基于混合模式移动客户端开发的安全性研究

郑海山
（厦门大学信息与网络中心 福建 厦门 361005）

【摘 要】:本论文介绍在移动客户端开发热潮中基于混合模式快速开发的方法,并给出该方法乃至于所有开发模式在源代码泄露、本地保存密码、未使用 HTTPS 加密、用设备 ID 代替认证、资源枚举漏洞、SQL 注入漏洞、XSS、CSRF、Clickjacking 等方面的安全性问题,并提供解决方法。应用本论文的方法后移动客户端的开发更加快速和安全。

【关键词】:移动客户端;混合模式开发;安全性

0 引言

根据中国互联网络信息中心发布的第 32 次《中国互联网络发展状况统计报告》，截至 2013 年 6 月底,中国网民规模达 5.91 亿,其中达 4.64 亿的手机网民规模促进了手机上各种应用的发展[1]。在手机等移动客户端开发中,目前有三种模式 :原生应用、网页应用和混合应用。Jim Cowart 对这三种应用模式的定义、优缺点、何时该选择哪种应用做了详细的介绍[2]。本论文推荐使用混合模式开发。混合模式门槛较低,然而正是由于其过低的门槛,导致这些应用普遍安全性偏低。本文将对笔者分析过的多个移动客户端应用安全性进行剖析,并给出相应的解决方法。

1 移动客户端开发

使用混合模式开发移动客户端应用，可使用 PhoneGap[3]、Titanium、RhoMobile、AppCan 等跨平台工具打包应用。使用该方法使得一次开发即可适配 iOS、Android、Windows Phone、Palm、Blackberry 等多平台。跨平台工具生成的应用内嵌了移动终端浏览器,使用 HTML5+CSS3+JavaScript 开发的应用在内嵌的浏览器内运行。跨平台工具除了使用浏览器提供的功能外,还可使用 JavaScript 调用具体移动终端的功能，比如地理定位、摄像头、加速器、联系人、声音和振动等。任何一段 HTML 代码打包后即成为一个移动客户端应用。这种开发模式开发速度快、调试容易而受到普遍欢迎。

使用混合模式开发的移动客户端应用,应用本身基于 HTML5+CSS3+JavaScript 开发，前端 JavaScript 框架可选择 MVC 框架包括 AngularJs、Ember.js、Backbone.js、Knockout 等,展示框架可选择 JQuery Mobile、Sencha Touch、Bootstrap 等。后端调用服务器功能可使用 Ajax 调用远程 API 服务器或者直接显示远程 API 服务器返回的 HTML 代码。以上开发工具和语言跟原有的网站开发所掌握知识架构重叠,对开发人员要求低。

2 安全性分析

然而,也正由于其低门槛,导致混合模式开发的应用普遍安全性较弱,甚至于比在桌面浏览器运行的 Web 网站更弱。其根源在于 :桌面浏览器运行的 Web 网站可以看到访问的 URL 地址，可以直接查看生成的 HTML 代码，而移动客户端应用更像一个黑盒,在这个伪黑盒的蒙蔽下，开发人员的安全意识就会松懈。开发人员因为用户无法像桌面浏览器一样查看网页地址和 HTML 源代码就认为应用是安全的。实际上移动客户端应用在被反编译和网络抓包工具捕获分析下，网页地址和源代码也是完全暴露在黑客面前。而且由于移动客户端应用需要调用远端 API 服务器,所以原先 Web 开发方面的安全漏洞也还是存在。而 API 调用的接口简单,比 Web 网站的服务端程序更容易遭到攻击。下面举例笔者在实践中对移动客户端应用分析后归纳出的几种较为普遍的安全漏洞,并一一给出解决方法。

2.1 源代码泄露

移动客户端应用文件,比如 Android 客户端 APK 文件是 ZIP 文件格式的，所以源代码很容易被窃取。通过反编译，基于 HTML5+CSS3+JavaScript 的资源文件就会全部展示在黑客面前。除了知识产权无法得到有效保护外，黑客还会通过分析源代码漏洞来对 API 服务器实施攻击。所以应对 JavaScript 代码和应用代码进行代码混淆,减少代码泄露的危险性。

2.2 本地保存密码

由于移动设备使用人固定，而且输入字符较为麻烦，所以移动客户端应用会更多使用本地保存密码功能。本地保存密码一般会使用平台自带的对称加密功能或自行加密保存在本地数据库内。但是这在移动设备丢失或者被植入木马后会导致密码泄露。若用户密码跟其他网站的密码一样会导致用户暴露在很大的风险下。所以安全的做法是：若用户选择了保存密码，则提交用户名和密码到服务端验证，如果验证通过，生成临时的令牌返回给客户端加密保存以备下次登录时验证。令牌有一定的时效，同时令牌在用户在其他地方修改密码后失效，这种方法可以保护明文密码不被保存在本地，有效提高安全性。

