

CSDN

首页 博客 学院 下载 论坛 图文课 问答 商城 活动 专题 招聘 ITeye GitChat APP VIP会员 续费8折 疯狂Python

0

原创

phpstudy后门文件检测及利用

2019-09-23 22:56:22

tdcoming

阅读量 664

更多

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/qc\\_29647709/article/details/101231998](https://blog.csdn.net/qc_29647709/article/details/101231998)

2019.9.20得知非官网的一些下载站中的phpstudy版本存在后门文件，基于研究的目的，于是有了以下此文。复现使用5.4版本的，互联网随便下载了一个

0X00检测脚本(来源Chamd5安全团队)

- Linux

```
1  #!/bin/bash
2  # author: pcat@chamd5.org
3  # http://pcat.cc
4
5  # trojan feature
6  trojan=@eval
7
8  function check_dir(){
9      for file in `ls $1`
10     do
11         f2=$1/"$file
12         if [ -d $f2 ]
13         then
14             check_dir $f2
15             # just check dll file
16             elif [ "${file##*.}"x = "dll"x ]
17             then
18                 strings $f2 |grep -q $trojan
19                 if [ $? == 0 ]
20                 then
21                     echo "====" $f2 "===="
22                     strings $f2 |grep $trojan
23                 fi
24             fi
25         done
26     }
27     # . stand for current directory
28     check_dir .
```

- windows

```
1  # -*- coding:utf8 -*-
2  __author__='pcat@chamd5.org'
3  __blog__='http://pcat.cc'
4
5  import os
6  import string
7  import re
8
9
10 def strings(file) :
11     chars = string.printable[:94]
12     shortestReturnChar = 4
13     regExp = '[%s]{%d,}' % (chars, shortestReturnChar)
14     pattern = re.compile(regExp)
15     with open(file, 'rb') as f:
16         return pattern.findall(f.read())
17
```

VIP



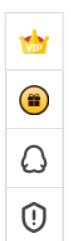
```
18
19 def grep(lines,pattern):
20     for line in lines:
21         if pattern in line:
22             yield line
23
24
25 def pcheck(filename):
26     # trojan feature
27     trojan='@eval'
28     # just check dll file
29     if filename.endswith('.dll'):
30         lines=strings(filename)
31         try:
32             grep(lines,trojan).next()
33         except:
34             return
35     print '=== {0} ==='.format(filename)
36     for line in grep(lines,trojan):
37         print line
38     pass
39
40
41 def foo():
42     # . stand for current directory
43     for path, dirs, files in os.walk(".", topdown=False):
44         for name in files:
45             pcheck(os.path.join(path, name))
46         for name in dirs:
47             pcheck(os.path.join(path, name))
48     pass
49
50
51 if __name__ == '__main__':
52     foo()
```

