
applications
vulnerabilities
web
attacks
application
security
internet
within
may
cyber
new
crimes
motivations
vulnerability
including
developers
increasing
Cross-Site
attackers
research
number
illegal
offline
information
computer
using
access
able
etc
high

SQLMAP

Plan

- Introduction
- C’est quoi injection SQL
- Conséquences
- SQLMAP
- Techniques
- Comment choisir les cibles ?
- Caractéristiques
- Démonstrations

Introduction

- La plupart des développeurs des applications web sous-estiment le risque de l’injection SQL (classé la 1ére par la communauté OWASP en 2013), cependant, il ’y a deux approches pour réaliser ce genre d’attaque

- La première approche consiste à faire des injections manuellement, alors que la deuxième se base sur l’utilisations des outils automatisées pour détecter et exploiter les vulnérabilités liés à un codage imparfait

C’est quoi injection SQL

- Une injection SQL est une méthode d’exploitation d’une faille de sécurité liée à une base données

- Consister en l’insertion ou l’injection d’une requête SQL par l’intermédiaire des données d’entrée provenant du client à l’application

- Permettre d’obtenir beaucoup d’informations allant de la version du serveur jusqu’à la base de données compléte

Conséquences

- Bypasser une authentification
- Lire des données sensibles depuis les tables de base de données
- Injecter le nom et le schéma de la base de données,
- Lire et écrire dans le système de fichier,
- Exécuter du code PHP,

SQLMAP

- SQLMAP est un outil de test de pénétration open source qui permet de :

  ✓Identifier les paramètres vulnérable (id par exemple)

  ✓Identifier la technique d’injection SQL qui peut être utilisée pour exploiter cette vulnérabilité

  ✓Obtenir la base de données qui contient le gestionnaire d’empreintes digitales,

  ✓Enumérer les données de la base de données en question

  ✓Prendre le contrôle totale sur le serveur de base de données,

Techniques

- SQLMAP détecte et exploite cinq types d’injections SQL:
  - Boolean-Based blind
  - Time-Based blind
  - Error-based
  - UNION query-based
  - Stacked queries

Boolean-based blind

- Le pirate injecte du code, mais ne peut pas accéder directement aux données,
- Cette injection change le comportement de l’application web,
- Le pirate Analyse les pages de réponses à la recherche de différence entre les pages de réponses vraies et celles fausses via:
  - Différentes structure HTML
  - Différents patterns (mots clés)
  - Différents comportements (temps de réponse)
  - Différentes tables de hachages
- Exemples

Time-Based Blind

- Lorsque le pirate ne trouve pas de différences entre les pages de réponses vraies et les pages de réponses fausses, il peut utilisé « Time Delays »,
- Forcer un délai dans la page de réponse lorsque la condition injectée est vrai,
- Les fonctions de délais:
  - SQL Server: waitfor
  - Oracle:dbms_lock,sleep
  - MySQL:sleep or Benchmark Function
- Exemples

•Error-Based

- Le pirate injecte du code provoquant ainsi l’affichage d’un message d’erreur dans la page en question,
- Le message contient des informations sensibles sur le serveur de base de données tels que:

  - La version de MySQL
  - Les noms des différentes bases de données
  - Les noms des tables de chaque base de données
  - Les informations sur les colonnes
- Exemples

Union query-based

- L’opérateur UNION est utilisé dans les injections SQL pour rejoindre une requête
- Permettre d’obtenir le résultat de la requête forgé ainsi que la requête d’origine
- Permettre à l’appareil d’essai d’obtenir les valeurs des colonnes des autres tables

Stacked queries

- Consiste à exécuter plusieurs requêtes dans une même transaction

	ASP.NET	ASP	PHP
MySQL	Supported	Not supported	Not Supported
MSSQL	Supported	Supported	Supported
Postgresql	Supported	Supported	Supported

Exemples:

SELECT name FROM record WHERE id = 1; DROP table record; DROP table address--

Comment choisir les cibles ?

- Fournir un seul URL cible,
- Fournir une liste d’URL(s) cibles depuis les requêtes du fichier log de Burp proxy ou WebScarab proxy,
- Obtenir les requêtes http à partir d’un fichier texte,
- Obtenir la liste des cibles en fournissant à sqlmap un Google dork (interroge le moteur de recherche Google et analyse sa page de résultats),
- Définir des expressions régulières afin d’identifier les adresses analysées pour tester,

Caractéristiques

- Analyser les formulaires HTML à partir de l’URL cible,
- Estimer la durée d’arrivée pour chaque requête,
- Enregistrer automatiquement la session sur un fichier texte en temps réel lors de l’extraction des données,
- Soutenir la reproduction de la structure et les entrées des tables de base de données,
- S’intégrer avec d’autres projets de sécurité informatique open source tel que Metasploit et w3af,

Caractéristiques (Suite)

- Récupérer la bannière SGBD, l’utilisateur de la session et les informations de base de données actuelle,
- Enumérer les utilisateurs, les mots de passes hachés, les privilèges, les rôles, les bases de données, les tables et les colonnes,
- Vider le contenu des tables de base de données, une plage d’entrées ou des colonnes spécifiques selon le choix de l’utilisateur,
- Télécharger et envoyer des fichiers à partir du système de fichiers serveur de base de données pour les bases de données MySQL, PostgreSQL ou Microsoft SQL Server,

Démonstrations