安全小课堂第九十六期【web漏洞挖掘之上传漏洞】

京东安全应急响应中心 5月21日

文件上传漏洞是指用户上传了一个可执行的脚本文件，并通过此脚本文件获得了执行服务器端命令的能力。这种攻击方式是最为直接和有效的，“文件上传”本身没有问题，有问题的是文件上传后，服务器怎么处理、解释文件。如果服务器的处理逻辑做的不够安全，则会导致严重的后果。

JSRC **安全小课堂第九十六期**，邀请到**xfkxfk**作为讲师就**web漏洞之上传漏洞挖掘**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

文件上传后导致的常见安全问题一般有哪些？

京安小妹

xfkxfk：

文件上传成功一般直接获取系统的webshell，此时导致网站源代码泄露，数据脱裤，网站篡改，肉鸡，跳板，挖矿，内网渗透，后门等。如果是系统权限那么就可以干更多的事情，为所欲为，如果www权限的话应该需要提权获取系统权限。然后再进行后渗透。

讲师

文件上传漏洞一般常发生在什么情况下？

京安小妹

xfkxfk：

在漏洞挖掘的过程中，任何存在上传文件操作的地方都可能存在文件上传漏洞，特别是在网站后台出现文件上传漏洞的概率最大。一般在用户中心上传头像，博客或者论坛上传图片，上传附件，数据备份恢复等地方容易出现文件上传漏洞。

讲师

文件上传漏洞的原理是什么呢？

京安小妹

xfkxfk：

文件上传漏洞，从字面意思应该就能理解，在正常上传文件的时候未进行正确的处理，导致上传脚本文件被web服务器解析导致获取webshell。比如在写文章时需要上传图片，但是后台判断你上传文件是否为图片时存在缺陷，或者没有判断直接上传，所以就可以上传jsp或者php文件到web服务器导致漏洞产生。

文件上传漏洞常见的利用方式有哪些？

京安小妹

xfkxfk：

一般你需要收集操作系统，语言，服务器，版本等信息，还需要判断正常上传和非法上传之后的响应已经提示，来确定能上传哪些，不能上传哪些，通过测试猜测后台判断逻辑可能是怎么判断的，然后在构造不同请求进行测试。

比如你发现这个服务器存在解析漏洞，那么就简单了，直接上传以文件进行解析就可以了。但是如果过滤的很严格，你需要从MIME类型，文件内容，文件后缀这些地方进行fuzz，最后找到正确上传的姿势。

讲师

文件上传漏洞的绕过方法有哪些？

京安小妹

xfkxfk：

文件上传一般都会检测文件MIME类型、文件扩展名、文件内容等
白盒情况下结合代码中的逻辑已经防御构造特定的请求来绕过。
黑盒情况下首先需要进行一些信息收集，操作系统，语言，服务器，版本，上传异常提示，上传返回结果等等：
a、比如前端js判断文件后缀内容等直接通过禁用js或者抓包重放即可；
b、通过请求头中的content-type来判断文件类型已经确定文件后缀，也可以抓包重发绕过；
c、通过后台mime_content_type或者Fileinfo或者getimagesize之类判断文件内容，可以通过构造文件头绕过；
d、通过判断上传文件内容的语言标签，比如php的<?php标签，可以通过其他解析形式上传shell内容；
e、如果限制后缀名可以使用截断操作，或者通过fuzz进行测试；
f、通过不同操作系统的特性来绕过，比如windows的NTFS ADS特性；
g、通过不容web服务器的特性来绕过，主要是解析漏洞，Apache，IIS，Nginx，PHP CGI都存在解析漏洞；
h、还有同.htaccess和.user.ini来修改当前解析配置已经目录执行权限等配置；
等等，还有很多不同场景下的绕过方式。

讲师

文件上传漏洞的防御？

京安小妹

xfkxfk：

a、首先需要解决web容器的解析漏洞，并且配置好容器的解析规则。

b、尽量不使用黑名单，万一要是用的话尽量使用白名单，或者根据业务功能固定后缀。

c、尽量不使用正则来判断（正则最容易出问题），使用系统自带函数进行文件信息获取。

d、还有就是逻辑上不要出现漏洞，导致前面的防御系统虚设。

讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心