攻防世界(web篇)---warmup

原创

肖萧然 于 2021-12-30 16:14:31 发布 274 收藏 1

分类专栏： # WEB MyCTF 文章标签： php 安全 web安全

本文链接：https://blog.csdn.net/qq_52549196/article/details/122239599

WEB 同时被 2 个专栏收录

12 篇文章 0 订阅

订阅专栏

MyCTF

45 篇文章 1 订阅

订阅专栏

攻防世界—warmup

文章目录

攻防世界---warmup

题目 php代码审计

用到的php知识

highlight_file(__FILE__)

emmm::checkFile($_REQUEST['file'])

mb_substr

mb_strpos

REQUEST函数

include

题解

打开题目，f12发现:

访问hint.php

条件 if中的全为ture

emmm

payload

题目 php代码审计

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

用到的php知识

highlight_file(FILE)

> 高亮并显示代码文件

emmm::checkFile($_REQUEST['file'])

> 类的调用

mb_substr

```
echo mb_substr("12345",0,2); //12
```

> 截断

mb_strpos

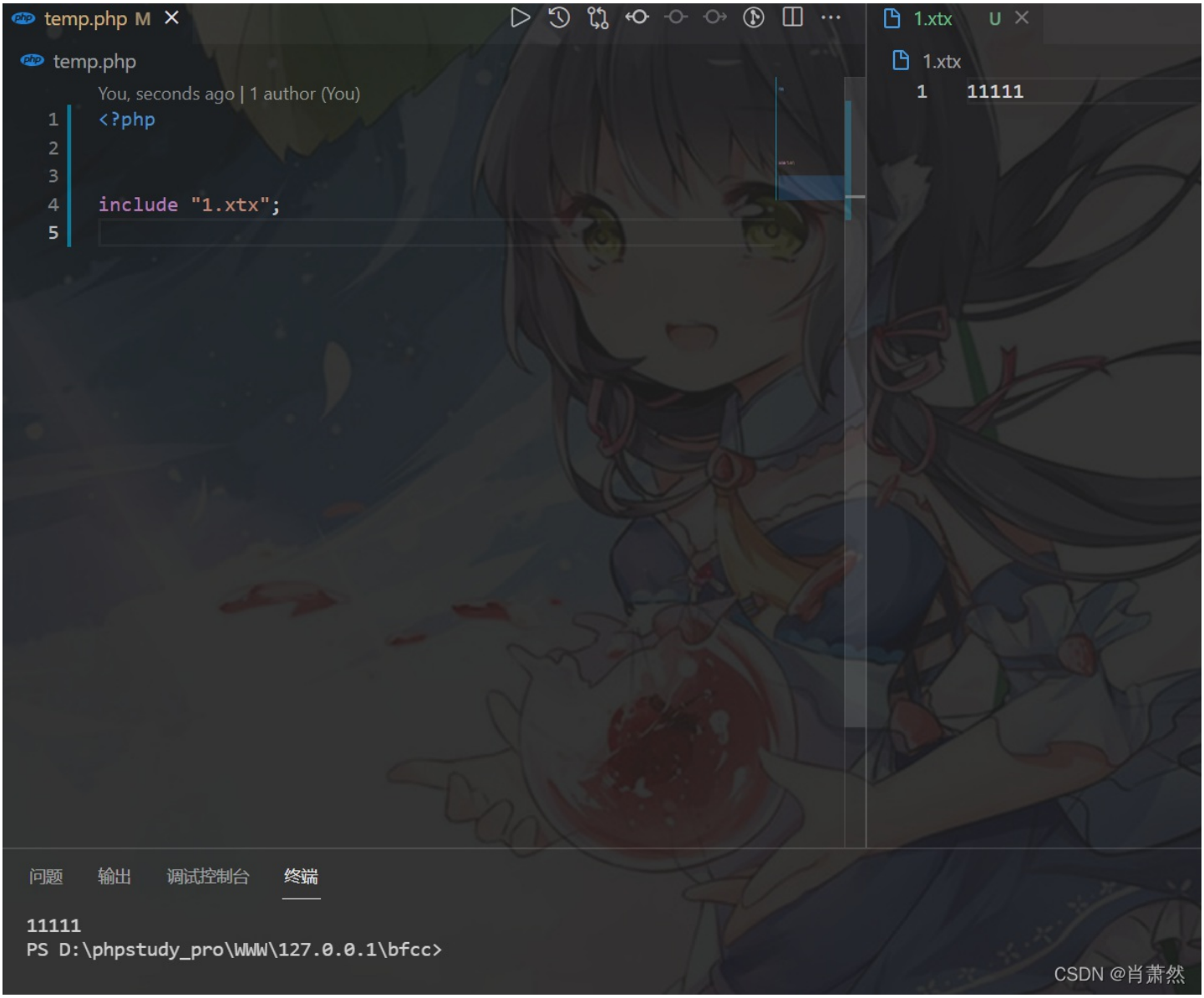
```
echo mb_strpos("12345",2); //1
```

