Upload-labs文件上传漏洞（getimagesize函数）——Pass14

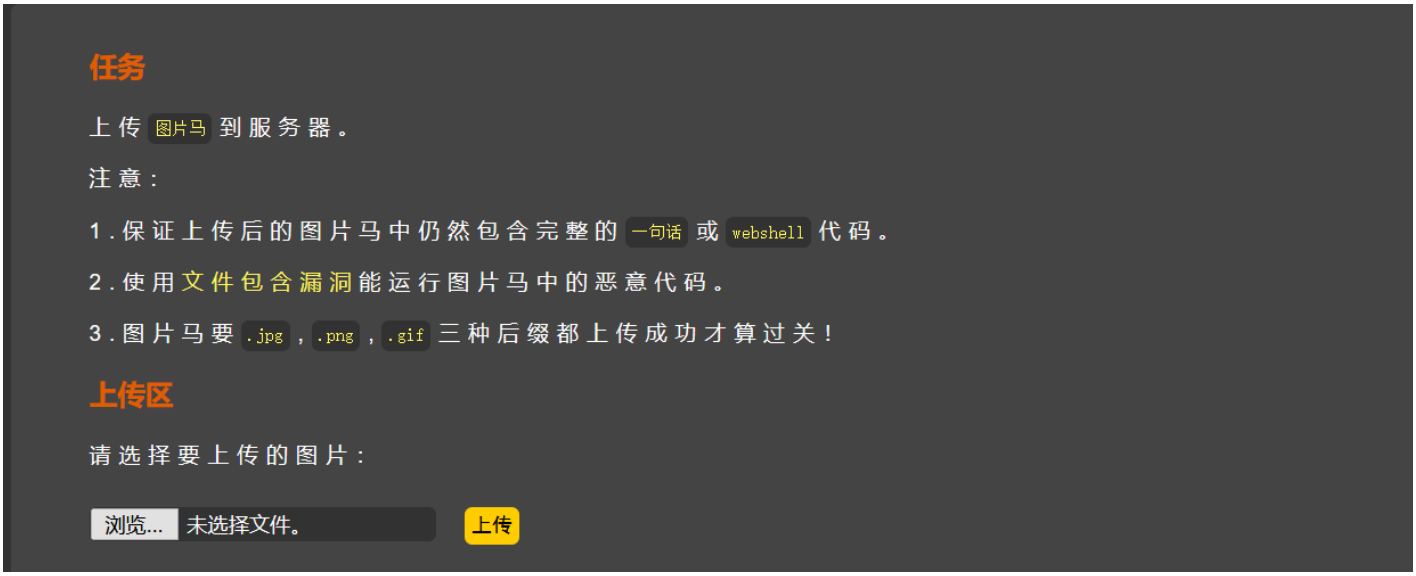
原创

Zichel77 于 2020-07-29 15:23:44 发布 445 收藏 1
