Report S3/L3

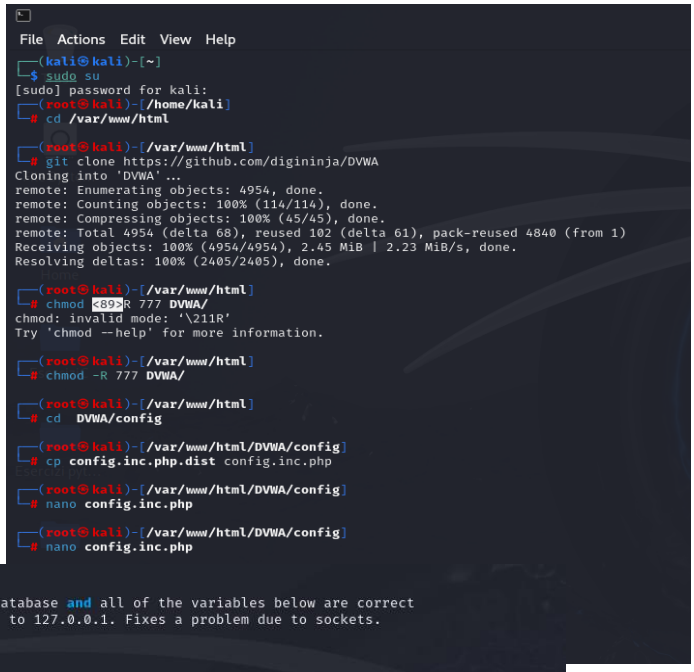
Matteo Congiu

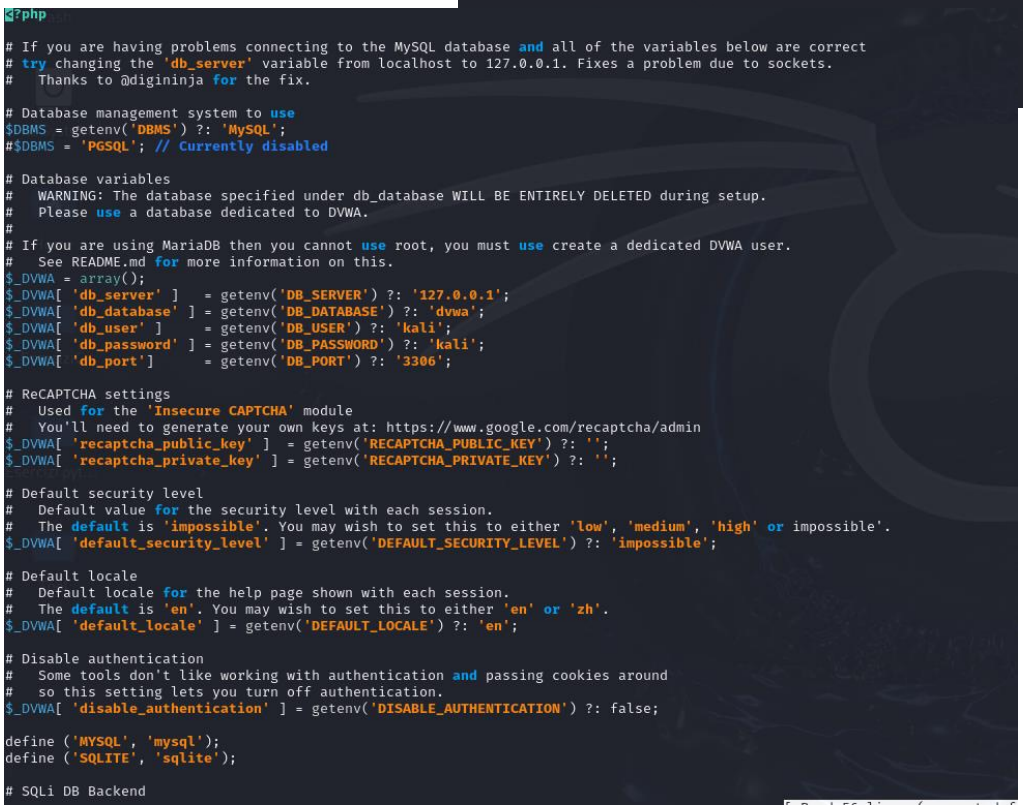
Traccia: Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test.

