



WEBSEC

• Mobile Hacking 101 – • A Cross-Platform Audit Journey



WEBSEC

¡ATENCIÓN!



Toda la información incluida en este medio es para fines educativos y profesionales, en ningún caso los organizadores de este evento, ni yo, somos responsables de cualquier mal uso de esta información.

Possible abuso de memes.....

Whoami

Cesar Calderon

Senior Security Consultant –
Websec MX

Ex-Content Developer in
Tryhackme

eJPT - eMAPT



WEBSEC



Un poco de repaso...

APK

• /Payload/

OWASP-2016		OWASP API Security Top-10 2023		Open 2016-2024
M1: Improper Platform Usage	M1: Improper Platform Usage	API1 Broken Object Level Authorization	Same	6 to M3
M2: Insecure Data Storage	M2: Inadequate Encryption Standard	API2 Broken Authentication	Updated	3 to M5
M3: Insecure Communication	M3: Insecure Communication	API3 Broken Object Property Level Authorization	Updated	9 to M7
M4: Insecure Authentication	M4: Insufficient Transport Layer Protection	API4 Unrestricted Resource Consumption	Updated	[M10]
M5: Insufficient Cryptography	M5: Insecure Cryptographic Storage	API5 Broken Function Level Authorization	Same	2 to M9
M6: Insecure Authorization	M6: Inadequate Access Control	API6 Unrestricted Access to Sensitive Business Flows	New	5 to M10
M7: Client Code Quality	M7: Insufficient Code Review	API7 Server-Side Request Forgery (SSRF)	New	
M8: Code Tampering	M8: Secure Code	API8 Security Misconfiguration	Same	
M9: Reverse Engineering	M9: Insecure Deserialization	API9 Improper Inventory Management	Updated	
M10: Extraneous Functionality	M10: Insufficient Validation	API10 Unsafe Consumption of APIs	New	

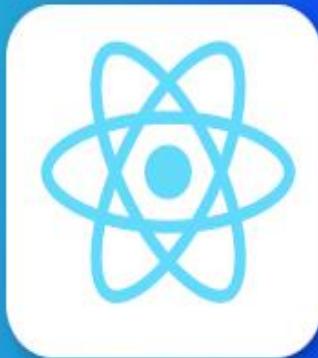
Herramientas generales

The screenshot shows the Genymotion virtual device manager. On the left, a sidebar lists various tools: Connect, Files, Apps, Network, CoreTrace, Messaging, Settings, Frida, Console, Port Forwarding, Sensors, and Snapshots. The 'Network' option is currently selected. In the center, a virtual device named 'vintage-hummin' is connected, displaying a jailbreak exploit for iOS. The screen shows a large white 'Dopamine' logo with the text 'Jailbreak' below it. To the right of the device screen, a physical iPhone X is shown with its home screen visible, displaying various app icons like Calendar, Photos, Camera, etc. A context menu is open on the iPhone screen, showing options such as 'Settings', 'Restart SpringBoard', 'Reboot Userspace', and 'Credits'. At the bottom of the Genymotion interface, there is a log window showing the URL as '/' and the Content-type as 'text/html; charset=utf-8', along with the start date and time: 'Jan 12, 55148 4:00 PM'. The Genymotion header includes links for 'Solutions', 'Use cases', 'Pricing', 'Help', and 'Blog', along with 'Contact Us', 'Trial', and 'Sign In' buttons.

Introducción



WEBSEC

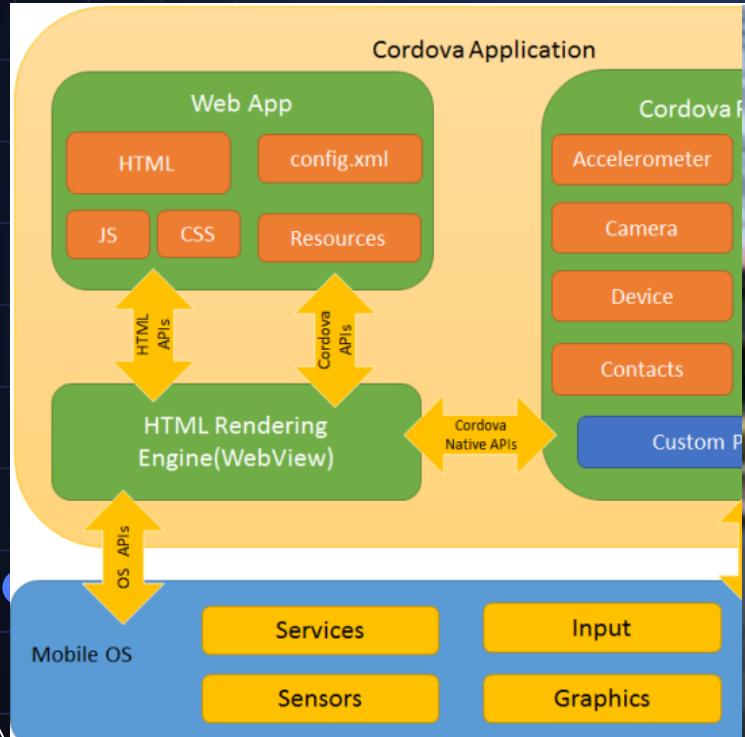




WEBSEC



Ionic/Cordova



Consideraciones de Análisis



```
urces
sets
www
└── 1234567890
    ├── plugins
    ├── cordova.js
    ├── cordova_plugins.js
    ├── index.html
    └── robots.txt
appboy-html-in-app-message-javascript-component.js
fontawesome-webfont.ttf
```

el proxy en proxydroid y colocarlo como invisible en burpsuite.

el proxy en WiFi.

, fingerprinting, funcionan adecuadamente

funcionan, esto debe identificar manualmente en los archivos .js.

ara interceptar el tráfico para esto no es necesario root, si la app tiene

implementado ssl pinning se debe tener equipo con jailbreak.

Caso #1: Implementación insegura de CryptoJS



WEBSEC





WEBSEC



Caso #2: Validaciones a Nivel de cliente

root@kali: ~/com.mobition.promerica.mobileBankingHN.Prod/assets/www

Tiempo de expiración de sesión definido en la utilidad "js/HO/User.js"

File Edit View Search Terminal Tabs Help

root@kali: ~/Mobile-Sec... x root@kali: ~/com.mobti... x root@kali: ~/com.mobti... x +

