
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.

Posible abuso de memes…..

Whoami

Cesar Calderon

Senior Security Consultant– Websec MX

Ex-Content Developer in Tryhackme

eJPT - eMAPT

Un poco de repaso...

APK

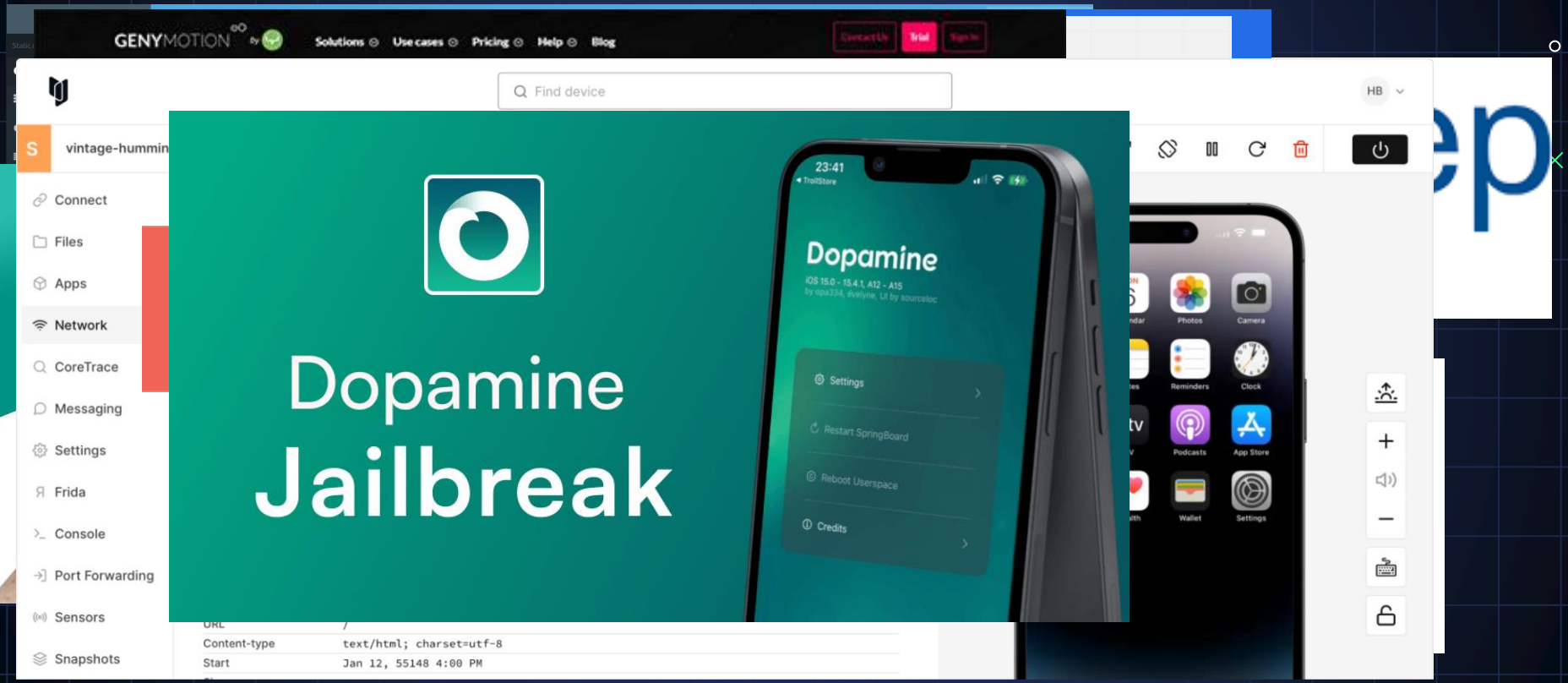
- /Payload/

OWASP-2016	
M1: Improper Platform Usage	M1: Impro
M2: Insecure Data Storage	M2: Inade
M3: Insecure Communication	M3: Insecu
M4: Insecure Authentication	M4: Insuffi
M5: Insufficient Cryptography	M5: Insecu
M6: Insecure Authorization	M6: Inade
M7: Client Code Quality	M7: Insuffi
M8: Code Tampering	M8: Secur
M9: Reverse Engineering	M9: Insecu
M10: Extraneous Functionality	M10: Insuf

OWASP API Security Top-10 2023	
API1 Broken Object Level Authorization	Same
API2 Broken Authentication	Updated
API3 Broken Object Property Level Authorization	Updated
API4 Unrestricted Resource Consumption	Updated
API5 Broken Function Level Authorization	Same
API6 Unrestricted Access to Sensitive Business Flows	New
API7 Server-Side Request Forgery (SSRF)	New
API8 Security Misconfiguration	Same
API9 Improper Inventory Management	Updated
API10 Unsafe Consumption of APIs	New