Svolgimento

Per iniziare sono andato sul terminale di kali e sono entrato nella modalità root con il comando -**sudo su**, poi ho seguito i seguenti comandi:

- **cd /var/www/html**
- **git clone https://github.com/digininja/DVWA**
- **chmod –R 777 DVWA/**
- **cd DVWA/config**
- **cp config.inc.php.dist config.inc.php**
- **nano config.inc.php**





Nel file file config.inc.php ho cambiato le credenziali user e passord come richiesto e ho salvato con **ctrl+o**.

Successivamente ho fatto partire il servizio mysql con il comando: **service mysql start**

Poi mi son connesso al db utilizzando le credenziali precedentemente cambiate. Il comando usato è: **mysql –u root –p**

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.7-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)]>
```

Ho creato un'utenza sul db con: **create user 'kali'@'127.0.0.1' identified by 'kali' ;**

e gli ho assegnato i privilegi di root: **grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ;**

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by'kali' ;
Query OK, 0 rows affected (0.009 sec)

MariaDB [(none)]> exit
Bye

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

Dopo aver terminato la configurazione ho lanciato il comando per il servizio apache: **service apache2 start**

Mi son spostato nella cartella apache2 con: **cd /etc/php/8.2/apache2**

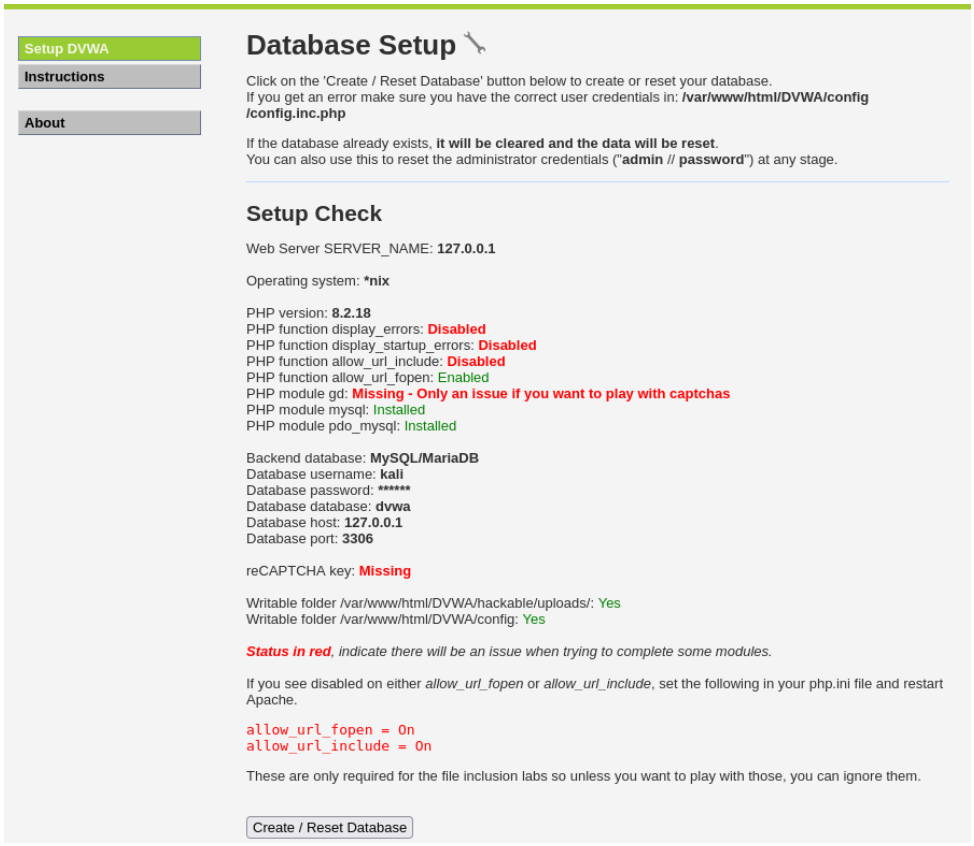
Nel file **php.ini** modificato le voci **allow_url_fopen** e **allow_url_include** configurandole su ON.

