SQLMAP

- **sqlmap对URL干嘛**
  - 1.判断可注入的参数
  - 2.判断可以用哪种SQL注入技术来注入
  - 3.识别出哪种数据库
  - 4.读取用户选择的数据库
- **5种注入模式**
  - 基于布尔的盲注
  - 基于时间的盲注
  - 基于报错的注入
  - 联合查询注入
  - 堆查询注入
- **支持哪些数据库注入**
  - MySql、Oracle、PostgreSQL
  - Microsoft SQL Server、Microsoft Access、IBM DB2
  - SQLite、Firebird、Sybase和SAP MaxDB
- **参数**
  - 1.观察数据
    - -v参数，共有7个等级，默认为1
    - -v 0 只显示python错误以及严重的错误信息
    - -v 1 同时显示基本信息和警告信息
    - -v 2 同时显示debug信息
    - -v 3 同时显示注入的payload
    - -v 4 同时显示HTTP请求
    - -v 5 同时显示HTTP响应头
    - -v 6 同时显示HTTP响应页面
  - 2.获取目标的方式
    - 1.直接连接到数据库 —— 参数： -d
    - 2.目标URL —— 参数：-u
  - 3.请求方式
  - 4.列数据
    - 标志 —— -b: 返回数据库版本号
    - 用户 —— --current-user:获取管理数据库的用户
    - 当前数据库 —— --current-db: 返回当前连接的数据库
    - 当前用户是否为管理员 —— --is-dba:如果是会返回true
    - 列出数据库管理用户 —— --users:有权限读取数据库的用户
    - 列出破解用户数据库的hash —— --passwords
    - 列出数据库管理员的权限 —— --privileges
    - 列出数据库系统中的数据库 —— --dbs:当前用户有权限读时，即可列出数据库
    - 列出数据库中的表 —— --tables
    - 列出数据库表中的字段 —— --columns;-D xxx：来指定数据库
    - 列出数据库的架构 —— --schema：包含所有数据库、表和字段以及各自的类型
    - 列出表中数据的个数 —— --count
    - 获取整个表的数据 —— --dump：获取指定库中所有表的内容
    - 获取所有数据库表的内容 —— --dump-all
    - 运行自定义SQL语句 —— --sql-query
    - 搜索字段、表、数据库 —— --search
  - 暴力破解
    - 暴力破解表名 —— --common-tables:当-tables无法获取数据库的表时，可以使用此参数
    - 暴力破解列名 —— --common-columns

试用版 XMind:ZEN 试用版