Hunting Vulnerable JavaScript Libraries In Android Packages

ISE5601

Author: Varghese Palathuruthil, varghese.palathuruthil@student.sans.edu
Advisor: *Michael Long*

Accepted: *December, 2020*

Abstract

The Android operating system provides the WebView framework to deliver web pages in mobile applications for the Android system. JavaScript libraries are used to leverage JavaScript features in web applications. JavaScript libraries can also be used to build web pages for mobile applications for the Android system. Web and mobile applications using JavaScript often do not stay up-to-date on patching JavaScript libraries. Although tools exist in evaluating web applications for vulnerable JavaScript libraries, no such utility evaluates mobile applications for the Android platform to verify whether they contain vulnerable JavaScript libraries. This paper examines the feasibility of developing a tool that could scan mobile application artifacts built for the Android operating system to determine whether they contain vulnerable JavaScript libraries.

1. Introduction

JavaScript libraries can be used to leverage JavaScript features in web applications. The Android operating system provides the WebView interface to deliver a web page as part of a mobile application deployed in Android (“Building web apps in WebView”, 2020). Mobile applications deployed on the Android system that use the WebView interface could use JavaScript libraries to build the web page for the application. JavaScript libraries are pieces of software that need to be kept up-to-date with patches to protect against reported vulnerabilities. There are tools to identify vulnerable JavaScript libraries in web applications. However, no such utility exists to evaluate Android applications for vulnerable JavaScript libraries. This research examines the feasibility of developing a tool that scans Android applications to determine whether they contain vulnerable JavaScript libraries.

2. The Android WebView Framework

There are several ways to build applications for the Android platform. Native applications for the Android platform utilize the system framework to provide the optimal experience of Android features. Native applications have limits to user interface controls compared to traditional web applications. The WebView framework provided by the Android platform is used to deliver web pages in an Android application. (“Guide to Web-based content in Android”, 2020). Figure 1 below compares web content displayed in a traditional web browser on the Android system and an Android application.

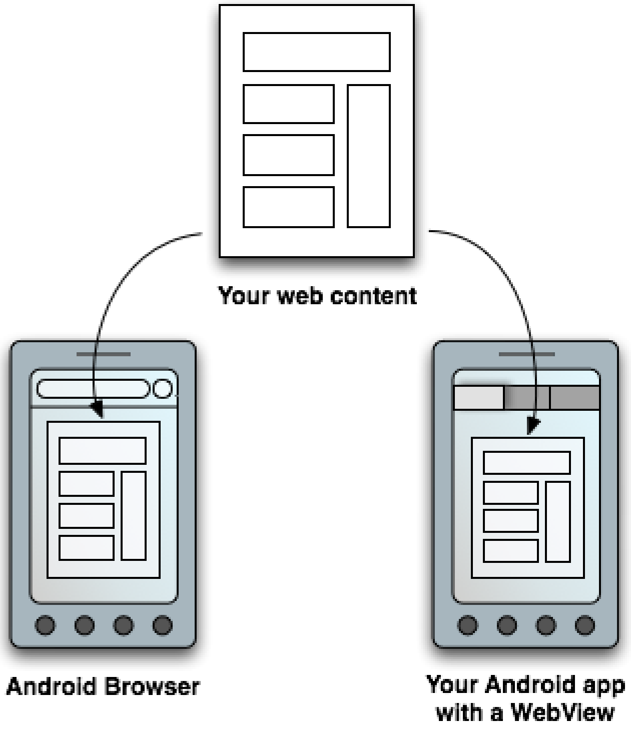


Figure 1. Using WebView layout to display web content in Android applications similar to the traditional web browser.
Source: Guide to Web-based content in Android. (2019)

Web pages are typically built using technologies such as Cascaded Style Sheets (CSS), Hypertext Markup Language (HTML), and JavaScript. These technologies are also used to create web pages for the Android application. The Android WebView framework also defines interface such as the `JavascriptInterface` ("Android WebKit Reference", 2020) which allows JavaScript in web pages to invoke function calls on the underlying Android architecture.

The need to access Android system features available in native applications and the need for fine-grain user interface controls available in web pages has resulted in a blend known as a hybrid mobile application ("Ionic Framework Hybrid App Development", 2020).

3. Hybrid Mobile Applications

Hybrid mobile applications use technologies such as HTML, CSS, and JavaScript. Hybrid mobile applications run from within a native application and its own embedded browser ("Ionic Framework Hybrid App Development", 2020). In the Android platform, the WebView element will display the application. Two hybrid mobile application frameworks that provide such a solution are Apache Cordova (also known as PhoneGap) and the Ionic Framework.

In a Cordova-built hybrid mobile application, the Cordova-enabled WebView may provide the application with its entire user interface ("Apache Cordova Overview", 2018). Figure 2 below illustrates how Cordova architecture uses the Cordova-enabled WebView to render the user interface. In the Android platform, the Cordova-enabled WebView uses the `CordovaWebView` component to interact with the Android WebView framework ("Apache Cordova-enabled WebView for Android", 2016).

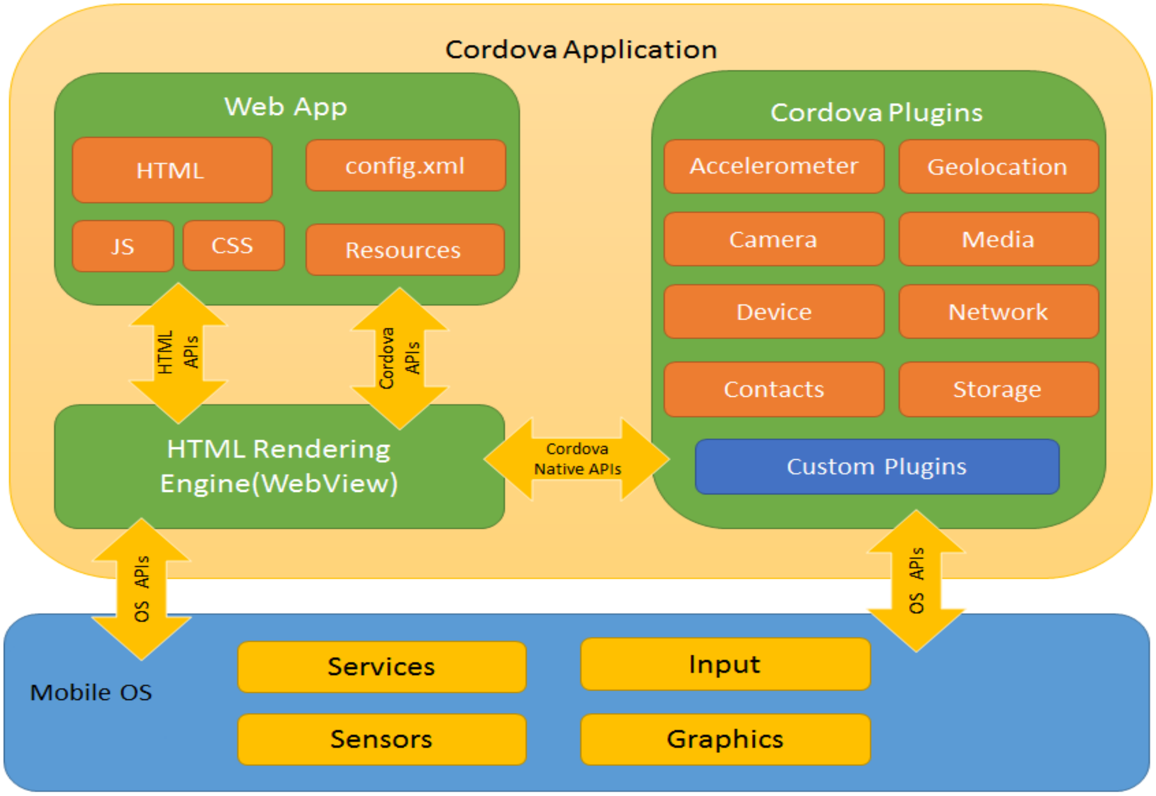


Figure 2. A high-level view of the Cordova application architecture
Source: Apache Cordova Overview. (October 17 2018).

The Xamarin platform uses .NET and C# technologies to build cross-platform applications for the mobile device (“Xamarin”, 2020). The Xamarin platform uses Xamarin.Forms, an open-source framework to build consistent user interface design in the mobile application (“Xamarin.Forms”, 2020). Xamarin.Forms use WebView for displaying web and HTML content in the mobile application. The Xamarin.Forms WebView interface supports JavaScript to build web content (“Xamarin.Forms WebView”, 2020).

4. Risk of Vulnerable JavaScript Libraries in Mobile Applications

The Open Web Application Security Project (OWASP) lists client-side injection in its 2014 top 10 mobile risks (“OWASP Top 10 Mobile Risks 2014”, 2020), and poor code quality in its 2016 top 10 mobile risks (“OWASP Top 10 Mobile Risks 2016”, 2020).

Client-side injection results in malicious code execution on the mobile device via the mobile application ("OWASP 2014 M7: Client Side Injection", 2020). This injection technique includes JavaScript injection. Application cookie and session identifier theft are examples of the exploits that may result from JavaScript injection vulnerability. The proposed OWASP remediation includes disabling JavaScript and Plugin support for WebView in the Android platform.

Poor code quality could result in code-level implementation problems in the mobile application such as buffer overflows and format string vulnerabilities. Document Object Model (DOM) based Cross-Site Scripting (XSS) issue in a WebView mobile application is an example of poor code quality issue (“OWASP 2016 M7: Poor Code Quality”, 2020). JavaScript code should be vetted to ensure it is not vulnerable to XSS exploits.

The Open Web Application Security Project (OWASP) third-party JavaScript management cheat sheet list three risks to consider when invoking third party JavaScript code such as JavaScript libraries (“OWASP Third Party JavaScript Management Cheat Sheet”, 2020).

1. Loss of control over changes to the client application.
2. The execution of arbitrary code on client systems.
3. The disclosure or leakage of sensitive information to 3rd parties.

4.1. Loss of control over changes to the client application

OWASP lists the compromise of hosted solutions of third-party JavaScript library as the most significant risk to using the third-party JavaScript library ("OWASP Third Party JavaScript Management Cheat Sheet", 2020). This risk compromises the integrity of the JavaScript library that may be downloaded and embedded in the mobile application to be used with WebView on the Android platform. The implanted JavaScript library in the mobile application needs to stay updated with patching and the latest available versions.

4.2. The execution of arbitrary code on client systems

OWASP notes the inconsistent practice of reviewing third-party JavaScript code prior to integration with application leading to the risk of execution of arbitrary third-party JavaScript code ("OWASP Third Party JavaScript Management Cheat Sheet", 2020). Execution of arbitrary code may lead to privilege escalation and injection attacks such as Cross-Site Scripting (XSS). Poor code quality (“OWASP 2016 M7: Poor Code Quality”, 2020) and client-side injection (“OWASP 2014 M7: Client Side Injection”, 2020) are known top risks to mobile applications listed by OWASP.

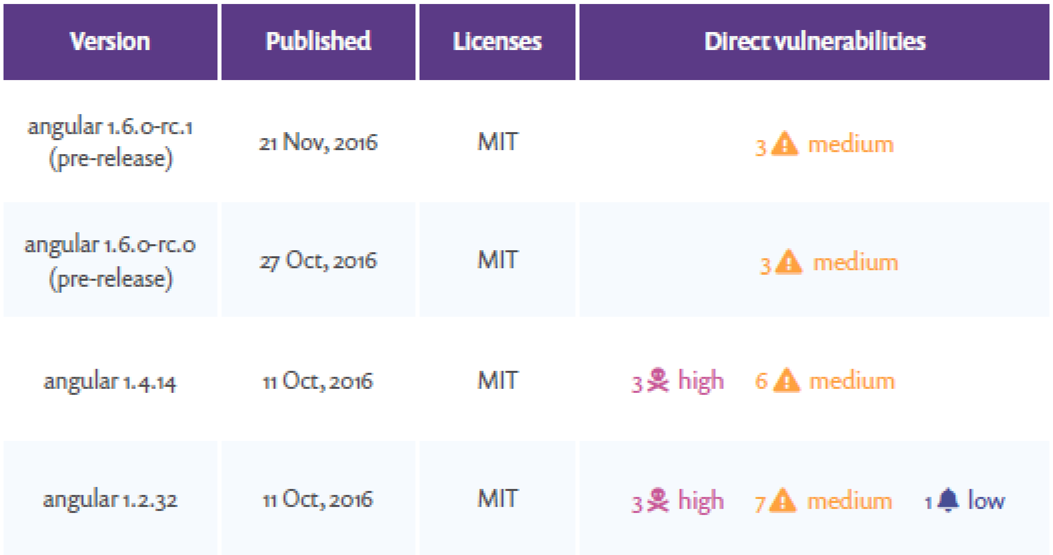
4.3. The disclosure or leakage of sensitive information to 3rd parties

OWASP lists the risk of disclosure of sensitive information such as HTTP headers, IP address, referrer, and cookies when the invocation of third party JavaScript libraries may lead to communication with third party servers ("OWASP Third Party JavaScript Management Cheat Sheet", 2020). If the mobile application utilizes embedded JavaScript libraries for use cases such as analytics on user behavior with the mobile application, then there is a risk of sensitive information disclosure.