```
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service apache2 start

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2

┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php

┌──(root㉿kali)-[/etc/php]
└─# ls
8.2

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

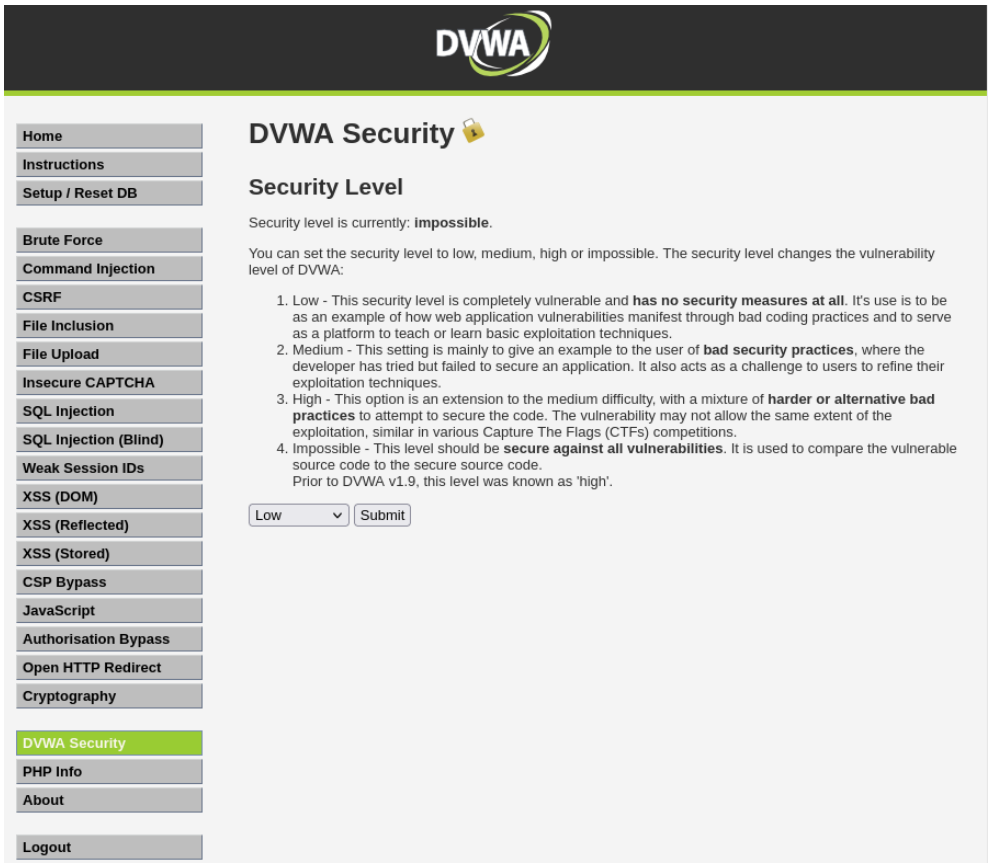
Ho eseguito nuovamente il comando **service apache2 start.**

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

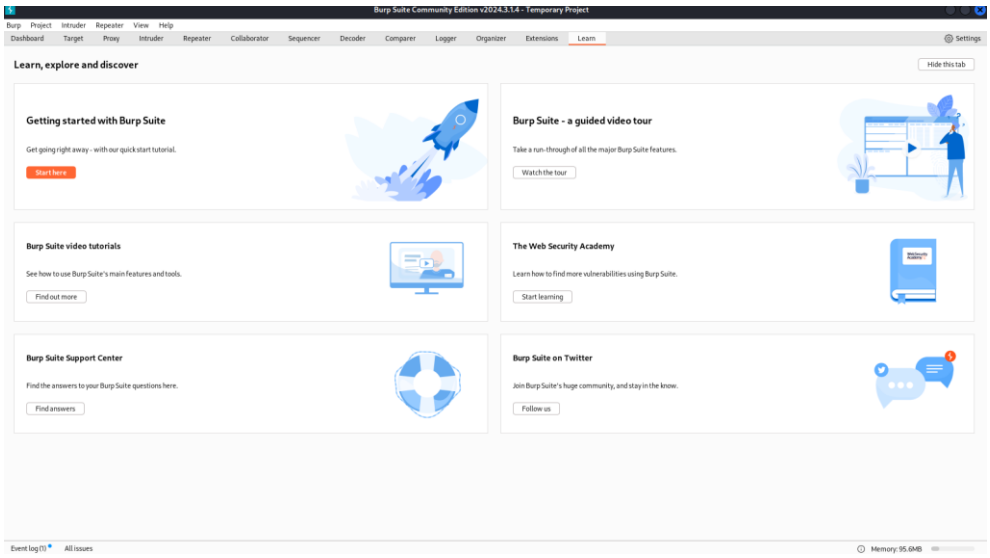
Successivamente con il browser firefox ho aperto la pagina **127.0.0.1/DVWA/setup.php** e ho cliccato su **«Create / Reset Database»** e in seguito ho fatto l'accesso con le credenziali di default **Username: admin - Password: password.**

