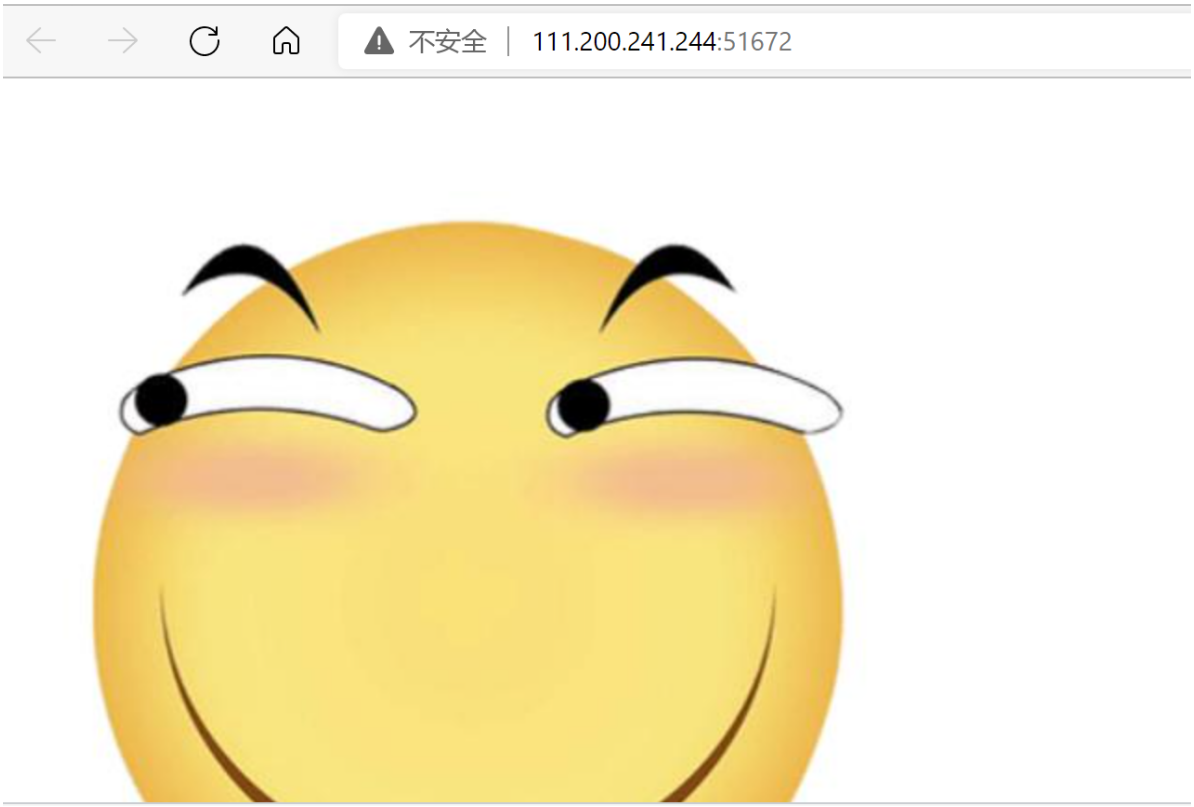
攻防世界 WarmUp web练习题

打开提供的界面，只有一个笑脸



看了一圈没啥可看的，F12看一下

看到一个被注释的页面

输入看看，显示了下面的代码，还有个hint.php

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

查看hint.php弹出来这个界面

flag not here, and flag in ffffllllaaaagggg

回到source.php研究源码，发现了一处令人在意的地方

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

是一个关于file的判断。满足以下三个条件就会包含并运行file（include函数）：

1. file变量是字符串
2. file不为空
3. checkFile返回true

阅读checkFile函数

```
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;
        }
}
```

可以看到列出了白名单source.php和hint.php

传入checkFile的参数为page，需要满足以下条件：

1. page变量不是字符串会返回false
2. page变量存在于白名单中会返回true
3. 截取传进参数中首次出现`?`之前的部分，判断该部分是否存在于`$whitelist`数组中，存在则返回true
4. 对构造的 payload 进行 url 解码，再截取传进参数中首次出现`?`之前的部分，并判断该部分是否存在于`$whitelist`中，存在则返回 true

也就是说我们可以利用3或4 构建payload，？ 之前在白名单内，后面是我们要读取的路径

尝试构造了以下payload：

`?file=source.php?/fffffllllaaaagggg`

不成功。百思不得其解。后来看了解析说ffffllllaaaagggg是暗示有四层子目录，好吧（.....

构造以下payload 成功

`?file=source.php?/../../../../fffffllllaaaagggg`

flag{25e7bce6005c4e0c983fb97297ac6e5a}

附：

include函数

include

(PHP 4, PHP 5, PHP 7, PHP 8)
include 表达式包含并运行指定文件。

以下文档也适用于 require。

被包含文件先按参数给出的路径寻找，如果没有给出目录（只有文件名）时则按照 include_path 指定的目录寻找。如果在 include_path 下没找到该文件则 include 最后才在调用脚本文件所在的目录和当前工作目录下寻找。如果最后仍未找到文件则 include 结构会发出一条 E_WARNING ； 这一点和 require 不同，后者会发出一个 E_ERROR 。

注意如果文件无法访问， include 和 require 在分别发出最后的 E_WARNING 或 E_ERROR 之前，都会发出额外一条 E_WARNING。

如果定义了路径——不管是绝对路径（在 Windows 下以盘符或者 \ 开头，在 Unix/Linux 下以 / 开头）还是当前目录的相对路径（以 . 或者 .. 开头）——include_path 都会被完全忽略。例如一个文件以 ../ 开头，则解析器会在当前目录的父目录下寻找该文件。

有关 PHP 怎样处理包含文件和包含路径的更多信息参见 include_path 部分的文档。

php include使用：php include的使用法详解-php教程-PHP中文网

include官方文档：PHP: include - Manual

include_path：PHP: php.ini 核心配置选项说明 - Manual