分类专栏： Upload-labs web学习

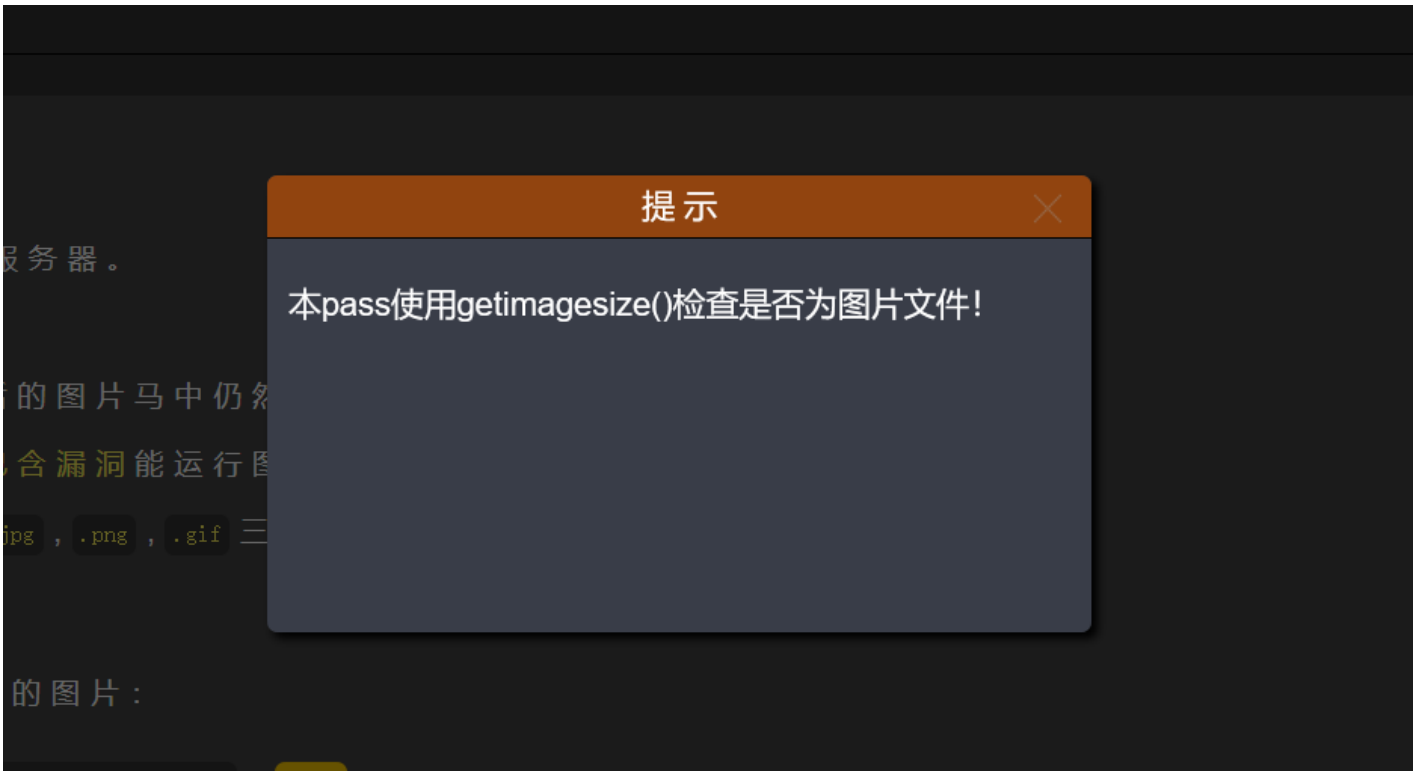
本文链接：https://blog.csdn.net/weixin_43965597/article/details/107663572