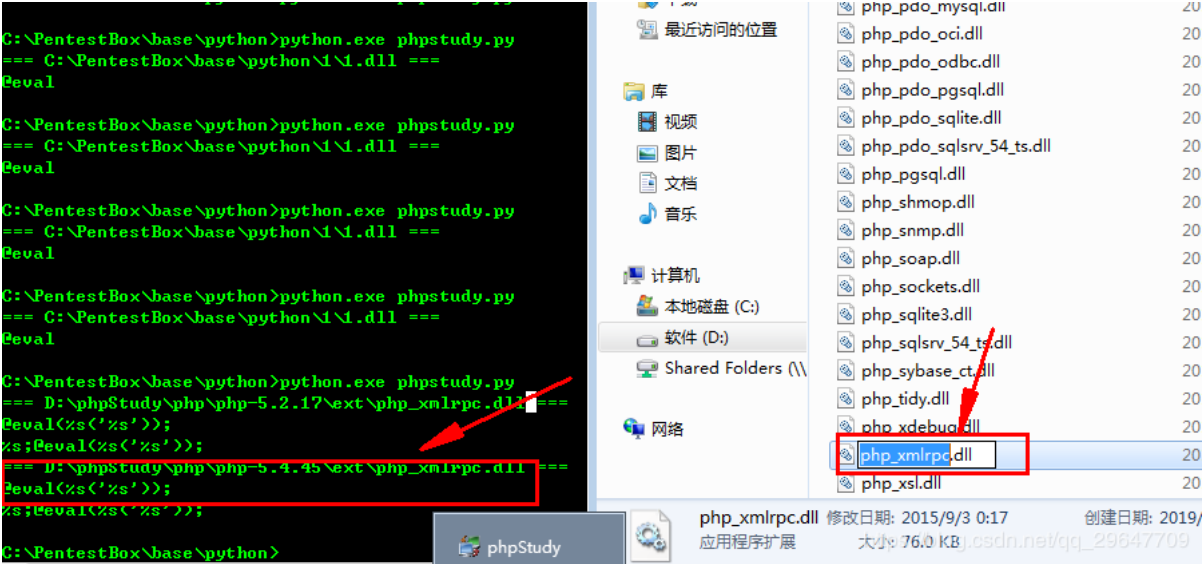
## 0X01检测后门示例

用windows系统的为例,

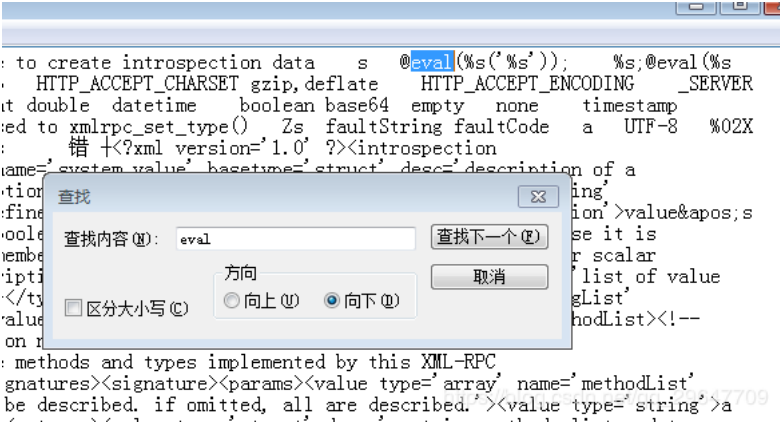


运行脚本发现php\_xmlrpc.dll存在问题



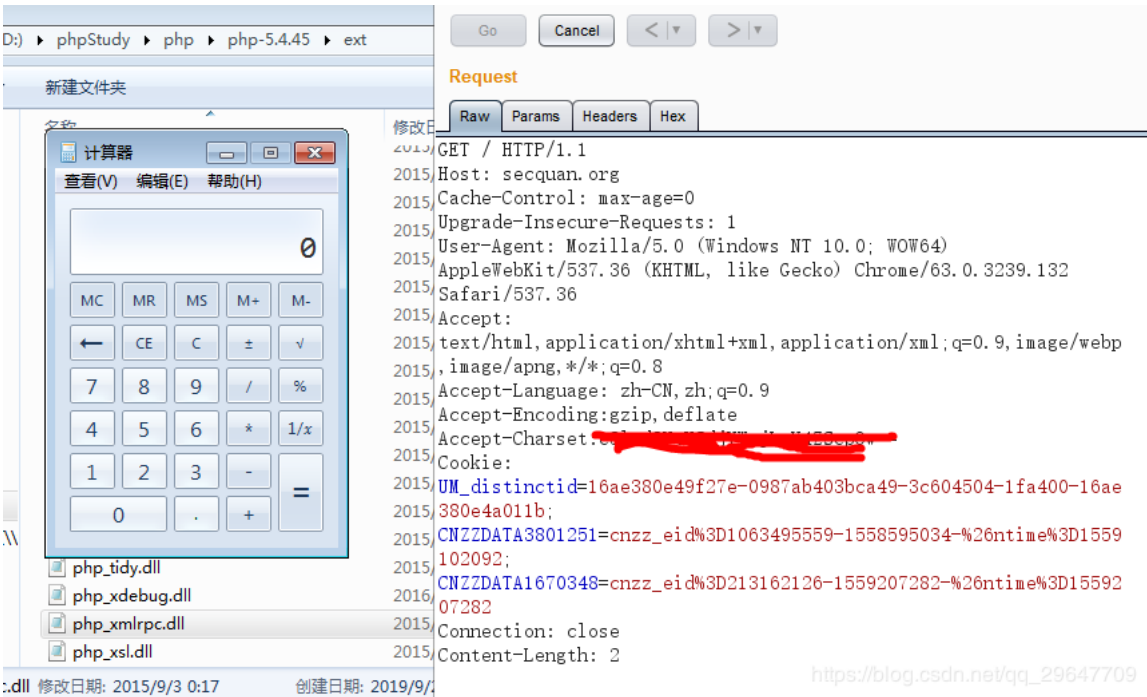


也可以直接打开，搜索关键字eval



## 0X02 利用

- 使用exp成功弹出计算器（来源于圈子社区）



exp不对外公开，更多关注密圈

## 0X03 安全修补


为了减少系统已产生的后门带来的危险，可以继续做以下工作：

- 不需要对外开放的端口同一关闭，或者做 IP 访问限制，防止已有后门继续和外界保持通讯
- 对于所有访问请求的 URL 进行记录（可以通过 Apache 或 nginx 访问日志记录），定期分析所有的请求是否有异常情况
- 去除后门或更新最新版本phpstudy

## 0X04 参考链接

- <https://mp.weixin.qq.com/s/dlDfgFxHlqenKRUSW7Oqkw>


  
0














更多关注小密圈：



（信安之路-技术交流）



（信安圈子-干活分享）

[https://blog.csdn.net/vqq\\_29647709](https://blog.csdn.net/vqq_29647709)  
<https://mp.weixin.qq.com/s/dlDfgFxHlqenKRUSW7Oqkw>

文章最后发布于: 2019年

### Phpstudy隐藏后门

阅读数 552

Phpstudy隐藏后门1.事件背景Phpstudy软件是国内的一款免费的PHP调试环境的程序集成包，通过集... 博文 来自: [Sylon的博客](#)

 想对作者说点什么

### phpstudy漏洞

阅读数 3899

一直在使用的phpstudy，有以下几个漏洞可能存在着被黑的风险，最好能及时修正。1.通过修改服务器... 博文 来自: [qq\\_17054659...](#)

