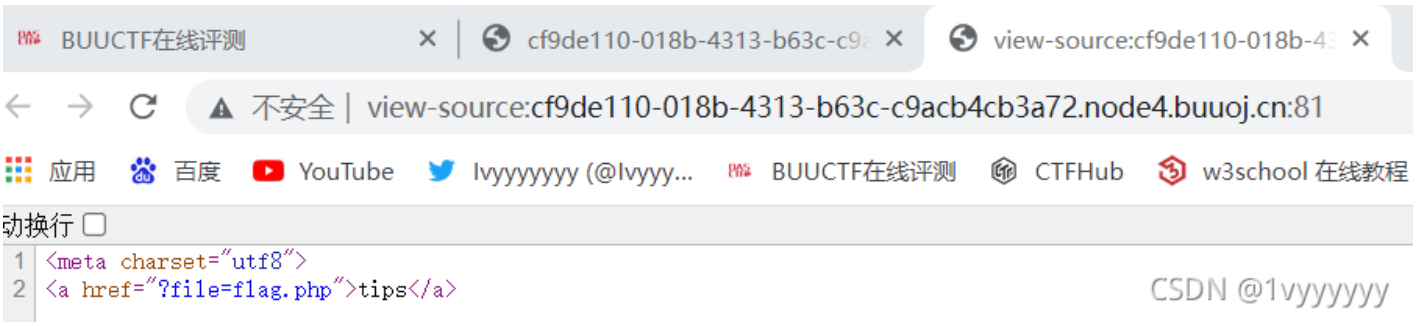
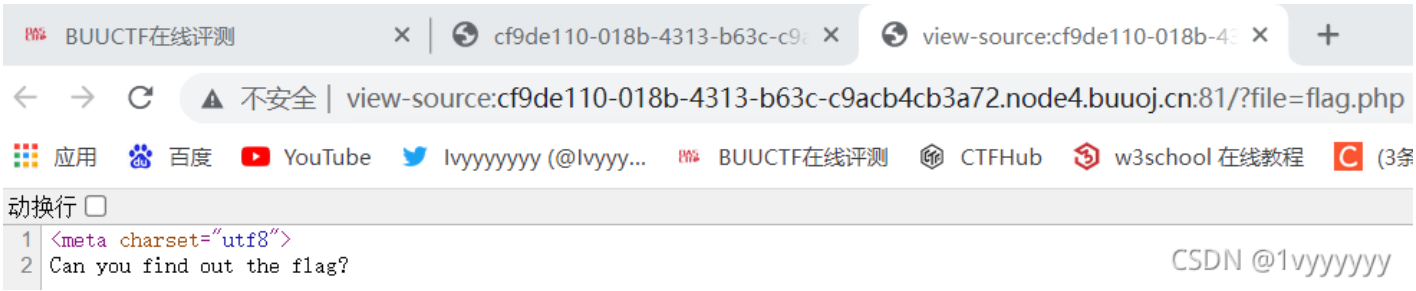
BUU 文件包含漏洞-[ACTF2020 新生赛]Include

