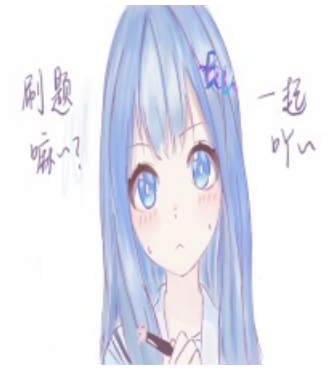
buuctf——Warmup

原创

马戏团小丑 于 2022-03-05 11:02:15 发布 134 收藏

分类专栏： buuctf杀我 文章标签： python c语言 开发语言

本文链接：https://blog.csdn.net/qq_51796436/article/details/123290479



打开题目F12有注释source.php

那访问网址： `题目/source.php` 出现如下题目代码：

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you cant see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?' , '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you cant see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

`/hint.php`的内容：`flag not here, and flag in fffflllllaaaagggg`

定义了一个静态函数checkFile,形参为$page的引用。入口点在在下面的if判断，在if三个条件参数不为空、字符串类型、checkFile返回ture，则文件包含传进来的参数

> 在checkfile函数中按顺序只要能返回一个ture就是通过，但是光通过还不行，还要利用文件包含读到flag

重点函数介绍

- in_array()在数组内匹配指定值
- mb_substr()从字符串内返回指定值（substr()只针对英文字符，如果需要分割中文字符则需要mb_substr()),左闭右开比如mb_substr(0,2)得到0,1位字符
- mb_strpos()返回某字符在数组中首次出现的位置

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)//page形参来自Request($file)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];//对传入的file参数定义了一个白名单，列表里只有source.php和hint.php
            if (! isset($page) || !is_string($page)) {
                echo "you cant see it";
                return false;
            }//参数为空或者非字符串则错误

            if (in_array($page, $whitelist)) {
                return true;
            }//搜索page数组内是否有白名单的匹配值，需要完全相同，所以这个true是实现不了的

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')//在$page拼接?的字符串中，查找?出现的位置
            );//分割字符串，从第0位开始分割至拼接的?，比如?file=123213?dwqwe，在这里得到的page=123213
            if (in_array($_page, $whitelist)) {
                return true;
            }//验证上述分割的字符串在白名单内

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you cant see it";
            return false;
        }
    }//url解码后和上面的操作一样取?前的内容再判断一次，防止被url编码绕过

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];//文件包含，这里有重头戏
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

函数内的解析如上。一切都看起里顺理成章。既然利用?前面的进行白名单判断，那直接利用本地包含读flag就行了嘛`?file=source.php?/../../../../ffffllllaaaagggg`

> 但是`include(source.php?/../../../../ffffllllaaaagggg)`真的能执行吗，实际上在传参的时候有很重要的一点，我们request传参进去，传入函数的是引用，而这种地址的传参修改了page的值在函数外也会修改，指针懂吧

那在函数内对?进行了两次分割，有两种思路

- 直接让第二个if判断成立，return ture退出函数
  `payload:?file=source.php?/../../../../fffflllaaaagggg`
- 对?进行url编码避开第二个if判断，使第三个if判断成立
  `payload:?file=source.php%3f/../../../../fffflllaaaagggg`

拿到flag

flag{29022425-9200-4cfe-9221-2dfaa72a58a9}