0×00 题目概述

与13差不多



但是不是读取字节，而是使用函数检查



0×01 源代码

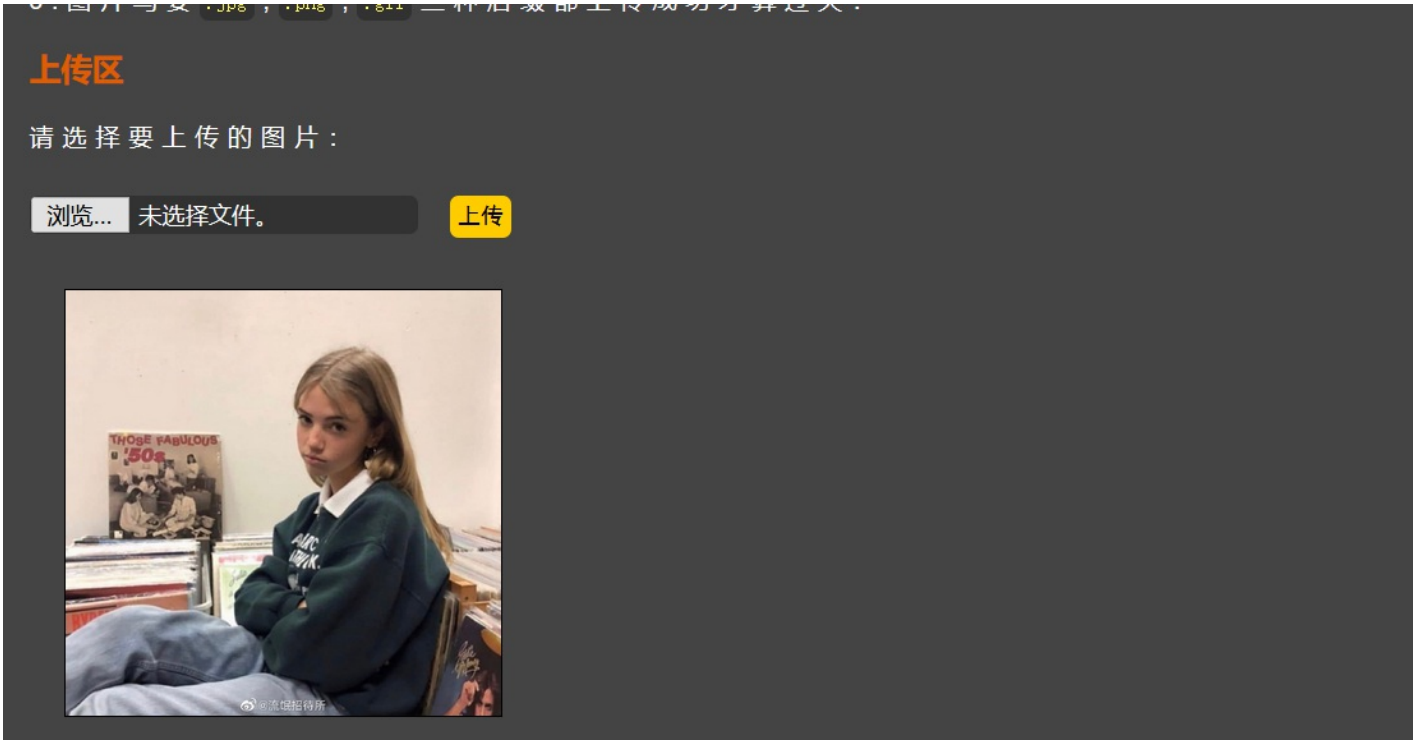
```
function isImage($filename){
    $types = '.jpeg|.png|.gif';
    if(file_exists($filename)){
        $info = getimagesize($filename);
        $ext = image_type_to_extension($info[2]);
        if(stripos($types,$ext)>=0){
            return $ext;
        }else{
            return false;
        }
    }else{
        return false;
    }
}

$is_upload = false;
$msg = null;
if(isset($_POST['submit'])){
    $temp_file = $_FILES['upload_file']['tmp_name'];
    $res = isImage($temp_file);
    if(!$res){
        $msg = "文件未知，上传失败！";
    }else{
        $img_path = UPLOAD_PATH."/".rand(10, 99).date("YmdHis").$res;
        if(move_uploaded_file($temp_file,$img_path)){
            $is_upload = true;
        } else {
            $msg = "上传出错！";
        }
    }
}
```

