S3/L3 -DVWA e BurpSuite

Nel laboratorio di oggi vedremo ho configurato una DVWA – ovvero Damn Vulnerable Web Application in Kali Linux.

Dopo aver clonato la repository github tramite il comando git clone, ho modificato tramite il text editor nano il file di configurazione config.inc.php modificando i valori di username e password:

```
┌──(kali㉿kali)-[/var/www/html]
└─$ sudo 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% (45/45), done.
remote: Total 4954 (delta 68), reused 102 (delta 61), pack-reused 4840 (from 1)
Receiving objects: 100% (4954/4954), 2.42 MiB | 1.88 MiB/s, done.
Resolving deltas: 100% (2420/2420), done.
```

```
$_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';
```

Ho inoltre avviato il servizio mysql tramite il comando **service mysql start** e mi sono connesso al database con utenza root tramite il comando **mysql -u root -p**

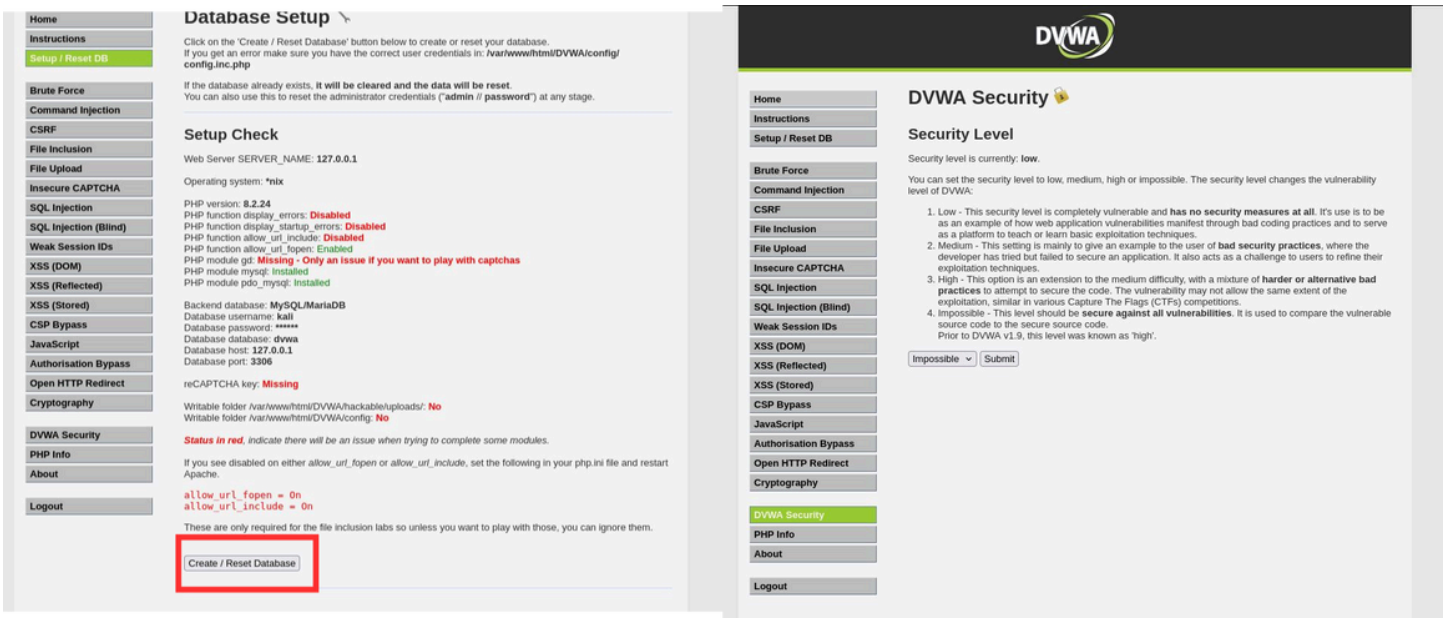
```
┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo nano config.inc.php

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ sudo service mysql start

┌──(kali㉿kali)-[/var/www/html/DVWA/config]
└─$ 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: 11.4.3-MariaDB-1 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
```

