S3-L2

Per la lezione pratica di oggi, l'obiettivo è quello di configurare una DVWA (Damn Vulnerable Web Application) in Kali Linux.

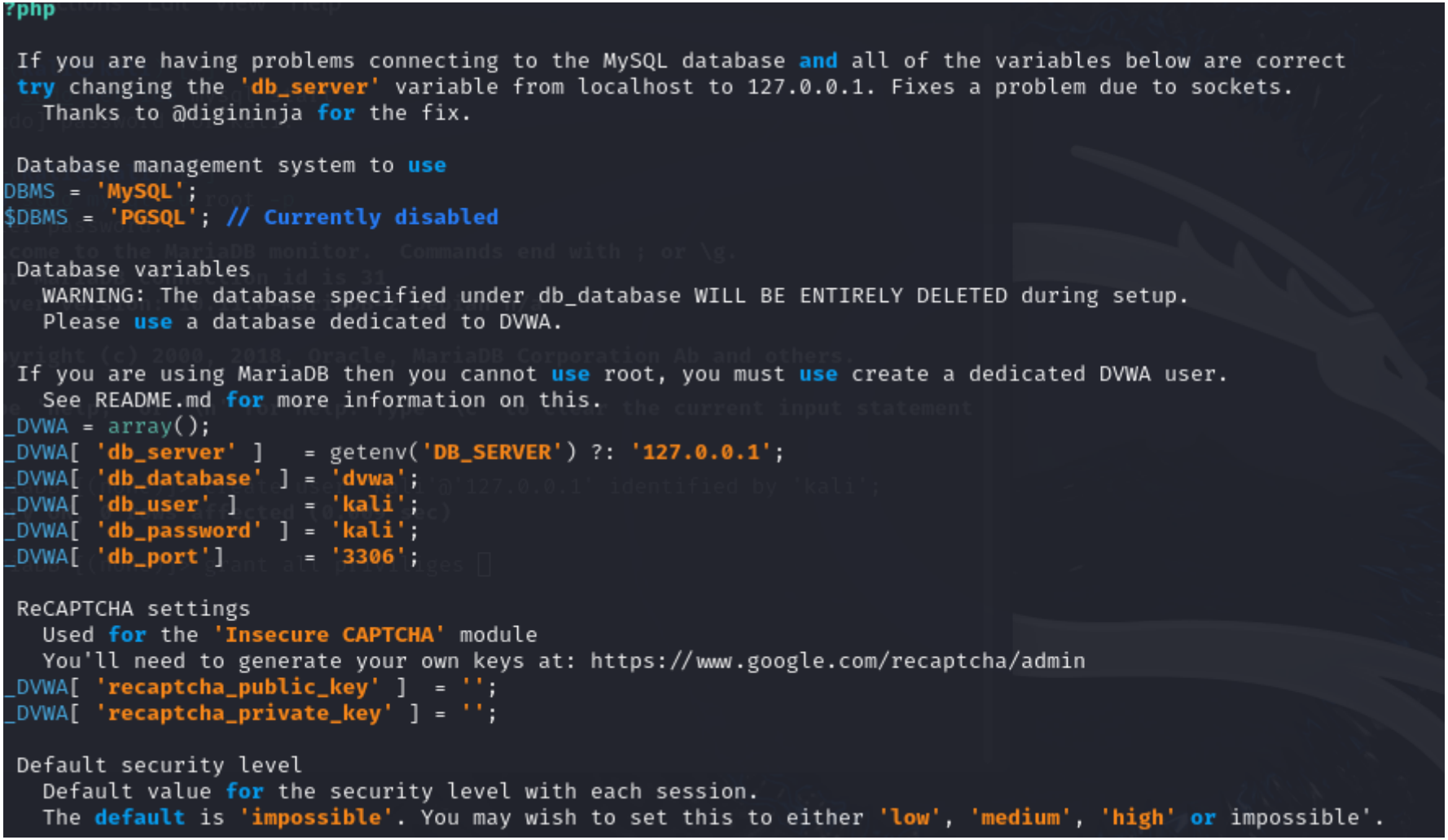
Ci assicuriamo di effettuare correttamente il setup delle risorse che andremo ad utilizzare.

