NeverLan writeup

原创

忙碌者61 于 2019-02-03 12:55:07 发布 125 收藏

分类专栏： CTF 文章标签： Hgame

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/qq_43154554/article/details/86757125

版权

CTF 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

NeverLan writeup

Things are not always what they seem

看到这么长的标题，以及题目这么明显的提示，

flag必然很浅显，果然，查看一下源代码直接发现。

```
you up"></div>

re career.<br>

't as it appears... flag{Whale_w0uld_y0u_l00k3y_th3r3}<
```

SQL FUN 1

本以为是sql注入，后来发现只是一个select与where的查询

于是构造下列语句：

select Password from users where Fname='Jimmy'

id	Username	Fname	Lname	Email	Password
2	JimWill	Jimmy	Willman	SQL@example.com	flag{SQL_F0r_Th3_W1n}

SQL FUN 2

这题套路与之前相同，就是涉及两个表，稍微绕了点弯

首先构造：select * from users where Lname='Miller'

得到下图：

id	Username	Fname	Lname	Email
5	DisUser	Tom	Miller	Miller@example.com

到这步，再用这些数据去尝试查询passwd表内的password，经测试，只有id有用。
select Password from passwd where id=5

结果却只得到了一堆乱码

Password
Tm9wZS4uLiBXcm9uZyB1c2Vy

猜想这有可能是base64，可惜不是，无奈之下，只好尝试展开所有表，于是构造：
select * from passwd where id=5
发现user_id,这就不寻常了，可能这才是真的id,于是抛却id，使用user_id,直接select,即构造
select * from passwd where user_id=5
得到ZmxhZ3tXMWxsX1kwdV9KMDFOX00zP30=
base64解码最终得到flag