5. JavaScript Vulnerability Databases

The Special Interest Group (SIG) of the Forum of Incident Response and Security Teams (FIRST) develops and maintains the Common Vulnerability Scoring System (CVSS) specification and the Common Vulnerabilities and Exposures (CVE) system to understand and prioritize the severity of a security vulnerability (Tal, "Scoring security vulnerabilities 101", 2019).

The state of JavaScript frameworks security report of 2019, published by Snyk, notes the lack of a consistent vulnerability database to track all of the JavaScript libraries' vulnerabilities. Many of the reported vulnerabilities in JavaScript libraries do not have a CVE reference. This is not a failure, but rather a common practice, as CVEs were designed with commercial vendors in mind, requiring substantial time and expertise to file. This does not always scale well for many open source JavaScript libraries. Without a CVE, vulnerabilities can only be tracked by dedicated analysts who manage and track open-source activity with customized methods ("The JavaScript frameworks security report", 2019). Two examples of vulnerability databases for JavaScript libraries are from the commercial tool vendor Snyk and the community-driven vulnerability database VULDB. Figure 3 below lists Snyk's vulnerability database for Angular 1.x.

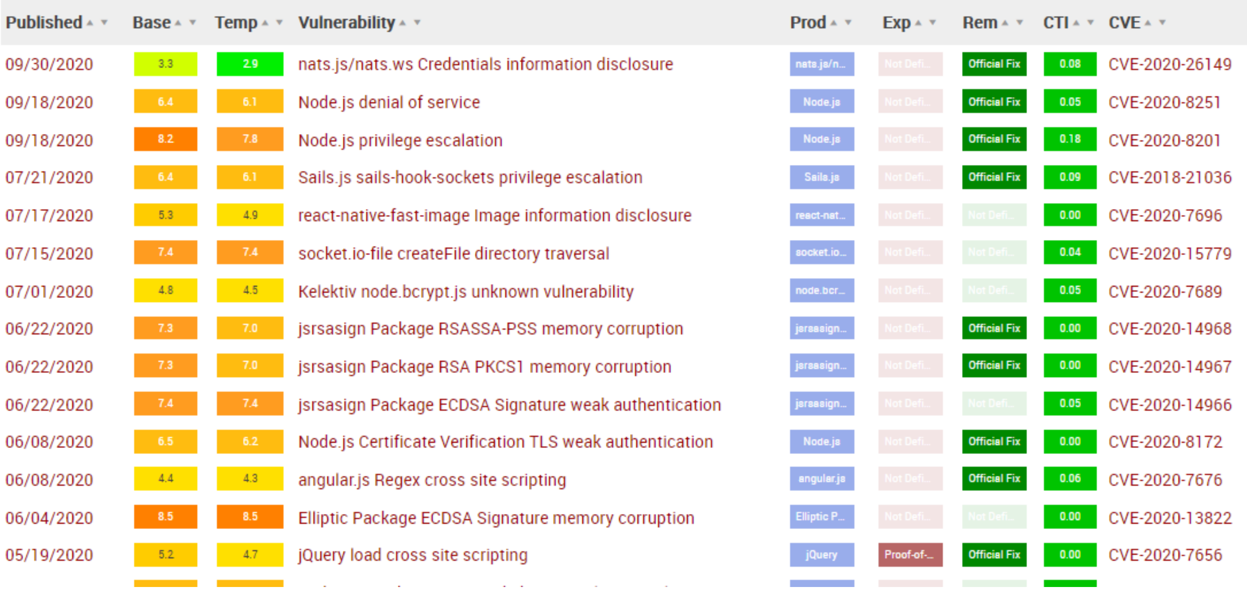


Version	Published	Licenses	Direct vulnerabilities
angular 1.6.0-rc.1 (pre-release)	21 Nov, 2016	MIT	3 ⚠ medium
angular 1.6.0-rc.0 (pre-release)	27 Oct, 2016	MIT	3 ⚠ medium
angular 1.4.14	11 Oct, 2016	MIT	3 ☠ high 6 ⚠ medium
angular 1.2.32	11 Oct, 2016	MIT	3 ☠ high 7 ⚠ medium 1 🔔 low

Figure 3. Snyk's vulnerability database for Angular 1.x

Source: Snyk - The state of JavaScript frameworks security report 2019. pg12. (2019).

Figure 4 below lists the VULDB vulnerability database for JavaScript libraries.



Published	Base	Temp	Vulnerability	Prod	Exp	Rem	CTI	CVE
09/30/2020	3.3	2.9	nats.js/nats.ws Credentials information disclosure	nats.js/n...	Not Defi...	Official Fix	0.08	CVE-2020-26149
09/18/2020	6.4	6.1	Node.js denial of service	Node.js	Not Defi...	Official Fix	0.05	CVE-2020-8251
09/18/2020	8.2	7.8	Node.js privilege escalation	Node.js	Not Defi...	Official Fix	0.18	CVE-2020-8201
07/21/2020	6.4	6.1	Sails.js sails-hook-sockets privilege escalation	Sails.js	Not Defi...	Official Fix	0.09	CVE-2018-21036
07/17/2020	5.3	4.9	react-native-fast-image Image information disclosure	react-nat...	Not Defi...	Not Defi...	0.00	CVE-2020-7696
07/15/2020	7.4	7.4	socket.io-file createFile directory traversal	socket.io...	Not Defi...	Not Defi...	0.04	CVE-2020-15779
07/01/2020	4.8	4.5	Kelektiv node.bcrypt.js unknown vulnerability	node.bcr...	Not Defi...	Not Defi...	0.05	CVE-2020-7689
06/22/2020	7.3	7.0	jsrsasign Package RSASSA-PSS memory corruption	jsrsasign...	Not Defi...	Official Fix	0.00	CVE-2020-14968
06/22/2020	7.3	7.0	jsrsasign Package RSA PKCS1 memory corruption	jsrsasign...	Not Defi...	Official Fix	0.00	CVE-2020-14967
06/22/2020	7.4	7.4	jsrsasign Package ECDSA Signature weak authentication	jsrsasign...	Not Defi...	Not Defi...	0.05	CVE-2020-14966
06/08/2020	6.5	6.2	Node.js Certificate Verification TLS weak authentication	Node.js	Not Defi...	Official Fix	0.00	CVE-2020-8172
06/08/2020	4.4	4.3	angular.js Regex cross site scripting	angular.js	Not Defi...	Official Fix	0.06	CVE-2020-7676
06/04/2020	8.5	8.5	Elliptic Package ECDSA Signature memory corruption	Elliptic P...	Not Defi...	Not Defi...	0.00	CVE-2020-13822
05/19/2020	5.2	4.7	jQuery load cross site scripting	jQuery	Proof-of-...	Official Fix	0.00	CVE-2020-7656

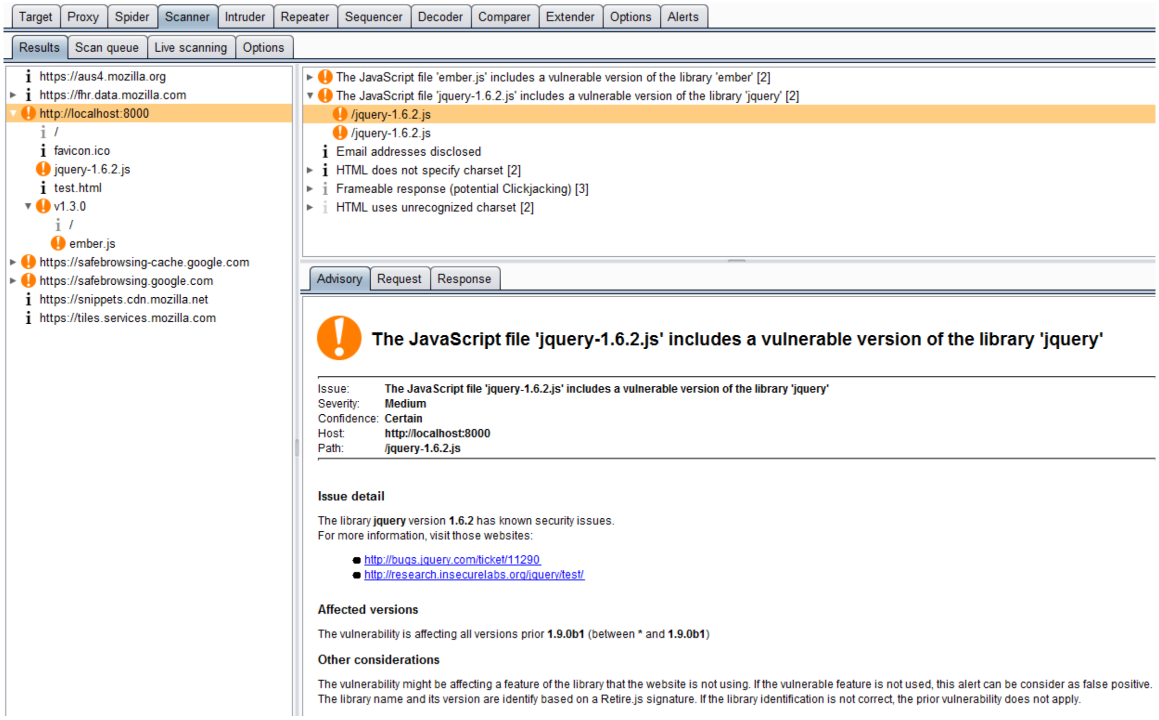
Figure 4. VULDB vulnerability database for JavaScript libraries

Source: VULDB vulnerability database for JavaScript libraries. (2020).

According to the OWASP Third Party JavaScript Management Cheat Sheet, one such open source tool to identify vulnerable JavaScript libraries is RetireJS ("OWASP Third Party JavaScript Management Cheat Sheet", 2020).

5.1. Retire.js - Tools to detect vulnerable versions of JavaScript libraries

The goal of the Retire.js (or RetireJS) open source project is to help analysts detect the use of versions of JavaScript libraries with known vulnerabilities in applications ("Retire.js. Detect use of versions of JavaScript libraries with known vulnerabilities", 2020). Retire.js can be used as a command-line scanner, or integrated with the build and compile tools such as grunt and gulp. Retire.js can be combined with penetration test tools such as Burp or OWASP Zap, or integrated with web browsers such as Chrome or Firefox as an extension. Figure 5 lists Retire.js' output as an extension to the Burp penetration test tool, and Figure 6 lists the output from the Retire.js grunt task when evaluating JavaScript libraries.



- https://aus4.mozilla.org
- https://fhr.data.mozilla.com
- http://localhost:8000
  - /
  - favicon.ico
  - jquery-1.6.2.js
  - test.html
  - v1.3.0
    - /
    - ember.js
- https://safebrowsing-cache.google.com
- https://safebrowsing.google.com
- https://snippets.cdn.mozilla.net
- https://tiles.services.mozilla.com

- The JavaScript file 'ember.js' includes a vulnerable version of the library 'ember' [2]
- The JavaScript file 'jquery-1.6.2.js' includes a vulnerable version of the library 'jquery' [2]
  - /jquery-1.6.2.js
  - /jquery-1.6.2.js
- Email addresses disclosed
- HTML does not specify charset [2]
- Frameable response (potential Clickjacking) [3]
- HTML uses unrecognized charset [2]

The JavaScript file 'jquery-1.6.2.js' includes a vulnerable version of the library 'jquery'

Issue: **The JavaScript file 'jquery-1.6.2.js' includes a vulnerable version of the library 'jquery'**
Severity: **Medium**
Confidence: **Certain**
Host: **http://localhost:8000**
Path: **/jquery-1.6.2.js**

Issue detail

The library **jquery** version **1.6.2** has known security issues.
For more information, visit those websites:

- http://bugs.jquery.com/ticket/11290
- http://research.insecurelabs.org/jquery/test/

Affected versions

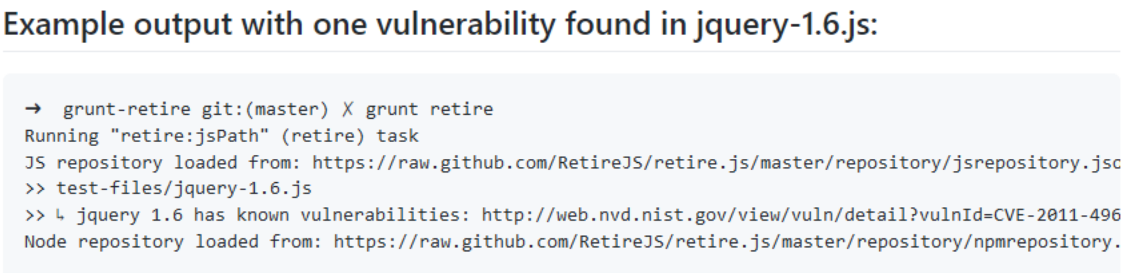
The vulnerability is affecting all versions prior **1.9.0b1** (between * and **1.9.0b1**)

Other considerations

The vulnerability might be affecting a feature of the library that the website is not using. If the vulnerable feature is not used, this alert can be consider as false positive.
The library name and its version are identify based on a Retire.js signature. If the library identification is not correct, the prior vulnerability does not apply.

