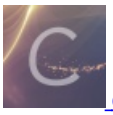
XCTF-warmup

原创

qq_39543838 于 2021-02-24 21:01:25 发布 31 收藏

分类专栏： ctf

本文链接：https://blog.csdn.net/qq_39543838/article/details/114041182



查看页面源码，找到source.php文件

代码如下

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

第七行提示hint.php

flag not here, and flag in ffffllllaaaagggg

继续查看代码

KaTeX parse error: Expected 'EOF', got '&' at position 22: …ST['file']值非空 &̲& is_string(_REQUEST[‘file’]) 值为字符串 && emmm::checkFile($_REQUEST[‘file’]) 通过checkFile函数校验

1.第一个``if``语句对变量进行检验，要求``$page``为字符串，否则返回false
2.第二个``if``语句判断``$page``是否存在于``$whitelist``数组中，存在则返回true
3.第三个``if``语句判断截取后的``$page``是否存在于``$whitelist``数组中，截取``$page``中```'?'```前部分，存在则返回true
4.第四个``if``语句判断url解码并截取后的``$page``是否存在于``$whitelist``中，存在则返回true

若以上四个``if``语句均未返回值，则返回false
有三个``if``语句可以返回true，第二个语句直接判断``$page``，不可用
第三个语句截取```'?'```前部分，由于?被后部分被解析为get方式提交的参数，也不可利用
第四个``if``语句中，先进行url解码再截取，因此我们可以将?经过两次url编码，在服务器端提取参数时解码一次，checkFile函数中解码一次，仍会解码为```'?'```，仍可通过第四个``if``语句校验。（```'?'```两次编码值为```'%253f'```）,构造url:
http:``//399fe153-1f62-43d5-a67f-e645a0e7ac66.node3.buuoj.cn/source.php?file=source.php%253f../ffffllllaaaagggg

经过测试发现无返回值，这可能是因为我们不知道ffffllllaaaagggg文件存放的具体位置
所以依次增加../,最终成功拿到flag