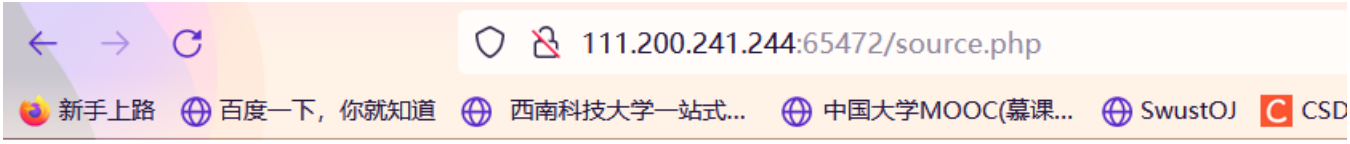
攻防世界warmup

原创

一只Traveler 于 2021-11-03 11:51:41 发布 1925 收藏
分类专栏： 笔记 文章标签： 安全

f12发现一个source.php，输入发现代码，一看就知道是代码审计绕过得文件包含；




```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;
                }
        }
```


构造file参数满足checkfile函数，通过代码知道：

第一个if page非空且是字符串；

第二个if page在白列表中；

接下来的mb_substr 是分隔字符串page，从0到page中第一次出现的？处；

if 继续判断page是否在白名单中；

然后编码，再分隔；

综上，构造file=hint.php(或source。php)? ../../../../../ffffllllaaaagggg

其中，ffffllllaaaagggg是用hint.php发现的，至于为什么是五个../，暂时未知，都是参考个方大佬，应该是../打开ffffllllaaagg时发现打不开，可能下面还有目录，继续试../直到第五个../时才打开。


```
                    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}
```