Sylvain THIROINE

Fiche n ° 10 : Installation et configuration de DVWA (Damn Vulnérable Web App)

1) Installation

⇒ apt-get -y install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php git
⇒ git clone https://github.com/digininja/DVWA.git
⇒ mv DVWA /var/www/html
⇒ cd /var/www/html/DVWA

2) configuration

⇒ service mysql start
⇒ mysql – modification des paramètres de mysql

```
create database dvwa;
create user dvwa@localhost identified by 'p@ssw0rd';
grant all on dvwa.* to dvwa@localhost;
flush privileges;
exit
```

⇒ nano config/config.inc.php.dist – pour vérification du port, utilisateur et mot de passe
⇒ chown -R www-data hackable/uploads/ - donner les droits
⇒ chown -R www-data external/ - donner les droits
⇒ chown -R www-data config/ - donner les droits
⇒ nano /etc/php/8.2/apache2/php.ini – modification des paramètres du fichier
allow_url_include = On - Permet les inclusions de fichiers distants (RFI)
allow_url_fopen = On - Permet les inclusions de fichiers distants (RFI)
display_errors = Off - Masque les messages d'avertissement PHP

⇒ service apache2 restart
⇒ cd /var/www/html/DVWA
⇒ mv config/config.inc.php.dist config/config.inc.php
⇒ service apache2 restart
⇒ http://192.168.1.16/DVWA/setup.php ou http://127.0.0.1/DVWA/setup.php
create reset database

⇒ http://IP_LOCAL/DVWA/login.php ou http://localhost/DVWA/login.php
⇒ User : admin – MDP : password