

原创

写不出代码的码农  于 2019-02-28 21:52:39 发布  300  收藏

分类专栏: [菜鸡啄米](#)

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\\_41840600/article/details/88045933](https://blog.csdn.net/qq_41840600/article/details/88045933)

版权



[菜鸡啄米](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

## 硬盘炸了, 临时凭记忆写了一点。。。

### 1、md5碰撞

#### md5 collision

Web 20pt

SOLVERS: 1682

源码 (PHP)

```
$md51 = md5('QNKCDZO');  
$a = @$_GET['a'];  
$md52 = @md5($a);  
if(isset($a)){  
if ($a != 'QNKCDZO' && $md51 == $md52) {  
    echo "nctf{*****}";  
} else {  
    echo "false!!!";  
}}  
else{echo "please input a:";}
```

题目地址

FLAG

取消

提交

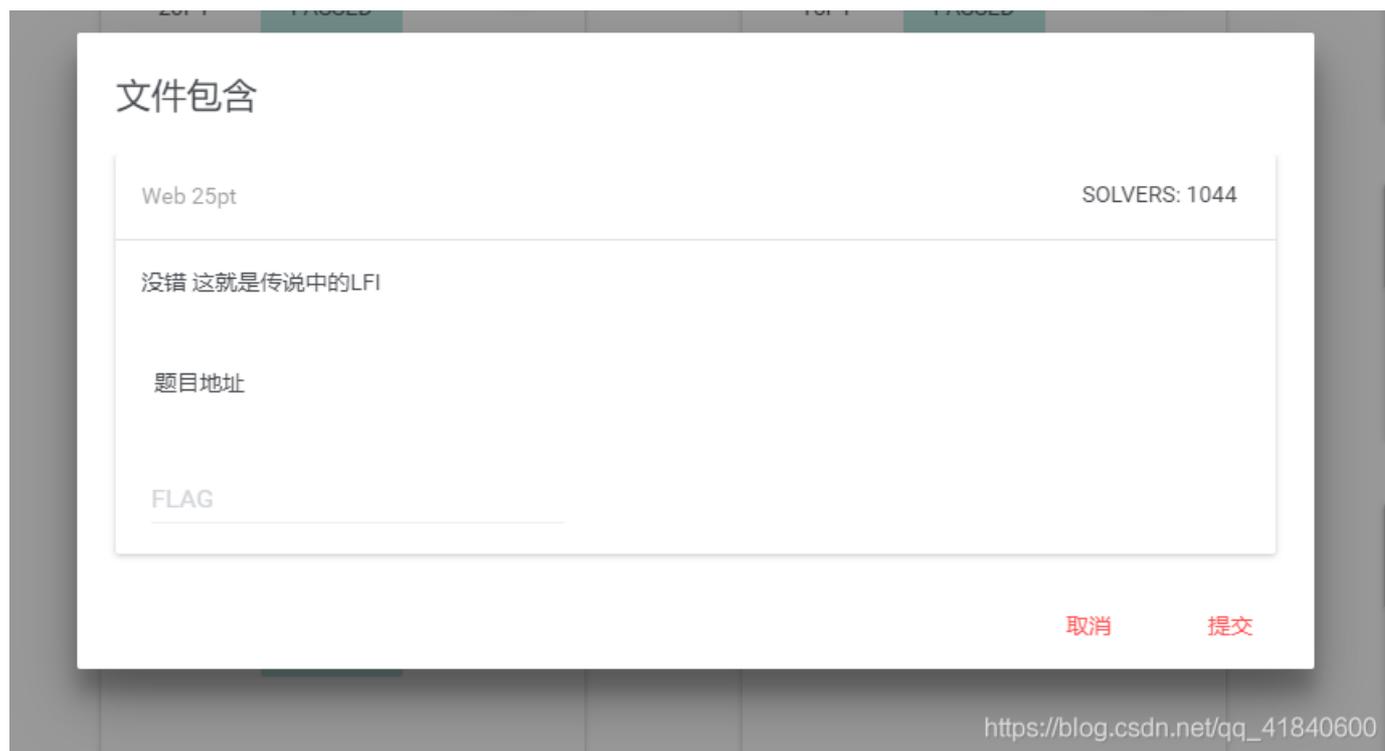
GBK Injection

/x00

bypa

[https://blog.csdn.net/qq\\_41840600](https://blog.csdn.net/qq_41840600)