ion(){
ies:fund
},
setVali
val
L2935681
o

nox No... 1:42

Stopwatch

00:05:01.03

Su sesión ha expirado

Ok

ticati

imgflip.com

Durante el proceso de assesment se identificó



Caso #3: Implementación insegura de protección de recursos de |



```
(self["webpackC"] || []).push(["src_pages_apertura-cuentas_firma_firma_module_ts"],

/* 55736:
 *-----*/
/*! ./src/pages/apertura-cuentas/firma/firma-routing.module.ts ***!
\-----*/
/*! (( _unused_webpack_module, __webpack_exports__, __webpack_require__ ) => {

"use strict";
__webpack_require__.r(__webpack_exports__);
/* harmony export */ __webpack_require__.d(__webpack_exports__, {
/* harmony export */ "FirmaPageRoutingModule": () => /* binding */ FirmaPageRoutingModule
/* harmony export */ });
/* harmony import */ var tslib__WEBPACK_IMPORTED_MODULE_1__ = __webpack_require__(/*! tslib */ 64762);
/* harmony import */ var _angular_core__WEBPACK_IMPORTED_MODULE_2__ = __webpack_require__(/*! @angular/core */ 37716);
/* harmony import */ var _angular_router__WEBPACK_IMPORTED_MODULE_3__ = __webpack_require__(/*! @angular/router */ 39895);
/* harmony import */ var _firma_page__WEBPACK_IMPORTED_MODULE_0__ = __webpack_require__(/*! ./firma.page */ 8562);

const routes = [
  {
    path: '',
    component: _firma_page__WEBPACK_IMPORTED_MODULE_0__.FirmaPage
  }
];
let FirmaPageRoutingModule = class FirmaPageRoutingModule {
};
FirmaPageRoutingModule = (0,tslib__WEBPACK_IMPORTED_MODULE_1__.decorate)(FirmaPageRoutingModule, [
  (0,_angular_core__WEBPACK_IMPORTED_MODULE_2__.NgModule)({
    imports: [_angular_router__WEBPACK_IMPORTED_MODULE_3__.RouterModule.forChild(routes)],
    exports: [_angular_router__WEBPACK_IMPORTED_MODULE_3__.RouterModule]
  })
], FirmaPageRoutingModule);

/* */
/* 29995:
 *-----*/
/*! ./src/pages/apertura-cuentas/firma/firma.module.ts ***!
\-----*/
/*! (( _unused_webpack_module, __webpack_exports__, __webpack_require__ ) => {

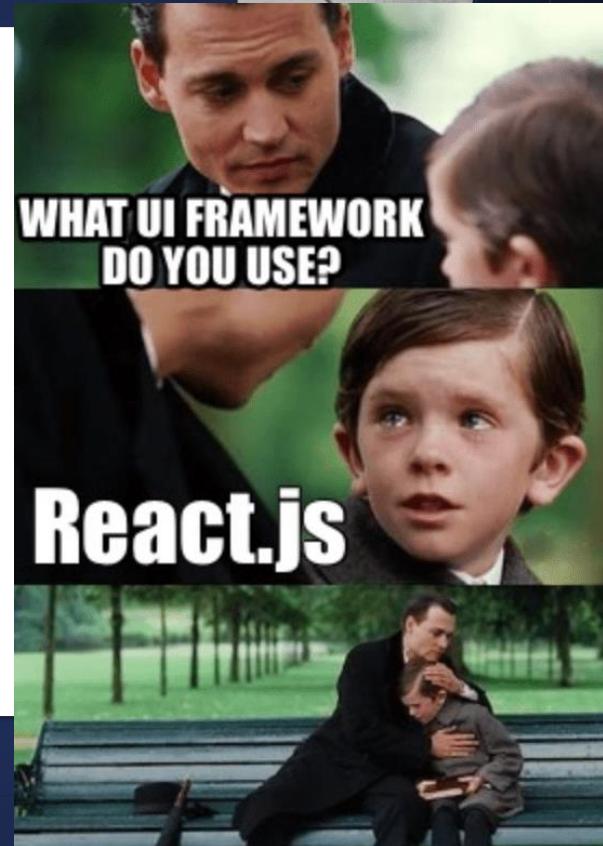
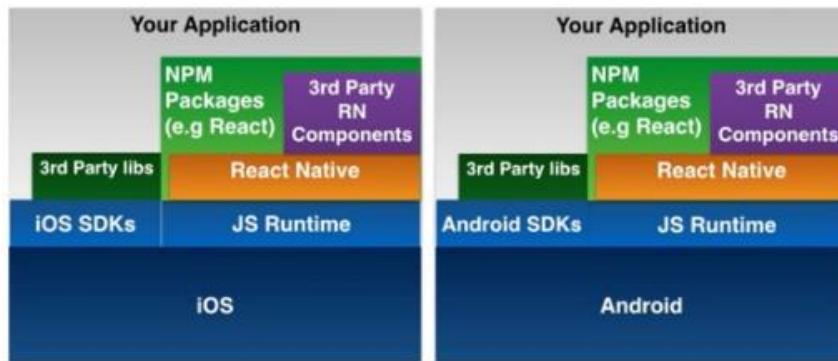
"use strict";
__webpack_require__.r(__webpack_exports__);
/* harmony export */ __webpack_require__.d(__webpack_exports__, {
/* harmony export */ "FirmaPageModule": () => /* binding */ FirmaPageModule
/* harmony export */ });
/* harmony import */ var _firma_page__WEBPACK_IMPORTED_MODULE_0__ = __webpack_require__(/*! ./firma.page */ 8562);


```

React Native



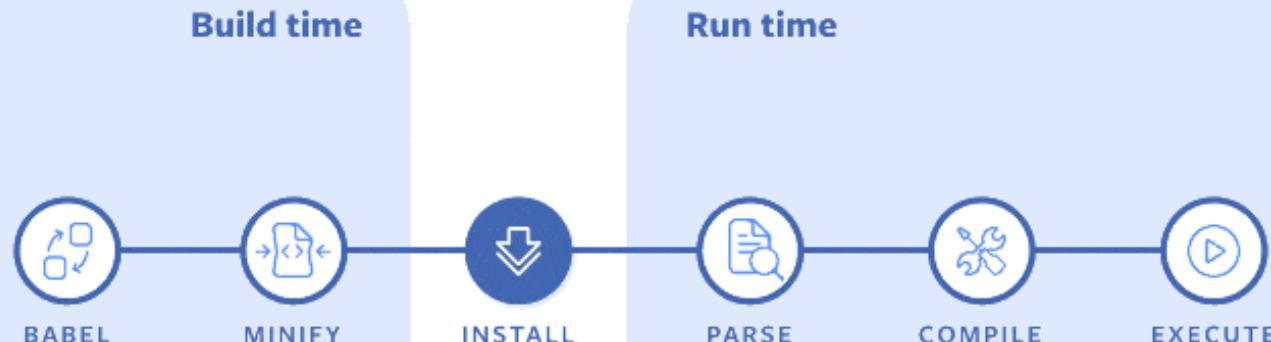
React Native App Architecture



Optimización de aplicativos con Hermes



Interpretation with conventional engine



Optimización de aplicativos con Hermes - Ejemplo



The screenshot shows a debugger interface with two main panes. The top pane displays assembly code in a highly obfuscated format, with several lines underlined in red, indicating they are currently being executed or are part of the current stack frame. The bottom pane shows variable definitions and their memory addresses. The variables include:

- u = L1((L1))
- 1 = t((d[6]))
- h = t((d[7]))
- f = r(d[8])
- p = r(d[9])
- v = r(d[10])
- S = t((d[11]))
- M = t((d[12]))
- x = t((d[13]))
- y = r(d[14])
- E = r(d[15])
- w = r(d[16])

The bottom pane also includes a search bar labeled "dialogFlow" and a status bar at the bottom right showing "18 of 21".