2.3 未使用 HTTPS 加密

在服务端性能允许的情况下应对移动客户端应用对远程 API 服务器的调用使用 HTTPS 加密，这可加大被网络数据包分析工具抓包获取 URL 而分析远程 API 调用地址和参数的难度。这是黑客实施攻击分析的第一步。

2.4 用移动设备的 ID 代替认证

使用移动设备的 ID 代替认证一般发生在设备较难保存数据的移动设备内。例如笔者曾经分析过一个和电视机机顶盒相关的移动客户端应用，该 APP 通过扫描电视显示的二维码与机顶盒绑定，而这个绑定就使用机顶盒的 32 位的设备 ID：STBID。绑定完成后的所有操作均使用设备的 ID 代替认证。然而这个机顶盒的 STBID 在同一个城市内前面 20 位是相同的。只要变换 STBID 字符串后面的 12 位数字，以变换后的 ID 去访问 API 服务器，即可窃取用户信息和控制用户的机顶盒。解决方法是不能依赖设备的 ID 来认证，可采用可变的令牌、其他认证手段辅助加强验证、对 API 服务器访问次数限制保证合理的调用频次等几种方法预防。

2.5 资源枚举漏洞

资源枚举漏洞是指通过变换 API 服务器调用的参数即可枚举出服务器某个资源所有数据的漏洞。笔者曾经分析过一个内建相册功能的 APP，API 调用地址为 http://www.example.com/api/album?id=123，通过替换 123，即可获取所有人的相册内容，而照片也可直接下载没有任何权限限制。出现这类问题的根源在于没有对资源进行权限保护。开发人员因为调用资源的 URL 地址没有显示在浏览器上无法被直接更改而认为是安全的。但是在源代码被反编译或网络抓包工具捕获分析下，黑客即可构造出任意的 API 调用实施攻击。这类漏洞的解决办法是对所有的 API 调用加上相应的权限判断。

2.6 SQL 注入漏洞

SQL 注入漏洞作为最早发现的漏洞至今还广泛存在着[4]。虽然移动客户端应用的注入漏洞的前期漏洞扫描没有 Web 网站那么容易，但是在客户端被网络抓包工具捕获或代理服务器捕获下，黑客还是可以分析得到 API 服务器的调用参数并实施漏洞扫描。解决方法是在 API 服务端对所有的调用应仔细分析用户提交过来的数据，过滤对数据库有威胁的数据。更好的做法是使用开发语言自带的数据库查询参数绑定方法一劳永逸地解决该问题。

2.7 XSS 跨站脚本攻击

由于混合模式开发的 HTML 代码本质上还是在浏览器里面运行，所以跨站脚本攻击[5]的风险还是存在的。而且，跨站脚本攻击会导致用户跳出他们的应用到另外一个网站，而 APP 内嵌的浏览器跟桌面浏览器不同的是用户无法查看到网站 URL，这导致用户无法分辨真实和虚假网站，用户有被钓鱼的危险。解决方法是对所有显示给用户的 HTML 代码都需要经过编码、过滤危险的 HTML 标签，特别需要注意的是不能遗漏在 JSON 数据格式内那些会直接展示的 HTML 代码。

2.8 CSRF 跨站请求伪造

CSRF[6]漏洞发生在桌面浏览器浏览时，然而因为 API 服务器跟桌面浏览器访问的 Web 网站有可能使用同一个域名，使用同一个 Cookie 认证身份，所以 API 服务器也会被当成 CSRF 攻击的目标。所以在开发 API 服务器时也需要预防这类漏洞。解决方法是首先保证 Web 网站的安全，防止 XSS 漏洞，Web 网站本身均需加上 CSRF 令牌防止直接提交，API 服务器可通过加上 HTTP Referer 部分防范。

2.9 Clickjacking 点击劫持

点击劫持[7]是指用户点击的是某个按钮，但是真正却是点击了隐藏在这个按钮下面某个层的另外一个按钮而导致执行了用户不想要执行的其他操作。移动客户端又导致拖放劫持变得更加容易。点击劫持一般发生在 Web 网站上。如果配合 XSS 跨站脚本攻击使得移动客户端跳到别的网站，则点击劫持也会在移动客户端上发生。解决方法可通过禁止 API 服务端的网页代码被嵌入 iframe 或者禁止嵌入 iframe 时执行脚本来保证安全。