> 返回参数中首次出现的位置

REQUEST函数

> REQUEST函数可以同时接受get与post方法提交的变量。

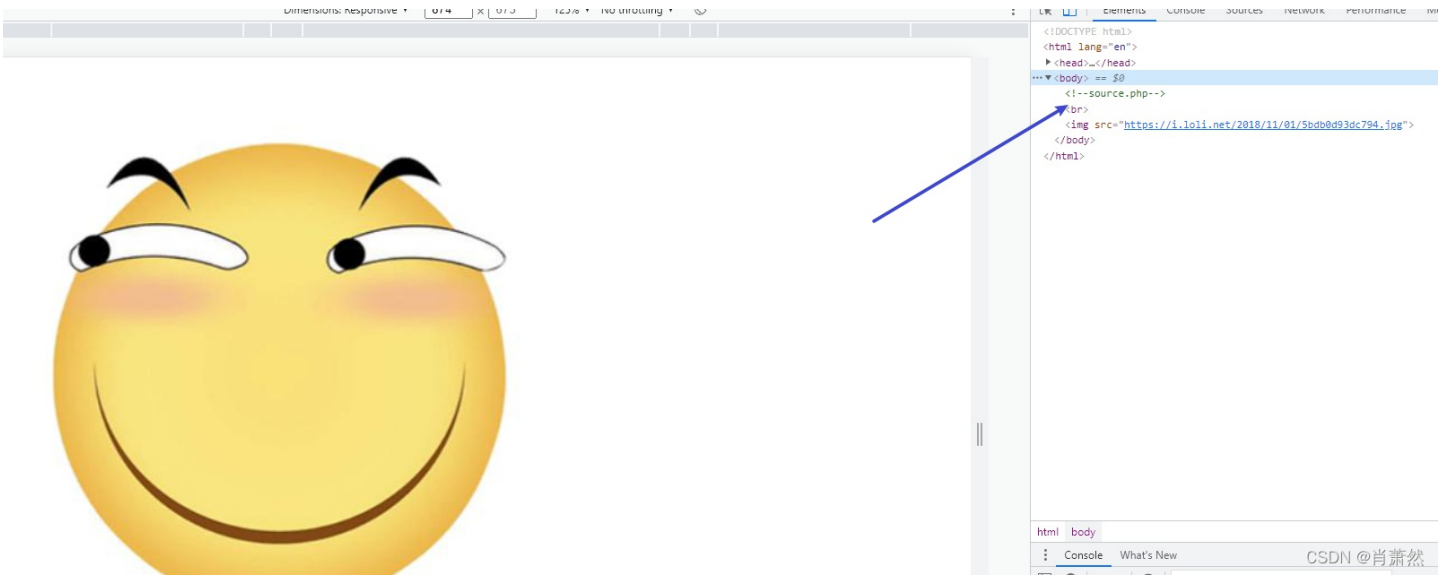
include



> 请求路径下的任何文件 如果php文件的会执行

题解

打开题目，f12发现：



访问hint.php

flag not here, and flag in ffffllllaaaagggg

> ffffllllaaaagggg 是文件名的意思

include 请求文件的不在同一目录,所以要加…/…/…/

条件 if中的全为ture

```
if  (!  empty($_REQUEST['file'])
        &&  is_string($_REQUEST['file'])
        &&  emmm::checkFile($_REQUEST['file'])
)  {
        include  $_REQUEST['file'];
        exit;
```

emmm

```php
$whitelist = ["source"=>"source.php","hint"=>"hint.php"];
if (! isset($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;
```


- 截取有？分界
- 白名单
- return 后下面代码不再执行

payload

```
http://111.200.241.244:51684/?file=hint.php?/../../../../ffffllllaaaagggg
```


知识？知识？从不打败？运气问题？