Disassembling and assembling the Hermes Bytecode



```
1 instruction.hasm
https://pastebin.com/182874-182906
182874 GetById          Reg8:5, Reg8:4, UInt8:2, UInt16:2795
182875 ; Oper[3]: String(2795) 'counter'
182876
182877 LoadConstUInt8    Reg8:4, UInt8:1
182878 Add               Reg8:4, Reg8:5, Reg8:4
182879 PutNewOwnById    Reg8:1, Reg8:4, UInt16:2795
182880 ; Oper[2]: String(2795) 'counter'
182881
182882 Call2              Reg8:1, Reg8:2, Reg8:3, Reg8:1
182883 LoadFromEnvironment Reg8:1, Reg8:0, UInt8:0
182884 GetByIdShort       Reg8:1, Reg8:1, UInt8:1, UInt16:151
182885 ; Oper[3]: String(151) 'state'
182886
182887 GetById          Reg8:2, Reg8:1, UInt8:2, UInt16:2795
182888 ; Oper[3]: String(2795) 'counter'
182889
182890 LoadConstInt       Reg8:1, Imm32:336
182891 JNotGreaterEqual   Addr8:43, Reg8:2, Reg8:1
182892 GetGlobalObject     Reg8:1
182893 TryGetById        Reg8:2, Reg8:1, UInt8:3, UInt16:3716
182894 ; Oper[3]: String(3716) 'alert'
182895
182896 LoadFromEnvironment Reg8:4, Reg8:0, UInt8:0
182897 GetById          Reg8:3, Reg8:4, UInt8:5, UInt16:4072
182898 ; Oper[3]: String(4072) 'decrypt'
182899
182900 LoadConstString     Reg8:1, UInt16:1724
182901 ; Oper[1]: String(1724) 'ZXxZt3UWNXYYadJ2XJZzm25vJFX93ZXnX2f Optimización de aplicativos co...
182902
182903 LoadConstString     Reg8:0, UInt16:219
182904 ; Oper[1]: String(219) 'onPress'
182905
182906 Call13             Reg8:1, Reg8:3, Reg8:4, Reg8:1, Reg8:0
```



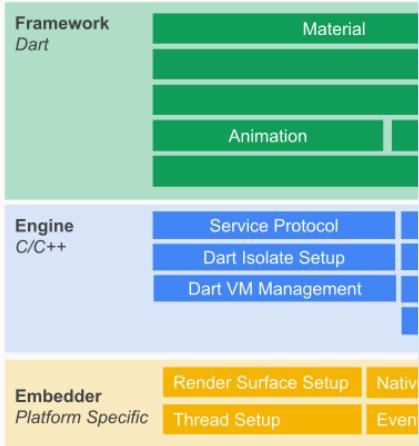


WEBSEC



Flutter

Flutter System Overview



El proyecto Flutter comenzó como un experimento de Google para ver si podían facilitar la codificación para los desarrolladores sin ningún conocimiento o experiencia previa. Permite a los desarrolladores crear aplicaciones y juegos desde sus hogares utilizando una base de código en dispositivos iOS y Android.

La mejor parte de este marco es que hace posible el desarrollo de aplicaciones incluso para pequeñas empresas y nuevas empresas. No se requiere tarifa por adelantado. En cambio, lo que paga se basa en los ingresos que genera su aplicación.

Consideraciones de Análisis



Análisis Estático Android/iOS

Mobsf:

- Para la identificación de los componentes de aplicación en AndroidManifest.xml y Info.plist.
- Posible identificación de posibles secretos en otras partes de código.

reFlutter:

- Crear dump .dart sobre el proceso de funciones

Blutter

Análisis Dinámico Android/iOS

- ✗ Android/iOS utilizar reFlutter para el parcheo de apps, Dart utiliza su propia base de certificados y los instalados por el usuario/sistema serán ignorados.

base.apk

Source code

```
├── a.a
├── android.support.v4
├── androidx
├── b
├── c
└── com
    └── d
        └── 0_2_2_2
```

```
(kali㉿kali)-[~/dojocon/blutter]
$ python blutter.py /home/kali/dojocon/blutter/sat_FLUTTER/lib/arm64-v8a/ SAT_FLUTTER
Dart version: 2.17.6, Snapshot: 1441d6b13b8623fa7fbf61433abebd31, Target: android arm64
flags: product no-code_comments no-dwarf_stack_traces_mode lazy_async_stacks no-lazy_dispatchers dedup_instructions no-asserts arm64-sysv compressed-pointers null-safety
Cloning into '/home/kali/dojocon/blutter/dartsdk/v2.17.6' ...
remote: Enumerating objects: 2256, done.
remote: Counting objects: 100% (2256/2256), done.
remote: Compressing objects: 100% (1845/1845), done.
remote: Total 2256 (delta 67), reused 1387 (delta 49), pack-reused 0
Receiving objects: 100% (2256/2256), 1.22 MiB | 14.73 MiB/s, done.
Resolving deltas: 100% (67/67), done.
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 25 (delta 0), reused 11 (delta 0), pack-reused 0
Receiving objects: 100% (25/25), 112.36 KiB | 1.40 MiB/s, done.
remote: Enumerating objects: 3298, done.
remote: Counting objects: 100% (3298/3298), done.
remote: Compressing objects: 100% (2272/2272), done.
remote: Total 3298 (delta 1105), reused 2223 (delta 993), pack-reused 0
Receiving objects: 100% (3298/3298), 8.65 MiB | 7.91 MiB/s, done.
Resolving deltas: 100% (1105/1105), done.
Updating files: 100% (3703/3703), done.
-- Configuring done (1.5s)
-- Generating done (0.0s)
-- Build files have been written to: /home/kali/dojocon/blutter/build/dartvm2.17.6_android_arm64
[101/263] Building CXX object CMakeFiles/dartvm2.17.6_android_arm64.dir/runtime/vm/os_thread.cc.o
```



WEBSEC

1338640dca3927636de

```
libflutter.so
003d929c 00 24 LAB_003d929c XREF [2]: 003d91fe(j), 003d9204(j)
003d929e 0b e0 b r4,#0x0
003d92a0 18 4a LAB_003d92a0 XREF [4]: 003d923e(j), 003d924c(j),
003d92a2 10 20 movs r2,[DAT_003d9304]
003d92a4 0b 21 movs r0,#0x10
003d92a6 4f f4 c3 73 movs r1,#0xb
003d92aa 7a 44 movs.w r3,#0x186
003d92ac c4 f7 e4 ff add r2==s_.../third_party/boringssl/src/_00090c6... = ".../third_party/boringssl/src/_00090c6...
003d92b0 00 24 bl FUN_0039e278 undefined FUN_0039e278()
003d92b2 02 a8 LAB_003d92b2 XREF [1]: 003d92f8(j)
add r0,s0.#4
003d92b4 01 20 LAB_003d92b4 XREF [1]: 003d92d6(j)
```

Split APKs is a technique used by Android to reduce the size of an application and allow users to download and use only the necessary parts of the application.

