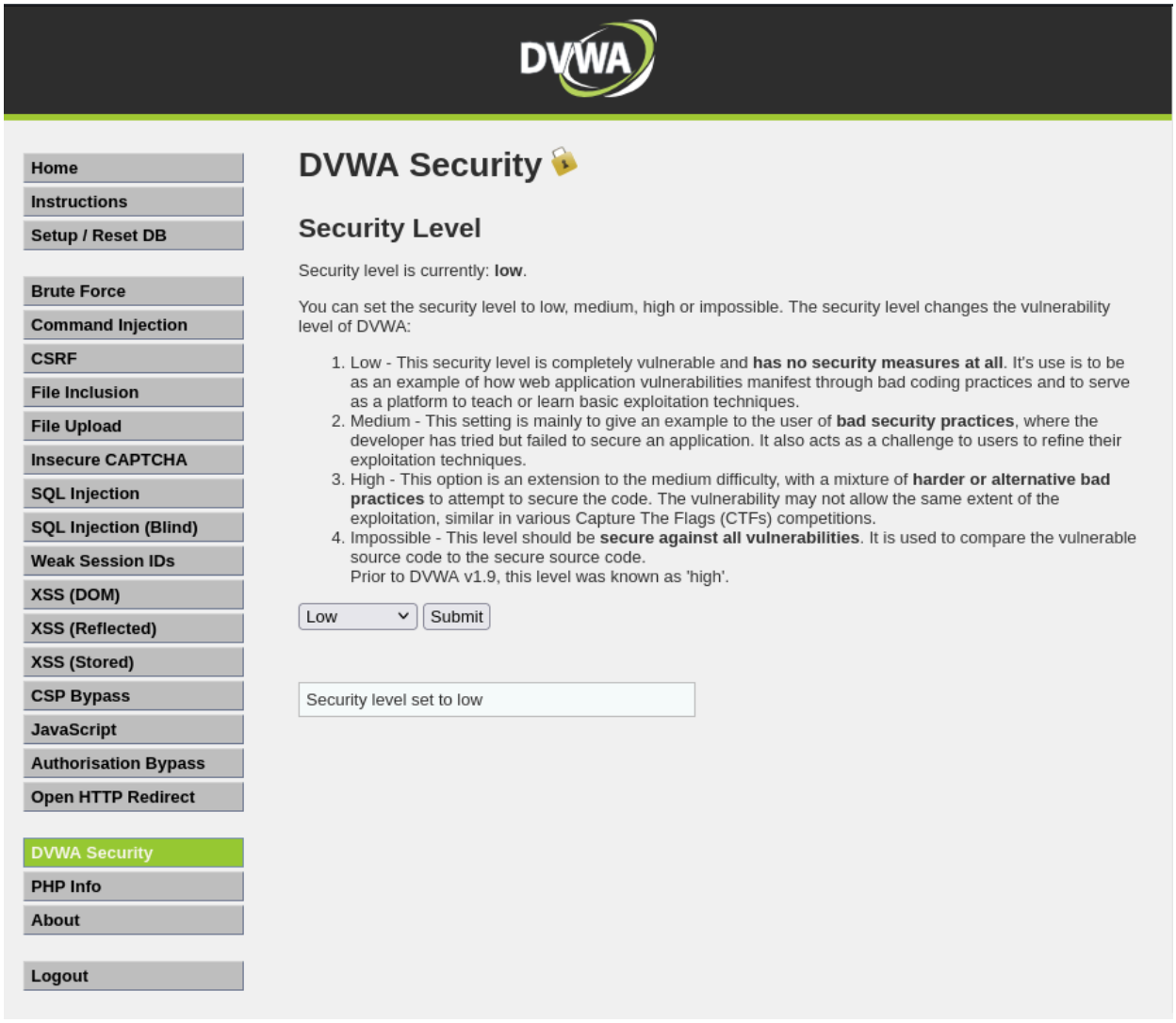
Creazione database



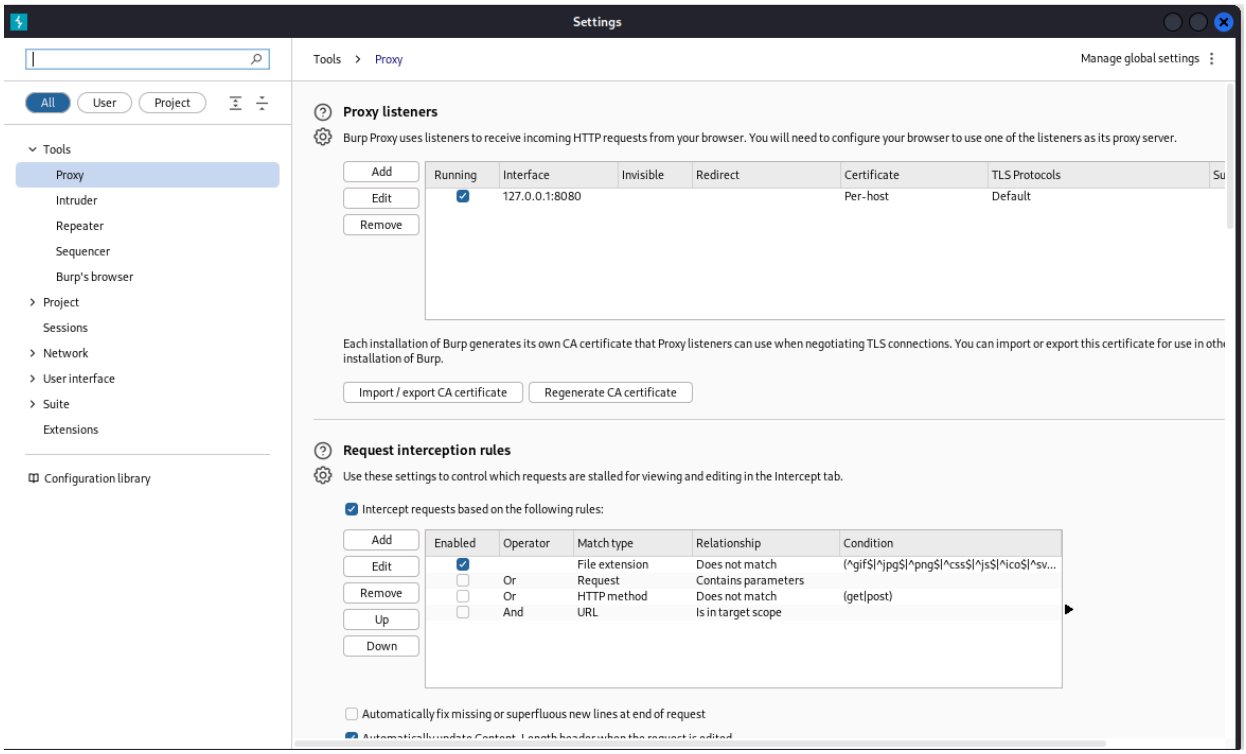
Login
Username: admin
password: password



Impostazione livello di sicurezza su “low”