en 2016-2024
6 to M3
3 to M5
9 to M7
[M10]
2 to M9
5 to M10

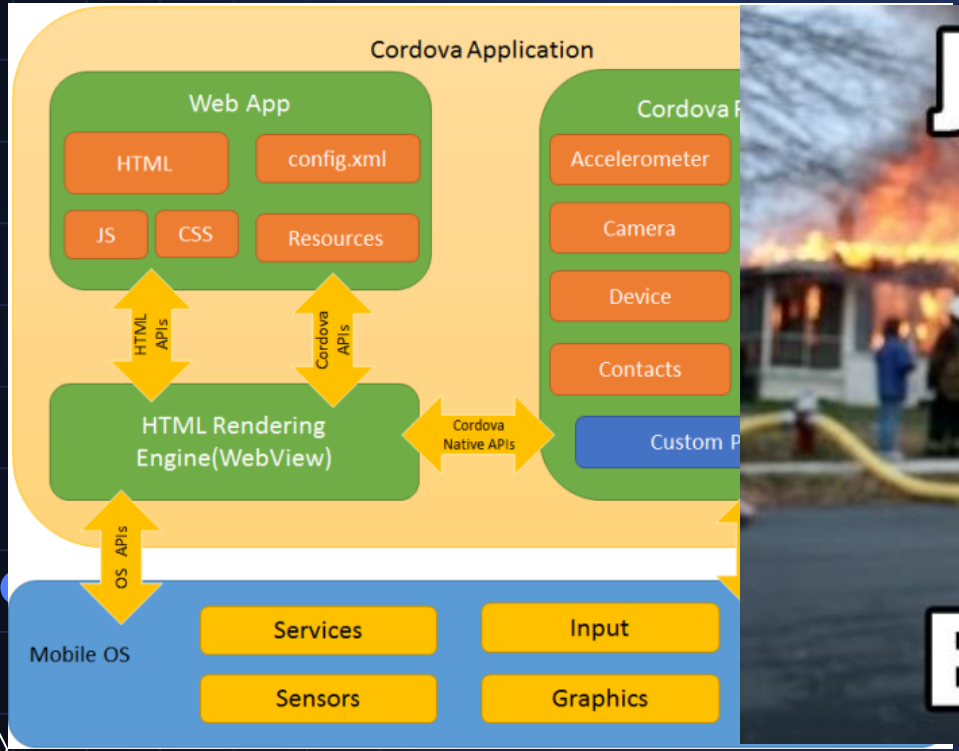
Herramientas generales



Introducción

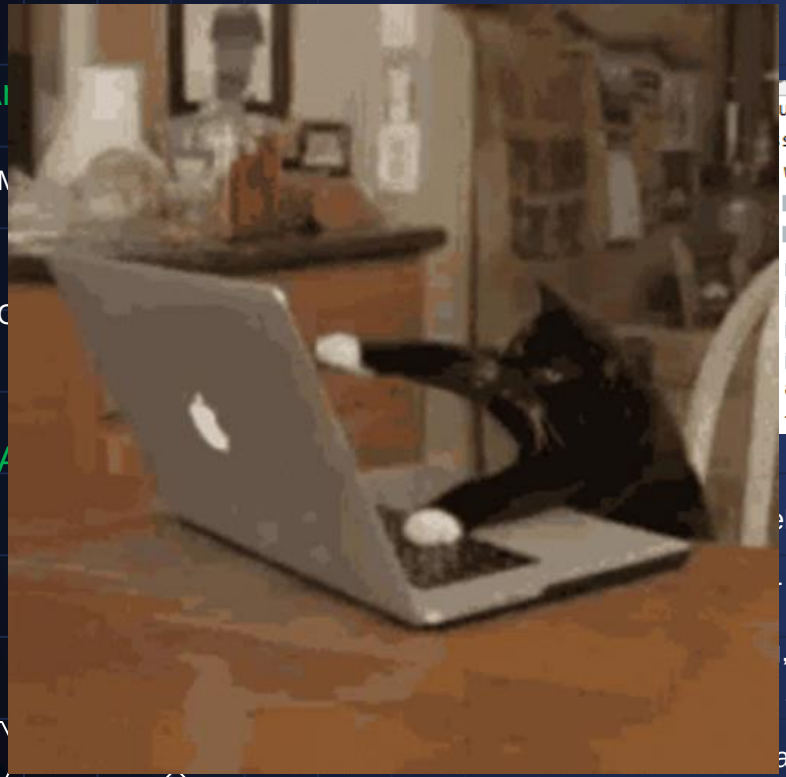
WEBSEC

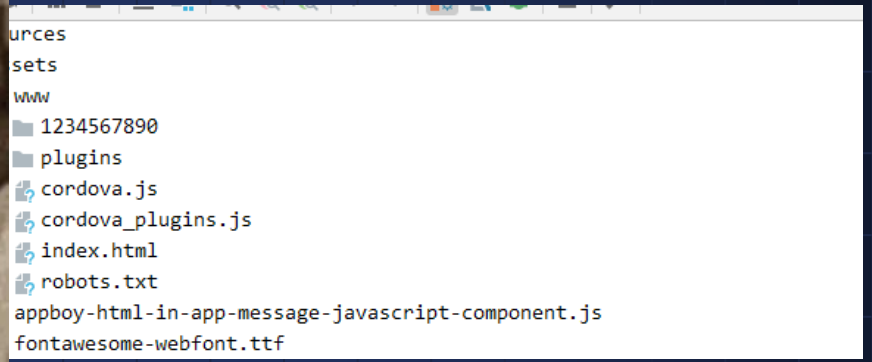
Ionic/Cordova



Consideraciones de Análisis

WEBSEC





el proxy en proxydroid y colocarlo como invisible en burpsuite.

el proxy en WiFi.

, fingerprinting, funcionan adecuadamente

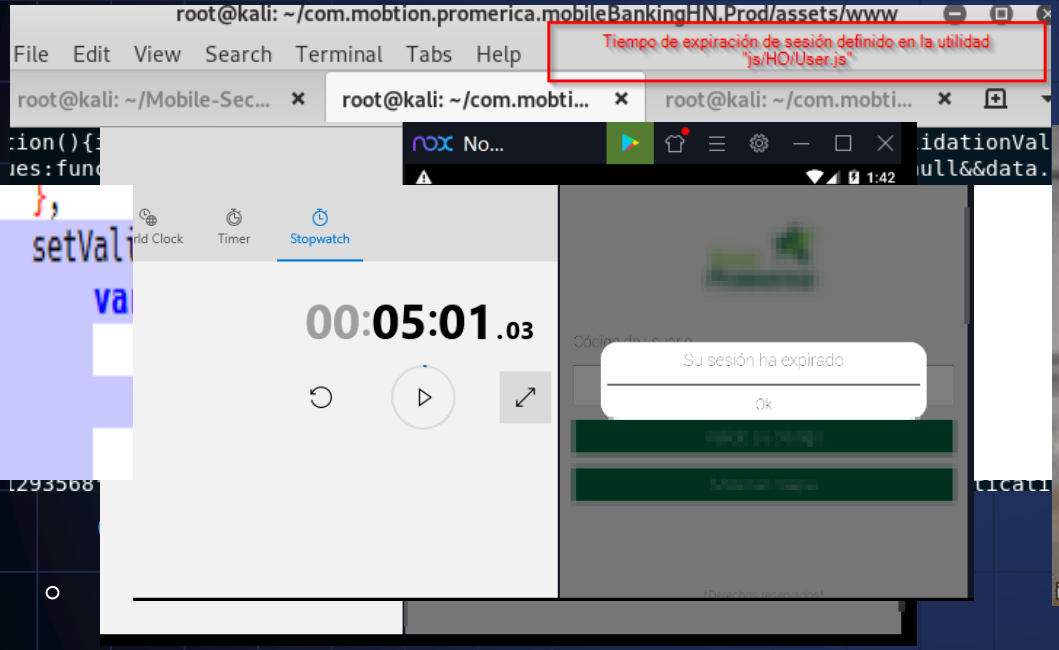
funcionan, esto debe identificar manualmente en los archivos .js.

