CS0424IT — ESERCITAZIONE S3L2 - CONFIGURAZIONE DVWA

Simone La Porta

GitHub

TRACCIA

Nella lezione pratica di oggi vedremo come configurare una DVWA (Damn Vulnerable Web Application)

SVOLGIMENTO

In questo documento, verranno illustrate le istruzioni per l'installazione e la configurazione della web application DVWA (Damn Vulnerable Web Application). DVWA è un progetto software che include intenzionalmente vulnerabilità di sicurezza, utile per esercitazioni e analisi nel campo della sicurezza informatica. Per iniziare, è necessario installare DVWA.

Dopo aver completato l'installazione, è necessario configurare DVWA modificando il file `config.inc.php`.

Per farlo, eseguire il seguente comando in terminale:

```
sudo nano config.inc.php
```

All'interno del file, aggiornare il nome utente e la password utilizzati per la connessione al database, impostandoli entrambi su `kali`. Il file `config.inc.php` dovrebbe contenere le seguenti righe:

```
┌──(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
```

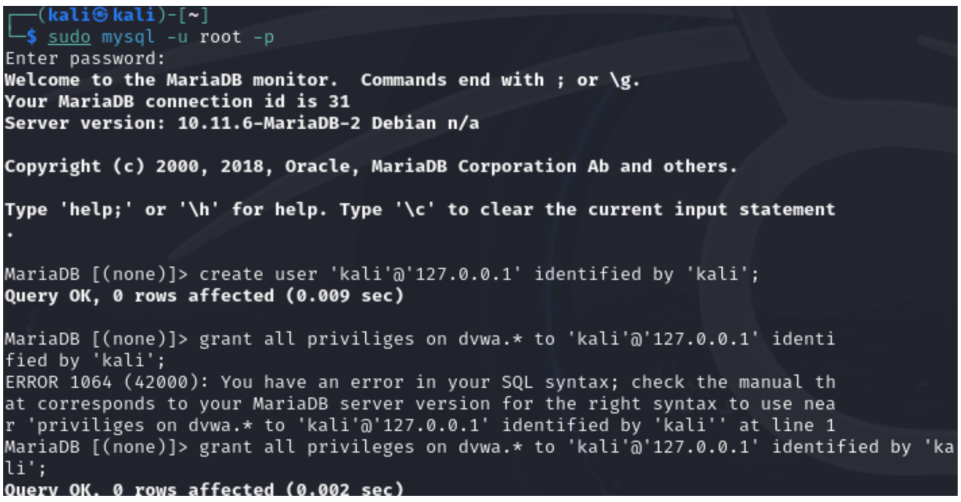

```
$_DVWA[ 'db_user' ] = 'kali';
$_DVWA[ 'db_password' ] = 'kali';
```

Una volta completata la configurazione, salvare le modifiche e chiudere l'editor. DVWA sarà ora pronto per essere utilizzato per le esercitazioni e le analisi delle vulnerabilità di sicurezza.

Dopo aver configurato le credenziali, è necessario avviare il servizio web Apache2 e il servizio database MySQL utilizzando i permessi di amministratore. Per farlo, eseguire i seguenti comandi:

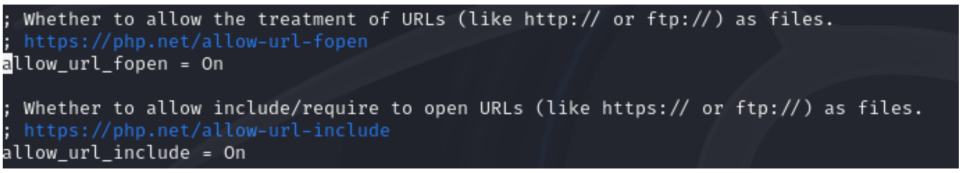
```
sudo service apache2 start
sudo service mysql start
```