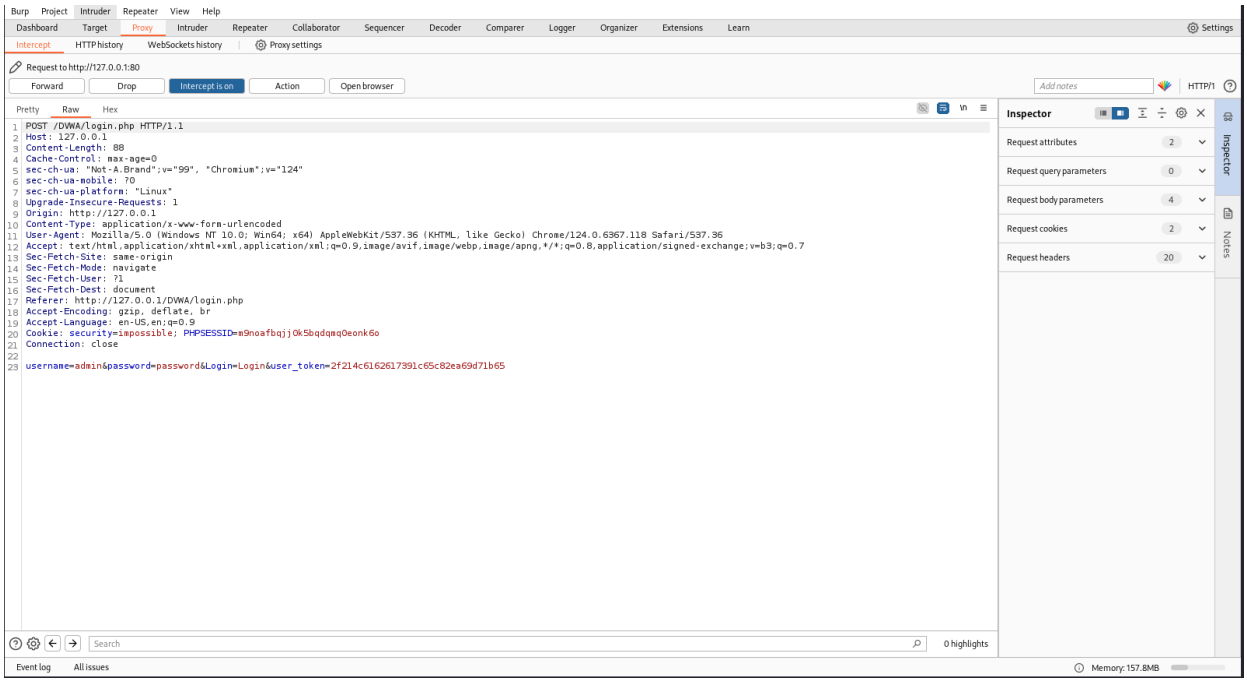


Verifica configurazione servizio proxy su Burpsuite

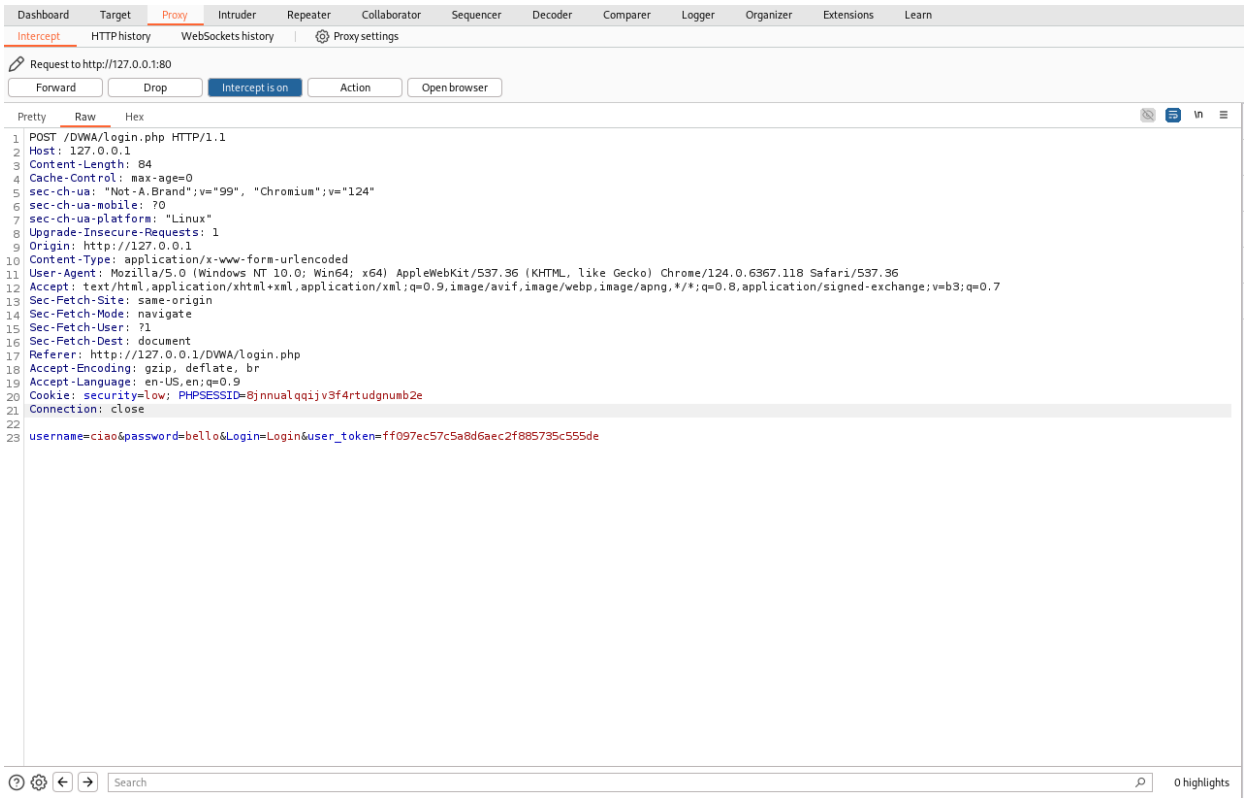


Utilizzo Burpsuite

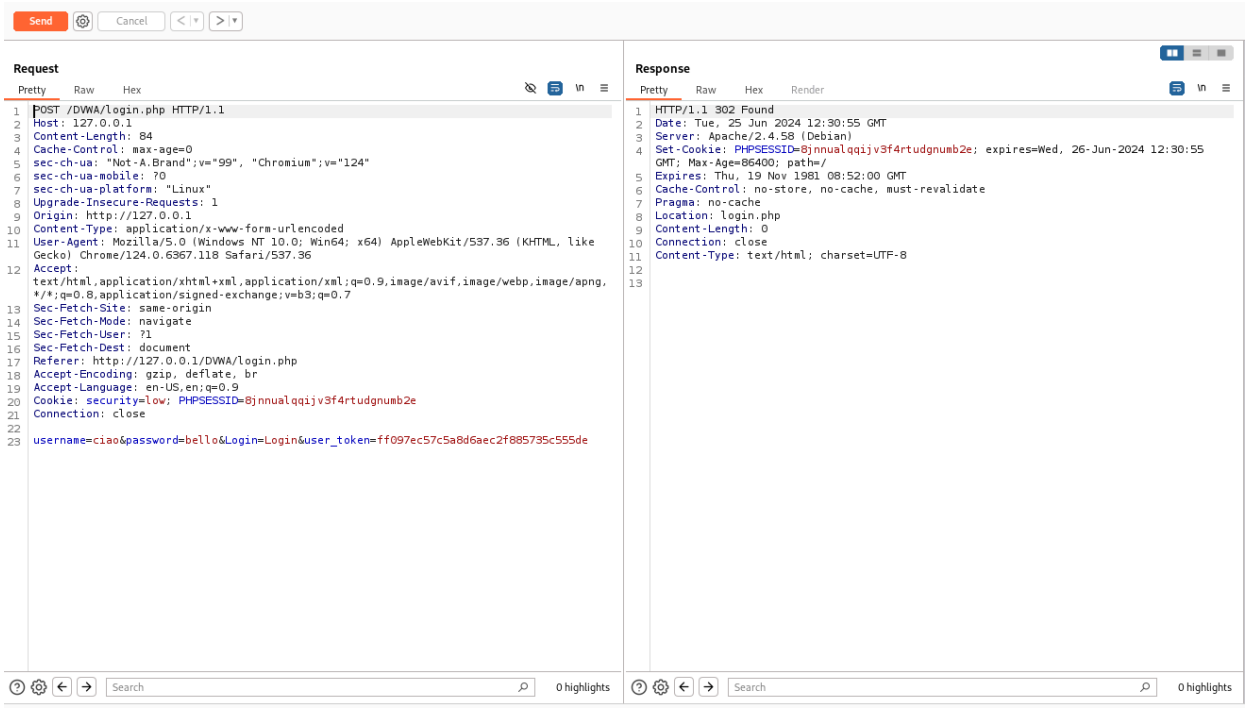
Dopo aver inserito l'indirizzo 1270.0.1/DVWA nel browser di Burpsuite, essere arrivati alla schermata di login e aver inserito nome utente e password, facciamo click su forward per passare dalla richiesta GET alla richiesta POST:



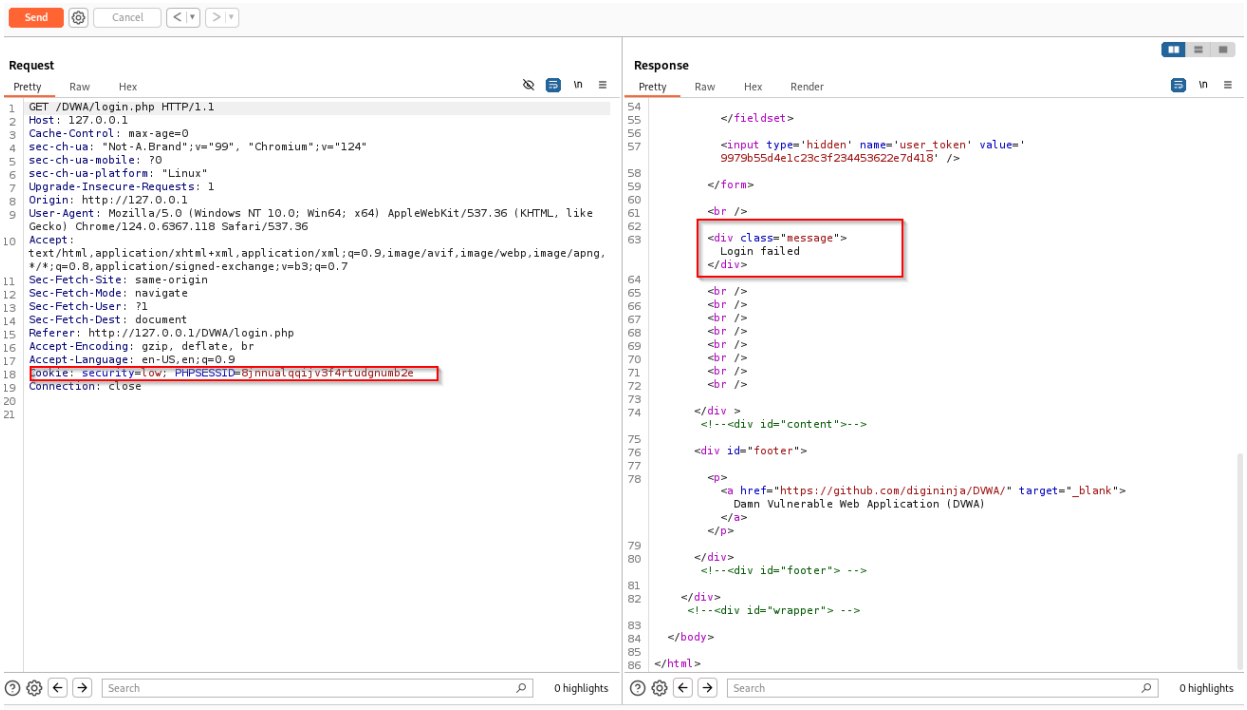
Proviamo a modificare i campi, ed inviare la richiesta inserendo delle credenziali sicuramente errate.