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

```
var CryptoJS = require("crypto-js" 4.1.1 );

var
mensaje='{"pSisCta":"TDB_CL","pCodigo":125,"pUsuario":"X","pSesionId":"X-
Google Nexus 5X - 6.0.0 - API 23 -
1080x1920","pIpUsuario":"X","pIp":"X","eUi":[{"pSmartPhone":"Google Nexus
5X - 6.0.0 - API 23 - 1080x1920","pTipoSmartPhone":"Google Nexus 5X -
6.0.0 - API 23 -
1080x1920","pSO":"Android","pUi":"X","pImei":"null","pVersionAPP":"3.0"}]}
';

var enc = CryptoJS.AES.encrypt(mensaje,
"CLAVENARREGLODEBYTES").toString();

var ciphertext = encodeURIComponent(enc.toString(CryptoJS.enc.Utf8));

Save on RunKit   Node 18   help   ▶ run

"U2FsdGVkX1%2BbzW7lzug7EiMC1H2BDMLhx75kpzhFB6z1u0cuig06JiTx…
DolzSmB2FtZK8vmbbhsbWkmzs535HDEl65Dv7B7ojV8wzSW8rtg%3D%3D"

U2FsdGVkX1%2BbzW7lzug7EiMC1H2BDMLhx75kpzhFB6z1u0cuig06JiTxWeHMkQYB%2FSj
zrmr2qVXiIrSz5fkZuzMq8PLqdEHZjUitY13u9Q4WEZhkb5eIX722AvTBF281CQSaw3I%2F
5r19w3CYZa8JhyU3xqdH4jkb3Xhp3T%2B6suQhE2yxPLB8RhrJzh6mNsYFumLTFgzdVG75P
ZSDLvZoueqFH9A3UxPpf%2F%2FTBgV7jBPLCaNDwT6WkByM%2Bpr9CcOEj0uGjOGGzjLTzl
FLuGFtZJlxcZq4hbOMgiyGQ2ABRqgJv1T%2Fv8x5JmABQ3Fykl5cdbSPxOYS%2FYeXwiHuT
1jm9ygrdjQtyo%2FlVpgo%2Bo9vRZ9prOeaJ%2FUFzkBBsJq3XVMD5WSrXLAL%2FvxDu4D2
0YhQ4fYIrnxCNvMjQaWDolzSmB2FtZK8vmbbhsbWkmzs535HDEl65Dv7B7ojV8wzSW8rtg%
3D%3D
```

Caso #2: Validaciones a Nivel de cliente



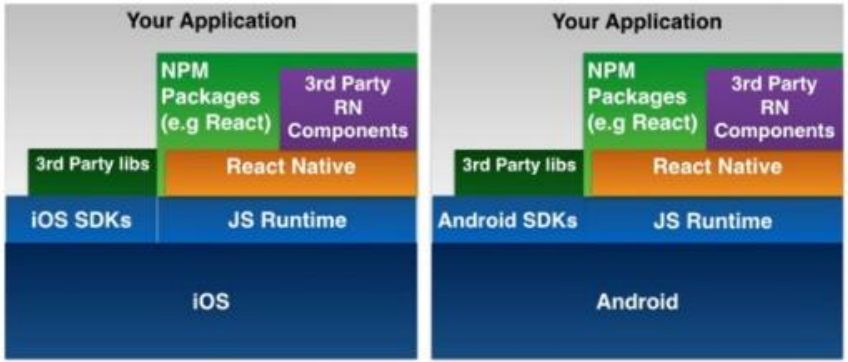
Durante el proceso de assesment se identificó

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


```
(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)([
    (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)
```