### (三) phpstudy下开启mysql，运用phpmyadmin管理执行sql语句，写入一句话后门getsh...

阅读数 660

学习mysql数据库漏洞整理过程中，想复现phpmyadmin写入一句话后门getshell的过程遇到很多问题... 博文 来自: [爱上卿的博客](#)

### 那些强悍的PHP一句话后门

阅读数 2643

以一个学习的心态来对待PHP后门程序，很多PHP后门代码让我们看到程序员们是多么的用心良苦。强... 博文 来自: [是大方子](#)



免费云虚拟主机试用一年

### 配置安装DVWA

阅读数 13

本文地址: <http://www.cnblogs.com/go2bed/p/4162313.html>... 博文 来自: [weixin\\_30278...](#)

### PHPStudy以后打开phpMyAdmin显示404


阅读数 680


首先是因为Mysql没有设置密码，现在进入PHPStudy→其他选项菜单→MySQL工具，第一个就是设置... 博文 来自: [han\\_cui的博客](#)


### 大商创-安装bug-在phpstudy安装完成之后需要安装zend


阅读数 2028

在phpstudy中选择5.6版本，注意一定要这个版本但是安装完成之后，却发现输入localhost只显示了很... 博文 来自: [darkalex001的...](#)









分别使用phpstudy自带mysql与本地mysql

阅读数 903

去年先安装了phpStudy，然后安装了MySQL5.7，二愣二愣的。今年学习数据库于是用cmd运行了一... 博文

来自: Laurel\_60的博客

phpStudy 发现存在重大的bug

阅读数 3226

确实是挺好用的,但是有些项目里面某些办法会错乱,会出问题,我已经排除不是项目代码问题了,我下载了... 博文

来自: u013926384...