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

```
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA
Cloning into 'DVWA' ...
remote: Enumerating objects: 4503, done.
remote: Counting objects: 100% (53/53), done.
remote: Compressing objects: 100% (44/44), done.
remote: Total 4503 (delta 19), reused 33 (delta 8), pack-reused 4450
Receiving objects: 100% (4503/4503), 2.30 MiB | 5.80 MiB/s, done.
Resolving deltas: 100% (2114/2114), done.
```

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

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

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

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



```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'.
```

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

┌──(kali㉿kali)-[~]
└─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-2 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
```

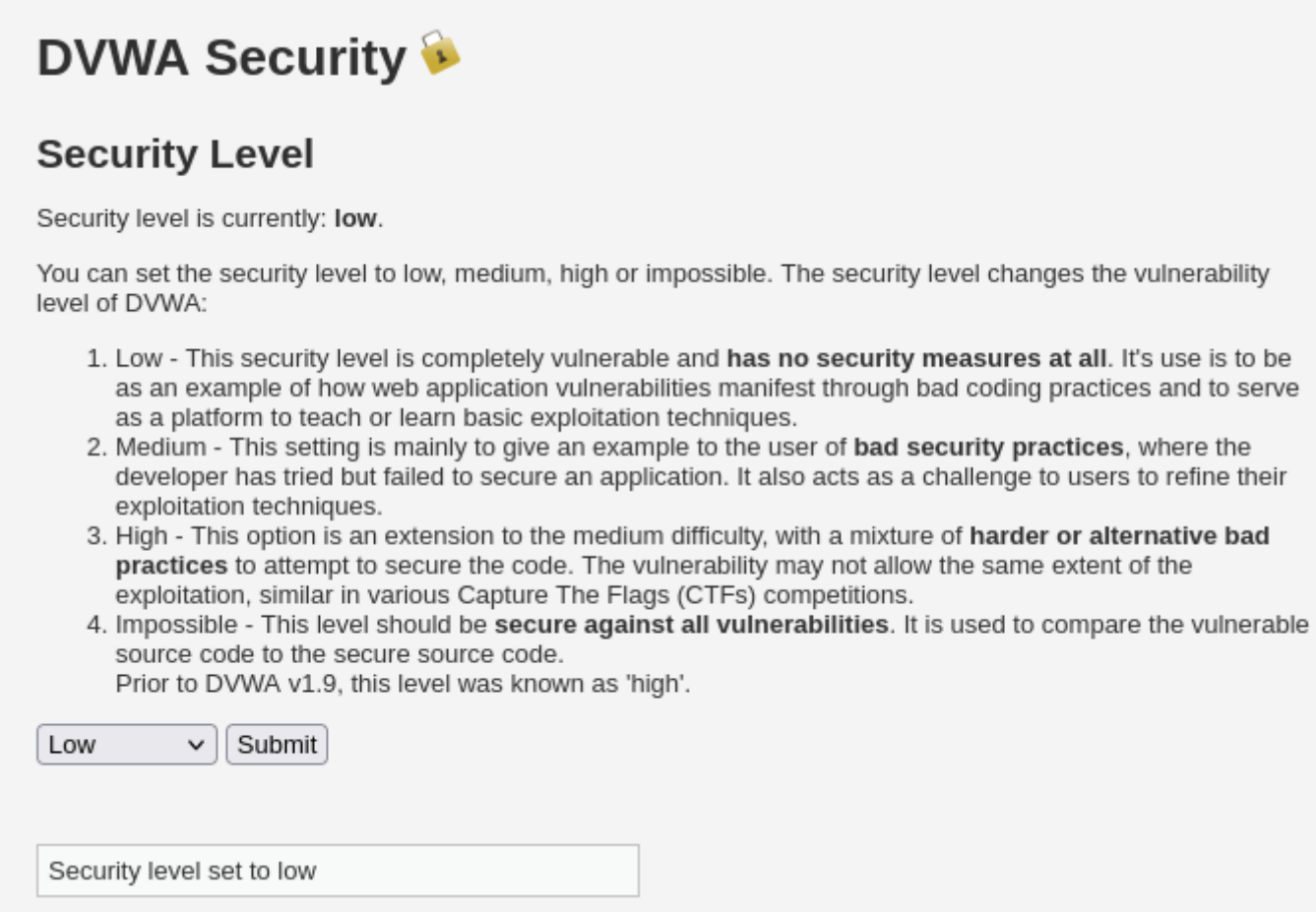
```
┌──(kali㉿kali)-[~]
└─$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-2 Debian n/a

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 (0.009 sec)

MariaDB [(none)]> grant all priviliges on dvwa.* to 'kali'@'127.0.0.1' identi
fied by 'kali';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual th
at corresponds to your MariaDB server version for the right syntax to use nea
r 'priviliges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali'' at line 1
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'ka
li';
Query OK, 0 rows affected (0.002 sec)
```

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

┌──(kali㉿kali)-[~]
└─$ cd /etc/php

┌──(kali㉿kali)-[/etc/php]
└─$ ls -l
total 4
drwxr-xr-x 5 root root 4096 Feb 25 10:47 8.2

┌──(kali㉿kali)-[/etc/php]
└─$ ls
8.2

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

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

