

实验吧 web渗透至后台登陆

原创

Chen 陈某人 于 2018-03-24 21:52:44 发布 3121 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/qq_35586327/article/details/79682067

版权

点开链接的源码可以发现密码是经过md5哈希加密的，所以先不考虑去破解密码，先看看有没有其他的提示可以看到php文件的名称并没有实际意义，于是就试了一下发现flag就是ffifyop，所以说这道题完全是靠脑洞的。。。

<http://ctf5.shiyanbar.com/web/houtai/ffifyop.php>

```
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 请用管理员密码进行登录~~
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 </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
```

彼此无挂也无牵