

后台登录（实验吧）writeup

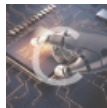
原创

[cheese0_0](#)  于 2018-07-30 16:44:53 发布  934  收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/cheese0_0/article/details/81287331

版权



[web](#) 同时被 3 个专栏收录

5 篇文章 0 订阅

订阅专栏



[安全](#)

16 篇文章 0 订阅

订阅专栏



[writeup](#)

5 篇文章 0 订阅

订阅专栏

本博客多为与信息安全相关的博文，我希望以此来记录自己的学习轨迹，如有错误，欢迎交流指正。

终于下定决心入门ctf，在实验吧上尝试第一道题、迈出第一步。

原题链接：<http://ctf5.shiyanbar.com/web/houtai/ffifdyop.php>

先看源码

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Document</title>
6 </head>
7 <body style="background-color: #999">
8   <div style="position:relative;margin:0 auto;width:300px;height:200px;padding-top:100px;font-size:20px;">
9     <form action="" method="post">
10      <table>
11        <tr>
12          <td>请用管理员密码进行登录~~</td>
13        </tr>
14        <tr>
15          <td>密码: </td><td><input type="text" name='password'></td>
16        </tr>
17        <tr>
18          <td><input type="submit" name='submit' style="margin-left:30px;"></td>
19        </tr>
20      </table>
21    </form>
22    flag is :flag{ffifdyop_has_trash} </div>
23    <!-- $password=$_POST['password'];
24    $sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
25    $result=mysqli_query($link,$sql);
26    if(mysqli_num_rows($result)>0){
27      echo 'flag is :'.$flag;
28    }
29    else{
30      echo '密码错误!';
31    } -->
32 </body>
33 </html>
34
```

https://blog.csdn.net/cheese0_0

关注这里的sql语句

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

然后，发现密码被MD5加密了，就是搜索与MD5相关内容，发现下面这些内容。

博文链接：https://blog.csdn.net/qq_31481187/article/details/59727015

MD5注入

```
$sql = "SELECT * FROM admin WHERE pass = '".md5($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

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

提供一个字符串：ffifdyop

于是直接输入ffifdyop就可以得到flag了。
其实先是发现ffifdyop就在url中，抱着碰运气的想法成功了。

请用管理员密码进行登录~~

密码:

提交

```
flag is  
:flag{ffifdyop_has_trash}
```

https://blog.csdn.net/cheese0_0



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)