S3/L3

1. Aggiornare il sistema e installare i componenti necessari (Apache, PHP, MySQL/MariaDB).

Avviare il servizio MySQL e configurarlo in modo sicuro.
Accedere a MySQL per configurare l'utente e il database per DVWA.

```
sudo apt update
sudo apt install apache2 php php-mysql mariadb-server
sudo service mysql start
sudo mysql_secure_installation
mysql -u root -p
```

2. Creare un database DVWA e un utente associato ad esso.

Concedere i privilegi necessari all'utente per gestire il database DVWA.

```
CREATE DATABASE dvwa;
CREATE USER 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
GRANT ALL PRIVILEGES ON dvwa.* TO 'kali'@'127.0.0.1' IDENTIFIED BY 'kali';
FLUSH PRIVILEGES;
exit;
```

3. Avviare il servizio Apache.

Navigare alla directory di configurazione di PHP per Apache.
Modificare il file **php.ini** per abilitare alcune opzioni necessarie.
Riavviare il servizio Apache per applicare le modifiche.

```
sudo service apache2 start
cd /etc/php/8.1/apache2
sudo nano php.ini
sudo service apache2 restart
```

4. Accesso a DVWA tramite il browser all'indirizzo **127.0.0.1/DVWA**.

Utilizzo dell'opzione "Create / Reset Database" per preparare il database DVWA.

5. Avvio di Burp Suite e configurazione del browser per utilizzarlo come proxy.

Utilizzo di Burp Suite per intercettare la richiesta di login DVWA.
Inoltramento della richiesta a Burp Repeater per modificarla.
Modifica dei campi della richiesta (ad esempio, inserimento di credenziali errate).

Invio della richiesta modificata e analisi della risposta.

Utilizzare Burp Suite per eseguire un attacco di tipo "man-in-the-middle" e modificare la richiesta di login.
Esaminare come l'applicazione gestisce le credenziali errate.

Questo esercizio simula un attacco di manipolazione della richiesta, in cui un aggressore può modificare i dati inviati a un'applicazione per ottenere un risultato desiderato. È un esempio di come le applicazioni dovrebbero essere progettate per resistere a tentativi di manipolazione dei dati, e gli sviluppatori dovrebbero implementare misure di sicurezza per proteggere le informazioni sensibili. L'obiettivo è comprendere come funzionano questi tipi di attacchi e come gli sviluppatori possono difendersi contro di essi.