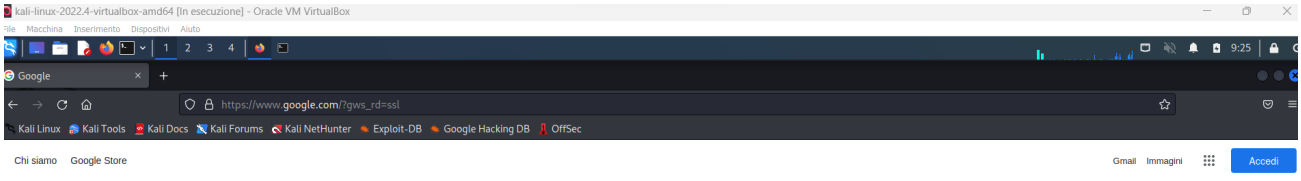
Configurazione DVWA in Kali Linux

Dopo aver modificato le impostazioni della scheda di rete (da internal a Bridged) e dopo aver selezionato da terminale "sudo nano /etc/network/interfaces", per modificare l'indirizzo statico con quello dinamico, la macchina Kali Linux ha accesso a internet.



Dopo aver inserito su terminale le istruzioni forniteci nell'esercizio nell'editor di testo, modifico user e password inserendo "kali" in entrambi gli sheet.

```
 GNU nano 6.4
?php

 If you are having problems connecting to the MySQL database and all of the variables below are cor
 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' ]   = '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 impos
_DVWA[ 'default_security_level' ] = 'impossible';

 Default PHPIDS status
   PHPIDS status with each session.
   The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
_DVWA[ 'default_phpids_level' ] = 'disabled';

 Verbose PHPIDS messages
   Enabling this will show why the WAF blocked the request on the blocked request.
   The default is 'disabled'. You can set this to be either 'true' or 'false'.
_DVWA[ 'default_phpids_verbose' ] = 'false';
```

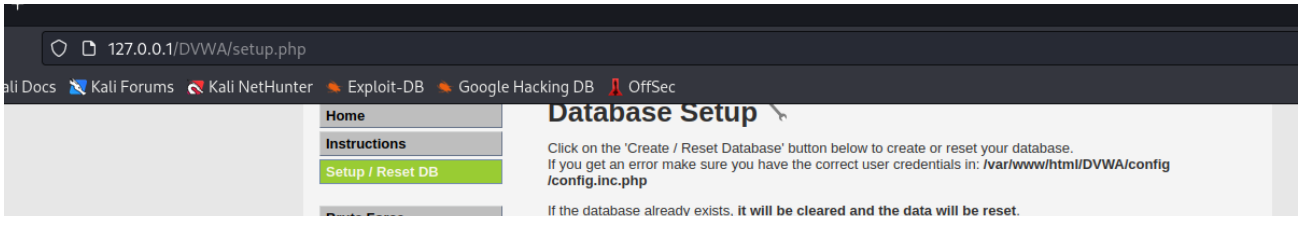
Creare un'utenza sul DB e assegnare i privilegi all'utente kali, usando mysql, nel modo seguente:

