2018.11.10HCTF warmup

原创

「已注销」 于 2018-11-13 23:45:24 发布 623 收藏

分类专栏： CTF 文章标签： HCTF writeup

友链：https://cutt.ly/7777aaaa

本文链接：https://blog.csdn.net/include_heqile/article/details/84038470

这道题其实是一道签到题，我们查看题目源代码，会发现提示我们查看`source.php`，然后我们审查源代码：

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

我们可以看到是白名单过滤，关键代码：

```php
$_page = mb_substr(
    $page,
    0,
    mb_strpos($page . '?', '?')
);
if (in_array($_page, $whitelist)) {
    return true;
}
```

因为？是可控的，我们可以在白名单文件名后面加上？来绕过，这样我们就可以查看任意文件了，根据hint.php的提示，我们在根目录下找到了包含了flag的文件