Figure 5. Retire.js extender use in Burp tool

Source: Retire.js Burp extender plugin. (2020).



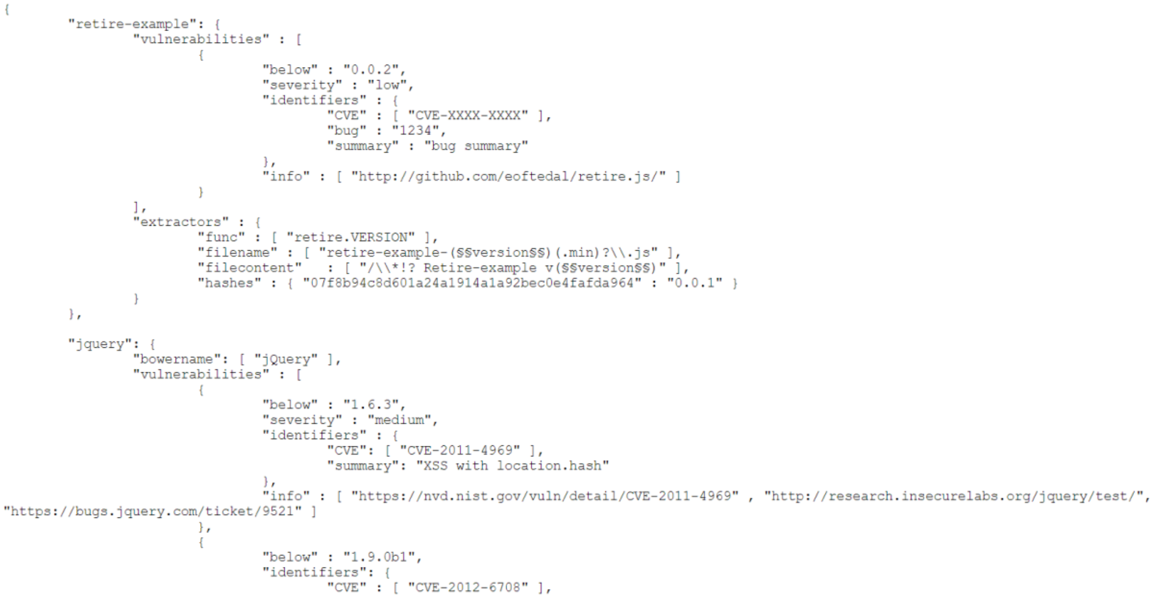
Example output with one vulnerability found in jquery-1.6.js:

```
➜  grunt-retire git:(master) ✗ grunt retire
Running "retire:jsPath" (retire) task
JS repository loaded from: https://raw.github.com/RetireJS/retire.js/master/repository/jsrepository.jso
>> test-files/jquery-1.6.js
>> ↳ jquery 1.6 has known vulnerabilities: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-496
Node repository loaded from: https://raw.github.com/RetireJS/retire.js/master/repository/npmrepository.
```

Figure 6. Grunt task for retire.js

Source: Grunt task for retire.js. (2020).

Retire.js team maintains a vulnerability database for JavaScript libraries at the Retire.js GitHub repository. The Readme document explains how contributions are submitted to the Retire.js vulnerability database ("Retire.js repository README", 2020). The Retire.js vulnerability database for JavaScript libraries is in JavaScript Object Notation (JSON) format. It is available for integration with analytical tools ("Retire.js list of JavaScript libraries with known vulnerabilities in JSON format", 2020). Figure 7 is a snippet from the latest version of the Retire.js vulnerability database for JavaScript libraries. The displayed JSON list contains the vulnerable versions of the impacted JavaScript libraries, along with their associated CVE information and bug summary.



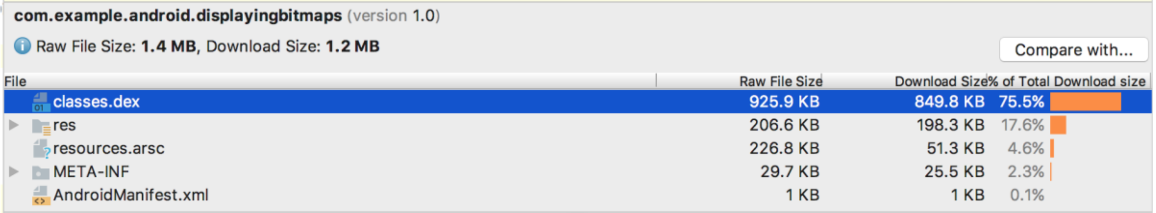
```
{
        "retire-example": {
                "vulnerabilities" : [
                        {
                                "below" : "0.0.2",
                                "severity" : "low",
                                "identifiers" : {
                                        "CVE" : [ "CVE-XXXX-XXXX" ],
                                        "bug" : "1234",
                                        "summary" : "bug summary"
                                },
                                "info" : [ "http://github.com/eoftedal/retire.js/" ]
                        }
                ],
                "extractors" : {
                        "func" : [ "retire.VERSION" ],
                        "filename" : [ "retire-example-(§§version§§)(.min)?\\.js" ],
                        "filecontent"   : [ "/\\*!? Retire-example v(§§version§§)" ],
                        "hashes" : { "07f8b94c8d601a24a1914a1a92bec0e4fafda964" : "0.0.1" }
                }
        },

        "jquery": {
                "bowername": [ "jQuery" ],
                "vulnerabilities" : [
                        {
                                "below" : "1.6.3",
                                "severity" : "medium",
                                "identifiers" : {
                                        "CVE": [ "CVE-2011-4969" ],
                                        "summary": "XSS with location.hash"
                                },
                                "info" : [ "https://nvd.nist.gov/vuln/detail/CVE-2011-4969" , "http://research.insecurelabs.org/jquery/test/",
"https://bugs.jquery.com/ticket/9521" ]
                        },
                        {
                                "below" : "1.9.0b1",
                                "identifiers": {
                                        "CVE" : [ "CVE-2012-6708" ],
```

Figure 7. Retire.js list of JavaScript libraries with known vulnerabilities in JSON format

Source: Retire.js list of JavaScript libraries with known vulnerabilities in JSON format. (2020).

6. The Android Package (APK) Structure

Android applications are compiled into an Android package known as APK. An APK file is an archive file with a .apk suffix ("Android Application Fundamentals", 2019). APKs are files that follow the ZIP file format ("Analyze your build with APK Analyzer", 2020). Figure 8 lists the file structure of an Android APK file.



com.example.android.displayingbitmaps (version 1.0)

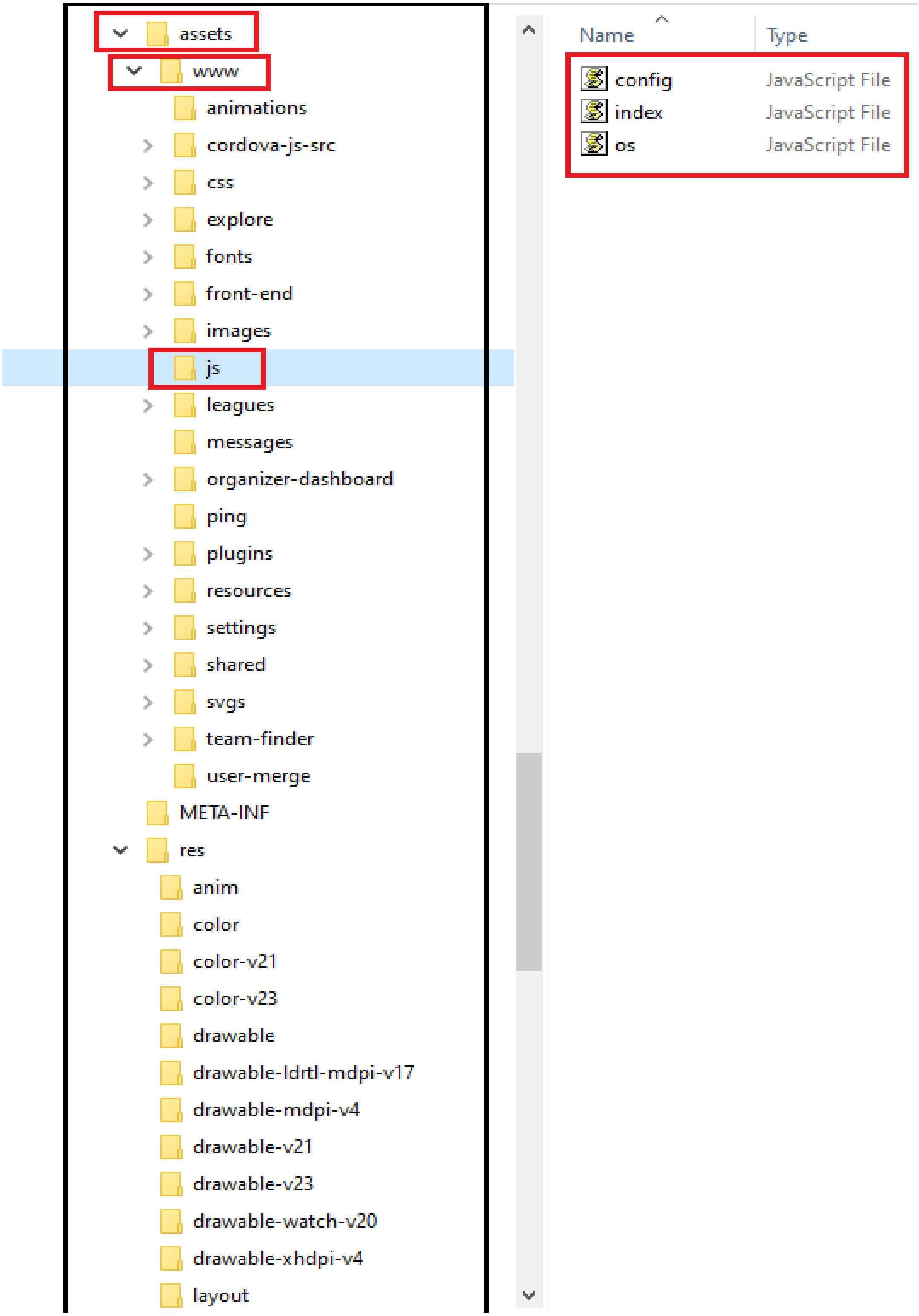
Raw File Size: 1.4 MB, Download Size: 1.2 MB

File	Raw File Size	Download Size	% of Total Download size
classes.dex	925.9 KB	849.8 KB	75.5%
res	206.6 KB	198.3 KB	17.6%
resources.arsc	226.8 KB	51.3 KB	4.6%
META-INF	29.7 KB	25.5 KB	2.3%
AndroidManifest.xml	1 KB	1 KB	0.1%

Figure 8. APK File Structure inspected by APK Analyzer

Source: Analyze your build with APK Analyzer. (2020).

In the case of an Android application built using a hybrid mobile application framework such as Cordova (PhoneGap), the HTML, CSS, and JavaScript artifacts are under the assets folder (E.g. assets -> www -> css, assets -> www -> js, assets -> www -> index.html) . Figure 9 lists the file structure of the Hockey Community Android application developed using the Cordova (PhoneGap) hybrid mobile application framework (“PhoneGap App Showcase”, 2016).