```
┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ sudo nano php.ini
sudo] password for kali:
```

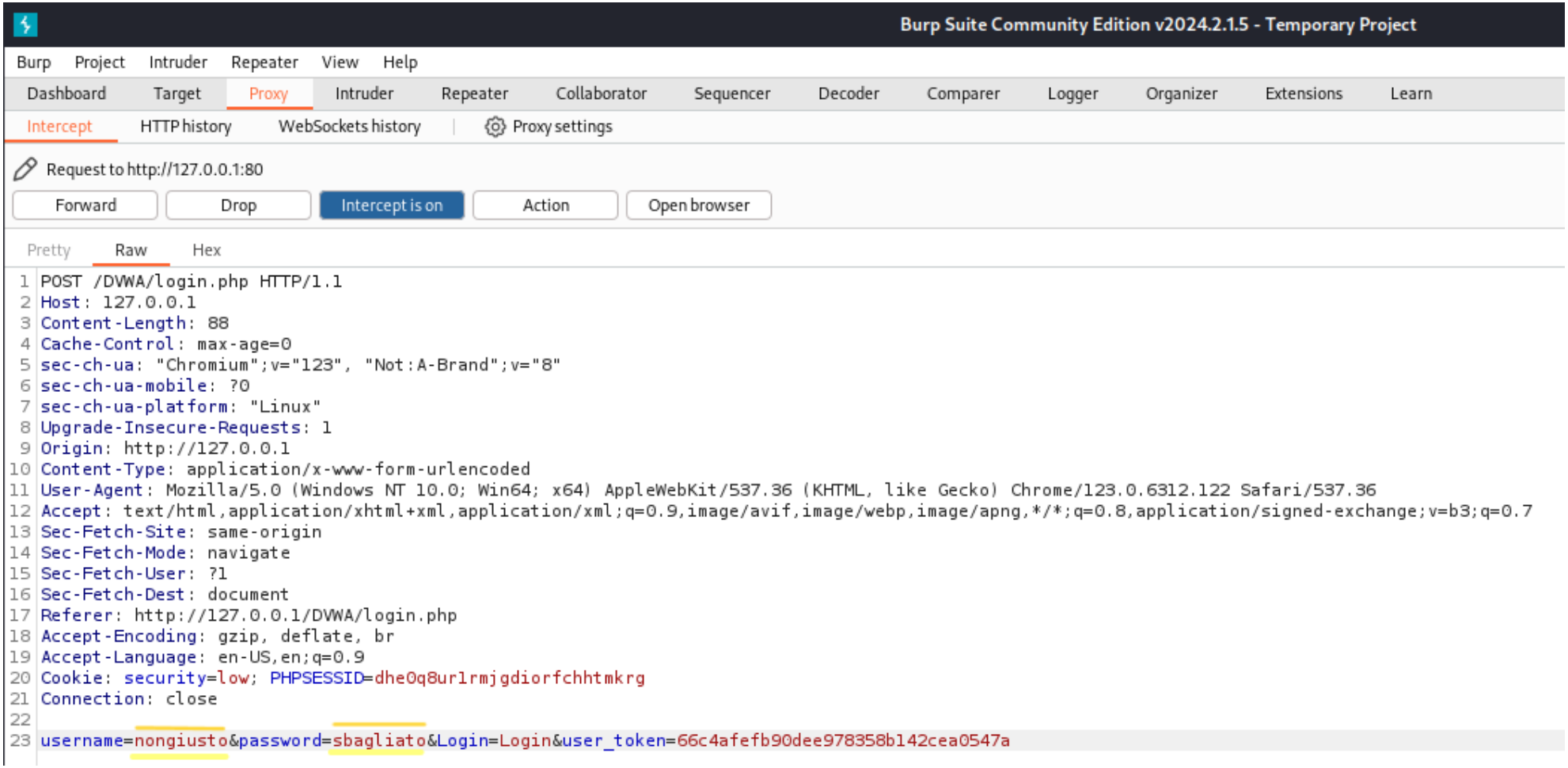
```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

Dopo esserci assicurati di avere tutto il necessario andiamo ad impostare il livello di sicurezza della nostra DVWA come bassa.