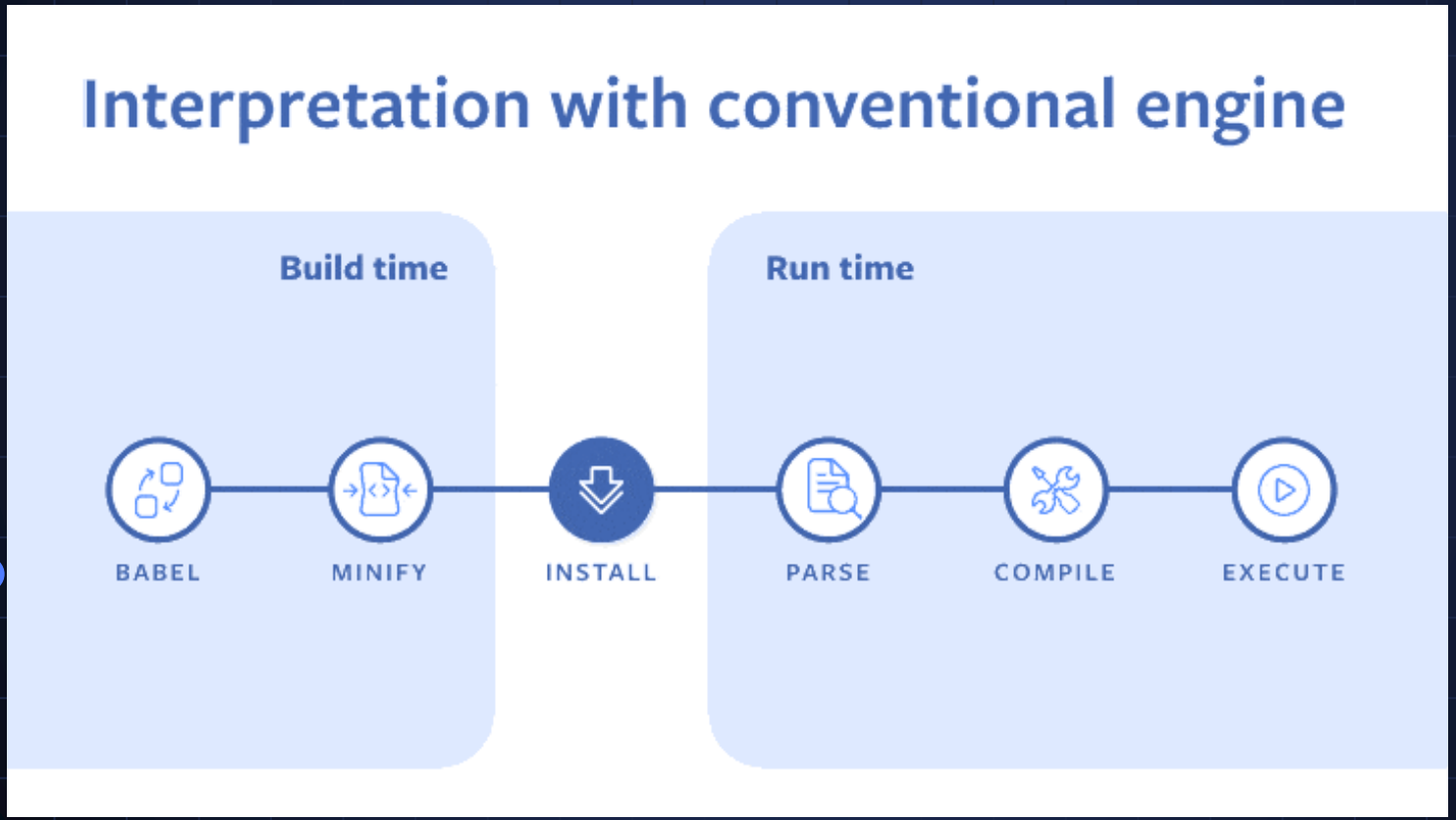
React Native

React Native App Architecture

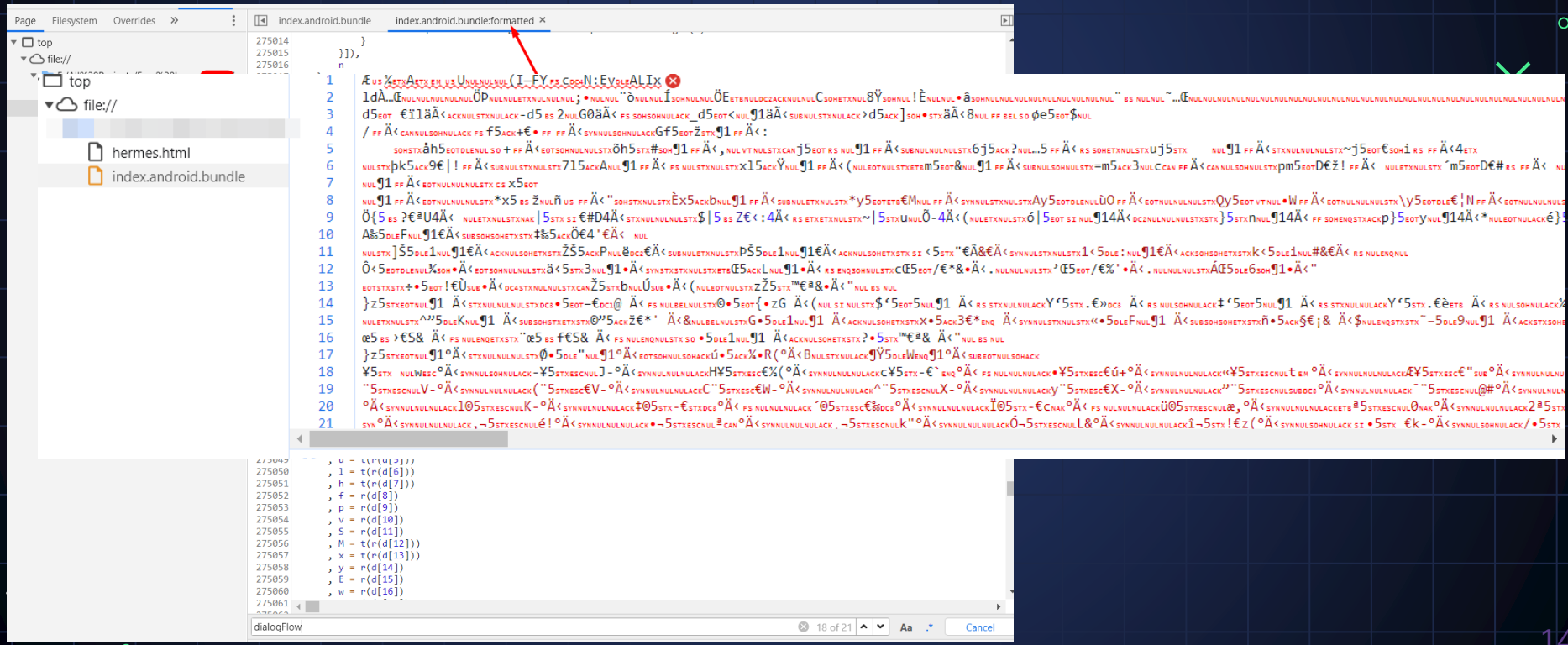


Optimización de aplicativos con Hermes

WEBSEC



Optimización de aplicativos con Hermes - Ejemplo



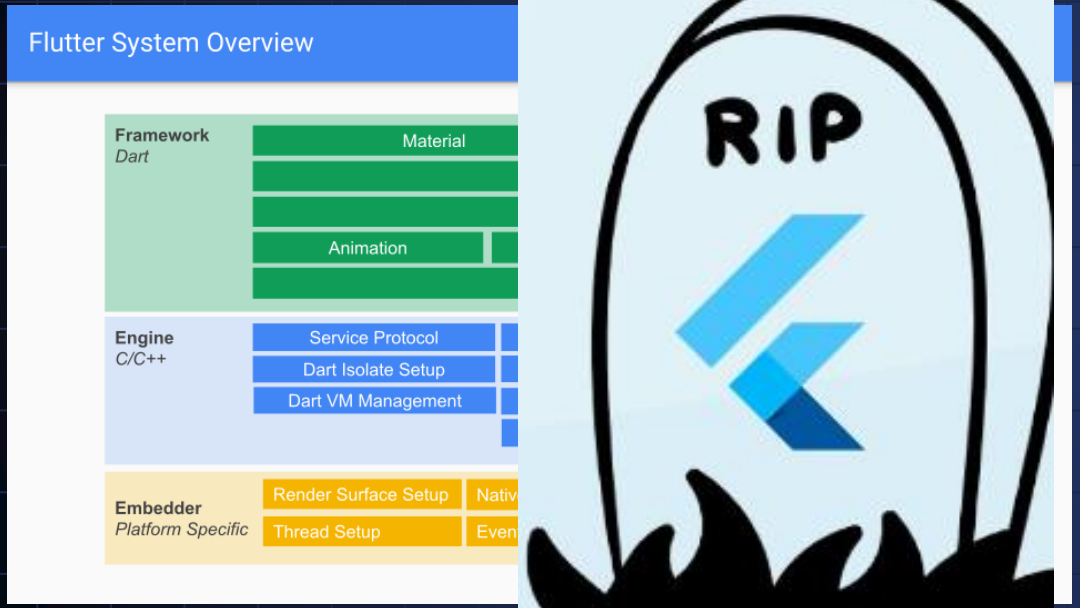
Disassembling and assembling the Hermes Bytecode

https

```
1 instruction.hasm
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, UInt8:151
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) 'ZXxZt3UWNXVYadJ2XJZzm25vJFX93ZXnX2f
182902
182903      LoadConstString         Reg8:0, UInt16:219
182904      ; Oper[1]: String(219) 'onPress'
182905
182906      Call3                   Reg8:1, Reg8:3, Reg8:4, Reg8:1, Reg8:0
```

Optimización de aplicativos co...

Flutter



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

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.

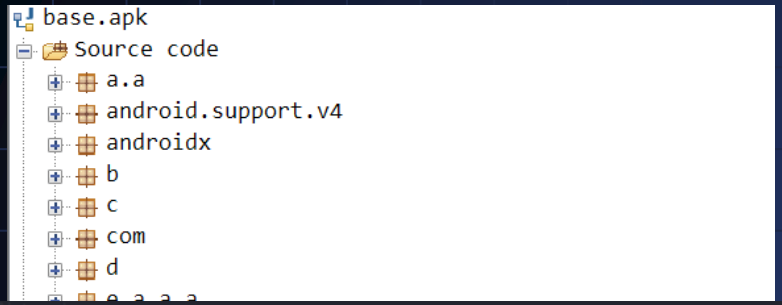
reFlutter:

- Crear dump .dart sobre el proceso de funciones

Blutter

Análisis Dinámico Android/iOS

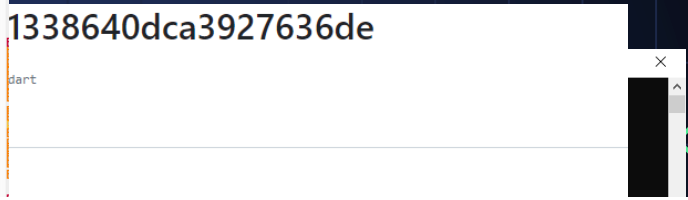
Android/iOS utilizar reFlutter para el parcheo de apps, Dart utiliza su propia base de certificados y los instalados por el usuario/sistema serán ignorados.




```
┌──(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
```

