

sqlmap 是使用 python 开发的,我们可以直接查看它的全部源代码,通过查看这些比较牛的工具的源码,有助于我们更好的学习 sql 注入。

sqlmap 支持 MySQL,Oracle,PostgreSQL,Microsoft SQL Server,Microsoft Access,IBM DB2,SQLite,Firebird,Sybase 和 SAP MaxDB 等数据库的各种安全漏洞检测。

sqlmap 支持五种不同的注入模式:

- | 基于布尔的盲注,即可以根据返回页面判断条件真假的注入;
- | 基于时间的盲注,即不能根据页面返回内容判断任何信息,用条件语句查看时间延迟语句是否执行(即页面返回时间是否增加)来判断;
- | 基于报错注入,即页面会返回错误信息,或者把注入的语句的结果直接返回在页面中;
- | 联合查询注入,可以使用 union 的情况下的注入;
- | 堆查询注入,可以同时执行多条语句的执行时的注入。