Instead of downloading a complete application in a single APK file, Split APKs divide the application into several smaller APK files, each of which contains only a part of the application such as resources, code libraries, assets, and configuration files.

```
adb shell pm path com.package
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/base.apk
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/split_config.arm64_v8a.apk
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/split_config.en.apk
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/split_config.xxhdpi.apk
```

For example, in Flutter if the application is a Split it's necessary patch `split_config.arm64_v8a.apk`, this file contains `libflutter.so`

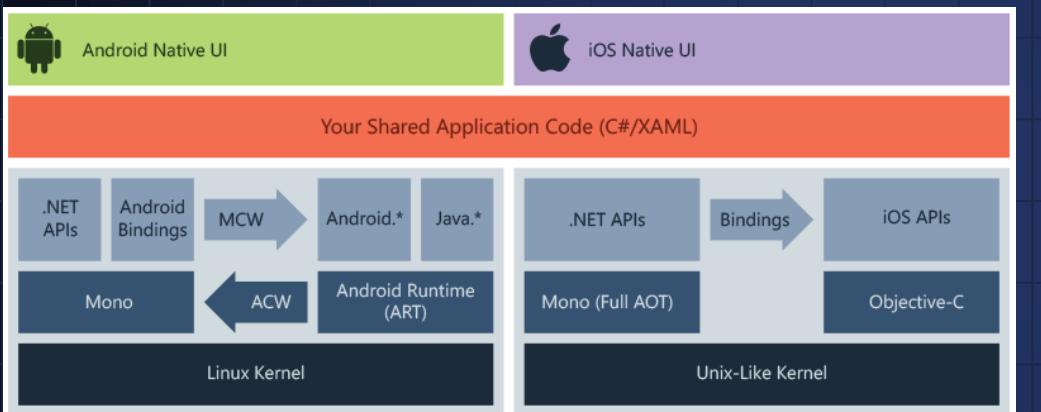
```
003d92e6 04 d8 cmp LAB_003d92e6 E
003d92e8 07 49 bhi LAB_003d92e8 E
003d92ea 79 44 ldr r1,[DAT_003d9304]
003d92ec 51 f8 20 00 add r1==DAT_003d9304
003d92f0 00 e0 ldr.w r0,[r1]
003d92f4 b LAB_003d92f4
```

Aug 20

Aug 20



Xamarin



Cuando se trata de React Native frente a Xamarin, Xamarin combina lo mejor de C# y .NET para desarrollar aplicaciones para Android, iOS y Mac. Mientras compila algo con lenguajes nativos, un desarrollador puede lograrlo con C# y Xamarin.

Los desarrolladores no pueden usar bibliotecas nativas de código abierto accesibles para iOS, Android y Xamarin. Para cumplir con estos requisitos, los desarrolladores pueden usar varias bibliotecas .NET y llenar el vacío.

Consideraciones de Análisis



WEBSEC

Análisis Estático Android/iOS

Mobsf:

- Para la identificación de los componentes de aplicación en AndroidManifest.xml y Info.plist.
- Posible identificación de posibles secretos en otras partes de código.

ILSpy:

- Explorador y descompilador de ensamblados NET

Métodos de compilación en Xamarin

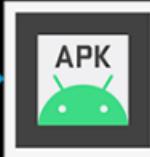
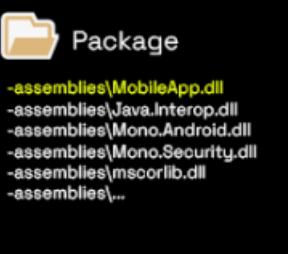


WEBSEC

Unbundled Build



Xamarin.Android
Package Builder



Bundled Build



Xamarin.Android
Package Builder

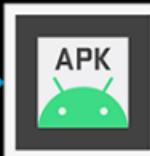


Build

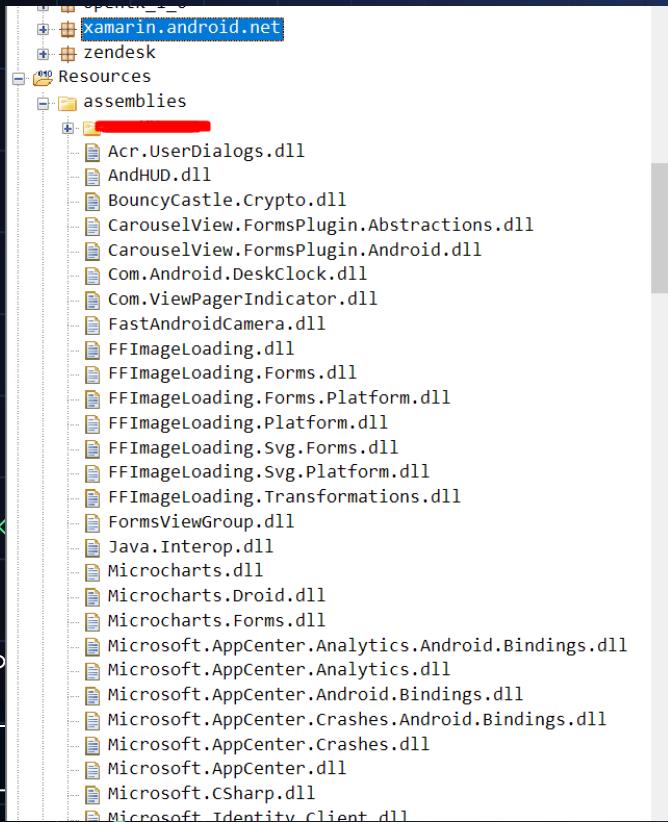
MobileApp.dll
Java.Interop.dll
Mono.Android.dll
Mono.Security.dll
mscorlib.dll
"



libmonodroid_bundle_app.so



Análisis de Aplicativos – Unbundled Build VI



The screenshot shows the dnSpy interface with the following details:

- Title Bar:** dnSpy v6.1.8 (64-bit, .NET)
- Menu Bar:** File, Edit, View, Debug, Window, Help
- Toolbar:** Back, Forward, Stop, Start, Search
- Assembly Explorer:** Shows the project structure:
 - MobileApp (1.0.0.0)
 - PE
 - Type References
 - References
 - {}
 - MobileApp
 - MainActivity @02000002
 - Resource @02000003
 - mscorlib (2.0.5.0)
 - Xamarin.AndroidX.AppCompat (1.0.0.0)
 - Xamarin.AndroidX.Fragment (1.0.0.0)
 - Xamarin.AndroidX.Activity (1.0.0.0)
 - Xamarin.AndroidX.Core (1.0.0.0)
 - Mono.Android (0.0.0.0)
 - Xamarin.Essentials (1.0.0.0)
 - Xamarin.Google.Android.Material (1.0.0.0)
 - System (2.0.5.0)
- Code Editor:** Displays the C# code for MainActivity.

```
13 namespace MobileApp
14 {
15     // Token: 0x02000002 RID: 2
16     [Activity(Label = "@string/app_name", Theme = "@style/AppTheme.NoActionBar", MainLauncher = true)]
17     public class MainActivity : AppCompatActivity
18     {
19         // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
20         protected override void OnCreate(Bundle savedInstanceState)
21         {
22             base.OnCreate(savedInstanceState);
23             this.InitCr32();
24             Platform.Init(this, savedInstanceState);
25             this.SetContentView(2131427356);
26             Toolbar supportActionBar = base.FindViewById<Toolbar>(2131230942);
27             this.SupportActionBar(supportActionBar);
28         }
29     }
30 }
```
- Locals:** A table showing local variables with their names and values.

Análisis de Aplicativos – Unbundled Build V2



Add support for compressed assemblies in APK #4686

Merged jonpryor merged 2 commits into xamarin:master from grendello:compress-assemblies on May 26, 2020

Conversation 36 · Commits 2 · Checks 0 · Files changed

ILSpy

File View Window Help

(Default) C# C# 9.0 / VS 2019.8

Assemblies SeeTheSharpFlag

grendello commented on May 13, 2020 • edited

Currently, xamarin.Android supports managed assembly compression in the APK archive if application is bundled (with Mono's `mkbundle`) into a native shared library. Managed assemblies are compressed using gzip compression and placed in an array inside the data section of the shared library. However, support for `mkbundle` is possibly going to be removed and we realized it is a feature some developers appreciate since the produced APKs are smaller and the impact on startup time isn't big enough to worry.