原创

1vyyyyyy 于 2021-10-16 22:17:38 发布
分类专栏： BUUCTF writeup 文章标签： php web安全

一、题目





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

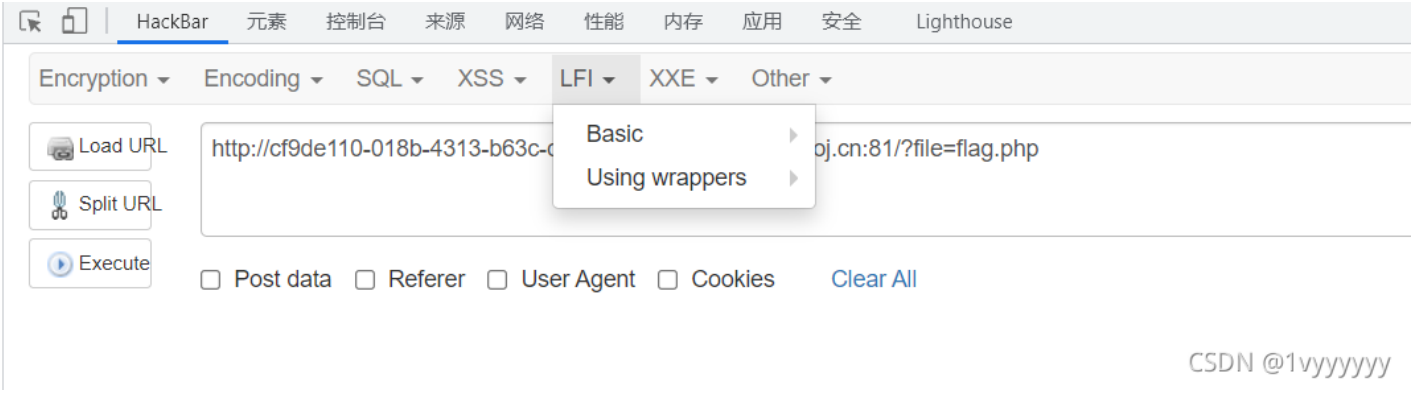
将要执行的php代码·直接用POST方式上传

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

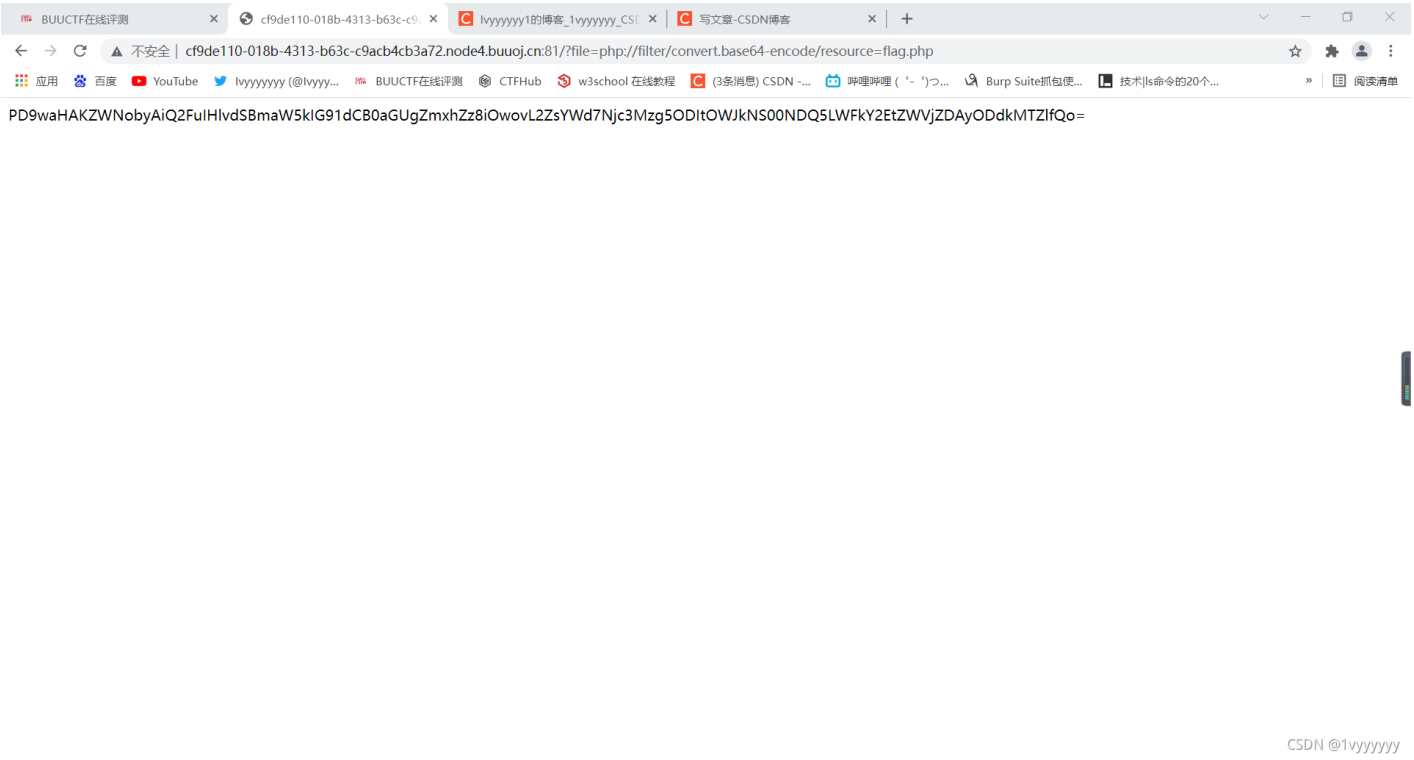
2. 这里用 hackbar 操作



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
```



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-eecd0287d16e}
```


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>';
}
?>
```


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