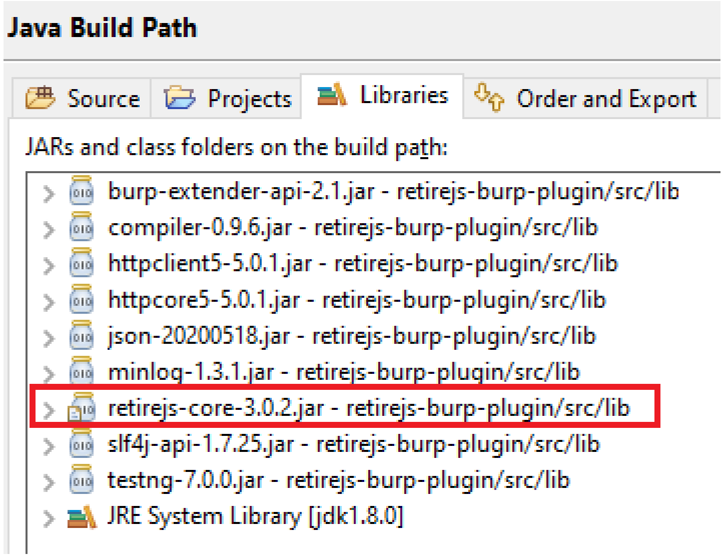
```
assets
  www
    animations
    cordova-js-src
    css
    explore
    fonts
    front-end
    images
    js
    leagues
    messages
    organizer-dashboard
    ping
    plugins
    resources
    settings
    shared
    svgs
    team-finder
    user-merge
META-INF
res
  anim
  color
  color-v21
  color-v23
  drawable
  drawable-ldrtl-mdpi-v17
  drawable-mdpi-v4
  drawable-v21
  drawable-v23
  drawable-watch-v20
  drawable-xhdpi-v4
  layout
```

Name	Type
config	JavaScript File
index	JavaScript File
os	JavaScript File

Figure 9. APK File Structure of the Hockey Community Android App

7. Scanning Android packages for Vulnerable JavaScript Libraries

Philippe Arteau created an open source extension for the Burp and OWASP ZAP penetration test tool to scan the target web application for vulnerable JavaScript libraries using the Retire.js repository ("Retire.js Burp extender plugin", 2020). The Java libraries bundled with the Retire.js Burp extender plugin, such as `retirejs-core-xxx.jar` ("Retire.js Burp extender plugin core library", 2020), are some of the dependency libraries used to build a tool to scan Android package files for vulnerable JavaScript libraries for this research. The goal is to use the tool to check Android package files for JavaScript files (.js files) and compare them against the Retire.js repository for listed vulnerabilities. Figure 10 lists the dependency Java libraries used to build the tool to scan Android package files for vulnerable JavaScript libraries.



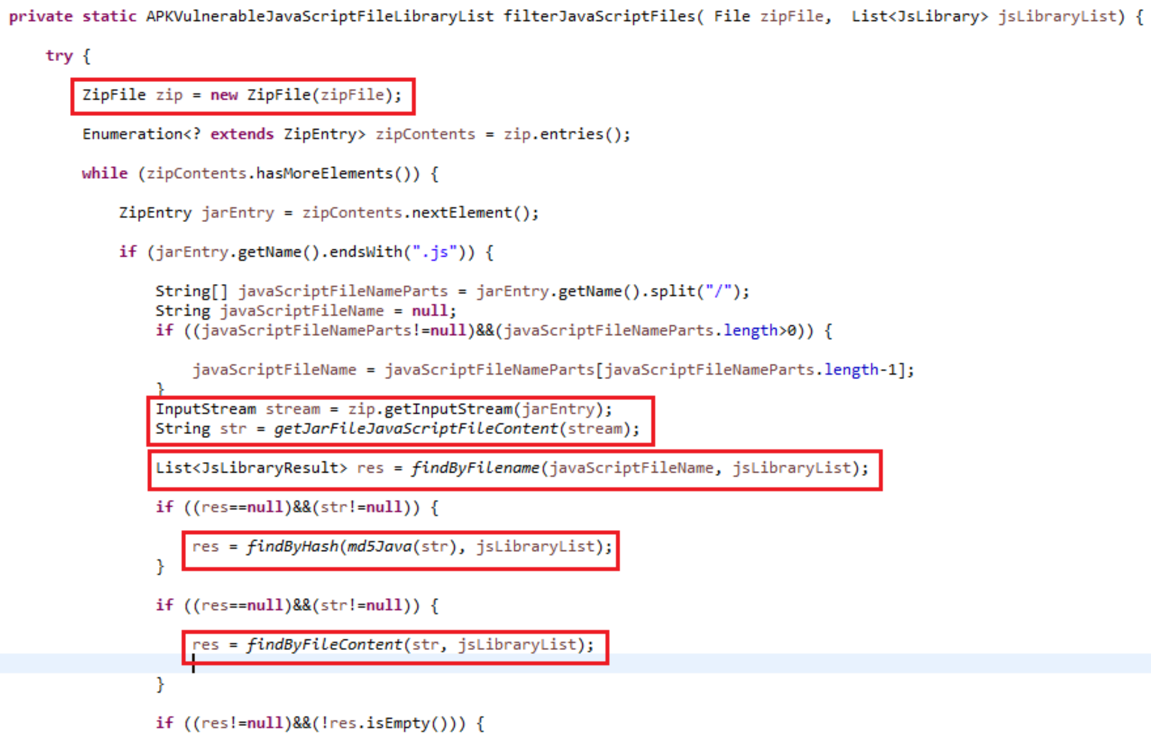
JARs and class folders on the build path:

- burp-extender-api-2.1.jar - retirejs-burp-plugin/src/lib
- compiler-0.9.6.jar - retirejs-burp-plugin/src/lib
- httpclient5-5.0.1.jar - retirejs-burp-plugin/src/lib
- httpcore5-5.0.1.jar - retirejs-burp-plugin/src/lib
- json-20200518.jar - retirejs-burp-plugin/src/lib
- minlog-1.3.1.jar - retirejs-burp-plugin/src/lib
- retirejs-core-3.0.2.jar - retirejs-burp-plugin/src/lib
- slf4j-api-1.7.25.jar - retirejs-burp-plugin/src/lib
- testng-7.0.0.jar - retirejs-burp-plugin/src/lib
- JRE System Library [jdk1.8.0]

Figure 10. Retire.js Burp extender dependency library used by the tool to scan Android package files

The Java programming language provides a rich set of interfaces to read files in the ZIP file format ("Package java.util.zip", 2020). This is useful as Android APKs are files that follow the ZIP file format ("Analyze your build with APK Analyzer", 2020). Figure 11 is a snippet of the Java code used to scan a given Android package using the

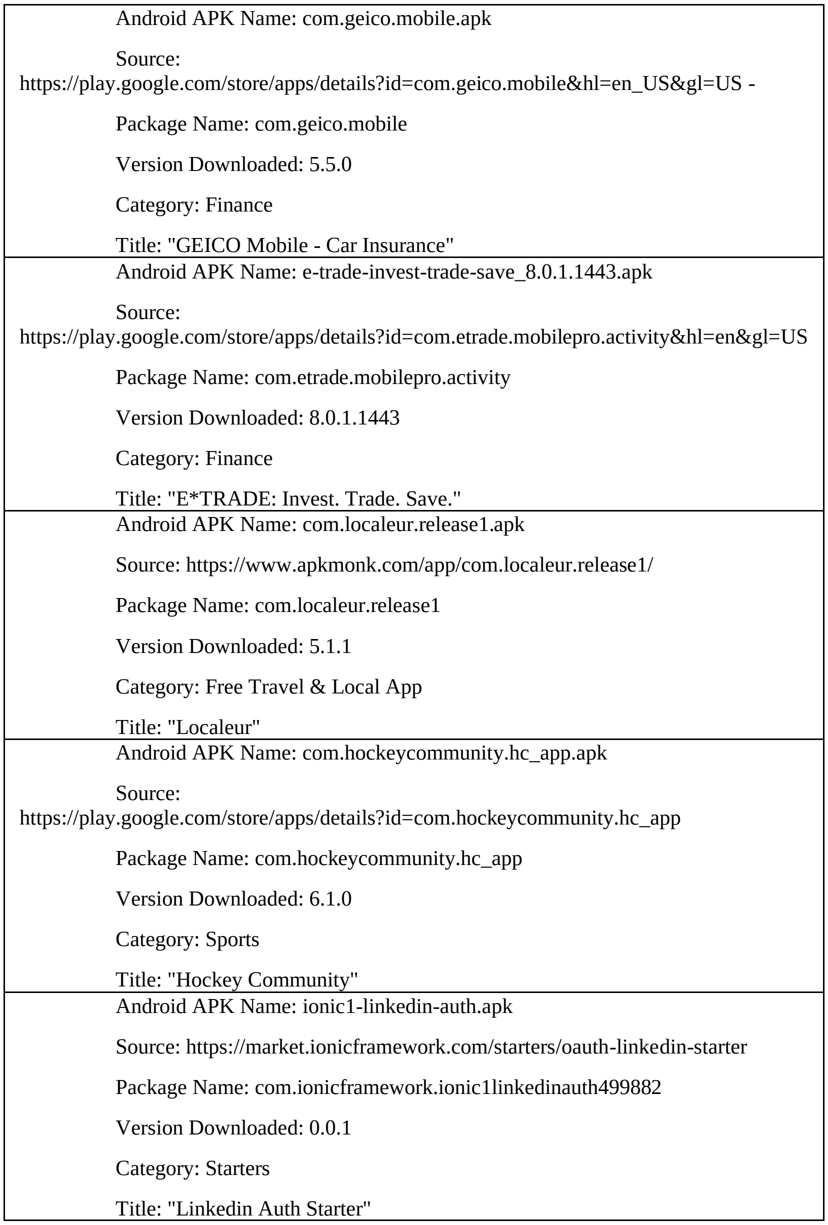
Java zip libraries. The Java code uses the Java programming language's file utilities to find and load JavaScript file contents within the Android package. The code then invokes the `findByFilename`, `findByHash`, and `findByFileContent` methods to check for vulnerable JavaScript library versions against the Retire.js repository using the retire.js core library created by Philippe Arteau. The search criteria used to scan the Retire.js repository is the JavaScript file name, the checksum hash of the JavaScript file, and the JavaScript file content.



```java
private static APKVulnerableJavaScriptFileLibraryList filterJavaScriptFiles( File zipFile,  List<JsLibrary> jsLibraryList) {

    try {

        ZipFile zip = new ZipFile(zipFile);

        Enumeration<? extends ZipEntry> zipContents = zip.entries();

        while (zipContents.hasMoreElements()) {

            ZipEntry jarEntry = zipContents.nextElement();

            if (jarEntry.getName().endsWith(".js")) {

                String[] javaScriptFileNameParts = jarEntry.getName().split("/");
                String javaScriptFileName = null;
                if ((javaScriptFileNameParts!=null)&&(javaScriptFileNameParts.length>0)) {

                    javaScriptFileName = javaScriptFileNameParts[javaScriptFileNameParts.length-1];
                }
                InputStream stream = zip.getInputStream(jarEntry);
                String str = getJarFileJavaScriptFileContent(stream);

                List<JsLibraryResult> res = findByFilename(javaScriptFileName, jsLibraryList);

                if ((res==null)&&(str!=null)) {

                    res = findByHash(md5Java(str), jsLibraryList);
                }

                if ((res==null)&&(str!=null)) {

                    res = findByFileContent(str, jsLibraryList);

                }

                if ((res!=null)&&(!res.isEmpty())) {
```

Figure 11. Retire.js Burp extender dependency library used by the tool to scan Android package files

Fifty-nine various Android packages are downloaded for analysis. Besides the Google Play Store ("Google Play Store", 2020), sample Android packages for this research are retrieved from APKCombo ("APKCombo", 2020), apkmonk ("apkmonk", 2020), and the Ionic Marketplace ("Ionic Marketplace", 2020). The categories of the mobile applications associated with the downloaded Android packages range from Finance, Travel, and Sports to Food. Figure 12 lists a sample of the Android packages that are scanned by the research tool. The full list of the Android packages used in this research is provided in the Appendix.



Android APK Name: com.geico.mobile.apk

Source: https://play.google.com/store/apps/details?id=com.geico.mobile&hl=en_US&gl=US -

Package Name: com.geico.mobile

Version Downloaded: 5.5.0

Category: Finance

Title: "GEICO Mobile - Car Insurance"

Android APK Name: e-trade-invest-trade-save_8.0.1.1443.apk

Source: https://play.google.com/store/apps/details?id=com.etrade.mobilepro.activity&hl=en&gl=US

Package Name: com.etrade.mobilepro.activity

Version Downloaded: 8.0.1.1443

Category: Finance

Title: "E*TRADE: Invest. Trade. Save."