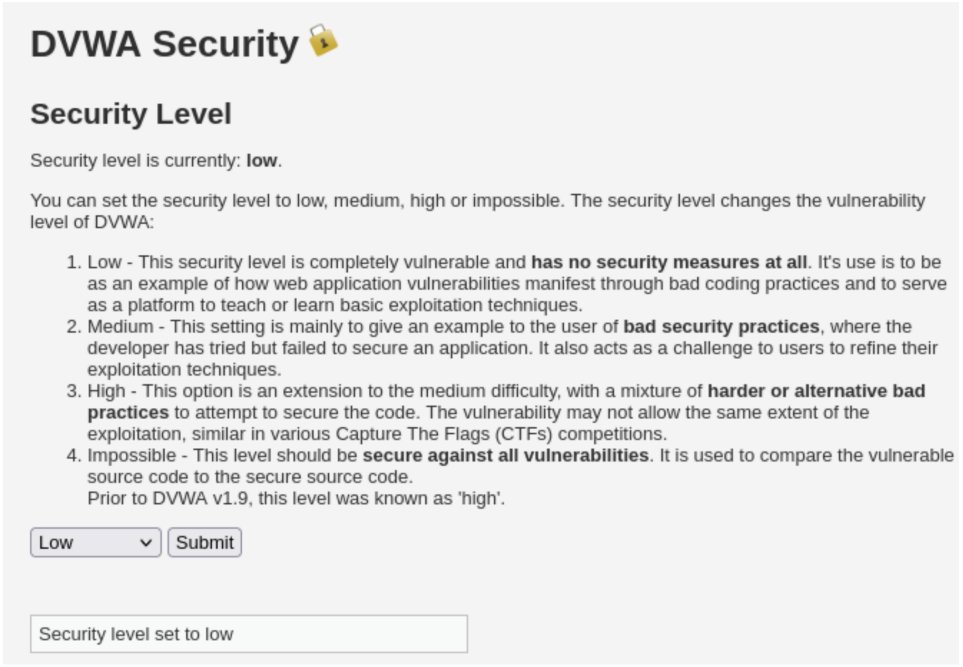
Il servizio MySQL verrà avviato utilizzando il database MariaDB. Successivamente, creare un'utenza `kali` e assegnarle i privilegi da amministratore.



Dopo aver configurato l'utenza, creare un database su DVWA. Accedere all'applicazione DVWA con `username: admin` e `password: password`. Quindi, selezionare il livello di sicurezza della web app impostandolo al minimo (*Low*). Un livello di sicurezza più basso rende meno complicato sfruttare le vulnerabilità.

A questo punto, utilizzare l'applicazione Burp Suite e scegliere un progetto temporaneo. Attivare l'intercettazione delle richieste di login su Burp Suite. Accedere tramite browser all'indirizzo `http://127.0.0.1/DVWA` e tentare di intercettare la propria richiesta di login.