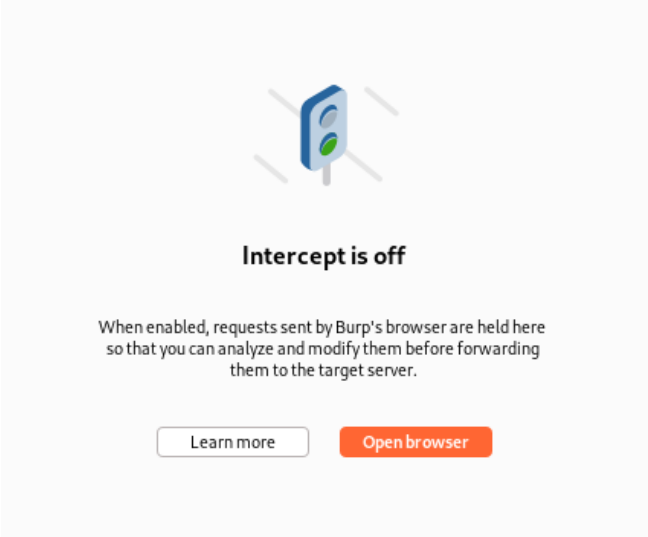


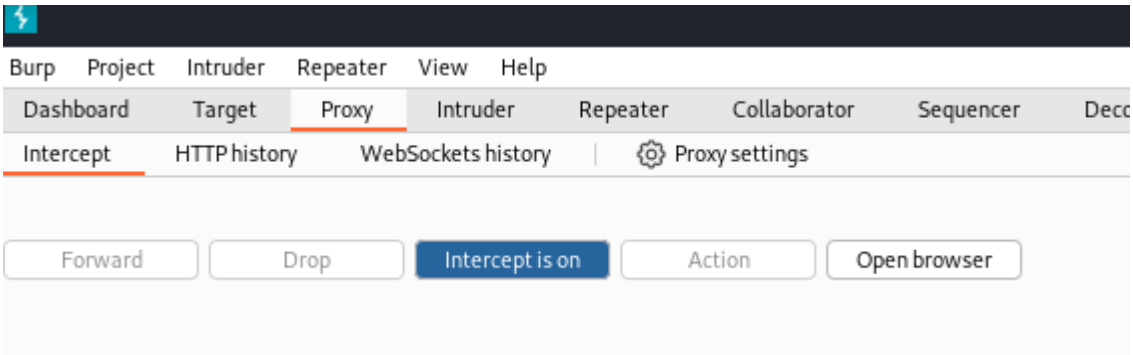
Una volta eseguito l'accesso ho cliccato sulla scheda **DVWA Security** e ho scelto il livello di sicurezza dell'APP. Più basso sarà il livello di sicurezza impostato, meno sarà complicato sfruttare le vulnerabilità.