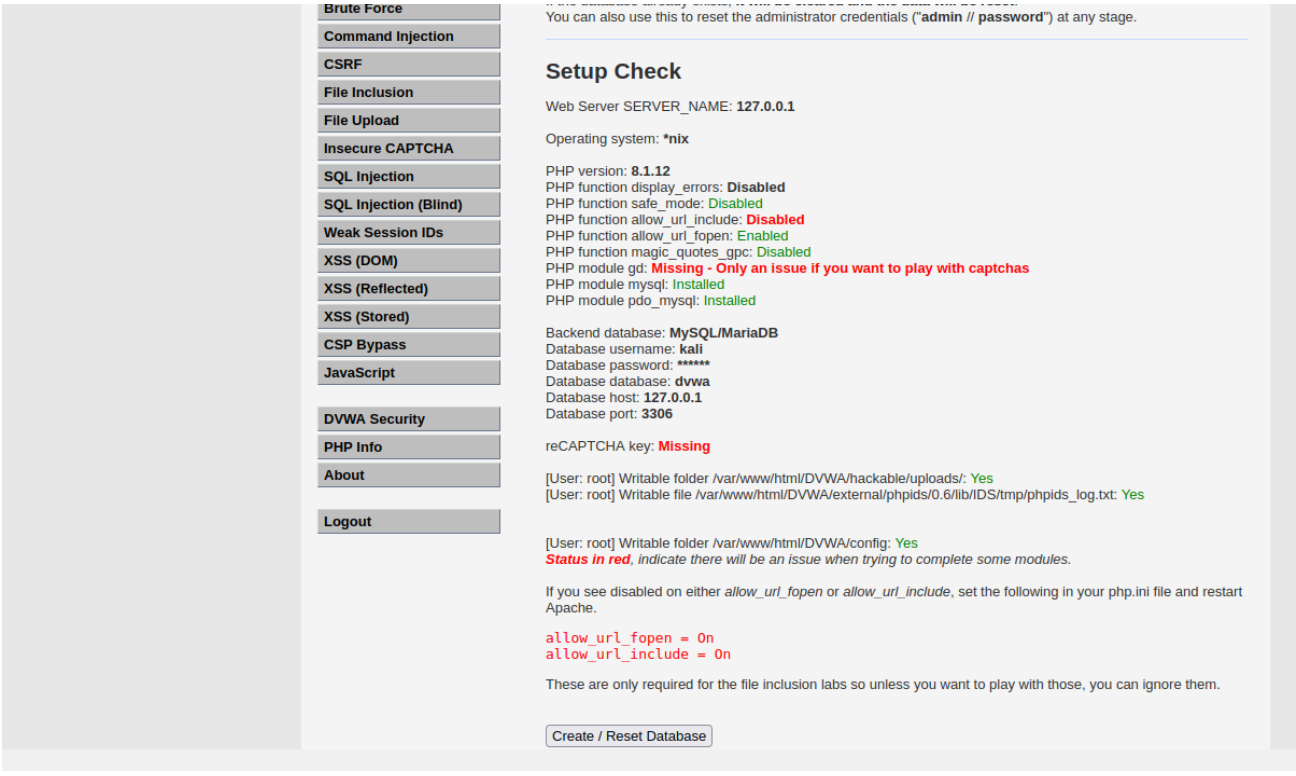
```
┌──(root㉿kali)-[~]
└─# service mysql start

┌──(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: 10.6.10-MariaDB-1+b1 Debian n/a

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 (0.023 sec)

[redacted]
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
```

A questo punto, procedo a configurare apache. Dopo essermi accertato che la versione presente su kali sia 8.1 apro la cartella php.ini su nano e configuro "allow_url_include" su ON.

