【XCTF高手进阶区】web4_Web_php_include writeup（一）

原创

Mitch311 于 2021-01-27 23:23:13 发布 148 收藏
分类专栏： CTF 文章标签： 字符串 php java web python

web4_Web_php_include

原题链接

key:php://伪协议+大小写绕过

> 此题其他解法□
>
> XCTF高手进阶区 web4_Web_php_include writeup（二）
>
> XCTF高手进阶区 web4_Web_php_include writeup（三）
>
> XCTF高手进阶区 web4_Web_php_include writeup（四）

①页面打开后是一串php代码□

```
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```

看到了include()函数，十有八九是道文件包含题

> **造成文件包含漏洞的函数通常有：**
> **include、require、include_once、require_once、highlight_file、show_source、file_get_contents、fopen、file、readline**

②进行代码审计

先来简单了解一下本题涉及到的几个php函数□

> **知识补充**
>
> **strstr() 函数搜索字符串在另一字符串中是否存在，如果是，返回该字符串及剩余部分，否则返回 FALSE（区分大小写）**
>
> **另外，stristr()函数 不区分大小写**
>
> **str_replace() 函数替换字符串中的一些字符（区分大小写）**
>
> **另外，str_ireplace()函数不区分大小写**

分析代码可知**程序过滤掉了page中存在的php://伪协议字符**

③既然题目想屏蔽php://伪协议

那么首先想到的思路就是把input输入流include包含进来

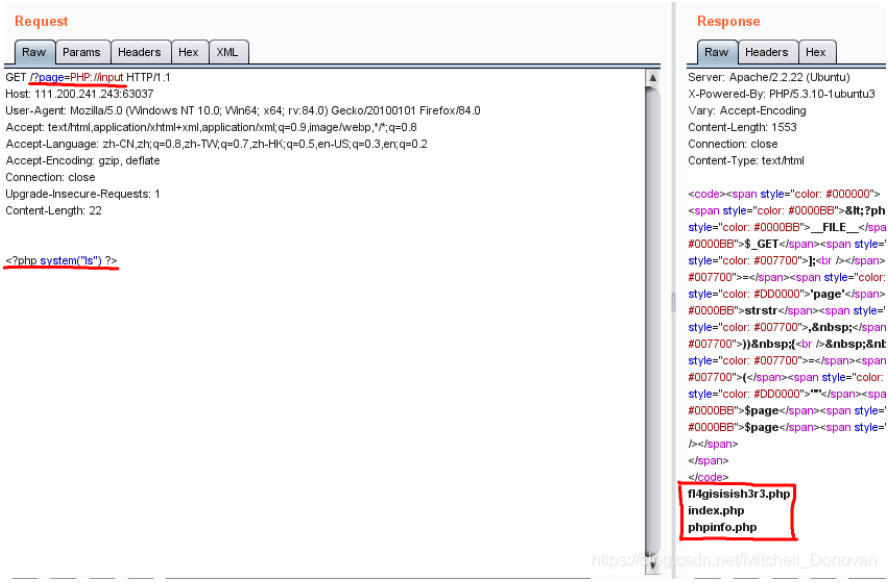
但是直接page=php://input肯定不行

但是strstr()函数区分大小写，可以**构造page=PHP://input**

然后再传入我们的system命令

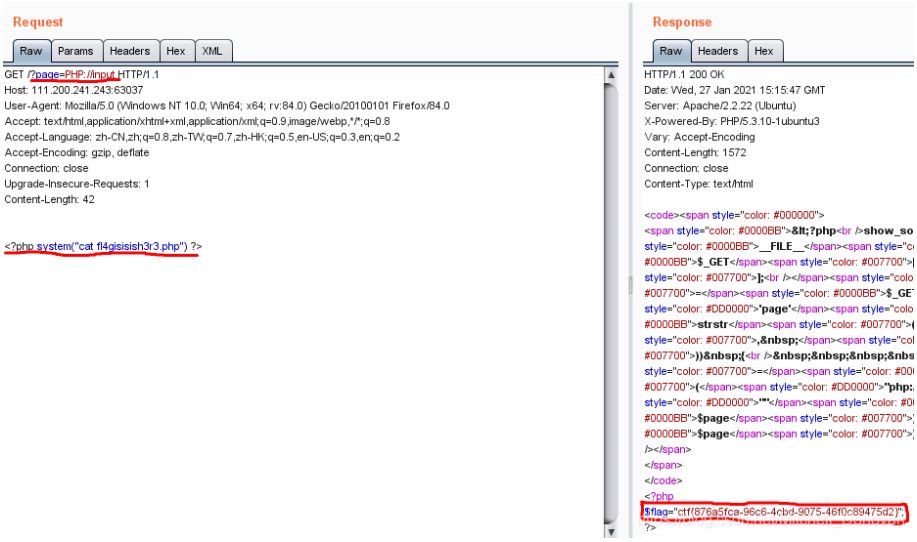
> **如何判断能否使用system命令**
>
> **可以先传入<?php phpinfo() ?>看看能否成功执行**

执行成功□



发现了目标文件fl4gisisish3r3.php

cat一下得到flag



另外我想说的是，不知道是我的原因还是题的原因，这题我用hackbar提交POST请求一直没有响应，被逼无奈只好用burpsuite了