Aná

WEBSEC

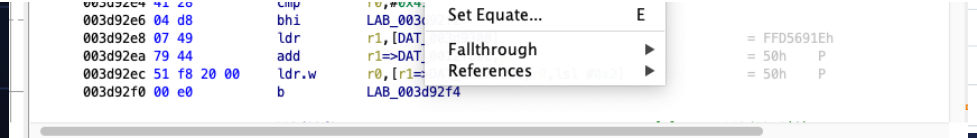


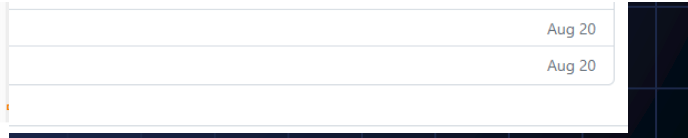
`Split APKs` is a technique used by Android to reduce the size of an application and allow users to download and use only the necessary parts of the application.

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.

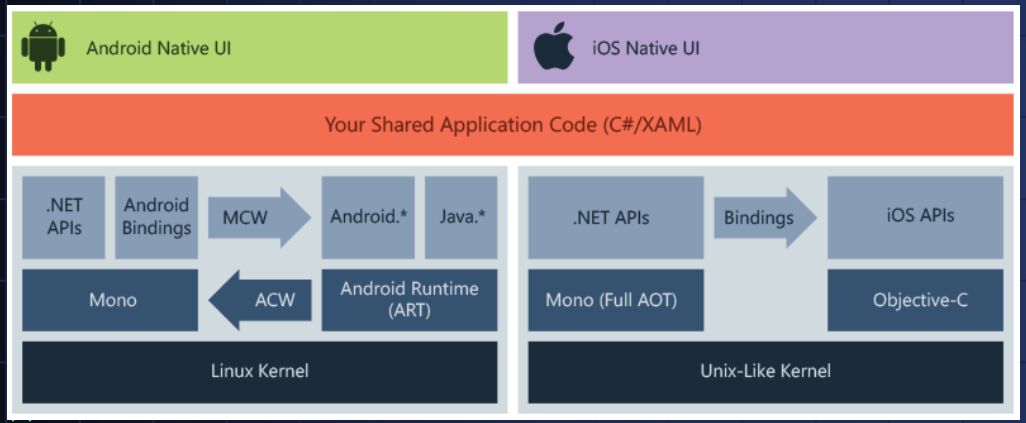
```
adb shell pm path com.package
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/base.apk
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/split_config.arm64_v8a.apk
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/split_config.en.apk