随后我百度md5值，巴拉巴拉一大长串，大概得出MD5值为弱口令，存在md5碰撞的方法，可以做到使头部相等得到\*对应的flag  
2、文件包含



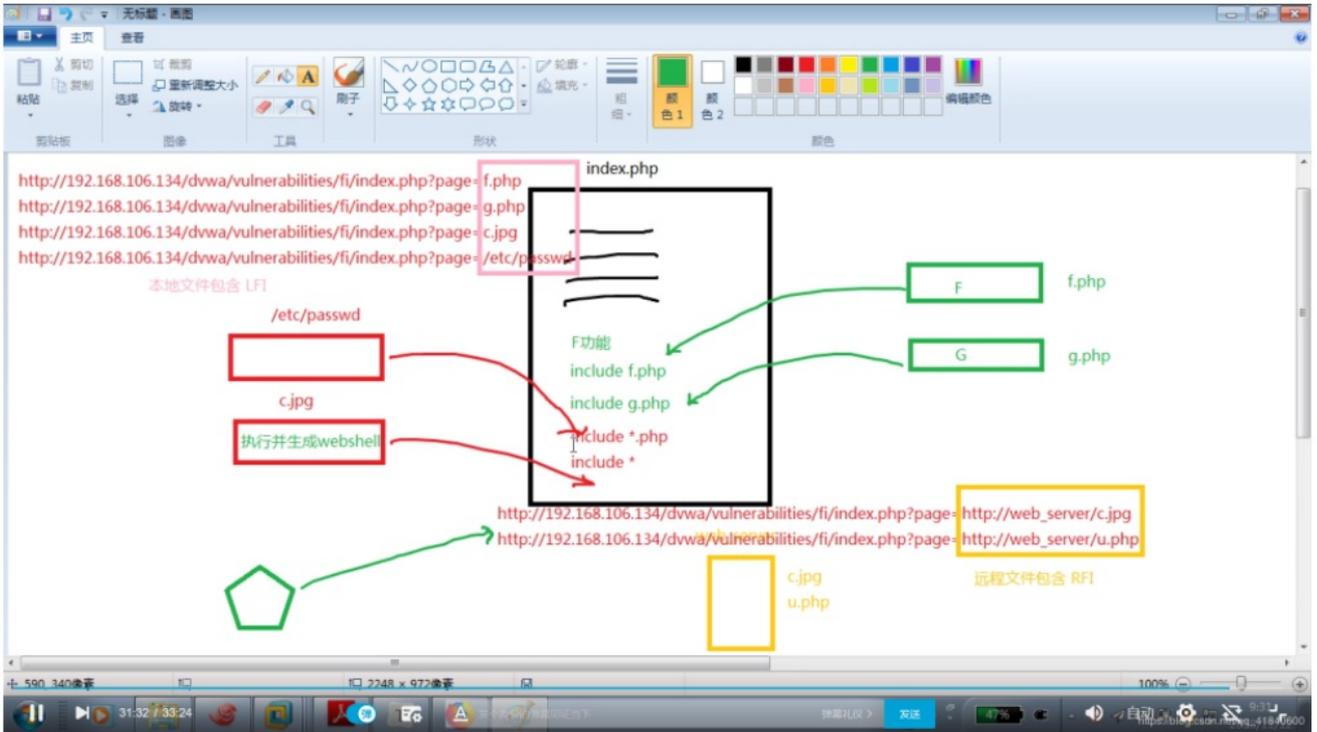
文件包含类似于c中的include作用，开发人员在写代码时要调用多个函数库就可以使用文件包含，文件包含又分为本地文件包含和远程文件包含。

这道题还有PHP的filter协议

[https://blog.csdn.net/qq\\_38183886/article/details/79374951](https://blog.csdn.net/qq_38183886/article/details/79374951)

