Consegna S3-L4

Consegna: Configurazione e Utilizzo di DVWA con Burp Suite

⚜️ **Tag:** #pentesting #dvwa #burpsuite

Obiettivo

Configurare e utilizzare **Damn Vulnerable Web Application (DVWA)** su Kali Linux per test di penetrazione. Configurazione del database, modifica dei file di configurazione, e verifica delle richieste HTTP tramite **Burp Suite**.

Procedura

1. Configurazione della rete:

- Assicurarsi che la macchina Kali Linux abbia accesso a internet con la scheda di rete impostata su **bridge**.

2. Installazione dei componenti necessari:

- MySQL (database).
- Apache (web server).
- Clonare il repository di DVWA:

```
cd /var/www/html
git clone https://github.com/digininja/DVWA.git
chmod -R 777 DVWA/
```

```
cd DVWA/config
cp config.inc.php.dist config.inc.php
nano config.inc.php
```

- Nel file `config.inc.php`, configurare:

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

3. Configurazione di MySQL:

- Avviare il servizio MySQL:

```
service mysql start
```

- Creare l'utente e assegnare i privilegi:

```
create user 'kali'@'127.0.0.1' identified by 'kali';
grant all privileges on dvwa.* to 'kali'@'127.0.0.1'
identified by 'kali';
```

- Uscire dal database con `exit`.

4. Configurazione di Apache:

- Avviare il servizio Apache:

```
service apache2 start
```

- Modificare i file di configurazione PHP se necessario:

```
cd /etc/php/8.1/apache2
nano php.ini
```

Abilitare i parametri:

```
allow_url_fopen = On
allow_url_include = On
```

5. Setup di DVWA:

- Aprire il browser e accedere a: `127.0.0.1/DVWA/setup.php`.
- Cliccare su **"Create / Reset Database"**.
- Accedere con le credenziali di default:
  - **Username:** admin
  - **Password:** password

6. Utilizzo con Burp Suite:

- Avviare Burp Suite e configurare il proxy.
- Inserire le credenziali `admin` e `password` nella pagina di login di DVWA.
- Intercettare la richiesta con Burp Suite.
- Modificare i parametri della richiesta (es. credenziali errate).
- Inviare la richiesta e verificare il messaggio **"Login failed"**.

🔑 **Chiavi:**
[pentesting, dvwa, burpsuite]