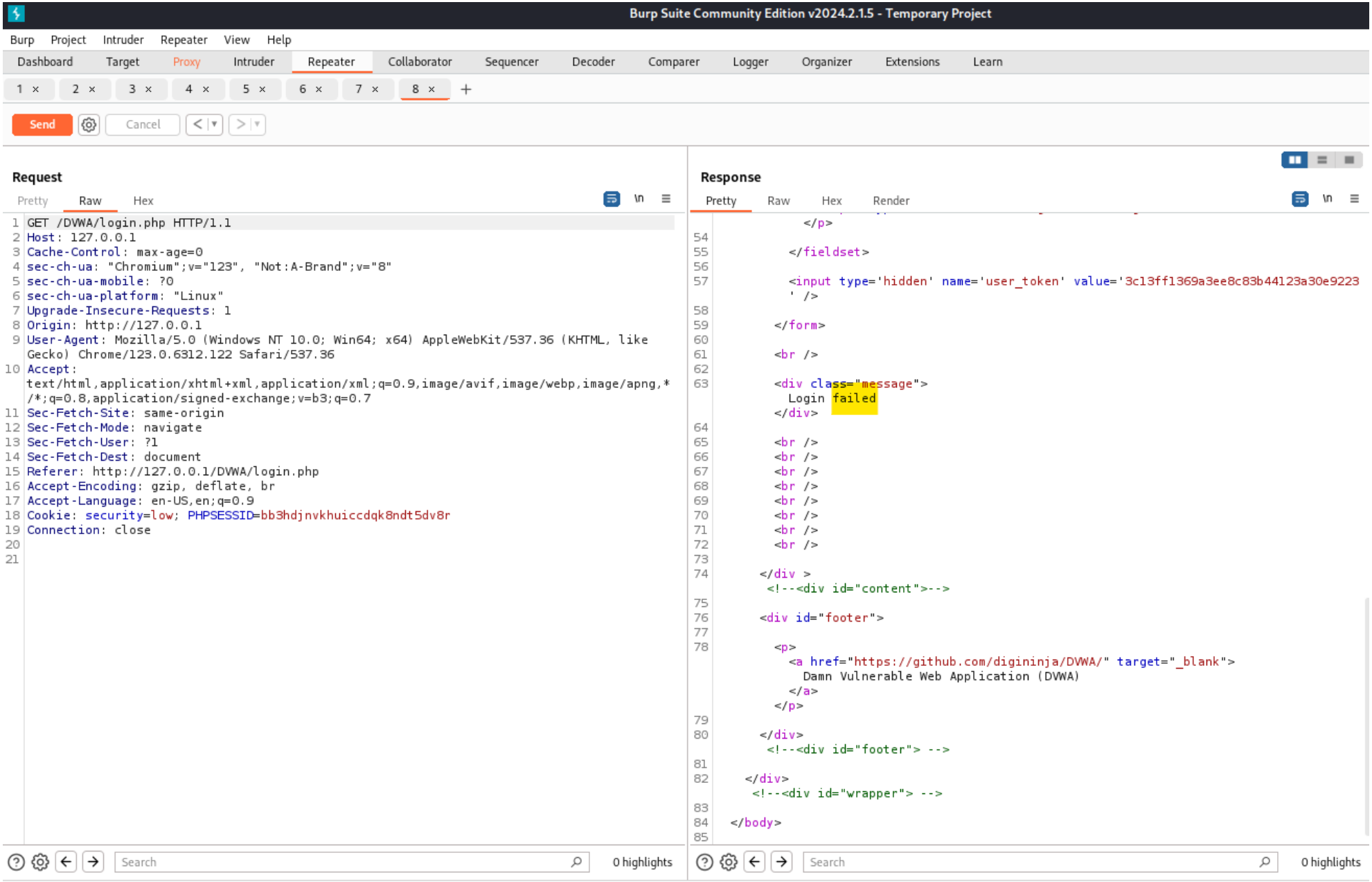


Cambiamo le impostazioni di gestione delle redirection responses del repeater, permettendogli di processare i cookies in redirects.

Seguendo le istruzioni intercettiamo un tentativo di login nella nostra DVWA, andiamo poi a modificare le credenziali in modo che non siano corrette.



Inviamo la richiesta modificata al repeater, la inviamo alla DVWA e ne seguiamo la redirection. Com'è possibile vedere in figura il login non è andato a buon fine, il nostro esperimento ha quindi avuto successo.



Possiamo infine vedere la traduzione grafica del codice HTML che ci mostra ancora una volta che il login è fallito.

Username

Password

Login

Login failed

Done by:

André Vinícius, Federico Biggi, Joel Landry, Lorenzo Franchi, Otman Hmich, Romano Cascialli, Samuele Aversa