Dopo aver creato una nuova utenza nel database ho modificato il file php.ini di apach2 ed avviato il servizio tramite 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
```

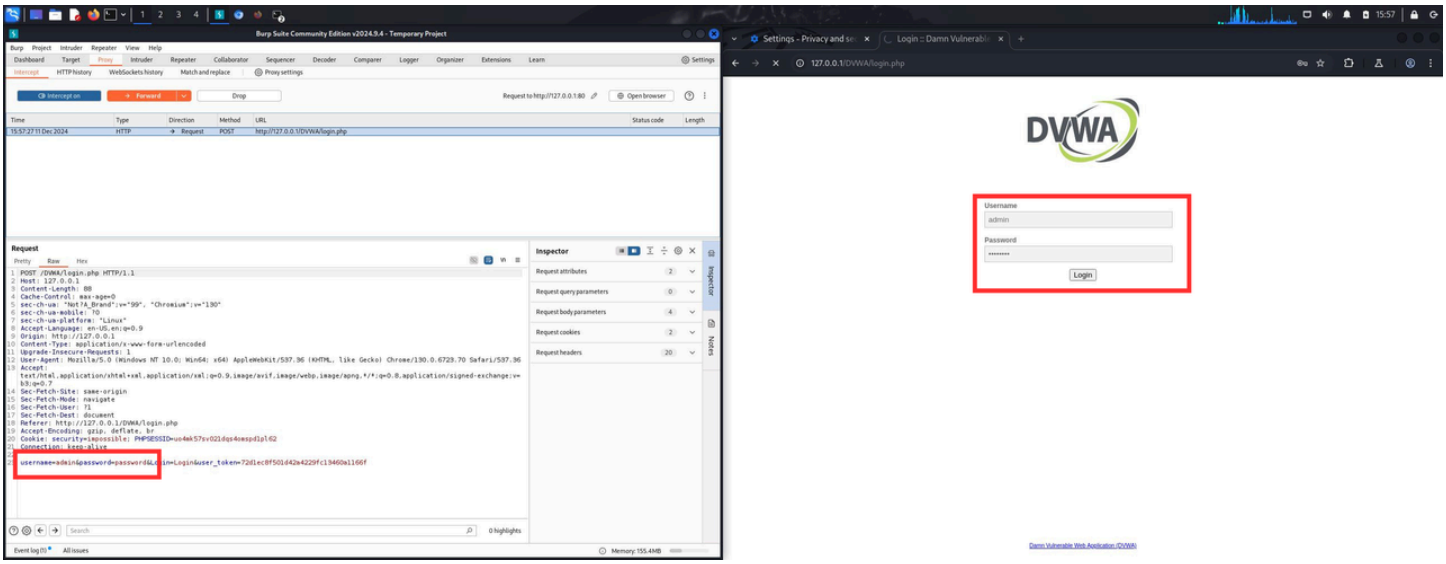
```
┌──(kali㉿kali)-[/etc/php/8.2/apache2]
└─$ sudo nano -lm php.ini

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

Ho creato un nuovo database nella web application nella pagina all'indirizzo 127.0.0.1/SVWA/setup.php ed effettuato il login con le credenziali admin e password.