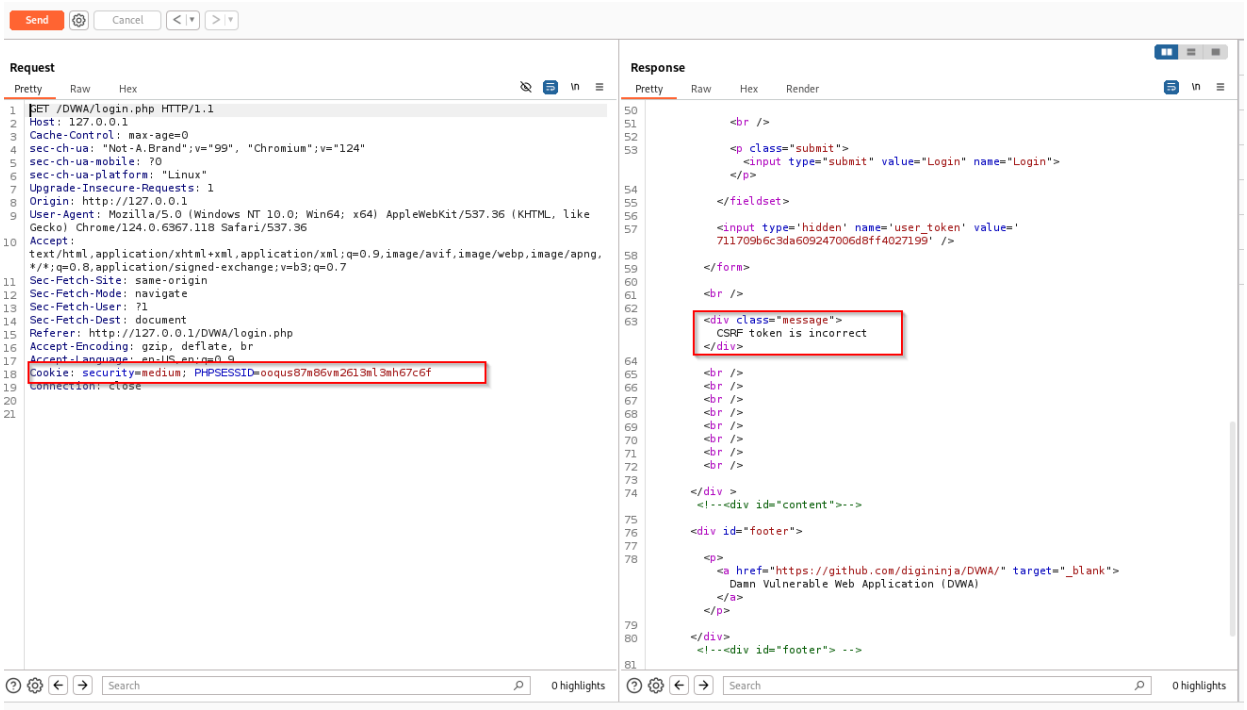


Prima di inviare la richiesta, clicchiamo con il tasto destro e selezioniamo «send to repeater» Clicchiamo su send per inviare la richiesta di login e poi su follow redirection. Livello sicurezza impostato: **Low**



Con le credenziali errate non si riesce a effettuare il login. Nel body della http response leggiamo «Login failed»





Per implementare un livello di sicurezza contro i brute force attacks nelle web app, spesso vengono incorporati nelle applicazioni dei token CSRF (Cross-Site Request Forgery) che sono sequenze random e difficili da indovinare. Le web app con un livello di sicurezza più elevato necessitano di un token CSRF che sia unico per ogni richiesta, di modo da ovviare a molteplici tentativi di indovinare le credenziali corrette per effettuare il login. Quindi se proviamo a cambiare le credenziali nella stessa sessione, riceveremo un messaggio relativo al CSRF scorretto.