网络安全与对抗 第2讲 Easy Sql 2

打开靶机就看到这个登录界面，随便输入一个密码看看有什么回显

随便输入一个弱口令进去（因为有些简单的web题密码真的就是弱口令，想在这里碰个运气但是貌似没成功），回显了一个提示让我们看看页面源代码

源代码如下，敏锐地发现sql语句，发现密码和账号是用一对单引号括起来的

```
</style>
<title>请登录</title>
</head>

<body>
<div id="msgbox">
    <div id="title">请登录</div>
    <div id="message">
    <!--有没有办法绕过一下呢?-->
    <!--SELECT * FROM user_tab WHERE user = '$name' AND password='$passwd'-->
    <form method="post" action="index.php">
    用户名: <input class="username_input" type="text" name="name" value="admin"
    <br /><br />
    密码: <input class="pass_input" type="password" name="passwd" value="">
    <br /><br />
    <input class="infsubmit" type="submit" value="提交">
    </form>
    </div>

    <div class="desc">

    </div>
    <div id="info">
    密码错误! <br>看看网页源代码会有发现哦(*^_^*)        </div>
</div>
/body></html>
```

那我们可以尝试一下用万能密码

万能密码的原理

mysql 中and和or的优先级

比如说:

() > and > or

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

复制

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

那么对于这道题我们可以在密码中输入XXX' or 1=1#(#用于注释掉后面的语句，防止后面的语句影响新构造的sql查询语句)

那么实行的sql查询语句就是

```
select * from user_tab where user = 'admin' and password = 'XXX' or 1=1#
```

因为and的优先级大于or，会先执行user = 'admin' and password ='XXX'，后再执行or后面的1=1，因为1=1恒成立，所以这个sql语句恒成立。所以能够获得flag