实验吧 登陆一下好吗?? 简单注入 By Assassin

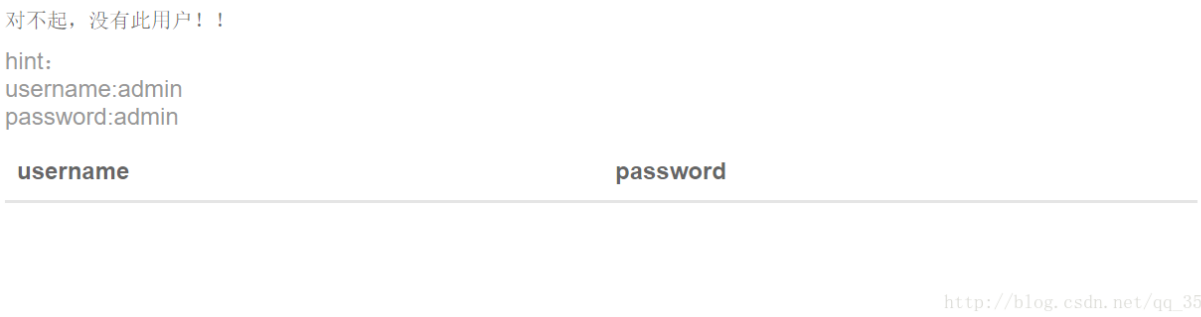
原创

Assassin__is__me 于 2017-01-30 11:33:07 发布 6282 收藏

分类专栏： Web

本文链接：https://blog.csdn.net/qq_35078631/article/details/54782596

题目想法挺简单的，是时候学习一下注入的套路了，真的要不简单的也想不到。



发现* / select union or 都被过滤了，一开始想的太复杂了，以为是个什么waf过滤什么的，但是看了pcat前辈的WP发现真的很基础吧。

但是and ‘什么的都没有过滤！

payload真的简单到淫荡，看一下就是这样的

admin-> ‘=’

password-> ‘=’

真是醉了，为什么呢，类似这样的语句

$sql = “select user from flag where user=’\$_POST[‘user’]’ and password=’\$_POST[‘password’]’”;

如果我们按照上面输入就成了

$sql = “select user from flag where user=’**‘=’**” and password=’**‘=’**‘”;

user=”返回的是NULL=”也是符合条件的，最后就是

$sql = “select user from flag where 1 and 1”;

ctf{[redacted]}

hint：
username:'='
password:'='

username	password
hell02w	69bc7cf459bcff03625939193ec71e0e
w0d3rkun	dbb9111e4ed03e2d4021c3c3b0ac8749
mut0r3nl	86846490336911c0f3c6e07cc197d22c

还是需要多实验啊~