package:/data/app/com.package-NW8ZbgI5VPzvSZ1NgMa4CQ==/split_config.xxhdpi.apk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

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





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:

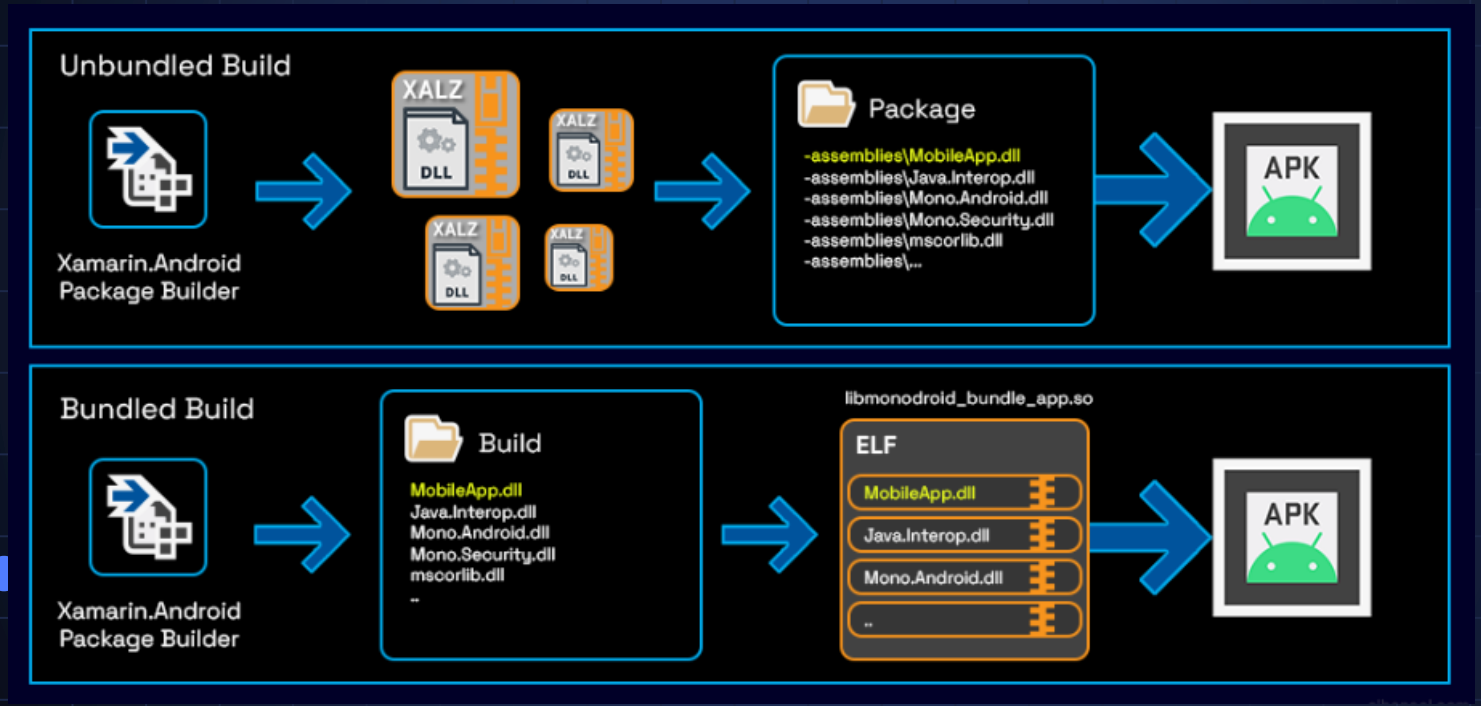
- Para la identificación de los componentes de aplicación en AndroidManifest.xml y Info.plist.
- Posible identificación de posibles secretos en otras partes de código.

ILSpy:

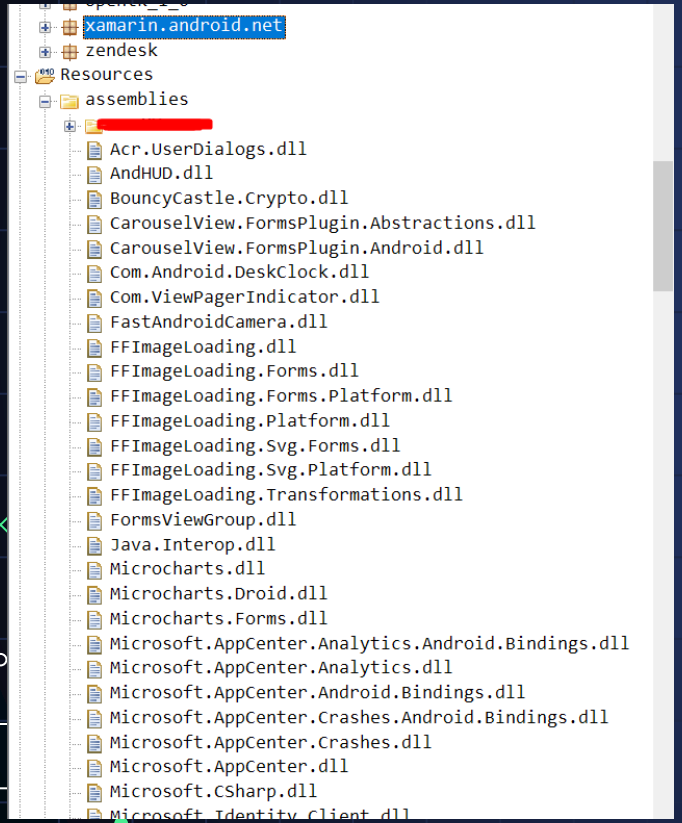
- Explorador y descompilador de ensamblados NET

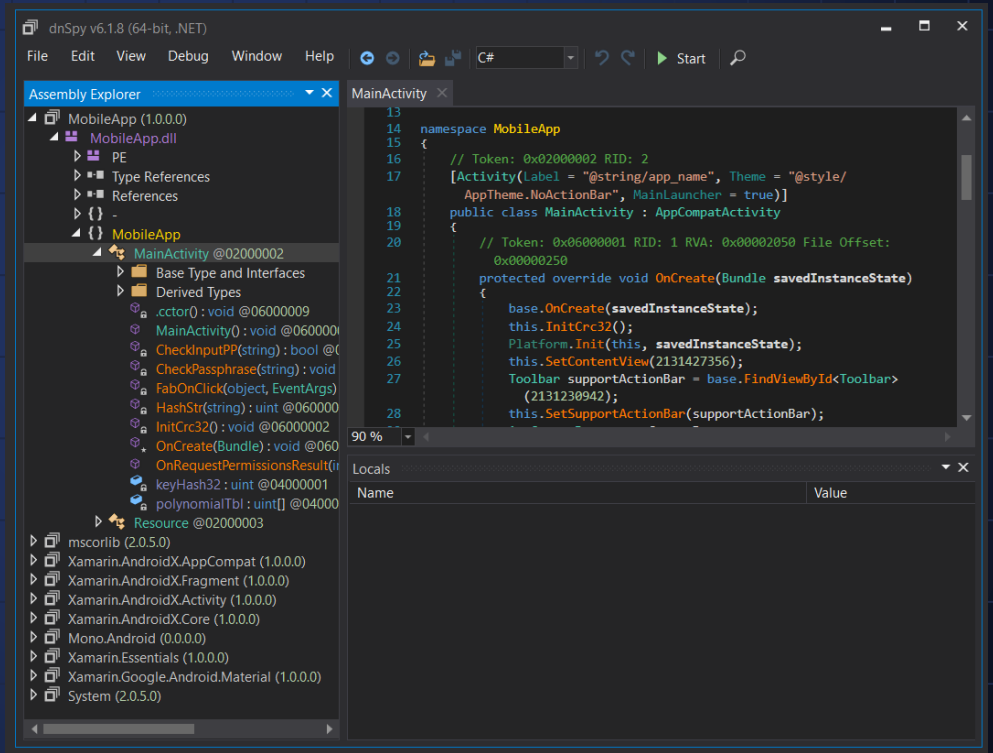
Métodos de compilación en Xamarim