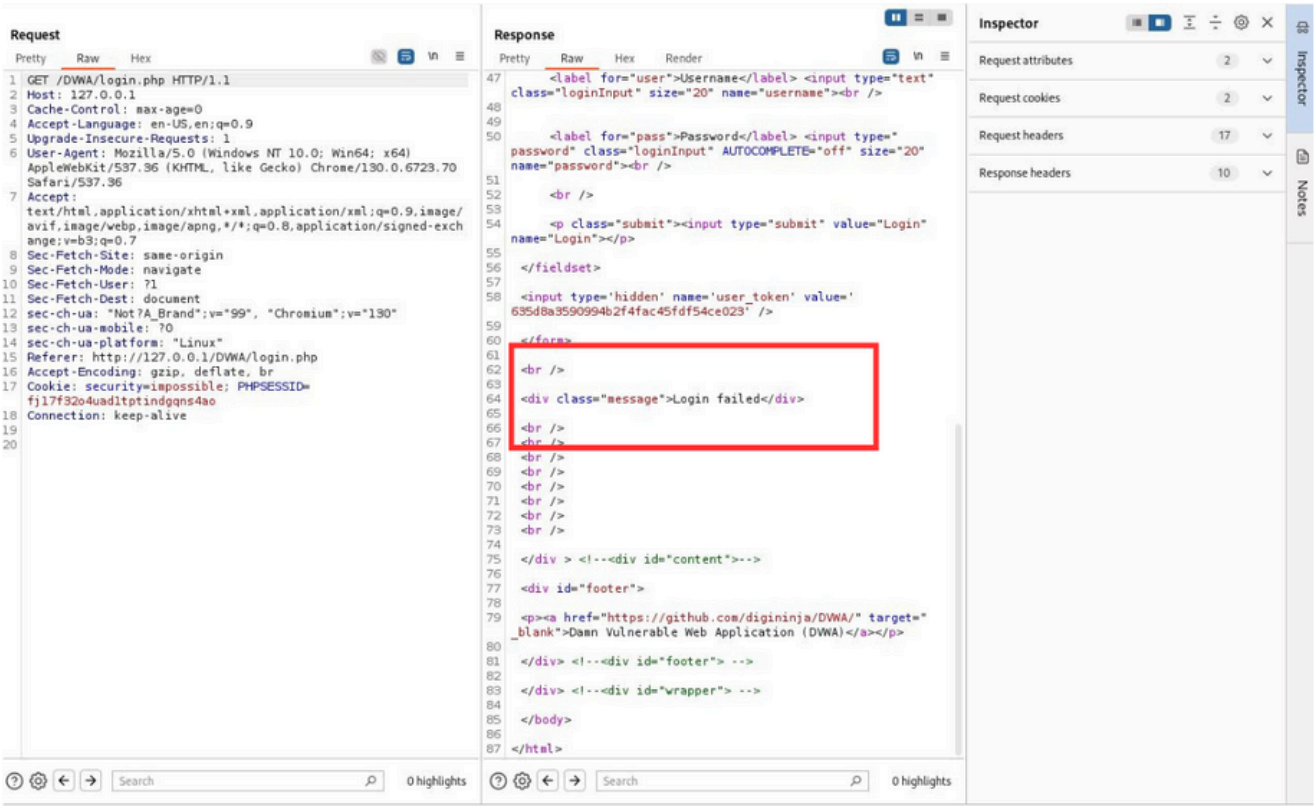
A questo punto ho utilizzato BurpSuite creando un nuovo progetto temporaneo. Tramite il browser ho inserito l'indirizzo della DVWA (127.0.0.1/DVWA) ed intercettato il traffico tramite il tab **proxy**

Ho inserito i valori <admin> di login e <password> per la password.

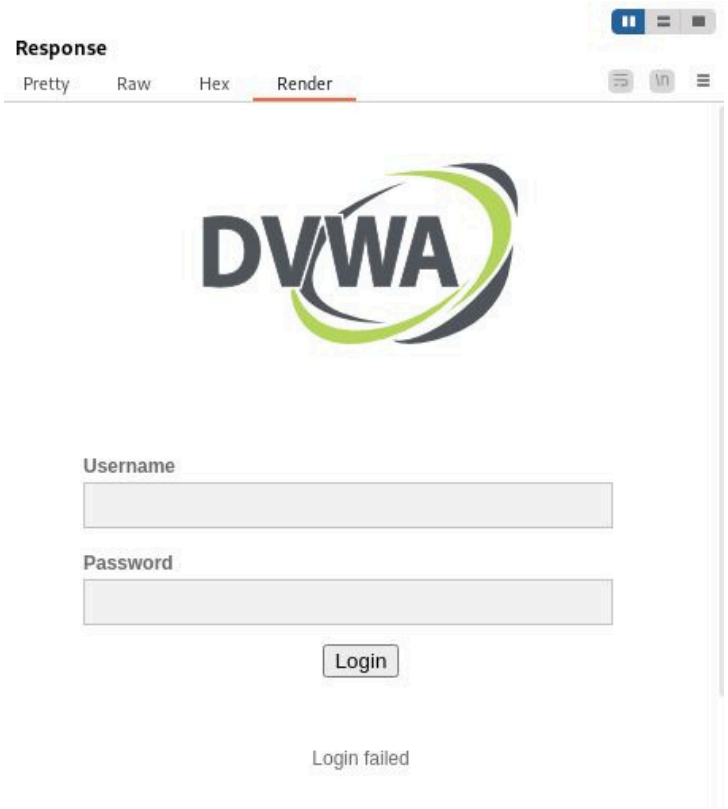


Come evidenziato dai rettangoli, i campi inseriti nel form di login possono essere completamente modificati prima di inviare la richiesta. Ho inviato al repeater modificando i valori e inviato la richiesta cliccando su **send** e poi su **follow redirection**.

Analizzando la risposta del server, come da attese, il server restituisce una HTTP response con messaggio “Login failed” a causa degli errati valori inviati.



BurpSuite mette anche a disposizione un render dell’anteprima della pagina HTTP dopo che abbiamo modificato e inviato la richiesta:



Inviando la richiesta con i valori corretti di username e password riusciamo a completare il login con successo.