Sqlmap 简介

目录 | CONTENTS

Part1 ： Sqlmap 基本知识

SqlMap 的基本知识

sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

sqlmap 是一个开源的渗透测试工具，它可以自动检测、利用 SQL 注入漏洞以及入侵数据库服务器的过程。它配备了强大的检测引擎，拥有许多渗透测试人员所需的良好特性，能够通过丰富的设置来实现数据库指纹识别、数据库获取数据、访问底层文件系统以及通过外部连接在操作系统上执行命令。

Sql 官网—— https://sqlmap.org/

SqlMap 的基本知识

SqlMap 是开源的自动化 SQL 注入工具，由 Python 写成，具有如下特点：
1、完全支持 MySQL、 Oracle、 PostgreSQL、 Microsoft SQL Server、 Microsoft Access、 IBM DB2、 SQLite、 Firebird、 Sybase、 SAP MaxDB、 HSQLDB 和 Informix 等多种数据库管理系统。
2、完全支持布尔型盲注、时间型盲注、基于错误信息的注入、联合查询注入和堆查询注入。
3、在数据库证书、 IP 地址、端口和数据库名等条件允许的情况下支持不通过 SQL 注入点而直接连接数据库。
4、支持枚举用户、密码、哈希、权限、角色、数据库、数据表和列。
5、支持自动识别密码哈希格式并通过字典破解密码哈希。
6、支持完全地下载某个数据库中的某个表，也可以只下载某个表中的某几列，甚至只下载某一列中的部分数据，这完全取决于用户的选择。
7、支持在数据库管理系统中搜索指定的数据库名、表名或列名
8、当数据库管理系统是 MySQL、 PostgreSQL 或 Microsoft SQL Server 时支持下载或上传文件。
9、当数据库管理系统是 MySQL、 PostgreSQL 或 Microsoft SQL Server 时支持执行任意命令并回现标准输出

Part2 ： sqlmap 下载

Sqlmap 下载

官网下载—— https://sqlmap.org/

THANKS!