Android APK Name: com.localeur.release1.apk

Source: https://www.apkmonk.com/app/com.localeur.release1/

Package Name: com.localeur.release1

Version Downloaded: 5.1.1

Category: Free Travel & Local App

Title: "Localeur"

Android APK Name: com.hockeycommunity.hc_app.apk

Source: https://play.google.com/store/apps/details?id=com.hockeycommunity.hc_app

Package Name: com.hockeycommunity.hc_app

Version Downloaded: 6.1.0

Category: Sports

Title: "Hockey Community"

Android APK Name: ionic1-linkedin-auth.apk

Source: https://market.ionicframework.com/starters/oauth-linkedin-starter

Package Name: com.ionicframework.ionic1linkedinauth499882

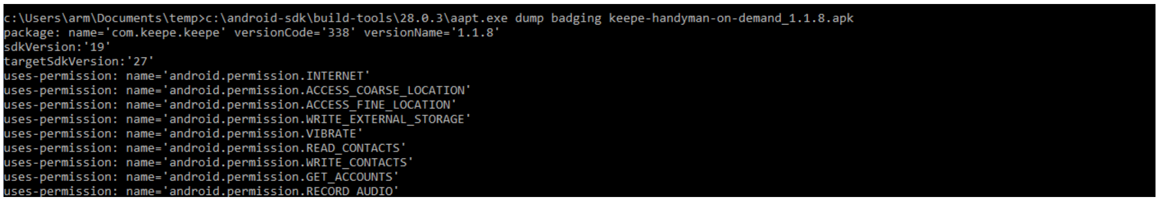
Version Downloaded: 0.0.1

Category: Starters

Title: "Linkedin Auth Starter"

Figure 12. A sample of Android packages that are scanned by the research tool

The legacy `aapt` command provided by the Android development kit ("Android AAPT2 Command Line Tool", 2020) verifies the versions of the applications bundled with the downloaded Android packages. Figure 13 is the snippet of the output printed when running the legacy `aapt` command against the "Keepe - Handyman on Demand" Android package. The information from the output of the aapt command is used to confirm the downloaded version of the Android package.



```
c:\Users\arm\Documents\temp>c:\android-sdk\build-tools\28.0.3\aapt.exe dump badging keepe-handyman-on-demand_1.1.8.apk
package: name='com.keepe.keepe' versionCode='338' versionName='1.1.8'
sdkVersion:'19'
targetSdkVersion:'27'
uses-permission: name='android.permission.INTERNET'
uses-permission: name='android.permission.ACCESS_COARSE_LOCATION'
uses-permission: name='android.permission.ACCESS_FINE_LOCATION'
uses-permission: name='android.permission.WRITE_EXTERNAL_STORAGE'
uses-permission: name='android.permission.VIBRATE'
uses-permission: name='android.permission.READ_CONTACTS'
uses-permission: name='android.permission.WRITE_CONTACTS'
uses-permission: name='android.permission.GET_ACCOUNTS'
uses-permission: name='android.permission.RECORD_AUDIO'
```

Figure 13. A snippet of aapt command output running against keepe-handyman-on-demand_1.1.8.apk

8. Findings

The research tool detects six of the fifty-nine Android packages to contain vulnerable JavaScript libraries. Figure 14 shows the vulnerable Android packages organized into application categories. Four of the six vulnerable Android packages fall in the generic "Apps" application category.

Application Category	Number of Android packages with vulnerable JavaScript libraries
Apps, Maps & Navigation	1
Apps, Productivity	1
Apps, Education	1
Apps, Tools	1
Business	1
Finance	1

Figure 14. Application category of Android packages with detected vulnerable JavaScript libraries

8.1. “assets” versus “res” directory in the Android package file structure

The research tool located vulnerable JavaScript libraries in the “assets” directory of identified Android packages. Figure 15 shows the location of the vulnerable JavaScript libraries in the six identified Android packages.

Android package	Location of vulnerable JavaScript libraries
apache-cordova-ejemplo-gmaps-ua_1.1.0.apk	assets/www/scripts/jquery.mobile-1.4.5.min.js
cordova-build-generator-app_0.1.3.apk	assets/www/lib/jquery/jquery-2.1.4.js
learn-android-code-play-ios-windows-hybrid-app_2.0.apk	assets/www/js/jquery-2.2.0.min.js
cuphead-mobile_0.6.1.apk	assets/www/jquery-2.1.1.min.js
insightly-crm_3.28.3.apk	assets/redactor/jquery-3.4.1.min.js
e-trade-invest-trade-save_8.0.1.1443.apk	assets/libs/angular/angular-1.4.3.min.js

Figure 15. Location of vulnerable JavaScript libraries in the identified Android packages

Original files and directories from the "assets" directory are directly accessible. Files and directories are not directly accessible from the "res" directory. Resources can only be read from the "res" directory with a valid resource ID ("Android App resources overview", 2020). Since valid resource IDs are attached to resources in the "res" directory, there are compile-time checks as opposed to resources in the "assets" directory, which are only evaluated during application runtime.

8.2. jQuery and AngularJS JavaScript vulnerabilities

The research tool identified jQuery and AngularJS JavaScript vulnerabilities in the six identified Android packages. Figure 16 breaks down the identified vulnerable JavaScript libraries by version and CVE reference.

Android package	JavaScript Library	Version	CVE Reference
apache-cordova-ejemplo-gmaps-ua_1.1.0.apk	jQuery Mobile	1.4.5	None. (Vulnerable to XSS attack)
cordova-build-generator-app_0.1.3.apk	jQuery	2.1.4	CVE-2015-9251 (Vulnerable to XSS attack)
learn-android-code-play-ios-windows-hybrid-app_2.0.apk	jQuery	2.2.0	CVE-2015-9251 (Vulnerable to XSS attack)
cuphead-mobile_0.6.1.apk	jQuery	2.1.1	CVE-2015-9251 (Vulnerable to XSS attack)
insightly-crm_3.28.3.apk	jQuery	3.4.1	CVE-2020-11022 (Vulnerable to XSS attack)
e-trade-invest-trade-save_8.0.1.1443.apk	AngularJS	1.4.3	CVE-2020-7676 (Vulnerable to XSS attack)

Figure 16. Breakdown of identified vulnerable JavaScript libraries by version and CVE reference

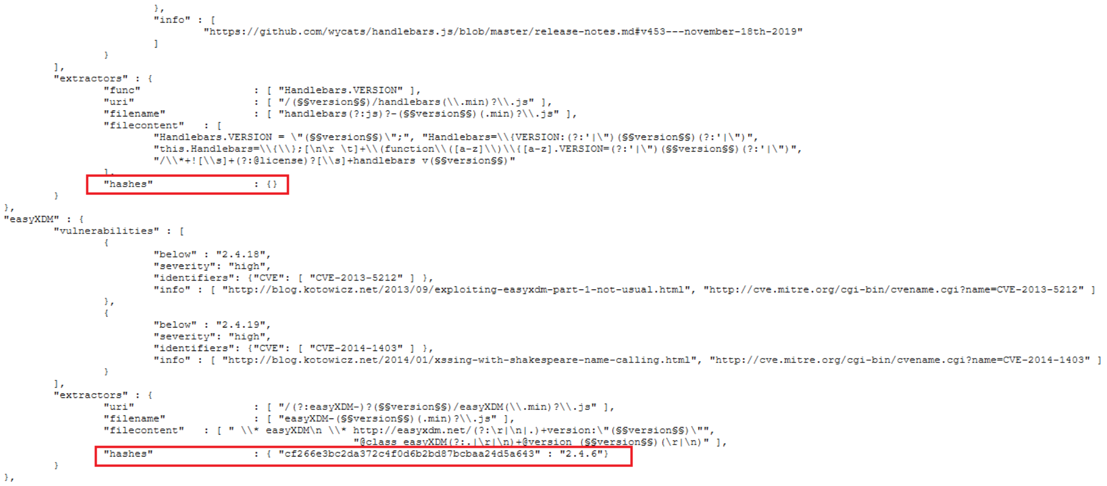
One identified Android package contains a vulnerable version of the AngularJS JavaScript library. Five of the six identified Android packages include vulnerable versions of the JQuery JavaScript library. This observation concurs with the state of JavaScript frameworks security report of 2019 published by Snyk, which notes the continued use of JQuery libraries in most web applications, especially versions below 3.4.0 ("The JavaScript frameworks security report", 12, 2019).

The vulnerability pertaining to CVE-2015-9251 impacts three of the identified Android packages. CVE-2015-9251 refers to jQuery vulnerability in versions of the library below 3.0.0. The vulnerability can be exploited by Cross-Site Scripting (XSS) attacks ("NIST CVE-2015-9251 Reference", 2020). The vulnerability pertaining to CVE-2020-11022 impacts one of the identified Android packages. CVE-2020-11022 refers to jQuery vulnerability in the library versions greater than or equal to 1.2 and below 3.5.0. The vulnerability can be exploited by executing untrusted code ("NIST CVE-2020-11022 Reference", 2020). This is a common vector for XSS attacks. The vulnerability pertaining to CVE-2020-7676 impacts one of the identified Android packages. CVE-2020-7676 refers to AngularJS vulnerability in versions of the library before 1.8.0. XSS attacks can exploit the vulnerability by turning the sanitized code into un-sanitized code using regex-based input HTML replacement ("NIST CVE-2020-7676 Reference", 2020). The vulnerability reported for JQuery Mobile JavaScript library version 1.4.5 pertaining to the apache-cordova-ejemplo-gmaps-ua_1.1.0.apk Android package does not have a corresponding CVE reference. The reporter noted that the version of the library is vulnerable to XSS attack when it fetches an unvalidated URL and manipulates the Document Object Model (DOM) of the page ("Unpatched (0day) jQuery Mobile XSS", 2017).

All six Android packages identified by the research tool are vulnerable to Cross-Site Scripting (XSS) attacks. An XSS attack is a typical client-side injection technique. This observation in this research confirms the OWASP 2014 top 10 mobile risks findings on client-side injection ("OWASP Top 10 Mobile Risks 2014", 2020). The OWASP proposed remediation includes disabling JavaScript and Plugin support for WebView in the Android platform.

8.3. File hash verification to identify vulnerable JavaScript libraries

The checksum hash of unmodified files is a reliable reference to compare against a vulnerability database. However, Lauinger, Chaabane, Arshad, Robertson, Wilson, and Kirda (2017) observed in their research that customized versions of JavaScript libraries are often deployed in web applications ("Analyzing the Use of Outdated JavaScript Libraries on the Web", 2017). This practice impacts the reliability of using a hash to match JavaScript libraries against a vulnerability database. Vulnerability database maintainers will need to compute and maintain file checksum hash values using multiple algorithms such as MD5 ("The MD5 Message-Digest Algorithm", 1992) or SHA ("US Secure Hash Algorithm 1", 2001). Currently, the Retire.js team considers the `hashes` property as an optional value ("Retire.js repository README", 2020) to be updated for a given vulnerable version of the JavaScript library in the Retire.js vulnerability database. Figure 18 lists a snippet of the Retire.js vulnerability database where the hash value is missing for `handlebars` JavaScript library but present for `easyXDM` JavaScript library.



```
            },
            "info" : [
                "https://github.com/wycats/handlebars.js/blob/master/release-notes.md#v453---november-18th-2019"
            ]
        }
    ],
    "extractors" : {
        "func"                  : [ "Handlebars.VERSION" ],
        "uri"                   : [ "/(§§version§§)/handlebars(\\.min)?\\.js" ],
        "filename"              : [ "handlebars(?:js)?-(§§version§§)(.min)?\\.js" ],
        "filecontent"   : [
            "Handlebars.VERSION = \"(§§version§§)\";", "Handlebars=\\{VERSION:(?:'|\")(§§version§§)(?:'|\")",
            "this.Handlebars=\\{\\};[\n\r \t]+\\(function\\([a-z]\\)\\{[a-z].VERSION=(?:'|\")(§§version§§)(?:'|\")",
            "/\\*+![\\s]+(?:@license)?[\\s]+handlebars v(§§version§§)"
        ],
        "hashes"                : {}
    }
},
"easyXDM" : {
    "vulnerabilities" : [
        {
            "below" : "2.4.18",
            "severity": "high",
            "identifiers": {"CVE": [ "CVE-2013-5212" ] },
            "info" : [ "http://blog.kotowicz.net/2013/09/exploiting-easyxdm-part-1-not-usual.html", "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5212" ]
        },
        {
            "below" : "2.4.19",
            "severity": "high",
            "identifiers": {"CVE": [ "CVE-2014-1403" ] },
            "info" : [ "http://blog.kotowicz.net/2014/01/xssing-with-shakespeare-name-calling.html", "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1403" ]
        }
    ],
    "extractors" : {
        "uri"                   : [ "/(?:easyXDM-)?(§§version§§)/easyXDM(\\.min)?\\.js" ],
        "filename"              : [ "easyXDM-(§§version§§)(.min)?\\.js" ],
        "filecontent"   : [ " \\* easyXDM\n \\* http://easyxdm.net/(?:\r|\n|.)+version:\"(§§version§§)\"",
                                  "@class easyXDM(?:.|\r|\n)+@version (§§version§§)(\r|\n)" ],
        "hashes"                : { "cf266e3bc2da372c4f0d6b2bd87bcbaa24d5a643" : "2.4.6"}
    }
},
```

Figure 18. Missing hash values in Retire.js vulnerability database

Source: Retire.js list of JavaScript libraries with known vulnerabilities in JSON format. (2020).