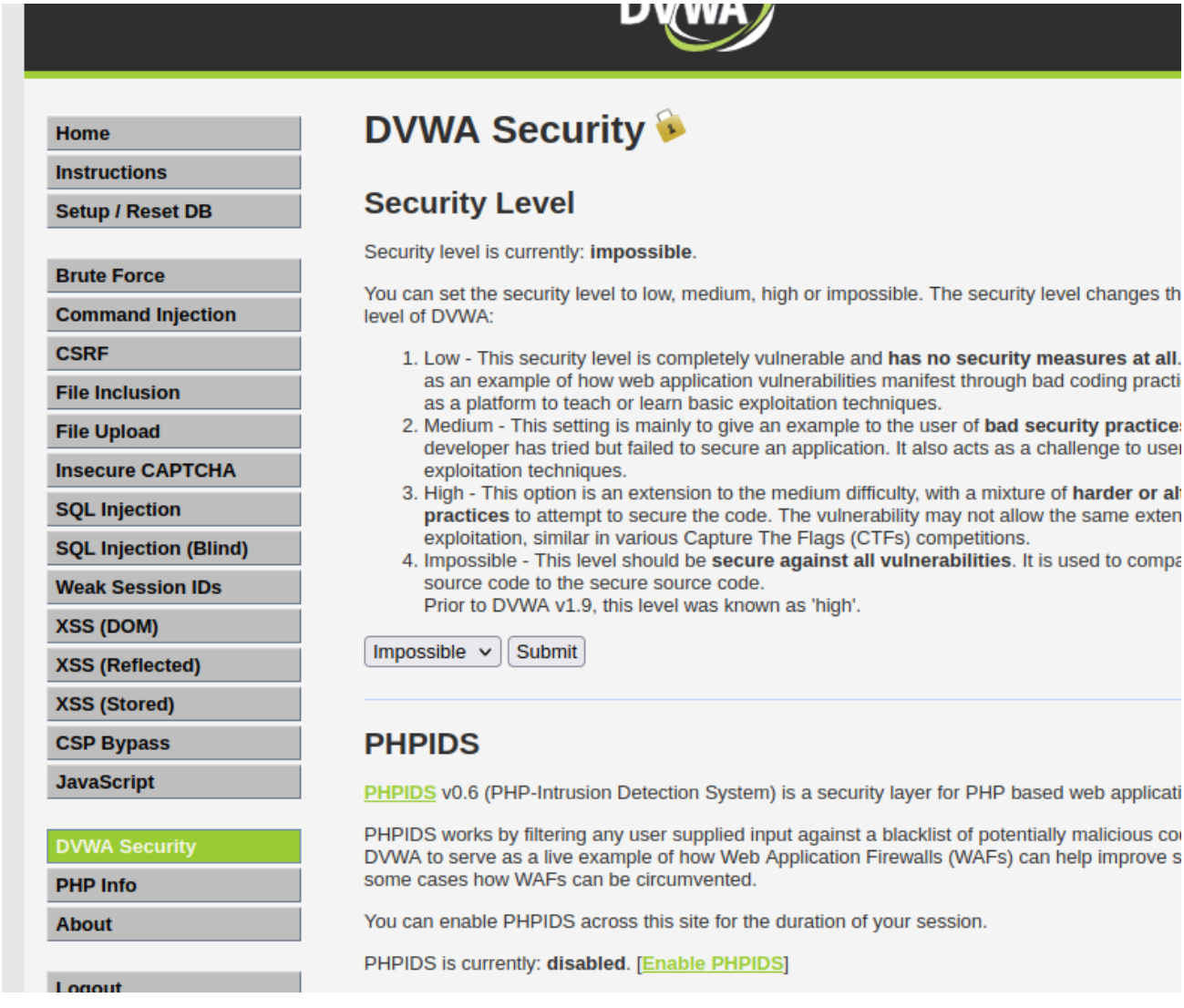
```
┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─# cd /etc/php/

┌──(root㉿kali)-[/etc/php]
└─# ls
8.1

┌──(root㉿kali)-[/etc/php]
└─# nano php.ini

┌──(root㉿kali)-[/etc/php]
└─# cd /etc/php/8.1/apache2

┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─# nano php.ini

┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─# service apache2 start

┌──(root㉿kali)-[/etc/php/8.1/apache2]
└─#
```

Andando sul browser ed inserendo "127.0.0.1/DVWA/setup.php nella barra degli indirizzi, mi si aprirà una schermata, da cui potrò creare/resettare un database.