WEBSEC

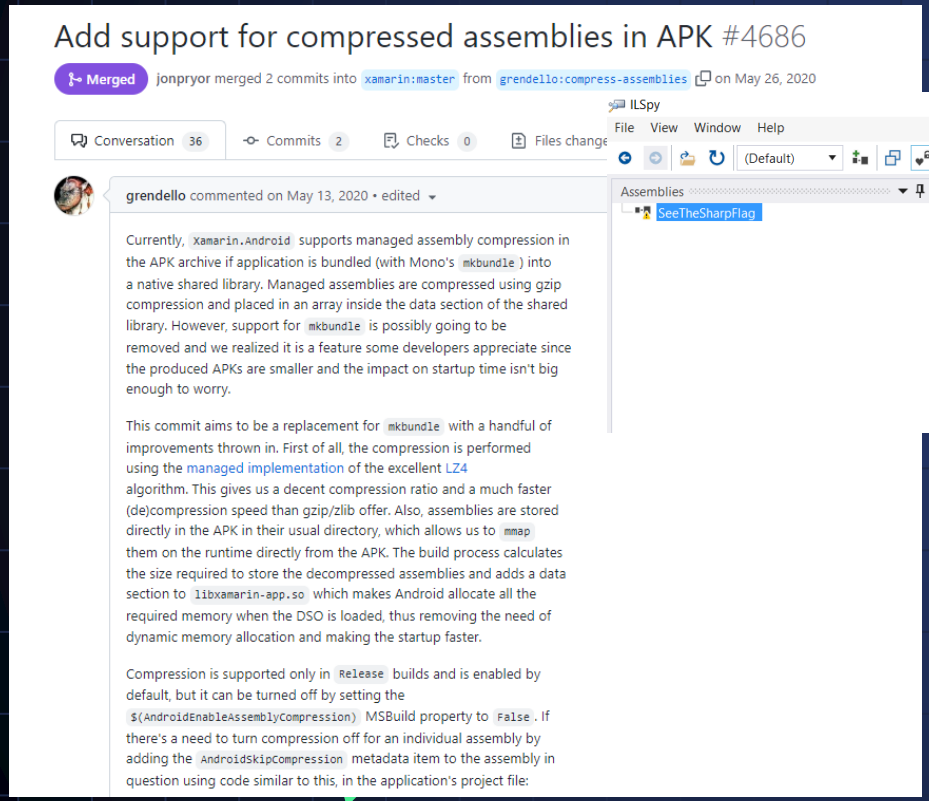


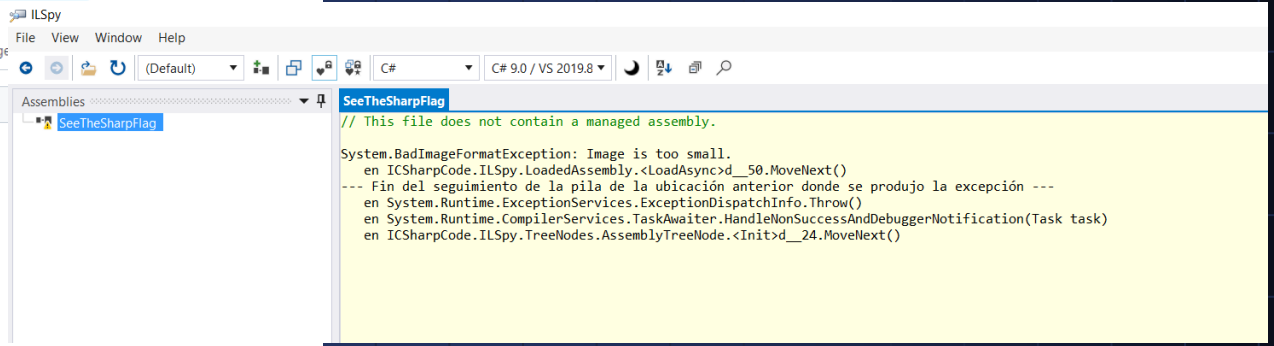
Análisis de Aplicativos – Unbundled Build V1





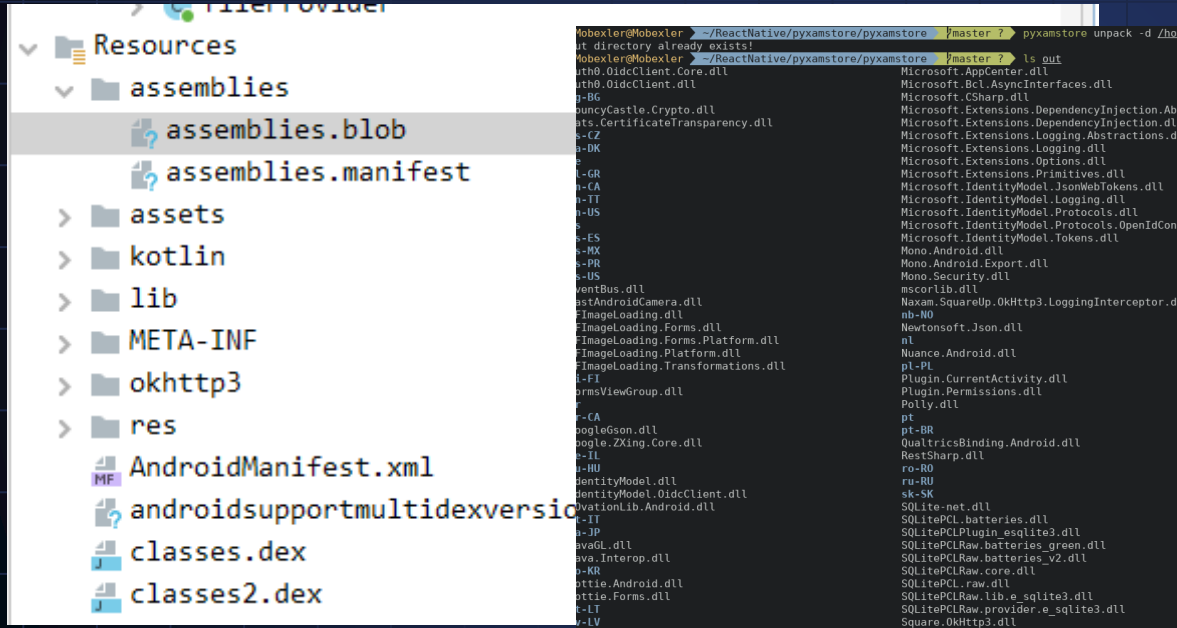
Análisis de Aplicativos – Unbundled Build V2





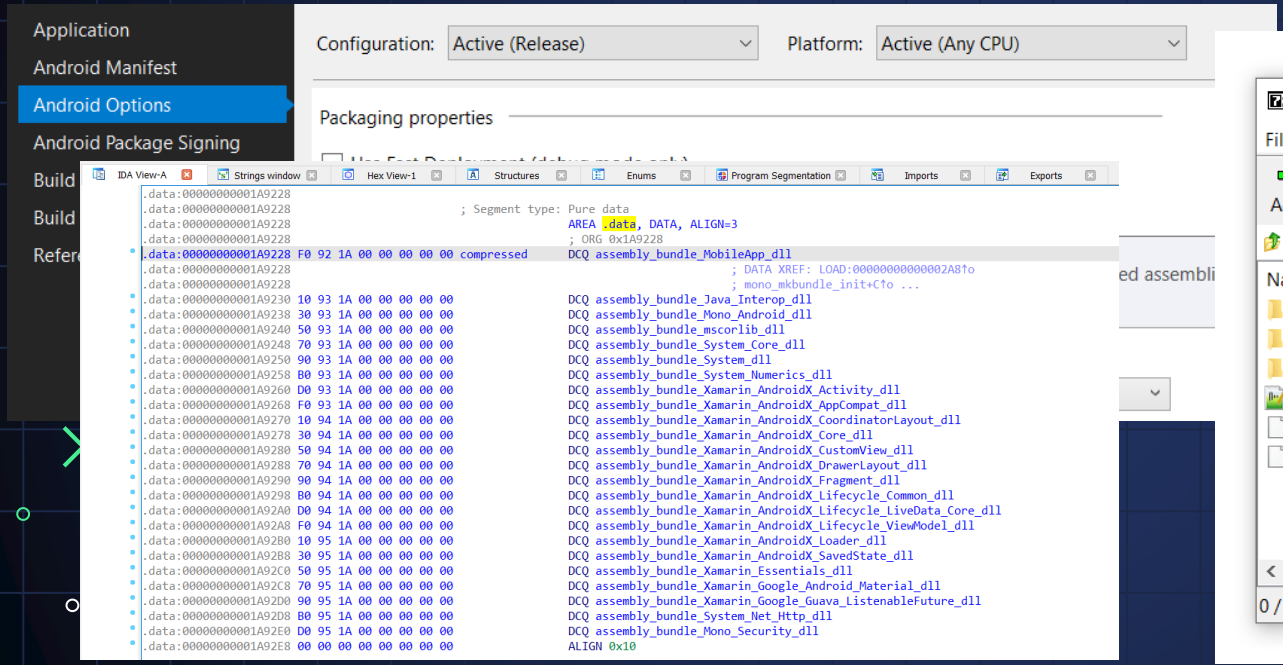
https://github.com/x41sec/tools/blob/master/Mobile/Xamarin/Xamarin_XALZ_decompress.py

Análisis de Aplicativos – Unbundled Build V3



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

Análisis de Aplicativos – Bundled Build



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

Análisis de Aplicativos - Bundled Build