3 结语

（下转第 48 页）

看到,有的学校学生到了企业,工作马虎、行为随便、不遵守职业道德,结果既损害了学校的形象,也损害了学生形象,导致校企合作意愿丧失。

4.情感机制--奠基校企长期合作

校企合作过程始终是人际交往、感情沟通的过程。特别是企业在培养人才缺乏法律规定和政策优惠的条件下, 推动校企之间合作的动力首先来自于人的情感。某企业的领导人与学校领导是同乡、同学、战友、朋友,可以带来两家的亲密无间和友好合作。情感永远是校企合作的动力源和润滑剂。情感机制是校企合作长效机制体系的重要组成部分。构建情感机制,一要加强校企信息的交流和沟通。涉及学校改革发展的重大事件、重要政策调整和人事变动等信息及时向企业发布,使企业感到学校对他的重视 ;同时,关注企业的发展变化,并及时给予信息回应,如企业开发了新产品、任命某一负责人,学校及时予以祝贺;企业遇到困难,积极帮助解决。二要重视相关人员的相互交往。交往产生感情,升华彼此关系。如学校经常走访校企合作的相关人员, 定期不定期召开校企合作相关人员参加的座谈会,讨论解决合作办学中存在的问题;节日上门慰问、特别是教师节,让专家委员会成员、特聘教授和兼职教师享受与本校老师一样的待遇。三是经常征求校企合作相关人员意见, 诚恳接受并积极改进校企合作工作。四要按照以人为本的原则充分尊重与校企合作相关人员劳动,关心其疾苦,帮助解决他们所遇到的困难和问题,使他们切身感受到自己是学校的一员。一旦企业的相关人员对学校及校企合作工作产生了感情,校企合作就有了稳固的基础和较高的质量,高技能人才培养也就落到了实处。

三、结论

总之,高职院校为了适应了现代经济社会的发展需要,走校企合作的道路是必然的,要想保证校企合作能够长期有效地进行, 制定相应的有效措施是前提,尤其在现代市场经济的前提下,能够使得高等职业院校与合作企业保持长期稳定、有效地合作显得尤为重要。

参考文献:

[1]谭属春. 试论高职教育产学研的长效机制[J].黑龙江高教研究,2010,(7):81—83.

[2]邓志军, 范淑娜. 高职院校与企业互动合作机制的构建[J]. 教育与职业,2010,(4):14—16.

[3]华耀军. 美国合作教育及启示[J].长沙民政职业技术学院学报,2011

[4]王志强,党庆志. 德国"双元制"职业教育制度简介[J]. 职业教育,2007. 12,(A):7.

(上接第 65 页)

使用混合模式开发后移动客户端开发变得简单快速,提高了开发人员的开发效率。而只要避免本论文提到的安全问题,则在原有网站外再引入的移动客户端就不会成为整个网站系统的一个弱点。移动客户端跨平台工具、CSS 框架、JavaScript 框架还在不断发展中,各个平台都有一定的优缺点和拥簇者,如何随着他们的进化而选择不同的平台是今后可研究的方向。安全没有止境,新的安全漏洞也会继续出现,而且攻击会伴随着多种攻击手段组合进行,今后也可在安全方面做进一步分析。

参考文献:

[1] 中国互联网络信息中心. 中国互联网络发展状况统计报告 [EB/OL]. (2013-07-17) [2013-10-20].http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201307/P020130717505343100851.pdf.

[2] COWART J. When to Go Native, Mobile Web or-Cross-Platform/Hybrid [EB/OL]. (2013-06-06) [2013-10-21]. http://tech.pro/blog/1355/when-to-go-native-mobile-web-or-cross-platformhybrid.

[3] 李晓明. 基于 HTML5 跨移动终端平台的微博系统研究与实现[D]. 成都:电子科技大学,2012.

[4] 陈智坚. 数据库 SQL 注入攻击技术与防范[J]. 福建电脑,2013(02):80-81+105.

[5] 刘海,徐芳,郭帆. 防范 XSS 攻击的研究综述[J]. 计算机与现代化,2011(08):174-178.

[6] 褚诚云. 跨站请求伪造攻击:CSRF 安全漏洞[J]. 程序员,2009(03):98-100.

[7] 王剑,张玉清. 点击劫持漏洞攻防技术研究[J]. 信息网络安全,2011(07):16-19.