谈谈上传漏洞——安全小课堂第二十二期

2016-08-12 京东安全应急响应中心

安全小课堂第二十二期

上传漏洞， 轻者可以造成xss、被"挂黑页"，严重的甚至可以获得服务器权限甚至system、root权限。本期咱们来聊一聊上传漏洞。

本期邀请到
同程网安全专家range
唯品会安全专家知行者
大家列队欢迎哟~

1

豌豆妹

咱们先了解下最基本的常识：什么是上传漏洞。

葫芦娃

漏洞名字直接解释了，上传漏洞就是由于开发者没有对上传的文件作过滤或者过滤机制不严格，导致恶意用户可以上传动态脚本页面，从而通过上传的脚本获取到网站的控制权。上传漏洞很多时候是结合解析漏洞来使用的，当然一些防护差的网站根本不需要利用解析漏洞，直接上传木马就行了。

小丸子

上传漏洞是指一些上传文件、服务远程更新、更改头像、操作文件等地方对用户提交的

参数没有检查或者过滤的不完整，导致攻击者可以直接上传敏感文件，甚至是webshell的一种漏洞。

2

豌豆妹

能总结一些上传漏洞利用方法吗？

哆啦A梦 

在我看来，有以下几点，有遗漏之处还请补充。
1、在上传文件的地方，先用敏感文件后缀(php, jsp, aspx等)尝试上传，如果刚刚选定文件就提示后缀不允许，多半是前台验证，换非敏感后缀上传，尝试burp抓包改包绕过。
2、如果后端验证，可以尝试其他可解析文件名绕过(php4, jspx, ashx等)、解析漏洞(apache解析漏洞，iis解析漏洞，nginx解析漏洞)或者用0x00截断后缀等方式绕过检查。
3、某些远程更新的地方，可以指定更新服务器，这样就能偷梁换柱，传上去自己的文件。
4、可能有些上传点可以上传任意后缀，但是目录无法执行脚本，或者所有脚本后缀都限制死了，那么只有最后一种可能的利用方式了：上传html文件，造成xss。不过这种一般会被认为是反射型。

小新 

时间关系，我可能说得也不太好，这里搜集了一些总结，大家也可以参考下：
http://blog.sina.com.cn/s/blog_64c5a9290100n5zq.html；
http://www.qxzxp.com/3761.html 。

3

豌豆妹

能说说上传漏洞的危害吗？

葫芦娃 

上传漏洞， 轻者可以造成xss、被"挂黑页"，严重的甚至可以获得服务器权限甚至system、root权限。

4

豌豆妹

那如何防范“上传漏洞”入侵呢？

小丸子 

(1)对后端源码中上传文件和操作文件的地方都检查一遍。

(2)部署通用waf拦截非法文件。
(3)非上传目录不给予写入权限，上传文件的目录禁止运行脚本或禁止访问。

小新

防范“上传漏洞”入侵建议在客户端以及服务器端同时检测：
1、客户端。使用JS对上传的内容进行检测，包括文件大小、文件扩展名、文件类型等
2、服务端。白名单方式过滤文件扩展名，除了同样对文件类型等基本属性检测外，还需对文件保存的路径进行检查，同时对上传的文件重命名。文件命名规则可采用时间戳拼接随机数等算法。

哆啦A梦

楼上说的也是主要防护方法了。我这里补充下，如果可以，对上传的文件做二次加载渲染，那这个防护方法就妥妥的。

豌豆妹

二次加载渲染是什么，求科普。

小新

例如说，二次渲染就是根据用户上传的图片，生成一个新的图片，然后删除用户上传的原始图片，将新图片存储到数据库中。那如果你是在图片中加入的一句话木马，就无法生效了。

豌豆妹

哈~懂了。那导致该漏洞的原因有哪些呢？

小丸子 

原因在于，代码作者没有对访客提交的数据进行检验或者过滤不严，可以直接提交修改过的数据绕过扩展名的检验。同时也跟网站服务器安全设置方面有关。

5

豌豆妹

如何修复上传漏洞呢？

哆啦A梦 

1、一般采用后缀名白名单过滤的方式严格限制文件后缀，识别文件类型。
2、不使用用户提交的文件名，将所有上传重命名，重命名不要可预测或者可以暴力遍历到。
3、老版本iis、apache和nginx要及时打补丁，防止解析漏洞。

豌豆妹

哈~本期话题到此结束，谢谢小伙伴们的热烈讨论哒~么么哒~

安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御；
8、电商和O2O行业诈骗那些事儿（上）；
9、电商和O2O行业诈骗那些事儿（下）；
10、CSRF的攻击与防御；
11、账户体系安全管理探讨；
12、远程代码执行漏洞的探讨；
13、服务器安全管控的探讨；
14、畅谈端口安全配置；
15、谈一谈github泄露；
16、撞库攻击是场持久战；
17、url重定向攻击的探讨；
18、聊聊弱口令的危害（一）；
19、聊聊弱口令的危害（二）；
20、聊聊XML注入攻击；
21、聊聊暴力破解。

谢谢支持JSRC