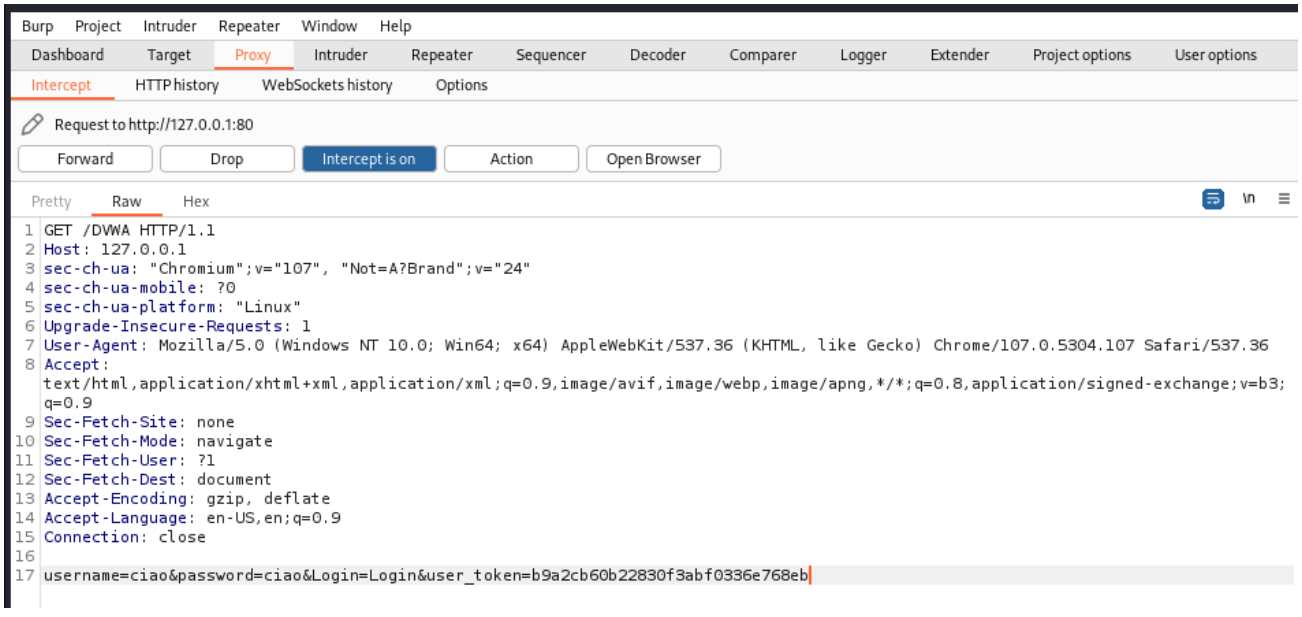


Seleziono DVWA Security dove posso impostare il livello di sicurezza

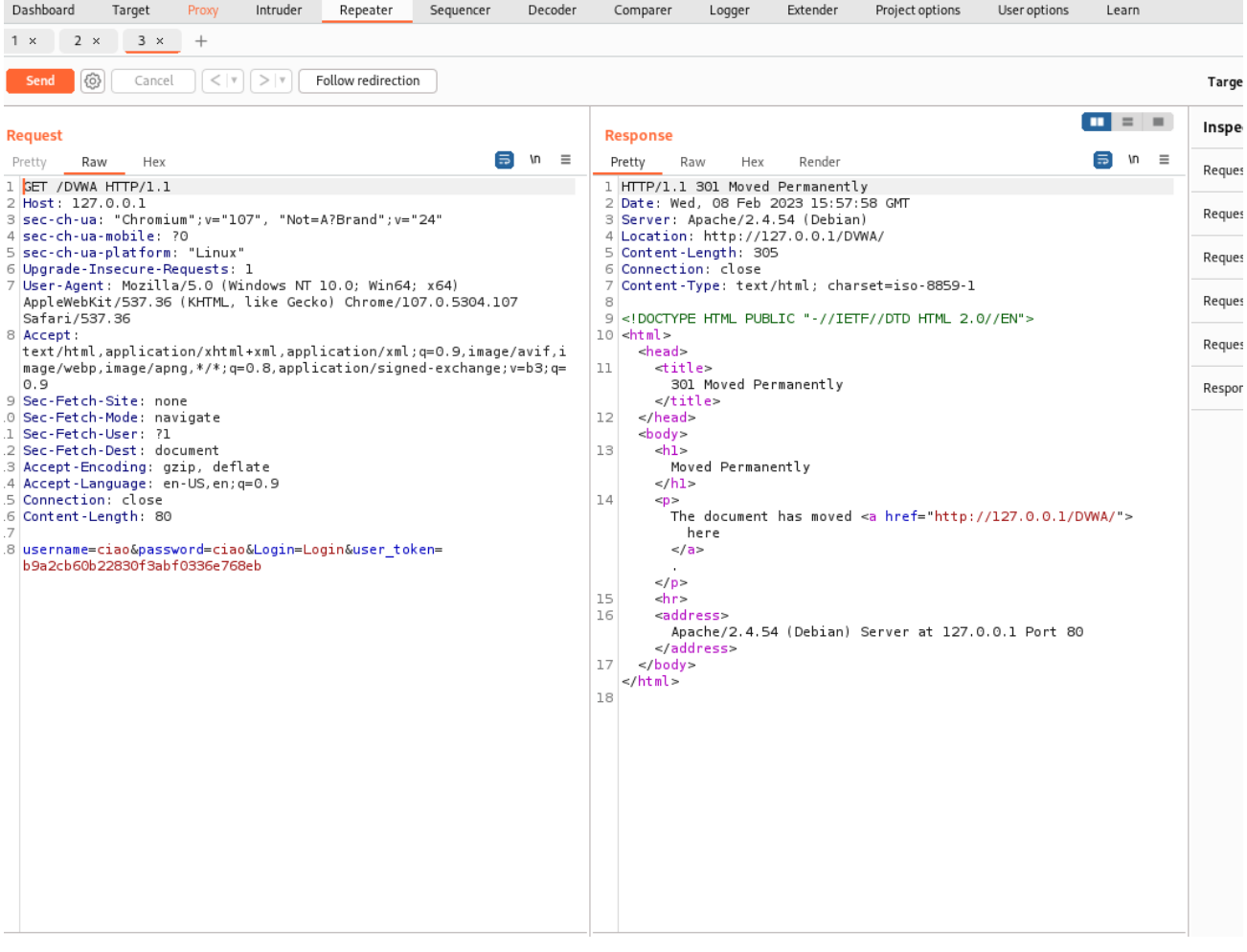


[Simulate attack] - [View IDS log]