9. Recommendations for Future Research

The research tool developed is a first step in auditing JavaScript libraries in Android packages. A few improvements are suggested below.

9.1. Integration with other audit tools

The research tool, in its current state, is a proof of concept to audit vulnerable versions of JavaScript libraries in Android packages. The mobile application ecosystem has a comparatively broader scope. Robust audit tools are used to provide an in-depth analysis of mobile applications' state of security built for varied mobile platforms. Mobile Security Framework (MobSF) is one such tool that performs malware analysis, and static and dynamic analysis of mobile application binary files ("Mobile Security Framework", 2020). MobSF scans and lists JavaScript files included in mobile application binary files. The integration of the research tool with MobSF could enable auditors to verify vulnerabilities in the JavaScript libraries included with the mobile application binary files.

9.2. Integration with other vulnerability databases

The Node Package Manager (NPM) is a popular package manager and registry for JavaScript libraries ("npm", 2020). It is the default package manager for Node.js. Node.js is a JavaScript runtime environment used to build web applications in JavaScript ("Node.js", 2020). The popularity of NPM and Node.js has resulted in its use for JavaScript coding and integration with JavaScript libraries to build web and mobile applications. The Cordova and Ionic hybrid mobile application frameworks extensively use NPM ("Apache Cordova Overview", 2018). Retire.js includes an NPM vulnerability database in JSON format ("Retire.js list of NPM libraries with known vulnerabilities", 2020). The research tool in its current state does not check the Retire.js NPM vulnerability repository for vulnerable versions of JavaScript libraries. Enhancement of the research tool to include checks against the Retire.js NPM list is recommended.

("Snyk", 2020) and ("VULDB", 2020) have their respective vulnerability databases to track JavaScript libraries' issues. Integration of research tool with VULDB and Snyk vulnerability database could aid in correlation and resolution of vulnerability tracking discrepancies such as the one reported for Retire.js ("Retire.js CVE severity mismatch issue# 332", 2020).

10. Conclusion

It is essential that vulnerabilities in mobile applications are identified as quickly as possible and then addressed. JavaScript libraries are used to build web pages for mobile applications for the Android system. JavaScript libraries have to be patched against vulnerabilities. The tool covered in this paper will identify vulnerable JavaScript libraries used in mobile applications for the Android system so that they can be patched against the reported vulnerabilities. Integrating such a tool with the software development life cycle will improve mobile application security and quality.

References

(August 12 2020). Retire.js. Detect use of versions of JavaScript libraries with known vulnerabilities. Retrieved from https://retirejs.github.io/retire.js/

(August 12 2020). Retire.js list of JavaScript libraries with known vulnerabilities in JSON format. Retrieved from https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/jsrepository.json

(August 12 2020). Retire.js repository README. Retrieved from https://github.com/RetireJS/retire.js/tree/master/repository

Arteau, Philippe (July 15 2020). Retire.js Burp extender plugin. Retrieved from https://github.com/h3xstream/burp-retire-js

(April 28 2020). Grunt task for retire.js. Retrieved from https://github.com/RetireJS/grunt-retire

(August 12 2020). Retire.js list of NPM libraries with known vulnerabilities in JSON format. Retrieved from https://raw.githubusercontent.com/RetireJS/retire.js/master/repository/npmrepository.json

(October 2 2020). Mobile Security Framework. Retrieved from https://github.com/MobSF/Mobile-Security-Framework-MobSF

(January 22 2020). Building web apps in WebView. Retrieved from https://developer.android.com/guide/webapps/webview

(October 6 2020). Guide to Web-based content in Android. Retrieved from https://developer.android.com/guide/webapps

(September 30 2020). Android WebKit Reference Documentation. Retrieved from https://developer.android.com/reference/android/webkit/JavascriptInterface

(October 17 2018). Apache Cordova Overview. Retrieved from https://cordova.apache.org/docs/en/latest/guide/overview/

(April 11 2018). Apache Cordova and WebView. Retrieved from https://cordova.apache.org/docs/en/latest/guide/hybrid/webviews/index.html

(March 17 2016). Apache Cordova-enabled WebView for Android. Retrieved from https://cordova.apache.org/docs/en/latest/guide/platforms/android/webview.html

Hybrid App Development. Retrieved from https://ionicframework.com/resources/articles/what-is-hybrid-app-development

(May 6 2020). Xamarin.Forms WebView. Retrieved from https://docs.microsoft.com/en-us/xamarin/xamarin-forms/user-interface/webview

(2020). Xamarin.Forms. An open-source framework for building iOS, Android, and Windows apps. Retrieved from https://dotnet.microsoft.com/apps/xamarin/xamarin-forms

(2020). Xamarin. An app platform for building Android and iOS apps with .NET and C#. Retrieved https://dotnet.microsoft.com/apps/xamarin

(February 18 2020). Top 10 Mobile Risks 2014 - M7: Client Side Injection. Retrieved from https://owasp.org/www-project-mobile-top-10/2014-risks/m7-client-side-injection

(June 2020). OWASP Third Party JavaScript Management Cheat Sheet. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Third_Party_Javascript_Management_Cheat_Sheet.html

(February 18 2020). Top 10 Mobile Risks 2016 - M7: Poor Code Quality. Retrieved from https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality

(December 27 2019). Android Application Fundamentals. Retrieved from https://developer.android.com/guide/components/fundamentals

(August 25 2020). Analyze your build with APK Analyzer. Retrieved from https://developer.android.com/studio/build/apk-analyzer

(2019). The state of JavaScript frameworks security report 2019. Retrieved from https://snyk.io/wp-content/uploads/snyk-javascript_report_2019.pdf

Tal, Liran. (May 16 2019). Scoring security vulnerabilities 101: Introducing CVSS for CVEs. Retrieved from https://snyk.io/blog/scoring-security-vulnerabilities-101-introducing-cvss-for-cve/

(2020). Snyk. Retrieved from https://snyk.io/

(2020). VULDB. Retrieved from https://vuldb.com/

(2020). VULDB vulnerability database for JavaScript libraries. Retrieved from https://vuldb.com/?type.javascript_library

(2020). Snyk vulnerability database. Retrieved from https://snyk.io/vuln

(2020). Package java.util.zip. Retrieved from https://docs.oracle.com/javase/8/docs/api/java/util/zip/package-summary.html

(2016) PhoneGap Hockey Community App Showcase. Retrieved from https://phonegap.com/app/hockey-community/

(September 4 2020). Hockey Community Android App. Retrieved from https://play.google.com/store/apps/details?id=com.hockeycommunity.hc_app

(May 22 2020). Retire.js Burp extender plugin core library. Retrieved from https://github.com/h3xstream/burp-retire-js/tree/master/retirejs-core

(2020). Google Play Store. Retrieved from https://play.google.com/store/apps/

(2020). APKCombo - APK Store. Retrieved from https://apkcombo.com/

(2020). apkmonk - one stop for all android apps. Retrieved from https://www.apkmonk.com/

(2020). Ionic Marketplace. Retrieved from https://market.ionicframework.com/

Lauinger, T., Chaabane A., Arshad S., Robertson W., Wilson C., Kirda Engin. (September 2017). Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web. Retrieved from https://arxiv.org/pdf/1811.00918.pdf

(2020). Java MessageDigest API. Retrieved from https://docs.oracle.com/javase/8/docs/api/java/security/MessageDigest.html

Rivest, R. (April 1992). The MD5 Message-Digest Algorithm. Retrieved from https://tools.ietf.org/html/rfc1321

Jones, P. (September 2001). US Secure Hash Algorithm 1 (SHA1). Retrieved from https://tools.ietf.org/html/rfc3174

(2020). npm - JavaScript package manager. Retrieved from https://www.npmjs.com/package/npm

(2020). Node.js. Retrieved from https://nodejs.org/en/

(2020). Android AAPT2 Command Line Tool. Retrieved from https://developer.android.com/studio/command-line/aapt2.

(2020). Android App resources overview. Retrieved from https://developer.android.com/guide/topics/resources/providing-resources

(2020). Add app resources. Retrieved from https://developer.android.com/studio/write/add-resources

(August 9 2020). Assets or Resource Raw folder of Android? Retrieved from https://medium.com/mobile-app-development-publication/assets-or-resource-raw-folder-of-android-5bdc042570e0

(July 14 2020). NIST CVE-2015-9251 Reference. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2015-9251

(September 25 2020). NIST CVE-2020-11022 Reference. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2020-11022

(October 8 2020). NIST CVE-2020-7676 Reference. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2020-7676

(February 8 2017). Unpatched (0day) jQuery Mobile XSS. Retrieved from http://sirdarckcat.blogspot.no/2017/02/unpatched-0day-jquery-mobile-xss.html

(2020). National Vulnerability Database. Retrieved from https://nvd.nist.gov/

(2020). Research Tool GitHub Repository. Retrieved from https://github.com/thealmostrealmccoy123/apk-js-lib-vuln-scan-test

Appendix

List of scanned Android packages

Android APK Name: com.geico.mobile.apk Source: https://play.google.com/store/apps/details?id=com.geico.mobile&hl=en_US&gl=US - Package Name: com.geico.mobile Version Downloaded: 5.5.0 Category: Finance Title: "GEICO Mobile - Car Insurance"
Android APK Name: com.meetalbert.apk Source: https://play.google.com/store/apps/details?id=com.meetalbert&hl=en_US&gl=US Package Name: com.meetalbert Version Downloaded: 2.4.3 Category: Finance Title: "Albert: Budget. Save. Invest"
Android APK Name: com.robinhood.android.apk Source: https://play.google.com/store/apps/details?id=com.robinhood.android&hl=en&gl=US Package Name: com.robinhood.android Version Downloaded: 4.16.1 Category: Finance Title: "Robinhood - Investment & Trading, Commission-free"
Android APK Name: e-trade-invest-trade-save_8.0.1.1443.apk Source: https://play.google.com/store/apps/details?id=com.etrade.mobilepro.activity&hl=en&gl=US Package Name: com.etrade.mobilepro.activity Version Downloaded: 8.0.1.1443 Category: Finance Title: "E*TRADE: Invest. Trade. Save."
Android APK Name: google-pay-pay-with-your-phone-and-send-cash_2.111.306893647.apk Source: https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en&gl=US Package Name: com.google.android.apps.walletnfcrel Version Downloaded: 2.111.306893647 Category: Finance Title: "Google Pay: Pay with your phone and send cash"
Android APK Name: irs2go_5.4.5.1.apk Source: https://play.google.com/store/apps/details?id=gov.irs&hl=en&gl=US Package Name: gov.irs Version Downloaded: 5.4.5.1 Category: Finance Title: "IRS2Go"

Android APK Name: td-ameritrade-mobile_4.7.1.apk Source: https://play.google.com/store/apps/details?id=com.tdameritrade.mobile3&hl=en&gl=US Package Name: com.tdameritrade.mobile3 Version Downloaded: 4.7.1 Category: Finance Title: "TD Ameritrade Mobile"
Android APK Name: apache-cordova-browser_1.0.0.apk Source: https://apkcombo.com/apache-cordova-browser/com.zib.apache.cordova.browser/ Package Name: com.zib.apache.cordova.browser Version Downloaded: 1.0.0 Category: Apps, Communication Title: "Apache Cordova Browser"
Android APK Name: com.localeur.release1.apk Source: https://www.apkmonk.com/app/com.localeur.release1/ Package Name: com.localeur.release1 Version Downloaded: 5.1.1 Category: Free Travel & Local App Title: "Localeur"
Android APK Name: gradepro-for-gradespeed_1.6.8.apk Source: https://play.google.com/store/apps/details?id=com.sleekerappstudios.gradeproforgradespeed Package Name: com.sleekerappstudios.gradeproforgradespeed Version Downloaded: 1.6.8 Category: Education Title: "GradePro for GradeSpeed"
Android APK Name: gudog-dog-sitters_4.3.1.apk Source: https://play.google.com/store/apps/details?id=com.gudog.app Package Name: com.gudog.app Version Downloaded: 4.3.1 Category: Travel & Local Title: "Gudog - Dog Sitting"
Android APK Name: sworkitapp.sworkit.com.apk Source: https://play.google.com/store/apps/details?id=sworkitapp.sworkit.com Package Name: sworkitapp.sworkit.com Version Downloaded: 10.5.0 Category: Health & Fitness Title: "Sworkit Fitness – Workouts & Exercise Plans App"
Android APK Name: clever-baby-free-log-track_1.7.0.apk Source: https://play.google.com/store/apps/details?id=com.mycleverbaby.cleverbaby&hl=en Package Name: com.mycleverbaby.cleverbaby Version Downloaded: 1.7.0 Category: Parenting Title: "Clever Baby - Free Log & Track"

