不安全文件下载与上传之——上传漏洞之——二次渲染绕过

原创

温柔小薛 于 2020-04-07 23:43:09 发布 566 收藏 1

分类专栏： web渗透测试与代码审计 #+ 不安全文件下载与上传 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_43079958/article/details/105377096

web渗透测试与代码审计 同时被 2 个专栏收录

113 篇文章 19 订阅

订阅专栏

#+ 不安全文件下载与上传

10 篇文章 0 订阅

订阅专栏

上传漏洞之二次渲染绕过

目录

二次渲染与检测大概流程

> 获得上传文件的基本信息，文件名，类型，大小，临时文件路径 // 获得上传文件的扩展名 //判断文件后缀与类型，合法才进行上传操作 //使用上传的图片生成新的图片

```
$im = imagecreatefromjpeg($target_path);
```

> //给新图片指定文件名 //显示二次渲染后的图片（使用用户上传图片生成的新图片）

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。

操作

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。

php图像二次渲染：
https://blog.csdn.net/hitwangpeng/article/details/48661433
https://blog.csdn.net/hitwangpeng/article/details/46548849
https://xz.aliyun.com/t/2657

```
        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。

https://github.com/LandGrey/upload-labs-writeup/blob/master/webshell/bypass-imagecreatefromjpeg-pass-LandGrey.jpg

也需要与其他漏洞结合使用