编写了isImage()函数

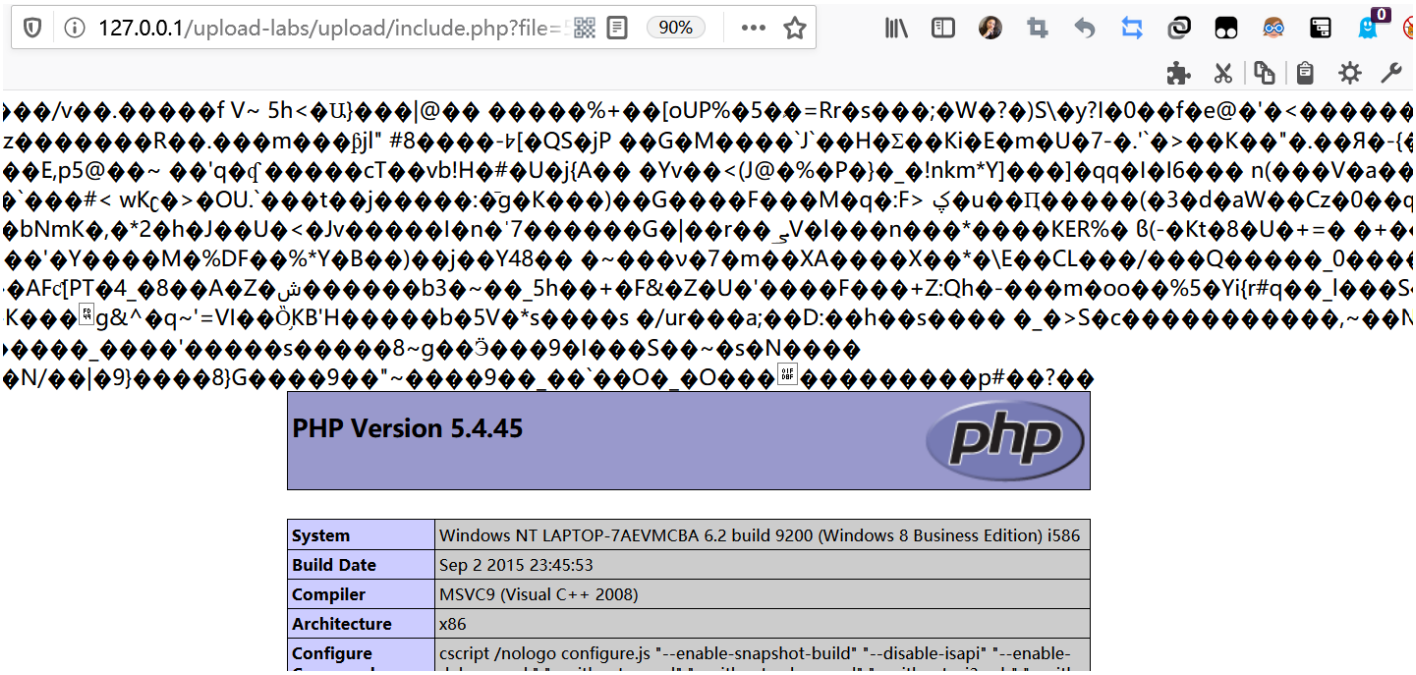
0×02 做题步骤

好像只要上传图片马就可以了



依旧可过

步骤与Pass13相同



0×03 关于getimagesize()函数

getimagesize() 函数将测定任何
GIF，JPG，PNG，SWF，SWC，PSD，TIFF，BMP，IFF，JP2，JPX，JB2，JPC，XBM 或 WBMP 图像文件的大小并返回图像的尺寸以及文件类型及图片高度与宽度。函数成功返回的就是一个数组，失败则返回 FALSE 并产生一条 E_WARNING 级的错误信息。

上一题我们利用自己写的文件包含漏洞页面脚本来检验webshell是否能被解析，这一题就自己写包含getimagesize()的php脚本，用来读取本地的图片，然后我们来看看这个函数的解析机理是怎么样的

代码如下

```
<?php
$local_png ='./1.jpeg';
$img_data = getimagesize($local_png);
var_dump($img_data );
?>
/*
测试函数，用getimagesize()函数对本地图片进行检查，然后将检查结果的数组打印出来
*/
```

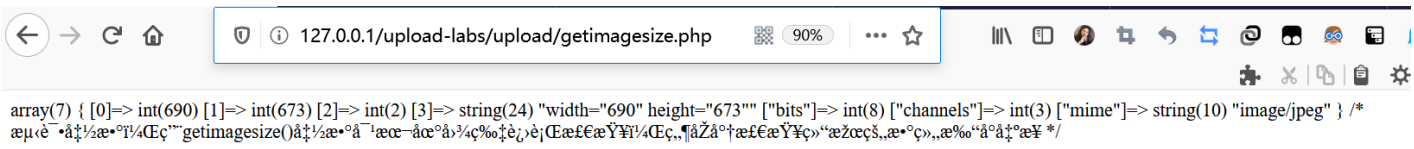
记住，要读取什么图片就在$local_png=后面的参数中写入文件的名字

然后将此文件命名为getimagesize.php，放入upload文件夹下

然后输入url

> http://127.0.0.1/upload-labs/upload/getimagesize.php

即可看到



array(7) { [0]=> int(690) [1]=> int(673) [2]=> int(2) [3]=> string(24) "width="690" height="673"" ["bits"]=> int(8) ["channels"]=> int(3) ["mime"]=> string(10) "image/jpeg" } /*
æµ‹è¯•å‡½æ•°ï¼Œç”¨getimagesize()å‡½æ•°å¯¹æœ¬åœ°å›¾ç‰‡è¿›è¡Œæ£€æŸ¥ï¼Œç„¶åŽå°†æ£€æŸ¥ç»“æžœçš„æ•°ç»„æ‰“å°å‡ºæ¥ */

返回的值是一个七位的数组

查阅资料得知

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");

在本次测试中并未出现索引channels，此处只做了解。

然后再看回本地源代码，发现只检查了索引2

```
$ext = image_type_to_extension($info[2]);
```

也就是图像的类型，所以和上一题大同小异，上传图片马即可通过。

参考链接：

https://www.zhaosimeng.cn/writeup/70.html