Pratica S3/L3

L'obbiettivo di questa esercitazione è configurare MySQL e Apache, installare DVWA (Damn Vulnerable Web Application) ed effettuare dei test tramite Burpsuite.

Terminale di Kali (configurazione di DVWA)

Tramite la serie di comandi sottostante, eseguiti da terminale di Kali Linux, si installa e configura DVWA.

- sudo su (acceso come utente root)
- cd /var/www/html (spostamento nella cartella)
- git clone https://github.com/digitalninja/DVWA (clonazione del repository)
- chown -R www-data:www-data DVWA/ (assegnazione dei permessi alla cartella)
- cd DVWA/config (spostamento nella cartella)
- cp config.inc.php.dist.config.inc.php (copia dei file di configura)
- nano config.inc.php: modificare username e password:
  1) $_DVWA['db_user'] ='**kali**';
  2) $_DVWA['db_password'] = '**kali**';
- service mysql start (avvio di MySQL)
- my -u root -p (accesso a MySQL)
- create user 'kali'@'127.0.0.1' identified by 'kali' ; (creazione di un utente per MySQL)
- grant all privileges on dvwa.* to 'kali'@'127.0.0.1' identified by 'kali' ; (assegnazione di tutti i privilegi)
- exit
- cd /etc/php/8.4/apache2 (spostamento nella cartella)
- nano php.ini: modificare queste righe:
  1) allow_url_fopen = On
  2) allow_url_include = On
- service apache2 restart (riavvio di apache)

Browser Internet (creazione del database)

Dopo aver configurato il tutto si apre il browser e si cerca: http://127.0.0.1/DVWA/setup.php. Si clicca su "Create / Reset Database" crea un database. Dopo aver creato il database si effettua il login tramite credenziali admin di default (admin/password).

Burpsuite

Dopo aver avviato Burpsuite, e aver creato un progetto temporaneo, si apre il browser integrato e si cerca http://127.0.0.1/DVWA e verrà aperta una pagina con una richiesta di login. Dopo aver effettuato l'accesso (admin/password) Burpsuite intercetta la richiesta e ci mostra i parametri. Come prova di manipolazione delle richieste http è possibile inviare una richiesta modificata, per esempio un login con credenziali errate, da Burpsuite e osservare la risposta.