This commit aims to be a replacement for `mkbundle` with a handful of improvements thrown in. First of all, the compression is performed using the [managed implementation](#) of the excellent LZ4 algorithm. This gives us a decent compression ratio and a much faster (de)compression speed than gzip/zlib offer. Also, assemblies are stored directly in the APK in their usual directory, which allows us to `mmap` them on the runtime directly from the APK. The build process calculates the size required to store the decompressed assemblies and adds a data section to `libxamarin-app.so` which makes Android allocate all the required memory when the DSO is loaded, thus removing the need of dynamic memory allocation and making the startup faster.

Compression is supported only in `Release` builds and is enabled by default, but it can be turned off by setting the `$AndroidEnableAssemblyCompression` MSBuild property to `False`. If there's a need to turn compression off for an individual assembly by adding the `AndroidSkipCompression` metadata item to the assembly in question using code similar to this, in the application's project file:

```
// This file does not contain a managed assembly.

System.BadImageFormatException: Image is too small.
  en ICSharpCode.ILSpy.LoadedAssembly.<LoadAsync>d__50.MoveNext()
--- Fin del seguimiento de la pila de la ubicación anterior donde se produjo la excepción ---
  en System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
  en System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
  en ICSharpCode.ILSpy.TreeNode.AssemblyTreeNode.<Init>d__24.MoveNext()
```

https://github.com/x41sec/tools/blob/master/Mobile/Xamarin/Xamarin_XALZ_decompress.py

Análisis de Aplicativos – Unbundled Build V3



WEBSEC

```
Resources
  assemblies
    assemblies.blob
    assemblies.manifest
  assets
  kotlin
  lib
  META-INF
  okhttp3
  res
  AndroidManifest.xml
  androidsupportmultidexversion
  classes.dex
  classes2.dex

mobexler@Mobexler: ~/ReactNative/pyxamstore/pyxamstore % master ? pyxamstore unpack -d /home/mobexler/ReactNative/ups/assemblies/
ut directory already exists!
mobexler@Mobexler: ~/ReactNative/pyxamstore/pyxamstore % master ? ls out
uth0.OidcClient.Core.dll
uth0.OidcClient.dll
j-BG
bcryptCastle.Crypto.dll
jtsCertificateTransparency.dll
s-CZ
s-DK
s-
L-GR
n-CA
n-TT
n-US
s
s-ES
s-MX
s-PR
s-US
NetBus.dll
astAndroidCamera.dll
FImageLoading.dll
FImageLoading.Forms.dll
FImageLoading.Forms.Platform.dll
FImageLoading.Platform.dll
FImageLoading.Transformations.dll
l-FI
formsViewGroup.dll
F
F-CA
googleGson.dll
google.Zxing.Core.dll
j-EU
j-HU
identityModel.dll
identityModel.OidcClient.dll
navigationLib.Android.dll
l-IT
s-JP
avaGL.dll
ava.Interop.dll
o-KR
ottle.Android.dll
ottle.Forms.dll
t-LI
j-LV
icross.AppCenter.Analytics.Android.Bindings.dll
icross.AppCenter.Analytics.dll

Microsoft.AppCenter.dll
Microsoft.Bcl.AsyncInterfaces.dll
Microsoft.CSharp.dll
Microsoft.Extensions.DependencyInjection.Abstractions.dll
Microsoft.Extensions.DependencyInjection.DiagnosticSource.dll
Microsoft.Extensions.DependencyInjection.dll
Microsoft.Extensions.Logging.dll
Microsoft.Extensions.Logging.Abstractions.dll
Microsoft.Extensions.Options.dll
Microsoft.Extensions.Primitives.dll
Microsoft.IdentityModel.JsonWebTokens.dll
Microsoft.IdentityModel.Logging.dll
Microsoft.IdentityModel.Protocols.dll
Microsoft.IdentityModel.Protocols.OpenIdConnect.dll
Microsoft.IdentityModel.Tokens.dll
Mono.Android.dll
Mono.Android.Export.dll
Mono.Security.dll
mscorlib.dll
Naxam.SquareUp.OkHttp3.LoggingInterceptor.dll
nb-ND
Newtonsoft.Json.dll
nl
Nuance.Android.dll
pl-PL
Plugin.CurrentActivity.dll
Plugin.Permissions.dll
Poly.dll
pt
pt-BR
QualtricsBind.Android.dll
RestSharp.dll
ro-RO
ru-RU
sk-SK
SQLite.net.dll
SQLitePCL.batteries.dll
SQLitePCLPlugin.esqlite3.dll
SQLitePCLRaw.batteries_green.dll
SQLitePCLRaw.batteries_v2.dll
SQLitePCLRaw.core.dll
SQLitePCLRaw.core.dll
SQLitePCLRaw.lib_e_sqlite3.dll
SQLitePCLRaw.provider_e_sqlite3.dll
Square.OkHttp3.dll
Square.OkIO.dll
Square.OkHttp3.Connections.dll
System.Buffers.dll
System.Core.dll
System.Data.dll
System.dll
System.Drawing.Common.dll
System.IdentityModel.Tokens.Jwt.dll
System.IO.Compression.dll
System.Net.Http.dll
System.Numerics.dll
System.Runtime.CompilerServices.Unsafe.dll
System.Runtime.Serialization.dll
System.ServiceModel.Internals.dll
System.Text.Encoding.Web.dll
System.Text.Json.dll
System.Threading.Tasks.Extensions.dll
System.Xml.dll
System.Xml.Linq.dll
Tealium.Common.dll
Tealium.Droid.dll
Tealium.Platform.Droid.dll
Tealium.Platform.Lifecycle.Droid.dll
Threatmatrix.Android.dll
tr-TR
UPS.MobileX.Droid.dll
UPS.MobileX.Forms.Common.dll
UPS.MobileX.Forms.Views.dll
UPS.MobileX.PCL.Resources.dll
UPS.MobileX.PCL.Services.dll
UPS.MobileX.XPCL.Services.dll
UserzoomSDKAndroid.dll
vi-VN
Xamarin.Android.Binding.InstallReferrer.dll
Xamarin.Android.Volley.dll
Xamarin.Android.Activity.dll
Xamarin.AndroidX.AppCompat.AppCompatResources.dll
Xamarin.AndroidX.AppCompat.dll
Xamarin.AndroidX.Biometric.dll
Xamarin.AndroidX.Browser.dll
Xamarin.AndroidX.CardView.dll
Xamarin.AndroidX.Collection.dll
Xamarin.AndroidX.CoordinatorLayout.dll
Xamarin.AndroidX.Core.dll
Xamarin.AndroidX.DrawerLayout.dll
Xamarin.AndroidX.Fragment.dll
Xamarin.AndroidX.RecyclerView.dll
Xamarin.AndroidLifecycle.dll
Xamarin.AndroidX.Loader.dll
Xamarin.AndroidX.Recyclerview.dll
Xamarin.AndroidX.Spannable.dll
Xamarin.AndroidX.SwipeRefreshLayout.dll
Xamarin.AndroidX.VersionedParcelable.dll
Xamarin.AndroidX.ViewPager.dll
Xamarin.Essentials.dll
Xamarin.Facebook.Android.dll
Xamarin.Facebook.AppLinks.Android.dll
Xamarin.Facebook.Common.Android.dll
Xamarin.Facebook.Core.Android.dll
Xamarin.Facebook.GamingServices.Android
Xamarin.Facebook.Login.Android.dll
Xamarin.Facebook.Messenger.Android.dll
Xamarin.Facebook.Share.Android.dll
Xamarin.FirebaseAnalytics.dll
Xamarin.Firebase.Iid.dll
Xamarin.Firebase.Messaging.dll
Xamarin.Forms.Core.dll
Xamarin.Forms.Maps.Android.dll
Xamarin.Forms.Maps.dll
Xamarin.Forms.Platform.Android.dll
Xamarin.Forms.Platform.dll
Xamarin.Forms.Xaml.dll
Xamarin.Google.Android.Material.dll
Xamarin.Google.ARCore.dll
Xamarin.Google.AutoValue.Annotations.dll
Xamarin.Google.Guava.ListenableFuture.dll
Xamarin.Google.PlayServices.Auth.dll
Xamarin.GooglePlayServices.Base.dll
Xamarin.GooglePlayServices.Basement.dll
Xamarin.GooglePlayServices.Maps.dll
Xamarin.GooglePlayServices.Tasks.dll
Xamarin.Jetbrains.Annotations.dll
Xamarin.Kotlin.StdLib.Common.dll
Xamarin.Kotlin.StdLib.dll
Xamarin.Kotlin.StdLib.Jdk7.dll
Xamarin.Kotlin.StdLib.Jdk8.dll
zh
zh-CN
zh-TW
ZXing.Net.Mobile.Core.dll
ZXingNetMobile.dll
```