## 文件包含漏洞

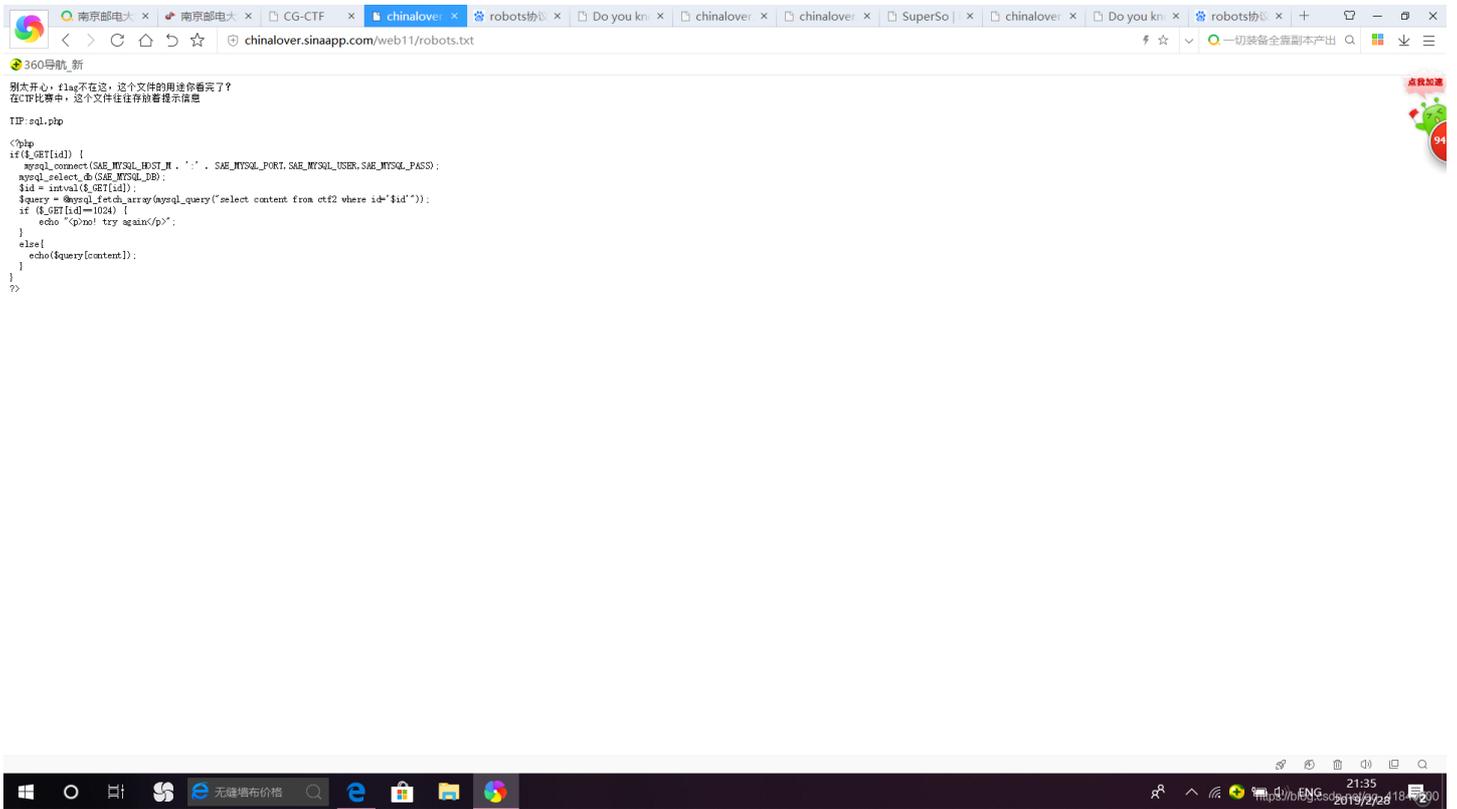
文件包含漏洞又分为本地文件包含和远程文件包含



文件包含可类比为c语言中的include，java中的import语句可以方便开发人员调用函数库  
其中本地文件包含指的是上传一个含有创建一个php指令的php或txt文件