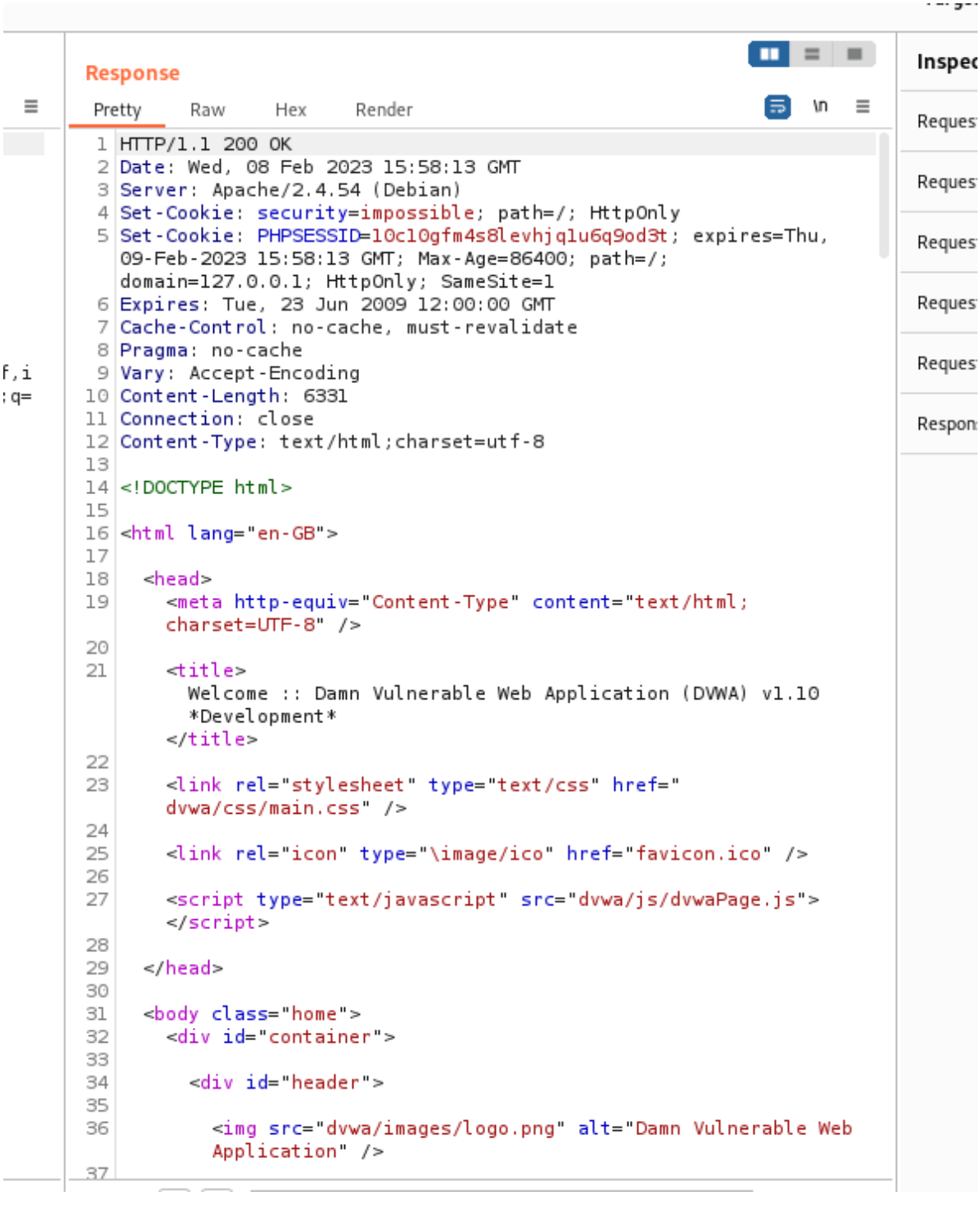
Lancio Burpsuite e provo a cambiare le credenziali (che non ci sono)



Clicco su Send



E poi su Follow Redirection



Riesco ad entrare perchè non ho impostato alcun login.