<https://github.com/jakev/pyxamstore/>

Análisis de Aplicativos – Bundled Build



Application
Android Manifest
Android Options
Android Package Signing

Build
Build
References

Configuration: Active (Release) Platform: Active (Any CPU)

Packaging properties

IDA View-A Strings window Hex View-1 Structures Enums Program Segmentation Imports Exports

```
.data:0000000000001A9228 ; Segment type: Pure data
.data:0000000000001A9228 ; AREA .data, DATA, ALIGN=3
.data:0000000000001A9228 ; ORG 0x1A9228
.data:0000000000001A9228 .DCQ assembly_bundle_MobileApp.dll
.data:0000000000001A9228 ; DATA XREF: LOAD:00000000000002A810
.data:0000000000001A9228 ; mono_mkbundle_init+0f0 ...
.data:0000000000001A9230 10 93 1A 00 00 00 00 00 00
.data:0000000000001A9238 30 93 1A 00 00 00 00 00 00
.data:0000000000001A9240 50 93 1A 00 00 00 00 00 00
.data:0000000000001A9248 70 93 1A 00 00 00 00 00 00
.data:0000000000001A9250 90 93 1A 00 00 00 00 00 00
.data:0000000000001A9258 B0 93 1A 00 00 00 00 00 00
.data:0000000000001A9260 D0 93 1A 00 00 00 00 00 00
.data:0000000000001A9268 F0 93 1A 00 00 00 00 00 00
.data:0000000000001A9270 10 94 1A 00 00 00 00 00 00
.data:0000000000001A9278 30 94 1A 00 00 00 00 00 00
.data:0000000000001A9280 50 94 1A 00 00 00 00 00 00
.data:0000000000001A9288 70 94 1A 00 00 00 00 00 00
.data:0000000000001A9290 90 94 1A 00 00 00 00 00 00
.data:0000000000001A9298 B0 94 1A 00 00 00 00 00 00
.data:0000000000001A92A0 D0 94 1A 00 00 00 00 00 00
.data:0000000000001A92A8 F0 94 1A 00 00 00 00 00 00
.data:0000000000001A92B0 10 95 1A 00 00 00 00 00 00
.data:0000000000001A92B8 30 95 1A 00 00 00 00 00 00
.data:0000000000001A92C0 50 95 1A 00 00 00 00 00 00
.data:0000000000001A92C8 70 95 1A 00 00 00 00 00 00
.data:0000000000001A92D0 90 95 1A 00 00 00 00 00 00
.data:0000000000001A92D8 B0 95 1A 00 00 00 00 00 00
.data:0000000000001A92E0 D0 95 1A 00 00 00 00 00 00
.data:0000000000001A92E8 00 00 00 00 00 00 00 00 00
```

File Edit View Favorites Tools Help

Add Extract Test Copy Move Delete Info

Name

- lib
- META-INF
- res

AndroidManifest.xml

classes.dex

resources.arsc

0 / 6 object(s) selected

<https://cihansol.com/blog/index.php/2021/08/09/unpacking-xamarin-android-mobile-applications/>

Análisis de Aplicativos - Bundled Build



WEBSEC

XamAsmUnZ
Author: Cihan

Z>XamAsmUnZ.exe -elf

\com.cihansol.mobileapp-packed\lib\arm64-v8a\libmonodroid_bundle_app.so

ELF file is of type: Bit64

Finding assembly bundles.

Bundle: [MobileApp.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [47358]
GZData Size Uncompressed: [131584]

Bundle: [Java.Interop.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [54778]
GZData Size Uncompressed: [162304]

Bundle: [Mono.Android.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [266626]
GZData Size Uncompressed: [973824]

Bundle: [mscorlib.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [679247]
GZData Size Uncompressed: [1870848]

Bundle: [System.Core.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [27538]
GZData Size Uncompressed: [54784]

Bundle: [System.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [167501]
GZData Size Uncompressed: [386048]

Bundle: [System.Numerics.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [12896]
GZData Size Uncompressed: [25600]

Bundle: [Xamarin.AndroidX.Activity.dll]
GZData Offset: [XamAsmUnZ.AssemblyBundle]
GZData Size Compressed: [2412]
GZData Size Uncompressed: [6144]

Nombre	Fecha de modificación	Tipo	Tamaño
Java.Interop.dll	6/10/2023 01:14	Extensión de la ap...	159 KB
MobileApp.dll	6/10/2023 01:14	Extensión de la ap...	129 KB
Mono.Android.dll	6/10/2023 01:14	Extensión de la ap...	951 KB
Mono.Security.dll	6/10/2023 01:14	Extensión de la ap...	107 KB
mscorlib.dll	6/10/2023 01:14	Extensión de la ap...	1,827 KB
System.Core.dll	6/10/2023 01:14	Extensión de la ap...	54 KB
System.dll	6/10/2023 01:14	Extensión de la ap...	377 KB
System.Net.Http.dll	6/10/2023 01:14	Extensión de la ap...	208 KB
System.Numerics.dll	6/10/2023 01:14	Extensión de la ap...	25 KB
Xamarin.AndroidX.Activity.dll	6/10/2023 01:14	Extensión de la ap...	6 KB
Xamarin.AndroidX.AppCompat.dll	6/10/2023 01:14	Extensión de la ap...	320 KB
Xamarin.Android.Core.dll	6/10/2023 01:14	Extensión de la ap...	154 KB
Xamarin.AndroidX.CustomView.dll	6/10/2023 01:14	Extensión de la ap...	9 KB
Xamarin.AndroidX.DrawerLayout.dll	6/10/2023 01:14	Extensión de la ap...	40 KB
Xamarin.AndroidX.Fragment.dll	6/10/2023 01:14	Extensión de la ap...	149 KB
Xamarin.AndroidX.Lifecycle.Common.dll	6/10/2023 01:14	Extensión de la ap...	15 KB
Xamarin.AndroidX.Lifecycle.LiveData.Corr...	6/10/2023 01:14	Extensión de la ap...	16 KB
Xamarin.AndroidX.Lifecycle.ViewModel.dll	6/10/2023 01:14	Extensión de la ap...	17 KB
Xamarin.AndroidX.Loader.dll	6/10/2023 01:14	Extensión de la ap...	36 KB
Xamarin.Android.SavedState.dll	6/10/2023 01:14	Extensión de la ap...	13 KB
Xamarin.Essentials.dll	6/10/2023 01:14	Extensión de la ap...	26 KB
Xamarin.Google.Guava.ListenableFuture.dll	6/10/2023 01:14	Extensión de la ap...	18 KB

<https://github.com/cihansol/XamAsmUnZ/releases>



WEBSEC



7:02 PM 7:02 PM 9:20 p.m.