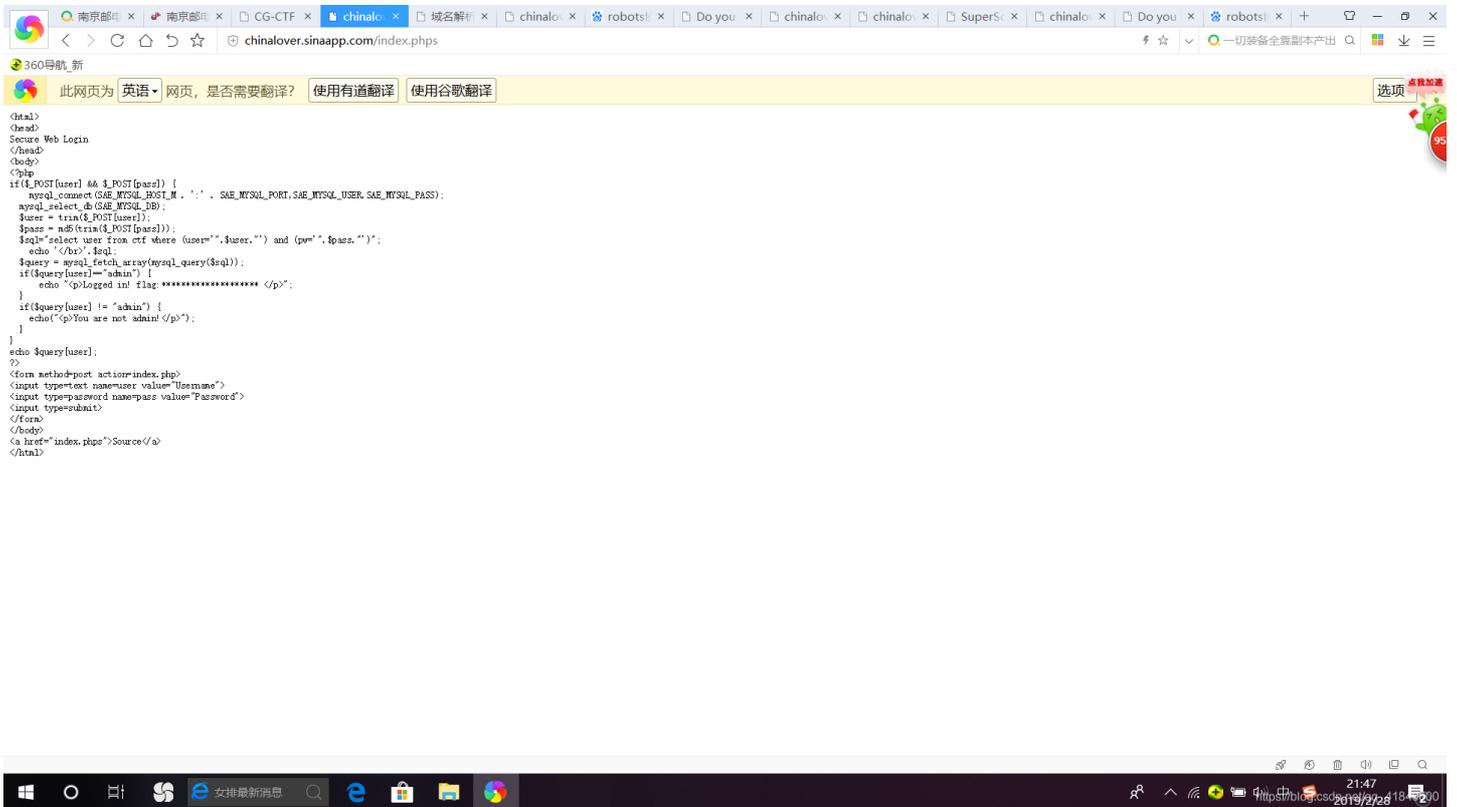
[https://blog.csdn.net/qq\\_41840600](https://blog.csdn.net/qq_41840600)





根据大概意思尝试提交1024，失败，1024.3得出flag。应该是精度问题

#### 4、sql注入



代码的意思就是post user与pass,然后提交post的user必须是admin.但是密码不知道,所以就

得在sql= 这句想办法绕过and(pw= " pass.") 这段

所以构造的语句就是这样

admin')#.

得到sql:

"select user from ctf where (user='admin')#.'"前者被注释，得到flag