实验吧-后台登录 Writeup

原创

baynk 于 2019-07-28 01:58:12 发布 238 收藏 1

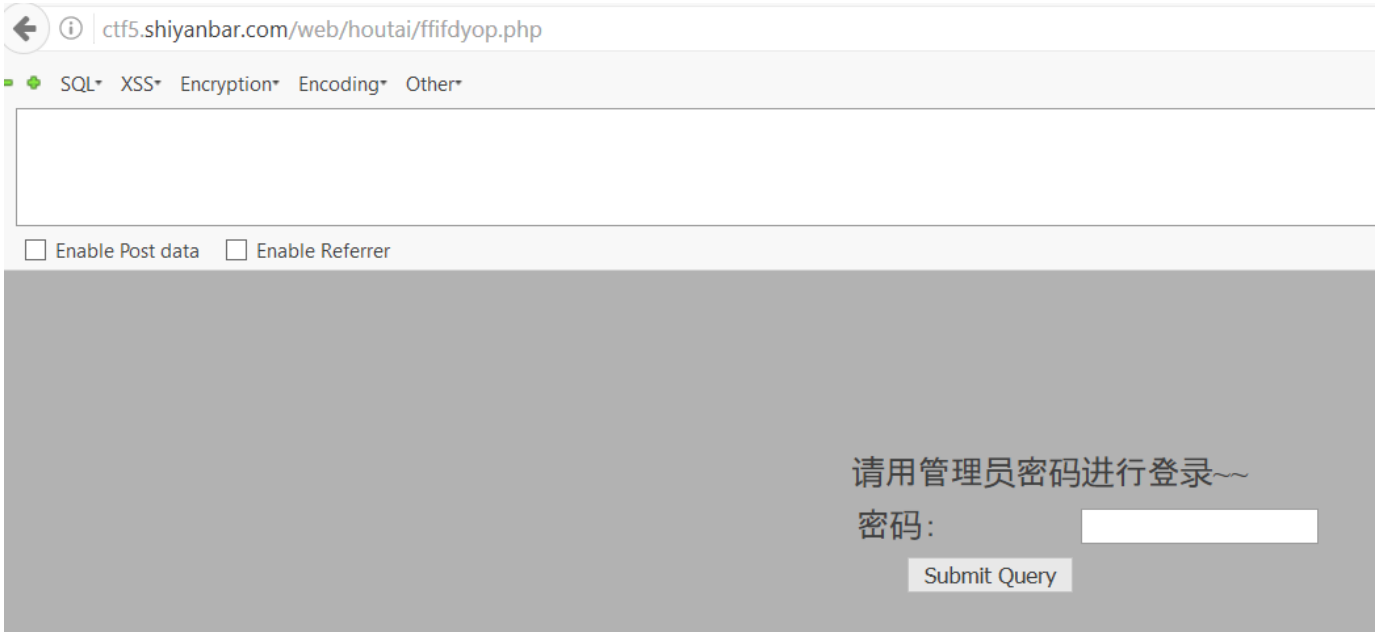
分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧

本文链接：https://blog.csdn.net/u014029795/article/details/97457928

感觉学习到了瓶颈了，最近还在备考S+，工作也特别忙，有空的话，每天搞个web相关的CTF题目做做吧，学些姿势。。

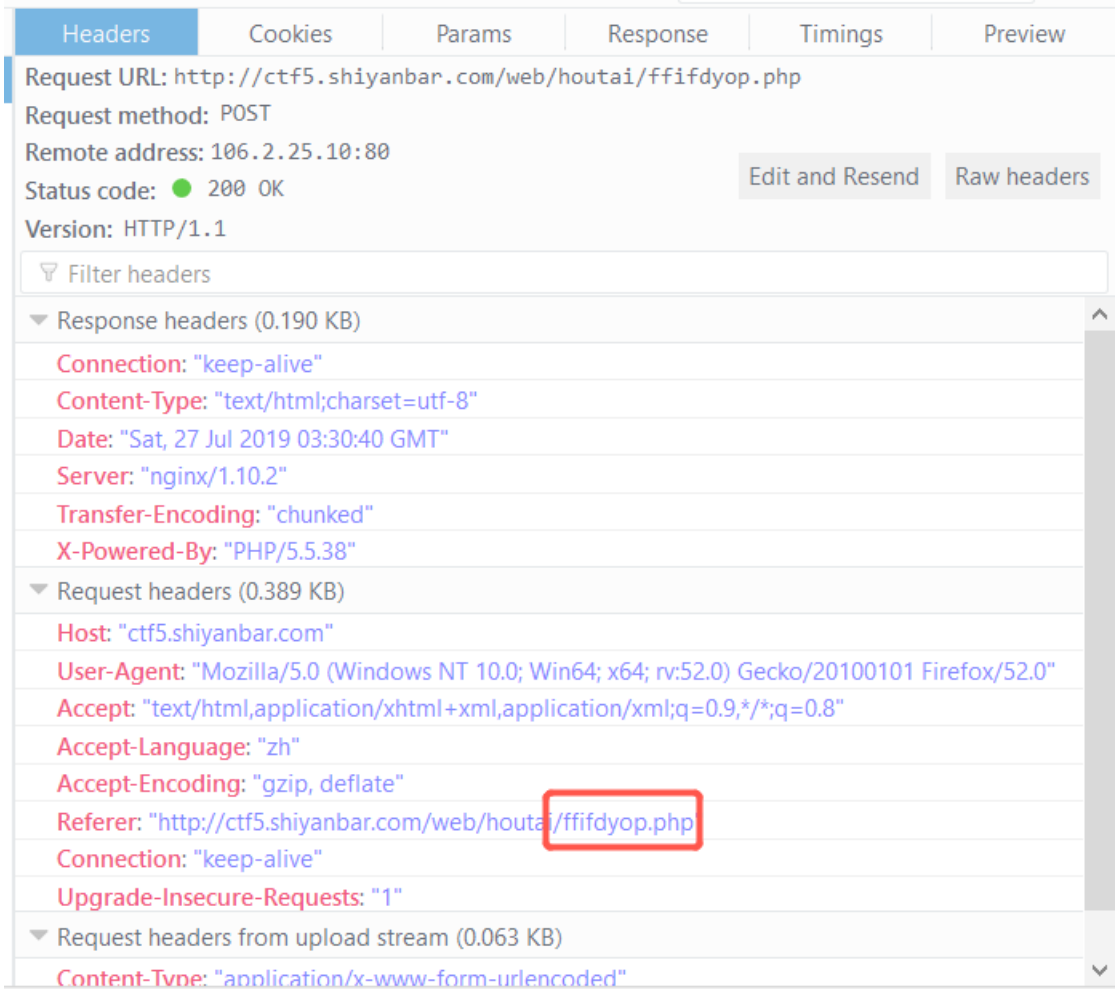
过程

1. 一进去就发现是需要登陆，第一反应是注入。。。

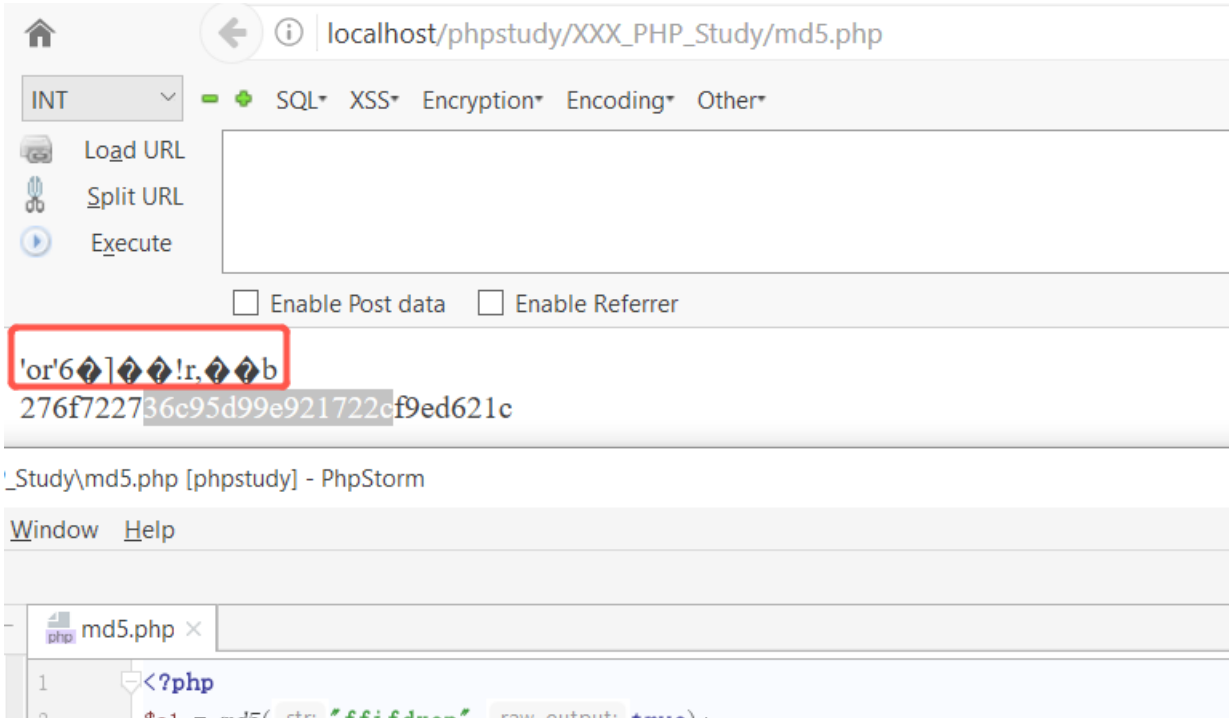


2. 试了一会，万能密码啥的发现都提示密码错误。。。
3. 审查元素，发现了注释，已经给了SQL语句了，发现密码是被md5加密的，并且只输出16位，并且以"raw binary"的形式输出，这个地方是真的怪，查的php官方手册，刚刚开始以为是16进制转2进制，然后2进制转字符串，结果完全不是那么回事，拿php写了以后才知道是啥子个情况，知道这玩意的可以告诉我下阿。。

4. 也就是说，想实现万能密码的功能，那么就必须在密码后面加上or，但是密码是被hash存储的，所以只能找一个字符串哈希以后能有or出现在中间就可以了，因为代码后面也只要求能查到数据即可。。。但是这个or怎么找。。。
5. 接着去检查头部信息，还真发现了一个可疑的单词。。



6. 试了下，真的成功了。。然后手工的还原了下不成功没有or，然后去php里面才还原成功，有点怪。。。。



```php
$a1 = md5( str: 'ffifdyop' , raw_output: true);
$a2 = md5( str: "ffifdyop");
echo $a1;
echo "<br>";
echo $a2;
?>
```

总结

虽然很顺利的拿下flag了。。。感觉没什么好的收获，php的Md5函数熟悉了点，还出了个大问题没解决，睡了睡了，下次再搞