Sin SIM

Config. certificados de confianza

Versión 2021072200

Magisk Trust User Certs Request

This module makes all installed user certificates part of the trust chain. This module makes it unnecessary to add certificates to the trust chain.

Accompanying blogpost [Intercepting HTTPS Traffic from Apps on Android 7+](#)

Installation

1. Install [Magisk](#)
2. Zip files `zip -r AlwaysTrustUserCerts.zip ./*`
3. Install in Magisk
4. Install client certificates through [normal flow](#)
5. Restart your device. Certificate copying happens automatically.
6. The installed user certificates can now be found in `/etc/certs`.

Adding certificates

Install the certificate as a user certificate and restart the device.

```
Pretty Raw Hex
1 POST /api/Autentica/autentica HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json, text/json, text/x-json, text/javascript, application/xml, text/xml
4 User-Agent: RestSharp/106.11.7.0
5 Content-Length: 120
6 Connection: close
7
8 Accept-Encoding: gzip, deflate, br
9
10 {
    "appId": "paakijhjhye254fdfg8",
    "appKey": "olhyghs54654nzqopio",
    "Sistema": "SM",
    "Session": "3154545",
    "Password": "aggagaha"
}
```

SECOM Trust Systems CO.,LTD.
Security Communication RootCA2

Si

CIONES DE ANÁLISIS

Consideraciones de Análisis



WEBSEC

The image shows three sequential screenshots of a web-based interface for managing OpenVPN profiles:

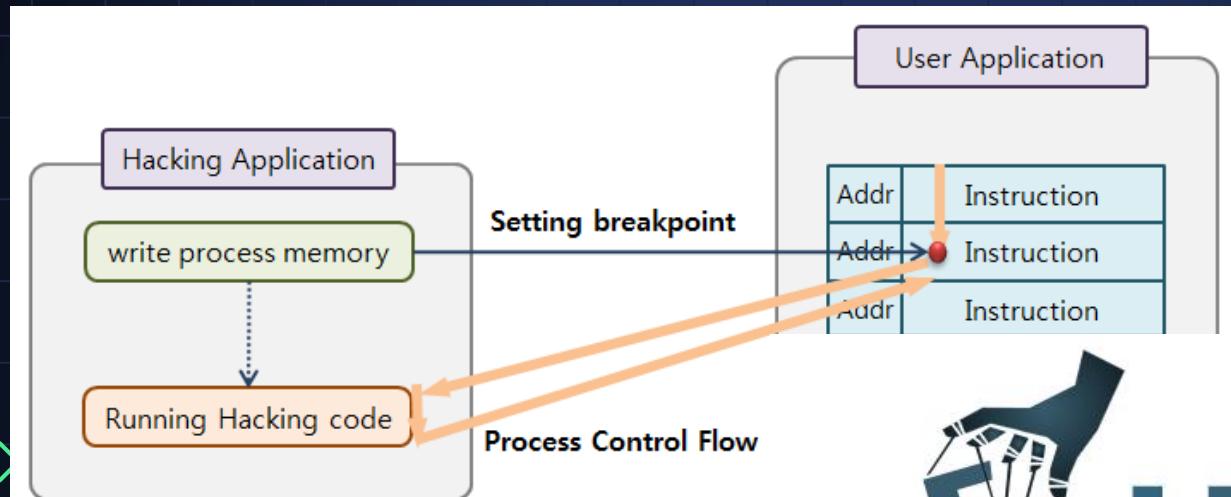
- Import Profile:** Shows a URL input field and a "FILE" tab. Below it, a message says "1 new OpenVPN profiles are available for import". A single profile is listed: "192.168.0.138 [salman]" (Standard Profile). Buttons for "ADD" and "DELETE" are visible.
- Imported Profile:** Shows the imported profile "192.168.0.138 [salman]" with a success message: "Profile successfully imported". It includes a "CONNECTED" section with an "OpenVpn" toggle switch and IP address "192.168.0.138". A "Connection ST" section shows "2.7KB/s" and "0B/s". Below are "BYTES IN" (4 B/S) and "DURATION" (00:01:12).
- ADD:** Shows a list of profiles: "192.168.0.138 [salman]".

The image shows the Burp Suite interface with the following details:

- Proxy Listeners:** A table showing a single listener: "192.168.0.138:8888" (Running, Interface: 127.0.0.1:8080, Invisible checked, Redirect checked, Certificate: Per-host, TLS Protocols: Default).
- Listening on burpsuite:** A message indicating the proxy is active.
- Edit proxy listener dialog:** A modal window titled "Edit proxy listener" with tabs for Binding, Request handling, Certificate, and TLS Protocols. It contains fields for "Redirect to host" and "Redirect to port", a "Force use of TLS" checkbox, and a "Support invisible proxying" checkbox which is checked and highlighted with a red border. Buttons for "OK" and "Cancel" are at the bottom.

<https://slmnsd552.medium.com/how-to-capture-non-proxy-aware-mobile-application-traffic-ios-android-xamarin-flutter-924fe044facf>

Consideraciones de Análisis



Mobile Helper Framework

```
class FrameWork:  
    REACT_NATIVE = "React Native"  
    REACT_NATIVE_IOS = "React Native ios"  
    CORDOVA = "Cordova"  
    FLUTTER = "Flutter"  
    FLUTTER_IOS = "Flutter ios"  
    XAMARIN = "Xamarin"  
    XAMARIN_IOS = "Xamarin ios"  
    NATIVESCRIPT = "NativeScript"  
    NATIVE = "Native (Java/Kotlin)"  
    NATIVE_IOS = "Native (Objective-C/Swift)"  
    XAMARINV2 = "Xamarin"  
  
    class Technology:  
        def __init__(self, framework, directories):  
            self.framework = framework  
            self.directories = directories  
  
    tech_list = [  
        Technology(  
            framework=FrameWork.REACT_NATIVE,  
            directories=[  
                "libreactnativejni.so",  
                "index.android.bundle",  
            ]  
        ),  
        Technology(  
            framework=FrameWork.REACT_NATIVE_IOS,  
            directories=[  
                "main.jsbundle",  
            ]  
        ),  
        Technology(  
            framework=FrameWork.CORDOVA,  
            directories=[  
                "index.html",  
                "cordova.js",  
                "cordova_plugins.js"  
            ]  
        ),  
        Technology(  
            framework=FrameWork.FLUTTER,  
            directories=[  
                "libflutter.so"  
            ]  
        ),  
        Technology(  
            framework=FrameWork.FLUTTER_IOS,  
            directories=[  
                "flutter.framework/Flutter"  
            ]  
        ),  
        Technology(  
            framework=FrameWork.XAMARIN,  
            directories=[  
                "Mono.Android.dll",  
                "libmonodroid.so",  
                "libmonosgen-2.0.so",  
            ]  
        ),  
        Technology(  
            framework=FrameWork.XAMARINV2,  
            directories=[  
                "assemblies.blob",  
                "assemblies.manifest",  
            ]  
        ),  
        Technology(  
            framework=FrameWork.XAMARIN_IOS,  
            directories=[  
                "monoarm64_ios.dll"  
            ]  
        ),  
    ]
```

```
        "index.android.bundle",  
    ],  
    Technology(  
        framework=FrameWork.REACT_NATIVE_IOS,  
        directories=[  
            "main.jsbundle",  
        ]  
    ),  
    Technology(  
        framework=FrameWork.CORDOVA,  
        directories=[  
            "index.html",  
            "cordova.js",  
            "cordova_plugins.js"  
        ]  
    ),  
    Technology(  
        framework=FrameWork.FLUTTER,  
        directories=[  
            "libflutter.so"  
        ]  
    ),  
    Technology(  
        framework=FrameWork.FLUTTER_IOS,  
        directories=[  
            "flutter.framework/Flutter"  
        ]  
    ),  
    Technology(  
        framework=FrameWork.XAMARIN,  
        directories=[  
            "Mono.Android.dll",  
            "libmonodroid.so",  
            "libmonosgen-2.0.so",  
        ]  
    ),  
    Technology(  
        framework=FrameWork.XAMARINV2,  
        directories=[  
            "assemblies.blob",  
            "assemblies.manifest",  
        ]  
    ),  
    Technology(  
        framework=FrameWork.XAMARIN_IOS,  
        directories=[  
            "monoarm64_ios.dll"  
        ]  
    ),  
]
```