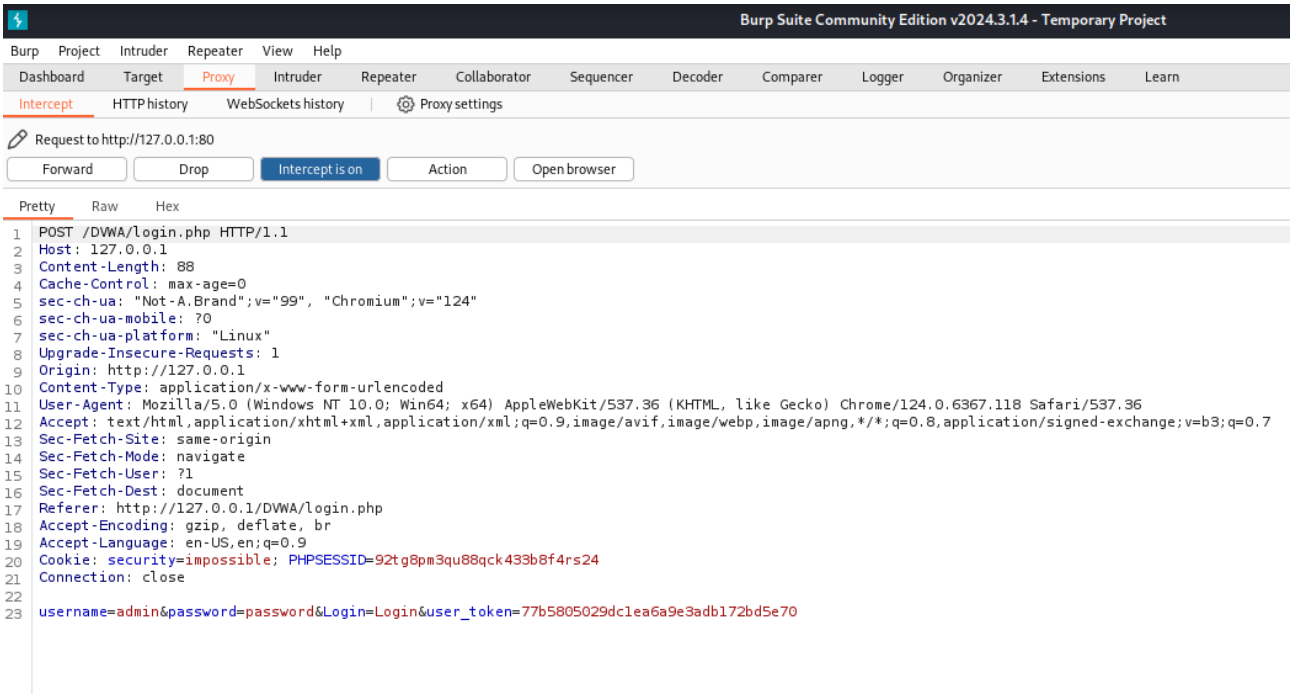


Ho avviato **Burpsuite** e sul suo browser ho cercato: **127.0.0.1/DVWA,** sul software ho cliccato su **intercept is off** per metterlo in **modalità on,** ho inserito le credenziali sulla pagina web e ho fatto l'accesso. Subito **Burpsuite** ha intercettato l'accesso comunicandomi il seguente messaggio:

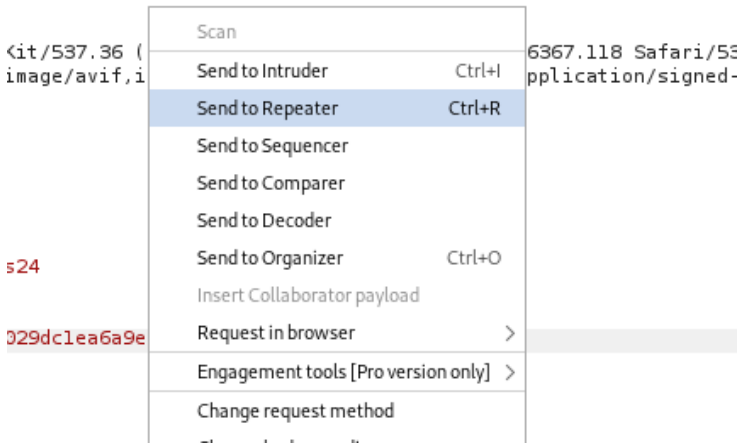


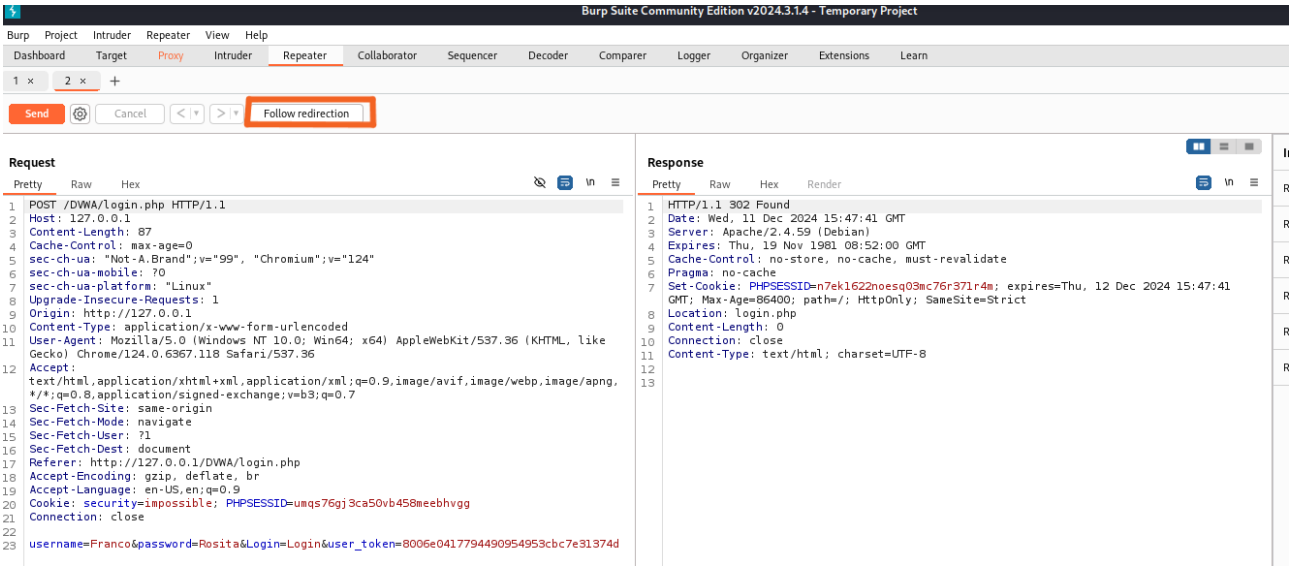


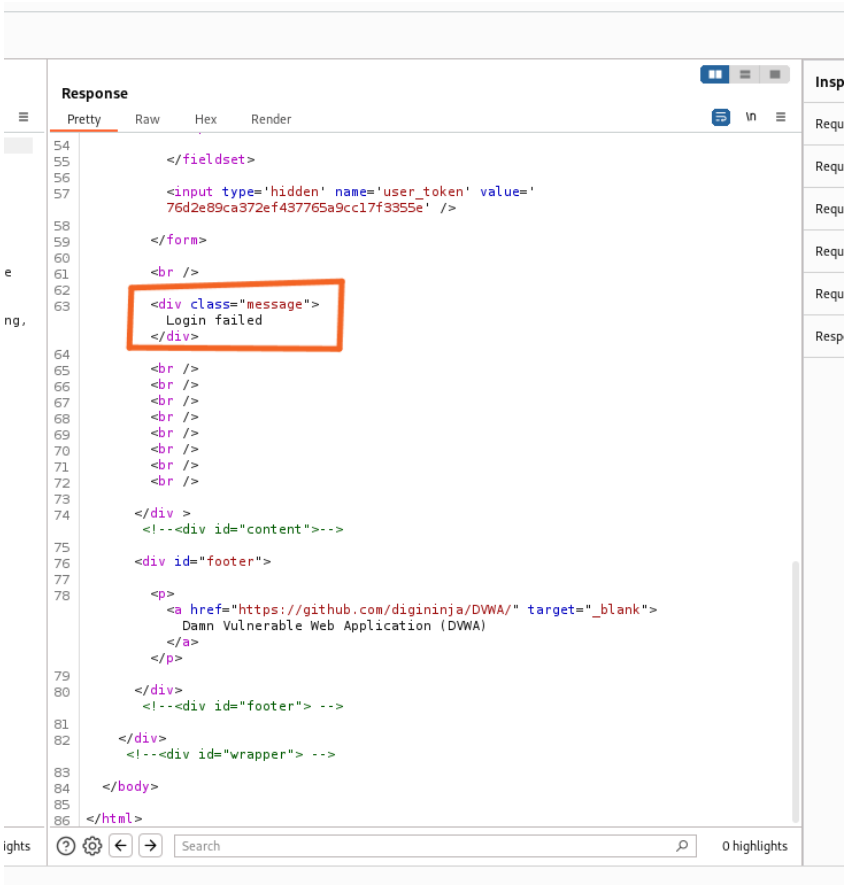




Ho provato a modificare i campi, ed inviare la richiesta inserendo delle credenziali **sbagliate**, user **Franco** e password **Rosita.** Prima di inviare la richiesta ho cliccato con il **tasto destro** e ho selezionato **send to repeater.** Mi son spostato sulla sezione **Repeater** e ho cliccato su **send** per inviare la richiesta di login ed e poi su **follow redirection**.








```
54
55            </fieldset>
56
57            <input type='hidden' name='user_token' value='
              76d2e89ca372ef437765a9cc17f3355e' />
58
59          </form>
60
61          <br />
62
63          <div class="message">
              Login failed
            </div>
64
65          <br />
66          <br />
67          <br />
68          <br />
69          <br />
70          <br />
71          <br />
72          <br />
73
74        </div >
            <!--<div id="content">-->
75
76        <div id="footer">
77
78          <p>
              <a href="https://github.com/digininja/DVWA/" target="_blank">
                Damn Vulnerable Web Application (DVWA)
              </a>
            </p>
79
80        </div>
            <!--<div id="footer"> -->
81
82      </div>
          <!--<div id="wrapper"> -->
83
84    </body>
85
86  </html>
```