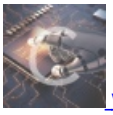
后台登录（实验吧）writeup

原创

cheese0_0 于 2018-07-30 16:44:53 发布 934 收藏


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

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Document</title>
</head>
<body style="background-color: #999">
    <div style="position:relative;margin:0 auto;width:300px;height:200px;padding-top:100px;font-size:20px;">
    <form action="" method="post">
        <table>
            <tr>
                请用管理员密码进行登录~~
            </tr>
            <tr>
                <td>密码：</td><td><input type="text" name='password'></td>
            </tr>
            <tr>
                <td><input type="submit" name='submit' style="margin-left:30px;"></td>
            </tr>
        </table>
    </form>
    flag is :flag{ffifdyop_has_trash}    </div>
    <!-- $password=$_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!';
        } -->
</body>
</html>
```


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。
原博文链接：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。