Es una herramienta que automatiza el proceso de identificar el marco de trabajo/tecnología utilizada para crear una aplicación móvil. Además, ayuda a encontrar información sensible o proporciona sugerencias para trabajar con la plataforma identificada.

<https://github.com/stuxctf/mhf>

Funcionalidades



WEBSEC

Features

This tool uses Apktool for decompilation of Android applications.

This tool renames the .ipa file of iOS applications to .zip and extracts the contents.

Feature	Note	Cordova	React Native	Native JavaScript	Flutter	Xamarin
JavaScript beautifier	Use this for the first few occasions to see better results.	✓	✓	✓		
Identifying multiple sensitive information	IPs, Private Keys, API Keys, Emails, URLs	✓	✓	✓	✓	✗
Split APKs is a technique used by Android to reduce the size of an application and allow users to download and use only the necessary parts of the application.						
Instead of downloading a complete application in a single APK file, Split APKs divide the application into several smaller APK files, each of which contains only a part of the application such as resources, code libraries, assets, and configuration files.						
Automatically extracts the APK files.						
Extracts:						
adb shell pm path com.package package:/data/app/com.package-Nw8ZbgI5VPzvSZ1NgMa4CQ==/base.apk package:/data/app/com.package-Nw8ZbgI5VPzvSZ1NgMa4CQ==/split_config.arm64_v8a.apk package:/data/app/com.package-Nw8ZbgI5VPzvSZ1NgMa4CQ==/split_config.en.apk package:/data/app/com.package-Nw8ZbgI5VPzvSZ1NgMa4CQ==/split_config.xhdpi.apk						
Example:						
For example, in Flutter if the application is a Split it's necessary patch split_config.arm64_v8a.apk, this file contains libflutter.so						
Detect if the resources are compressed.						
✗ Hermes ✓ ✗ ✗ XALZ ✓						
Detect if the app is split						
✗ ✗ ✗ ✗ ✗ ✗						

Ejemplo - Codova



WEBSEC

Ejemplo – React Native



WEBSEC

```
[+] App was written in React Native  
Do you want to look for possible interesting information in the bundle file associated with the application? (Y/n): Y  
Output directory already exists. Skipping decompilation.  
Do you want beautified the react code? (Y/n): n  
Continue with the operation? (Y/n): Y  
==>Searching possible internal IPs in the file  
  
==>Searching possible emails in the file  
[INFO] Emails found: {'rd': [REDACTED]  
==>Searching possible encryption functions in the file  
[INFO] Encryption function found in line 224203:  
CryptoJS.enc;  
==>Searching Private Keys in the file  
  
==>Searching possible interesting words in the file  
accessToken  
==>Searching high confidential secrets  
[INFO] Generic API Key identify C:/Users/ccalderon/Downloads/mcdonalds.REACT/assets/index.android.bundle:[
```

Ejemplo - Xamarin



WEBSEC

Do you want get DLL information? (Y/n): Y

Decompiling application [REDACTED].com.cihansol.mobileapp-nopack.apk

[!] APK compiled in mode Unbundled Build
The package builder will utilize LZ4 Compression and create files with the .dll extension

[!] To reverse
Windows
Windows
Linux,

Possible main

DLL Compressed

[+] App was written in Xamarin

Do you want get DLL information? (Y/n): Y

Output directory already exists. Skipping decompilation.

[!] APK compiled in mode Bundled Build
The package builder bundles .dll assemblies into native code, in the file:

Bundle path:

[REDACTED] com.cihansol.mobileapp-packed (1)\lib\arm64-v8a\libmonodroid_bundle_app.so
[REDACTED] com.cihansol.mobileapp-packed (1)\lib\armeabi-v7a\libmonodroid_bundle_app.so

For extraction of the .dll assemblies use: <https://github.com/cihansol/XamAsmUnz>

[REDACTED]\com.cihansol.mobileapp-nopack\unKnown\assemblies\system.numerics.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.Activity.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.AppCompat.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.Core.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.CustomView.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.DrawerLayout.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.Fragment.dll
[REDACTED]\com.cihansol.mobileapp-nopack\unknown\assemblies\xamarin.AndroidX.Lifecycle.Common.dll



git commit

git push

git add .

2024-07-08 19:49:47 [CHK] Getting possible browseable components

Exported Activities

com.pollocampero.pc_gt_mobile.MainActivity

org.apache.cordova.firebaseio.DynamicLinkActivity

com.facebook.CustomTabActivity

App

Pac

Mai

2024-07-08 19:51:26 [CHK] Getting possible security protections

Root Detection	Emulator Detection	Hooking Frameworks	SSL Pinning	Insecure Settings
isRooted	google_sdk emulator generic unknown Emulator Android SDK built for x86 Genymotion sdk simulator	none	checkServerTrusted getAcceptedIssuers X509TrustManager	none

Exported Providers

com.facebook.FacebookContentProvider

c_gt_mobile/

Referencias

<https://mas.owasp.org/checklists/>

<https://slmnsd552.medium.com/how-to-capture-non-proxy-aware-mobile-application-traffic-ios-android-xamarin-flutter-924fe044facf>

<https://swarm.ptsecurity.com/fork-bomb-for-flutter/>

<https://blog.tst.sh/reverse-engineering-flutter-apps-part-1/>

<https://cihansol.com/blog/index.php/2021/08/09/unpacking-xamarin-android-mobile-applications/>

<https://suam.wtf/posts/react-native-application-static-analysis-en/>

<https://book.hacktricks.xyz/mobile-pentesting/cordova-apps>

https://www.thecobraden.com/posts/unpacking_xamarin_assembly_stores/

 <https://book.hacktricks.xyz/mobile-pentesting/android-app-pentesting/react-native-application>

 https://www.youtube.com/watch?v=ovW3E09gWjY&list=PLZsnFVE_qTjB5FRgECU8gOQeVCPBoQOz9

 <https://github.com/worawit/blutter>

 <https://github.com/P1sec/hermes-dec>

 <https://www.justmobilesec.com/en/blog>



¡GRACIAS!



@_websec

@__stux