

【XCTF高手进阶区】web7_warmup writeup（二）

原创

Mitch311 于 2021-02-14 00:50:05 发布 57 收藏 1

分类专栏: [CTF](#)

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/113805121

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

订阅专栏

web7_warmup

[原题链接](#)

key:php代码审计+文件包含+URL二次编码

①环境打开后页面显示一个滑稽☹



https://blog.csdn.net/Mitchell_Donovan

查看源代码后发现线索source.php☹

```
Q 搜索 HTML
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <!--source.php-->
    <br>
    
  </body>
</html>
```

②在地址栏后加上/source.php访问, 获得一段php代码

```

<?php
highlight_file(__FILE__);
class emmm
{
    public static function checkFile(&$page)
    {
        $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
        if (! isset($page) || !is_string($page)) {    #$page不存在或不是字符串
            echo "you can't see it";
            return false;
        }

        if (in_array($page, $whitelist)) {    #$page存在于$whitelist数组
            return true;
        }

        $_page = mb_substr($page,0,mb_strpos($page . '?', '?')    #截取$page中首次出现?之前的部分
        );
        if (in_array($_page, $whitelist)) {    #该部分是否存在于$whitelist数组
            return true;
        }

        $_page = urldecode($page);    #对$page进行url解码
        $_page = mb_substr($_page,0,mb_strpos($_page . '?', '?'));    #截取$page中首次出现?之前的部分
        if (in_array($_page, $whitelist)) {    #该部分是否存在于$whitelist数组
            return true;
        }
        echo "you can't see it";
        return false;
    }
}

if (! empty($_REQUEST['file'])    #检查file变量是否为空
    && is_string($_REQUEST['file'])    #检查file变量是否是字符串
    && emmm::checkFile($_REQUEST['file'])    #调用检查函数checkFile()
) {
    include $_REQUEST['file'];    #包含并运行指定文件
    exit;
} else {
    echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
}

?>

```

③进行代码审计，除了source.php还发现了一个hint.php

文件名都暗示到这程度了，必须得去看看，果然获得了重要线索□

flag not here, and flag in fffffllllaaaagggg

④回来继续代码审计□

首先定义了一个类，类里面有一个检查函数

检查函数里首先定义了一个白名单变量（`$whitelist`），随后是一系列if语句，能返回true或false

类之后有一个if语句，同时满足三个条件后会包含并运行文件变量file，这个file是我们自己GET或POST提交的变量

这三个条件分别是：

- （1）检查file变量是否为空
- （2）检查file变量是否为字符串
- （3）检查函数返回值是否为true

传参变量file肯定不是空的（不然我们待会传它干嘛），当然也一定是字符串格式

关键问题就在于怎么让检查函数checkFile()返回值为true

现在我们再回来看检查函数checkFile()

第一个if语句，如果\$page不存在或不是字符串，返回false

第二个if语句，如果\$page存在于\$whitelist数组中，返回true

第三个if语句，截取\$page中首次出现?之前的部分，如果该部分存在于\$whitelist数组中，返回true

第四个if语句，先对构造的payload进行url解码，再截取传进参数中首次出现?之前的部分，如果该部分存在于\$whitelist中，返回true

⑤在这里我们不再用第三个if语句

第三个if语句解题———[XCTF高手进阶区 web7_warmup writeup \(一\)](#)

运用第四个if语句也可以达到目的

所以payload的前半部分就是source.php或hint.php，再用一个?截断，后面加上我们想本地包含并执行的文件路径就可以了

问题是现在我们只知道了目标文件名是ffffllllaaaagggg，还不知道它的路径