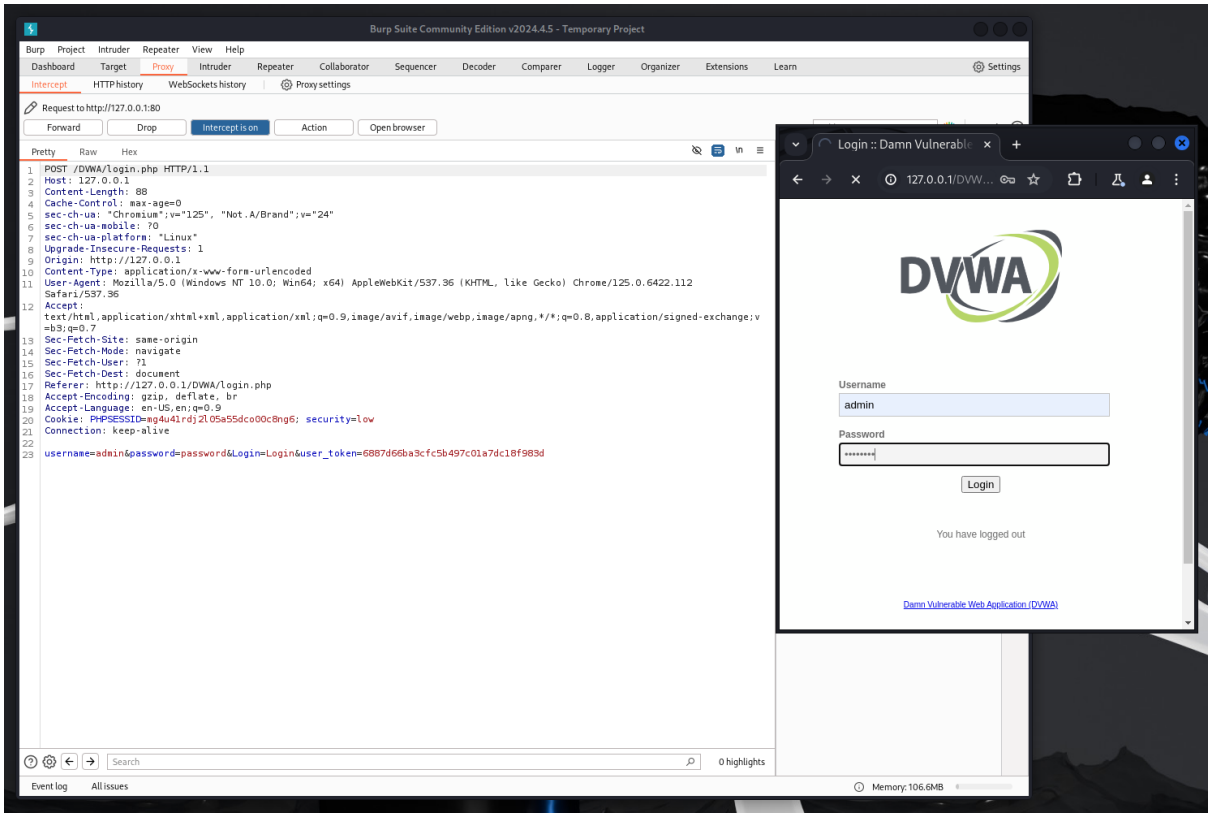


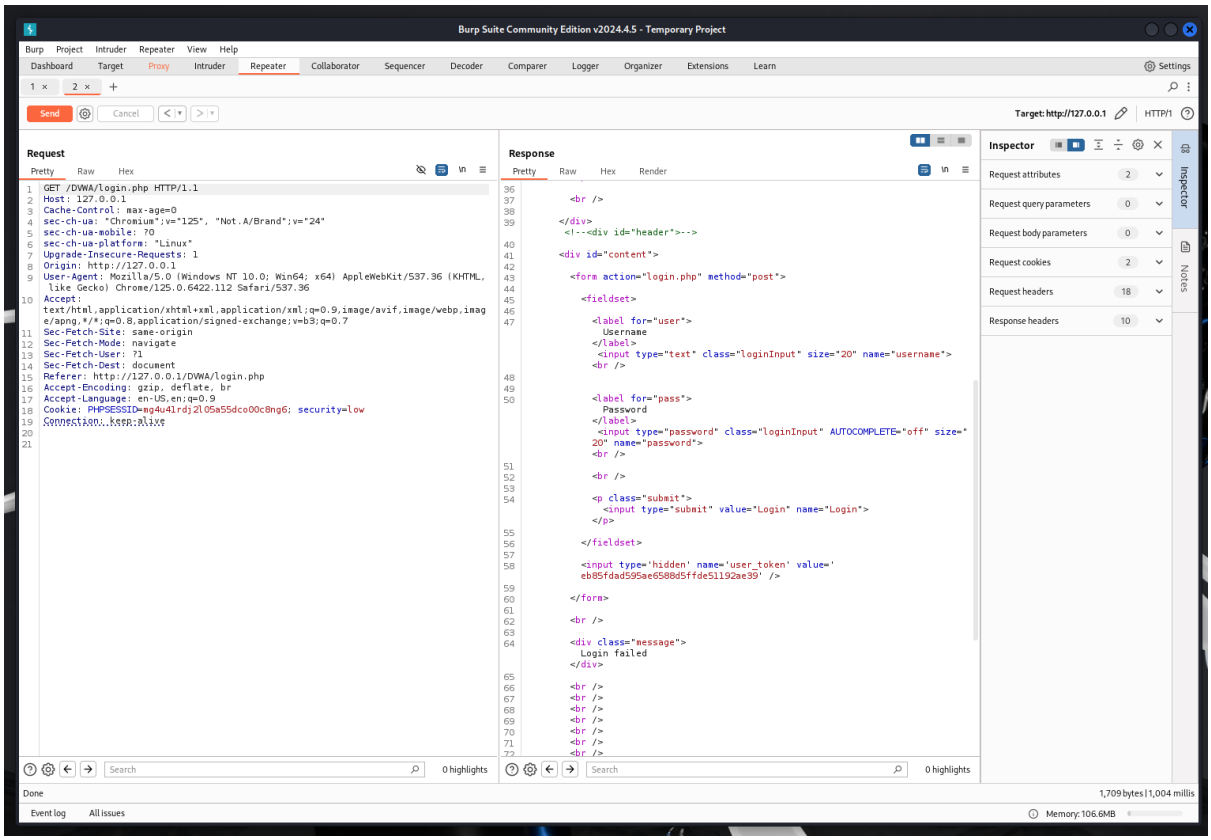


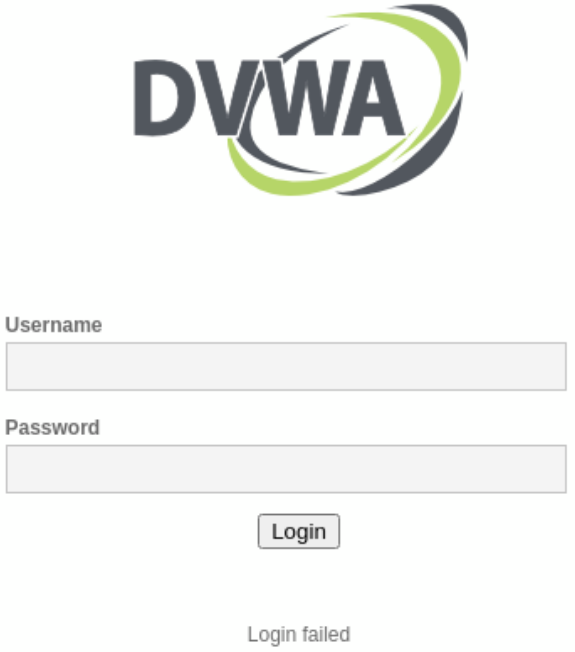
Per verificare il funzionamento dell'intercettazione, cambiare `username` e `password` iniziali con credenziali errate, proprio per verificare che il login fallisca.

Come previsto, con credenziali errate non sarà possibile effettuare il login. Questo sarà confermato dal corpo della risposta HTTP (*HTTP response*) dove si potrà leggere "`Login`

failed".


Burp Suite Community Edition v2024.4.5 - Temporary Project
Request to http://127.0.0.1:80
Forward
Drop
Intercept is on
Action
Open browser
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 88
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=mg4u41rdj2l05a55dco00c8ng6; security=low
Connection: keep-alive
username=admin&password=password&Login=Login&user_token=6887d66ba3cfc5b497c01a7dc18f983d
Login :: Damn Vulnerable
DVWA
Username
admin
Password
Login
You have logged out
Damn Vulnerable Web Application (DVWA)


Burp Suite Community Edition v2024.4.5 - Temporary Project
Request
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="125", "Not.A/Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.112 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=mg4u4lrdj2l05a55dco00c8ng6; security=low
Connection: keep-alive
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers


DVWA
Username
Password
Login
Login failed