HCTF2018 Warm up writeup

原创

JSMa4ter 于 2020-12-12 01:11:40 发布 122 收藏

分类专栏： web

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/JSMaster01/article/details/111056192

版权

web 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

HCTF2018 Warm up writeup

拿到题目之后发现这是一张滑稽的脸。查看源代码之后发现有注释的source.php。遂访问。得到源代码。

```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  can't  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  can't  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\"  />";
        }
?>
```

https://blog.csdn.net/JSMaster01

接下来就是复杂的代码审计工作。发现源代码当中存在hint.php。遂访问。得到“flag not here, and flag in ffffllllaaaagggg”。

源代码当中首先定义了一个类。类当中只是定义了一个方法，是一个checkfile的函数。观察if的代码块，得知我们可以用任意方法传入参数file，参数file的值可控。需要满足的条件是file参数的值不为空，参数的值类型为字符串且其能够通过上述类中定义的checkfile方法。接下来才可以include这个参数。

本来笔者认为这道题是考察绕过各种过滤去进行php文件包含读源码。但是我好像想多了，因为根据提示，hint.php已经告诉了我们flag就在ffffllllaaaagggg文件当中，那么我们只需要包含这个文件就可以了。不为空以及参数的值为字符串类型是非常好满足的。那么我们就要把重心放在如何能够绕过checkfile的检查机制，令其返回值为true并包含我们想要的ffffllllaaaagggg文件即可得到flag。

于是开始艰难的代码审计过程。首先熟悉一下PHP当中的类。PHP当中的类是为了方便代码的编写者在使用一类方法去完成一系列任务所创造的一种模式。事实上这道题直接定义一个新函数是一样的。

笔者写这篇博客实际上是面向初学者（也就是我自己）的，以便自己日后查看。说一下这个类中的checkfile函数当中所用到的知识点。

1.“||”表示或，也就是说，该类当中的

$page$变量必须满足其不为空或是其必须为字符串类型即可执行下一步，否则输出“$youcan't seeit.$”，并返回fa