Android APK Name: tripcase-–-travel-organizer_4.15.5.apk Source: https://play.google.com/store/apps/details?id=com.sabre.tripcase.android Package Name: com.sabre.tripcase.android Version Downloaded: 4.15.5 Category: Travel & Local Title: "TripCase – Travel Organizer"
Android APK Name: com.hockeycommunity.hc_app.apk Source: https://play.google.com/store/apps/details?id=com.hockeycommunity.hc_app Package Name: com.hockeycommunity.hc_app Version Downloaded: 6.1.0 Category: Sports Title: "Hockey Community"
Android APK Name: nativescript-plugins_2.1.0.apk Source: https://apkcombo.com/nativescript-plugins/org.nativescript.pluginshowcase/ Package Name: org.nativescript.pluginshowcase Version Downloaded: 2.1.0 Category: Apps, Libraries & Demo Title: "NativeScript Plugins"
Android APK Name: learn-cordova-video-tutorials_1.0.apk Source: https://apkcombo.com/learn-cordova-video-tutorials/com.sikapps.cordova/ Package Name: com.sikapps.cordova Version Downloaded: 1.0 Category: Apps, Education Title: "Learn Cordova : Video Tutorials"
Android APK Name: phonegap-developer_1.8.4.apk Source: https://apkcombo.com/phonegap-developer/com.adobe.phonegap.app/ Package Name: com.adobe.phonegap.app Version Downloaded: 1.8.4 Category: Apps, Productivity Title: "PhoneGap Developer"
Android APK Name: apache-cordova-ejemplo-gmaps-ua_1.1.0.apk Source: https://apkcombo.com/apache-cordova-ejemplo-gmaps-ua/com.dism.p1/ Package Name: com.dism.p1 Version Downloaded: 1.1.0 Category: Apps, Maps & Navigation Title: "Apache Cordova Ejemplo GMaps UA"
Android APK Name: cordova-build-generator-app_0.1.3.apk Source: https://apkcombo.com/cordova-build-generator-app/in.eternalsayed.cbg.app/ Package Name: in.eternalsayed.cbg.app Version Downloaded: 0.1.3 Category: Apps, Productivity

Title: "Cordova Build Generator App"
Android APK Name: learn-phonegap-video-tutorials_1.0.apk Source: https://apkcombo.com/learn-phonegap-video-tutorials/com.sikapps.phonegap/ Package Name: com.sikapps.phonegap Version Downloaded: 1.0 Category: Apps, Education Title: "Learn PhoneGap : Video Tutorials"
Android APK Name: cordova-ionic-vr-plugin-sample_2.0.0.apk Source: https://apkcombo.com/cordova-ionic-vr-plugin-sample/it.tangodev.cordovapluginvrviewsampleapp/ Package Name: it.tangodev.cordovapluginvrviewsampleapp Version Downloaded: 2.0.0 Category: Apps, Libraries & Demo Title: "Cordova ionic VR plugin sample"
Android APK Name: keepe-handyman-on-demand_1.1.8.apk Source: https://play.google.com/store/apps/details?id=com.keepe.keepe&hl=en_US Package Name: com.keepe.keepe Version Downloaded: 1.1.8 Category: Lifestyle Title: "Keepe - Handyman on Demand"
Android APK Name: com.healthtap.userhtexpress.apk Source: https://play.google.com/store/apps/details?id=com.healthtap.userhtexpress Package Name: com.healthtap.userhtexpress Version Downloaded: 7.23.1 Category: Medical Title: "HealthTap — 24/7 Telemedicine"
Android APK Name: cordova-project-app_1.0.0.apk Source: https://apkcombo.com/cordova-project-app/com.hong.cordovaproject1/ Package Name: com.hong.cordovaproject1 Version Downloaded: 1.0.0 Category: Apps, Education Title: "cordova Project App"
Android APK Name: learn-android-code-play-ios-windows-hybrid-app_2.0.apk Source: https://apkcombo.com/learn-android-code-play-ios-windows-hybrid-app/cordova.code.play/ Package Name: cordova.code.play Version Downloaded: 2.0 Category: Apps, Education Title: "Learn Android Code Play iOS, Windows, hybrid app"
Android APK Name: myo-cordova-demo_0.0.2.apk Source: https://apkcombo.com/myo-cordova-demo/com.tribalyte.app.myoplugindemo/ Package Name: com.tribalyte.app.myoplugindemo Version Downloaded: 0.0.2

Category: Apps, Libraries & Demo Title: "Myo Cordova Demo"
Android APK Name: demo-app-cordova-vue-hybrid-app_1.0.0.apk Source: https://apkcombo.com/demo-app-cordova-vue-hybrid-app/czkiam.myapp/ Package Name: czkiam.myapp Version Downloaded: 1.0.0 Category: Apps, Education Title: "Demo App (Cordova-Vue Hybrid App)"
Android APK Name: learn-cordova_1.5.apk Source: https://apkcombo.com/learn-cordova/in.softecks.cordova/ Package Name: in.softecks.cordova Version Downloaded: 1.5 Category: Apps, Education Title: "Learn - Cordova"
Android APK Name: untappd-discover-beer_3.5.3.apk Source: https://play.google.com/store/apps/details?id=com.untappdllc.app Package Name: com.untappdllc.app Version Downloaded: 3.5.3 Category: Food & Drink Title: "Untappd - Discover Beer"
Android APK Name: amtrak_4.1.1.apk Source: https://play.google.com/store/apps/details?id=com.amtrak.rider&hl=en_US Package Name: com.amtrak.rider Version Downloaded: 4.1.1 Category: Travel & Local Title: "Amtrak"
Android APK Name: com.ferdousulhaque.barcodempos_0.0.1.apk Source: https://market.ionicframework.com/starters/barcode-mpos Package Name: com.ferdousulhaque.barcodempos Version Downloaded: 0.0.1 Category: Starters Title: "Barcode mPOS"
Android APK Name: com.marketwatch.apk Source: https://play.google.com/store/apps/details?id=com.marketwatch&hl=en Package Name: com.marketwatch Version Downloaded: 6.4.4 Category: Finance Title: "MarketWatch"
Android APK Name: ionic1-linkedin-auth.apk Source: https://market.ionicframework.com/starters/oauth-linkedin-starter Package Name: com.ionicframework.ionic1linkedinauth499882

Version Downloaded: 0.0.1 Category: Starters Title: "Linkedin Auth Starter"
Android APK Name: joule-sous-vide-by-chefsteps_2.73.7.apk Source: https://play.google.com/store/apps/details?id=com.chefsteps.circulator&hl=en Package Name: com.chefsteps.circulator Version Downloaded: 2.73.7 Category: Food & Drink Title: "Joule: Sous Vide by ChefSteps"
Android APK Name: justwatch-the-streaming-guide-for-movies-shows_2.7.17.apk Source: https://play.google.com/store/apps/details?id=com.justwatch.justwatch&hl=en Package Name: com.justwatch.justwatch Version Downloaded: 2.7.17 Category: Entertainment Title: "JustWatch - The Streaming Guide for Movies & Shows"
Android APK Name: nmaahc-mobile-stories_2.1.3.apk Source: https://play.google.com/store/apps/details?id=com.ionicframework.nmaahc708324&hl=en Package Name: com.ionicframework.nmaahc708324 Version Downloaded: 2.1.3 Category: Education Title: "NMAAHC Mobile Stories"
Android APK Name: sanvello-for-anxiety-depression-stress_8.12.0.apk Source: https://play.google.com/store/apps/details?id=com.pacificalabs.pacifica&hl=en Package Name: com.pacificalabs.pacifica Version Downloaded: 8.12.0 Category: Medical Title: "Sanvello for Anxiety, Depression & Stress"
Android APK Name: mcdonald-s-mobil-yemek-siparişi-ver_7.6.0.05.apk Source: https://play.google.com/store/apps/details?id=com.clockwork.mcdonalds Package Name: com.clockwork.mcdonalds Version Downloaded: 7.6.0.05 Category: Food & Drink Title: "McDonald's - Mobil Yemek Siparişi Ver (McDonald's Turkey App)"
Android APK Name: parallyzed_2.0.8.apk Source: https://play.google.com/store/apps/details?id=com.doublecoconut.parallyzed Package Name: com.doublecoconut.parallyzed Version Downloaded: 2.0.8 Category: Arcade Title: "Parallyzed"
Android APK Name: pako-car-chase-simulator_1.0.7.apk Source: https://play.google.com/store/apps/details?id=com.treemengames.pako

Package Name: com.treemengames.pako Version Downloaded: 1.0.7 Category: Racing Title: "PAKO - Car Chase Simulator"
Android APK Name: crossy-road_4.3.21.apk Source: https://apkcombo.com/crossy-road/com.yodo1.crossyroad/download/apk Package Name: com.yodo1.crossyroad Version Downloaded: 4.3.21 Category: Games, Action Title: "Crossy Road"
Android APK Name: cuphead-mobile_0.6.1.apk Source: https://apkcombo.com/cuphead-mobile/com.skailogames.cupheadmobile/ Package Name: com.skailogames.cupheadmobile Version Downloaded: 0.6.1 Category: Apps, Tools Title: "Cuphead Mobile"
Android APK Name: shadowgun-legends-fps-and-pvp-multiplayer-games_1.0.5.apk Source: https://apkcombo.com/shadowgun-legends-fps-and-pvp-multiplayer-games/com.madfingergames.legends/ Package Name: com.madfingergames.legends Version Downloaded: 1.0.5 Category: Games, Action Title: "SHADOWGUN LEGENDS - FPS and PvP Multiplayer games"
Android APK Name: hearthstone_18.0.56359.apk Source: https://apkcombo.com/hearthstone/com.blizzard.wtcg.hearthstone/ Package Name: com.blizzard.wtcg.hearthstone Version Downloaded: 18.0.56359 Category: Games, Card Title: "Hearthstone"
Android APK Name: mobius-final-fantasy_2.1.105.apk Source: https://apkcombo.com/mobius-final-fantasy/com.square_enix.android_googleplay.mobiusff_ne/ Package Name: com.square_enix.android_googleplay.mobiusff_ne Version Downloaded: 2.1.105 Category: Games, Role Playing Title: "MOBIUS FINAL FANTASY"
Android APK Name: alto-s-adventure_1.7.6.apk Source: https://apkcombo.com/alto-s-adventure/com.noodlecake.altosadventure/ Package Name: com.noodlecake.altosadventure Version Downloaded: 1.7.6 Category: Games, Action Title: "Alto's Adventure"
Android APK Name: com.ChetanSurpur.Orbit.apk

Source: https://play.google.com/store/apps/details?id=com.ChetanSurpur.Orbit Package Name: com.ChetanSurpur.Orbit Version Downloaded: 2.2.5 Category: Puzzle Title: "Orbit - Playing with Gravity"
Android APK Name: com.nekki.shadowfight3.apk Source: https://play.google.com/store/apps/details?id=com.nekki.shadowfight3 Package Name: com.nekki.shadowfight3 Version Downloaded: 1.21.2 Category: Role Playing Title: "Shadow Fight 3"
Android APK Name: alaska-airlines-travel_3.39.apk Source: https://play.google.com/store/apps/details?id=com.alaskaairlines.android Package Name: com.alaskaairlines.android Version Downloaded: 3.39 Category: Travel & Local Title: "Alaska Airlines - Travel"
Android APK Name: ca-mobile_3.22.6976.apk Source: https://play.google.com/store/apps/details?id=ca.mobile.explorer Package Name: ca.mobile.explorer Version Downloaded: 3.22.6976 Category: Finance Title: "CA Mobile"
Android APK Name: captio.ongest.com.apk Source: https://play.google.com/store/apps/details?id=captio.ongest.com&hl=en Package Name: captio.ongest.com Version Downloaded: 4.2.7.1 Category: Finance Title: "Captio - Expense Reports"
Android APK Name: cloningbench_1.2.0.apk Source: https://play.google.com/store/apps/details?id=com.thermofisher.mobile.android.cloningbench&hl=en Package Name: com.thermofisher.mobile.android.cloningbench Version Downloaded: 1.2.0 Category: Books & Reference Title: "CloningBench"
Android APK Name: freshdirect_7.7.apk Source: https://play.google.com/store/apps/details?id=com.freshdirect.android Package Name: com.freshdirect.android Version Downloaded: 7.7 Category: Shopping Title: "FreshDirect"

Android APK Name: instrument-connect_4.5.6.apk Source: https://play.google.com/store/apps/details?id=com.thermofisher.icma_android&hl=en Package Name: com.thermofisher.icma_android Version Downloaded: 4.5.6 Category: Productivity Title: "Instrument Connect"
Android APK Name: radhalo_1.1.13.apk Source: https://play.google.com/store/apps/details?id=com.thermofisher.mobile.android.btservicemodule.app&hl=en Package Name: com.thermofisher.mobile.android.btservicemodule.app Version Downloaded: 1.1.13 Category: Tools Title: "RadHalo"
Android APK Name: storyo-smart-video-memories_1.7.2.apk Source: https://play.google.com/store/apps/details?id=com.StoryMatik.Storyo Package Name: com.StoryMatik.Storyo Version Downloaded: 1.7.2 Category: Photography Title: "Storyo - Smart Video Memories"
Android APK Name: world-bank-project-procurement_2.0.6.apk Source: https://play.google.com/store/apps/details?id=org.worldbank.operationsprocurement Package Name: org.worldbank.operationsprocurement Version Downloaded: 2.0.6 Category: Business Title: "World Bank Project Procurement"
Android APK Name: insightly-crm_3.28.3.apk Source: https://play.google.com/store/apps/details?id=com.insightly.droid&hl=en_US Package Name: com.insightly.droid Version Downloaded: 3.28.3 Category: Business Title: "Insightly CRM"

List of Android packages with vulnerable JavaScript Libraries

Android APK Name: apache-cordova-ejemplo-gmaps-ua_1.1.0.apk Source: https://apkcombo.com/apache-cordova-ejemplo-gmaps-ua/com.dism.p1/ Package Name: com.dism.p1 Version Downloaded: 1.1.0 Category: Apps, Maps & Navigation Title: "Apache Cordova Ejemplo GMaps UA"

Detected Vulnerable JavaScript Library: jQuery Mobile

Vulnerable Version: 1.4.5

Vulnerabity Severity: medium

CVE Reference: None

Vulnerabity Details: jQuery Mobile version 1.4.5 is vulnerable to XSS attack when it fetches unvalidated URL in the location.hash property of the web page Document Object Model (DOM) and puts it in the innerHTML property of the web page DOM.