别再玩假传奇了！这款传奇爆率9.8，你找到充值入口算我输！

贪玩游戏 · 顶新

利用phpStudy 探针 提权网站服务器

阅读数 1万+

声明:本教程仅仅是演示管理员安全意识不强,存在弱口令情况.网站被非法入侵的演示,请勿用于恶意用途!... 博文

来自: 逆向思维

针对phpStudy网站服务器的入侵

阅读数 62

今天客户服务器上出现报警，查找了下原因，发现根目录下有wk.phpE:\phpStudy\MySQL\bin\mysql... 博文

来自: aituochang18...

PeiSylon

39篇文章

排名:千里之外

关注

我是拍黄片的

10篇文章

排名:千里之外

关注

上卿

49篇文章

排名:千里之外

关注

大方子

393篇文章

排名:7000+

关注

Windows下基于phpStudy的DVWA web渗透测试漏洞平台搭建

阅读数 7130

搭建一个web渗透测试平台，对于学web渗透的初学者来说是一个不错的选择。（笔者也是一个初学者... 博文

来自: u014070086...

针对phpstudy默认设置的利用

阅读数 548

在phpstudy下载下来以后路径，设置没有修改的情况下可以使用此方法url：http://ip/phpmyadmin... 博文

来自: 洞若观火

c#次横坐标不显

c#dem文件

c#免安装版反编译工具

c# 深度 递归

c#网页如何调试

c# 添加自定义的属性

c#中去除窗体边框

dll ida修改c#

c#实现打印功能

c# 线程结束时执行

©2019 CSDN 皮肤主题: skin-city 设计师: CSDN官方博客

tdcoming

4 粉丝

TA的个人主页 >

原创

84

粉丝

143

喜欢

65

评论

35

等级: 博客 5

访问: 14万+

积分: 2131

排名: 3万+

勋章: 恒 笔

最新文章

CVE-2019-0708 远程桌面代码执行漏洞复现

Apache Tomcat CVE-2019-0232 远程代码执行漏洞

ThinkPHP 5.0 \* 远程代码执行漏洞分析

域测试---ms14-068 Kerberos漏洞

Pentest BOX安装和使用

最新评论

手机木马远程控制复现

weixin\_45651569: 可以解释下流程吗? 受这方面问题困扰

CVE-2019-0708 远程桌...

weixin\_39653966: 这几个加进去不报错? [-] WA  
RNING! The following modules could not l ...

手机木马远程控制复现

qq\_29647709: QQ group 906755997

ThinkPHP 5.0 \* 远...

qq\_29647709: QQ group 906755997

ThinkPHP 5.0 \* 远...

weixin\_45542709: 兄弟, 可以给个联系方式: .

分类专栏

	WEB安全	28篇
	漏洞利用	35篇
	运维安全	11篇
	内网渗透	13篇
	CTF	12篇

展开

归档

2019年9月	2篇
2019年4月	1篇
2019年1月	4篇
2018年12月	34篇
2018年11月	8篇
2018年9月	5篇
2018年8月	28篇
2018年7月	5篇

展开

云服务器低至18元/3月

云服务器学生专属优惠9元/  
元/3月,低至0.2元/日! ABC人  
培养,助你成就职场新机遇.



CSDN学院



CSDN企业招聘

👤 QQ客服      ✉ kefu@csdn.net  
🗣 客服论坛      ☎ 400-660-0108  
                    工作时间 8:30-22:00

关于我们   招聘   广告服务   网站地图

🔍 百度提供站内搜索 京ICP备19004658号

©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务   经营性网站备案信息

北京互联网违法和不良信息举报中心

中国互联网举报中心   家长监护   版权申诉

  
0

