

实验吧 后台登录

原创

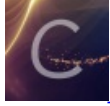
Hugo5332 于 2018-03-09 01:44:14 发布 7319 收藏 1

分类专栏: [信息安全](#)

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/xxxslinyue/article/details/79492109>

版权



[信息安全](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

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

先看下源码, 发现这个, emmm注入无疑了。

```
<!-- $password=$_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!';
} -->
```

ody> <http://blog.csdn.net/xxxslinyue>

咋整。。。没遇到过这种情况啊, 想着如何构造' or 1=1之类的, 什么情况下md5加密后会形成这玩意呢。。。搞来搞去搞不出。。回过头来看题。。。觉得url里面ffifyop有点奇怪, 这个是啥意思? 直接拿去交一发, 结果。。。。

请用管理员密码进行登录~~

密码:

提交

flag is :flag{ffifyop_has_trash}

<http://blog.csdn.net/xxxslinyue>

一时无语。。。还是经验太少。。