Vulnerabity Reference[1]: http://sirdarckcat.blogspot.no/2017/02/unpatched-0day-jquery-mobile-xss.html

Vulnerabity Reference[2]: https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2013.pdf

Location Of Vulnerable JavaScript Library in Android Artifact: assets/www/scripts/jquery.mobile-1.4.5.min.js

---

Android APK Name: cordova-build-generator-app_0.1.3.apk

Source: https://apkcombo.com/cordova-build-generator-app/in.eternalsayed.cbg.app/

Package Name: in.eternalsayed.cbg.app

Version Downloaded: 0.1.3

Category: Apps, Productivity

Title: "Cordova Build Generator App"

Detected Vulnerable JavaScript Library: jQuery

Vulnerable Version: 2.1.4

Vulnerabity Severity: medium

CVE Reference: CVE-2015-9251

Vulnerabity Details: jQuery before 3.0.0 is vulnerable to Cross-Site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerabity Reference[1]: https://github.com/jquery/jquery/issues/2432

Vulnerabity Reference[2]: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Vulnerabity Reference[3]: https://nvd.nist.gov/vuln/detail/CVE-2015-9251

Vulnerabity Reference[4]: http://research.insecurelabs.org/jquery/test/

Location Of Vulnerable JavaScript Library in Android Artifact: assets/www/lib/jquery/jquery-2.1.4.js

---

Android APK Name: learn-android-code-play-ios-windows-hybrid-app_2.0.apk

Source: https://apkcombo.com/learn-android-code-play-ios-windows-hybrid-app/cordova.code.play/

Package Name: cordova.code.play

Version Downloaded: 2.0

Category: Apps, Education

Title: "Learn Android Code Play iOS, Windows, hybrid app"

Detected Vulnerable JavaScript Library: jQuery

Vulnerable Version: 2.2.0

Vulnerabity Severity: medium

CVE Reference: CVE-2015-9251

Vulnerabity Details: jQuery before 3.0.0 is vulnerable to Cross-Site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerabity Reference[1]: https://github.com/jquery/jquery/issues/2432

Vulnerabity Reference[2]: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Vulnerabity Reference[3]: https://nvd.nist.gov/vuln/detail/CVE-2015-9251

Vulnerabity Reference[4]: http://research.insecurelabs.org/jquery/test/

Location Of Vulnerable JavaScript Library in Android Artifact: assets/www/js/jquery-2.2.0.min.js

Android APK Name: cuphead-mobile_0.6.1.apk

Source: https://apkcombo.com/cuphead-mobile/com.skailogames.cupheadmobile/

Package Name: com.skailogames.cupheadmobile

Version Downloaded: 0.6.1

Category: Apps, Tools

Title: "Cuphead Mobile"

Detected Vulnerable JavaScript Library: jQuery

Vulnerable Version: 2.1.1

Vulnerabity Severity: medium

CVE Reference: CVE-2015-9251

Vulnerabity Details: jQuery before 3.0.0 is vulnerable to Cross-Site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

Vulnerabity Reference[1]: https://github.com/jquery/jquery/issues/2432

Vulnerabity Reference[2]: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Vulnerabity Reference[3]: https://nvd.nist.gov/vuln/detail/CVE-2015-9251

Vulnerabity Reference[4]: http://research.insecurelabs.org/jquery/test/

Location Of Vulnerable JavaScript Library in Android Artifact: assets/www/jquery-2.1.1.min.js

Android APK Name: insightly-crm_3.28.3.apk

Source: https://play.google.com/store/apps/details?id=com.insightly.droid&hl=en_US

Package Name: com.insightly.droid

Version Downloaded: 3.28.3

Category: Business

Title: "Insightly CRM"

Detected Vulnerable JavaScript Library: jQuery

Vulnerable Version: 3.4.1

Vulnerabity Severity: medium

CVE Reference: CVE-2020-11022

Vulnerabity Details: In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This issue is vulnerable to XSS attacks. This problem is patched in jQuery 3.5.0

Vulnerabity Reference[1]: https://nvd.nist.gov/vuln/detail/CVE-2020-11022

Vulnerabity Reference[2]: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Vulnerabity Reference[3]: https://github.com/jquery/jquery/security/advisories/GHSA-gxr4-xjj5-5px2

Vulnerabity Reference[4]: https://snyk.io/vuln/SNYK-JS-JQUERY-567880

```
Location Of Vulnerable JavaScript Library in Android Artifact: assets/redactor/jquery-3.4.1.min.js

Android APK Name: e-trade-invest-trade-save_8.0.1.1443.apk
Source: https://play.google.com/store/apps/details?id=com.etrade.mobilepro.activity&hl=en&gl=US
Package Name: com.etrade.mobilepro.activity
Version Downloaded: 8.0.1.1443
Category: Finance
Title: "E*TRADE: Invest. Trade. Save."


Detected Vulnerable JavaScript Library: AngularJS
Vulnerable Version: 1.4.3
Vulnerabity Severity: medium
CVE Reference: CVE-2020-7676
Vulnerabity Details: angular.js prior to 1.8.0 allows Cross-Site Scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one. Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code.
Vulnerabity Reference[1]: https://nvd.nist.gov/vuln/detail/CVE-2020-7676


Location Of Vulnerable JavaScript Library in Android Artifact: assets/libs/angular/angular-1.4.3.min.js
```

Sample output from running the research tool against a list of Android packages

```
Found 6 artifacts with vulnerable JavaScript Libraries...


Scanning C:\Users\arm\Documents\temp\SANS\ISE5601\research\apk\hybrid\cordova\apache-cordova-ejemplo-gmaps-ua_1.1.0.apk
Found vulnerable JavaScript Library: assets/www/scripts/jquery.mobile-1.4.5.min.js...


jsLibraryResult.detectedVersion: 1.4.5.min
jsLibraryResult.regexRequest: jquery.mobile-([0-9][0-9.a-z_\\\\-]+)(.min)?\.js
jsLibraryResult.regexResponse: null
jsLibraryResult.jsVulnerability.atOrAbove: null
jsLibraryResult.jsVulnerability.below: 100.0.0
jsLibraryResult.jsVulnerability.info[1]: http://sirdarckcat.blogspot.no/2017/02/unpatched-0day-jquery-mobile-xss.html
jsLibraryResult.jsVulnerability.severity: medium


Scanning C:\Users\arm\Documents\temp\SANS\ISE5601\research\apk\hybrid\cordova\cordova-build-generator-app_0.1.3.apk
Found vulnerable JavaScript Library: assets/www/lib/jquery/jquery-2.1.4.js...


jsLibraryResult.detectedVersion: 2.1.4
```

```
        jsLibraryResult.regexRequest: jquery-([0-9][0-9.a-z_\\\\-]+)(\.min)?\.js
        jsLibraryResult.regexResponse: null
        jsLibraryResult.jsVulnerability.atOrAbove: 1.12.3
        jsLibraryResult.jsVulnerability.below: 3.0.0-beta1
        jsLibraryResult.jsVulnerability.info[1]: https://github.com/jquery/jquery/issues/2432
        jsLibraryResult.jsVulnerability.info[2]: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
        jsLibraryResult.jsVulnerability.info[3]: https://nvd.nist.gov/vuln/detail/CVE-2015-9251
        jsLibraryResult.jsVulnerability.info[4]: http://research.insecurelabs.org/jquery/test/
        jsLibraryResult.jsVulnerability.severity: medium


        Scanning C:\Users\arm\Documents\temp\SANS\ISE5601\research\apk\hybrid\cordova\learn-android-code-play-ios-windows-
hybrid-app_2.0.apk
        Found vulnerable JavaScript Library: assets/www/js/jquery-2.2.0.min.js...


        jsLibraryResult.detectedVersion: 2.2.0.min
        jsLibraryResult.regexRequest: jquery-([0-9][0-9.a-z_\\\\-]+)(\.min)?\.js
        jsLibraryResult.regexResponse: null
        jsLibraryResult.jsVulnerability.atOrAbove: 1.12.3
        jsLibraryResult.jsVulnerability.below: 3.0.0-beta1
        jsLibraryResult.jsVulnerability.info[1]: https://github.com/jquery/jquery/issues/2432
        jsLibraryResult.jsVulnerability.info[2]: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
        jsLibraryResult.jsVulnerability.info[3]: https://nvd.nist.gov/vuln/detail/CVE-2015-9251
        jsLibraryResult.jsVulnerability.info[4]: http://research.insecurelabs.org/jquery/test/
        jsLibraryResult.jsVulnerability.severity: medium

        Scanning C:\Users\arm\Documents\temp\SANS\ISE5601\research\apk\hybrid\unity\apk\cuphead-mobile_0.6.1.apk
        Found vulnerable JavaScript Library: assets/www/jquery-2.1.1.min.js...


        jsLibraryResult.detectedVersion: 2.1.1.min
        jsLibraryResult.regexRequest: jquery-([0-9][0-9.a-z_\\\\-]+)(\.min)?\.js
        jsLibraryResult.regexResponse: null
        jsLibraryResult.jsVulnerability.atOrAbove: 1.12.3
        jsLibraryResult.jsVulnerability.below: 3.0.0-beta1
        jsLibraryResult.jsVulnerability.info[1]: https://github.com/jquery/jquery/issues/2432
        jsLibraryResult.jsVulnerability.info[2]: http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/
        jsLibraryResult.jsVulnerability.info[3]: https://nvd.nist.gov/vuln/detail/CVE-2015-9251
        jsLibraryResult.jsVulnerability.info[4]: http://research.insecurelabs.org/jquery/test/
        jsLibraryResult.jsVulnerability.severity: medium

        Scanning C:\Users\arm\Documents\temp\SANS\ISE5601\research\apk\hybrid\xamarin\apk\insightly-crm_3.28.3.apk
        Found vulnerable JavaScript Library: assets/redactor/jquery-3.4.1.min.js...
```

```
jsLibraryResult.detectedVersion: 3.4.1.min
jsLibraryResult.regexRequest: jquery-([0-9][0-9.a-z_\\\\-]+)(\.min)?\.js
jsLibraryResult.regexResponse: null
jsLibraryResult.jsVulnerability.atOrAbove: null
jsLibraryResult.jsVulnerability.below: 3.5.0
jsLibraryResult.jsVulnerability.info[1]: https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
jsLibraryResult.jsVulnerability.severity: medium

Scanning C:\Users\arm\Documents\temp\SANS\ISE5601\research\apk\others\apk\e-trade-invest-trade-save_8.0.1.1443.apk
Found vulnerable JavaScript Library: assets/libs/angular/angular-1.4.3.min.js...

jsLibraryResult.detectedVersion: 1.4.3.min
jsLibraryResult.regexRequest: angular(?:js)?-([0-9][0-9.a-z_\\\\-]+)(.min)?\.js
jsLibraryResult.regexResponse: null
jsLibraryResult.jsVulnerability.atOrAbove: null
jsLibraryResult.jsVulnerability.below: 1.8.0
jsLibraryResult.jsVulnerability.info[1]: https://nvd.nist.gov/vuln/detail/CVE-2020-7676
jsLibraryResult.jsVulnerability.severity: medium
```