```
Z>XamAsmUnZ.exe -elf                                    com.cihansol.mobileapp-packed\lib\arm64-v8a\libmonodroid_bundle_app.so
XamAsmUnZ
Author: Cihan

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: [12096]
GZData Size Uncompressed: [25600]

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

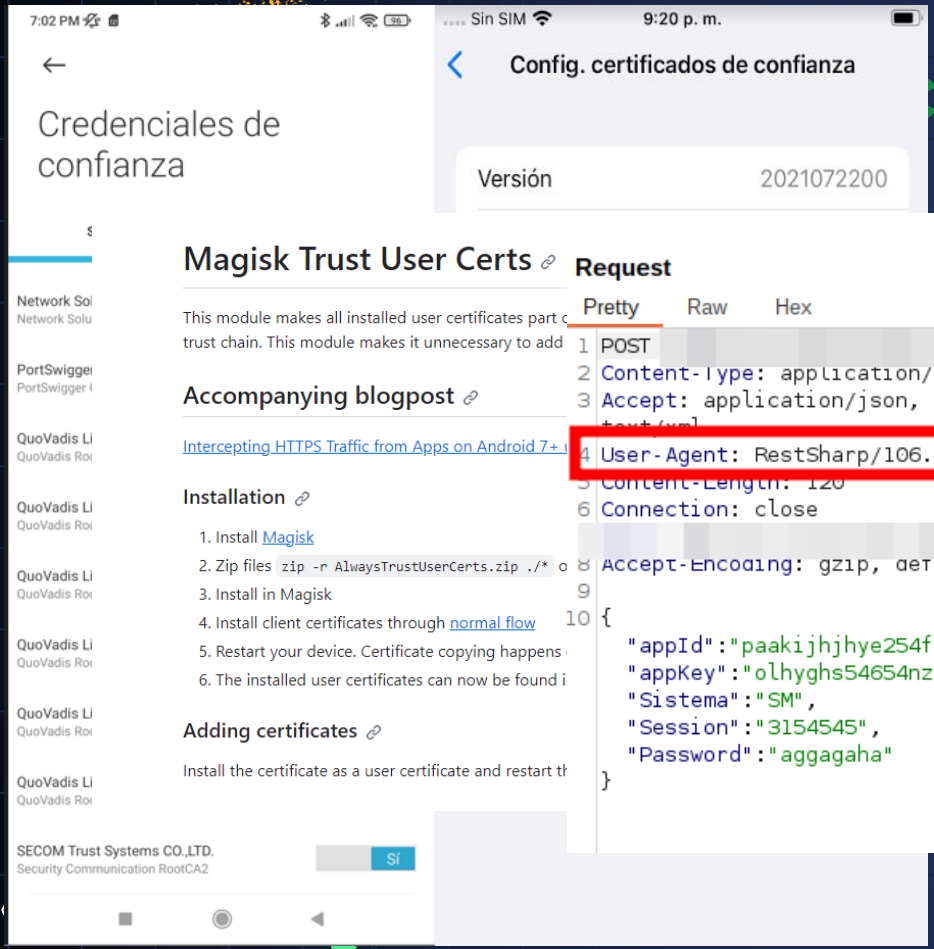
extracted_assemblies64

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.AndroidX.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.Cor...	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.AndroidX.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

...iones de Análisis



Magisk Trust User Certs

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

Accompanying blogpost

Intercepting HTTPS Traffic from Apps on Android 7+

Installation

1. Install Magisk
2. Zip files `zip -r AlwaysTrustUserCerts.zip ./*` o
3. Install in Magisk
4. Install client certificates through normal flow
5. Restart your device. Certificate copying happens
6. The installed user certificates can now be found i

Adding certificates

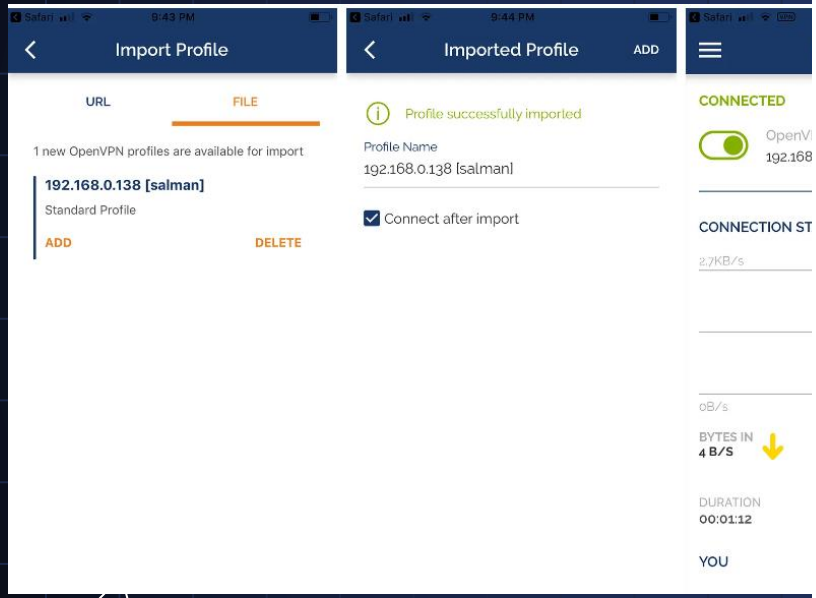
Install the certificate as a user certificate and restart th

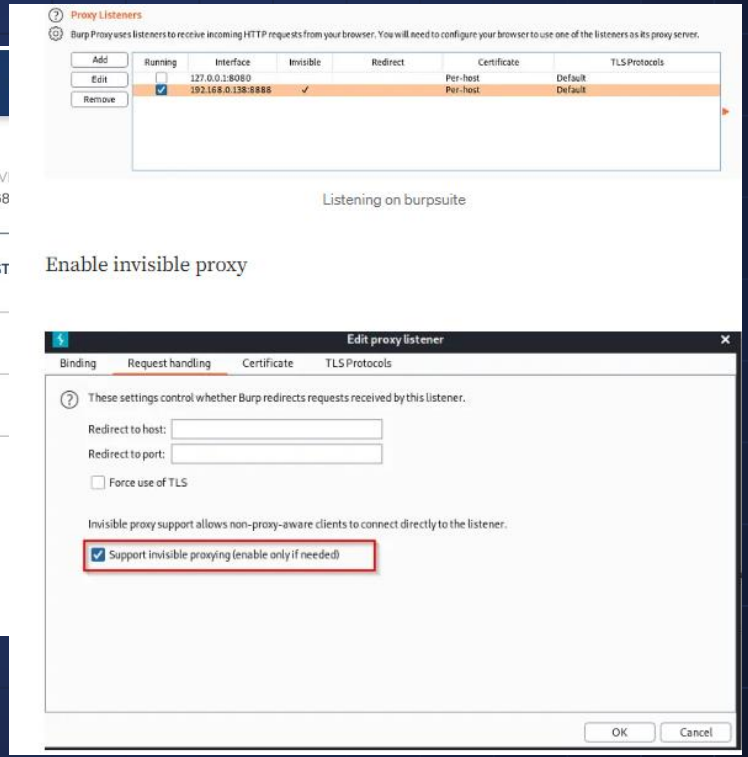
Request

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
8 Accept-Encoding: gzip, deflate, br
9
10 {
  "appId":"paakijhjhye254fdffg8",
  "appKey":"olhyghs54654nzqopio",
  "Sistema":"SM",
  "Session":"3154545",
  "Password":"aggagaha"
}
```

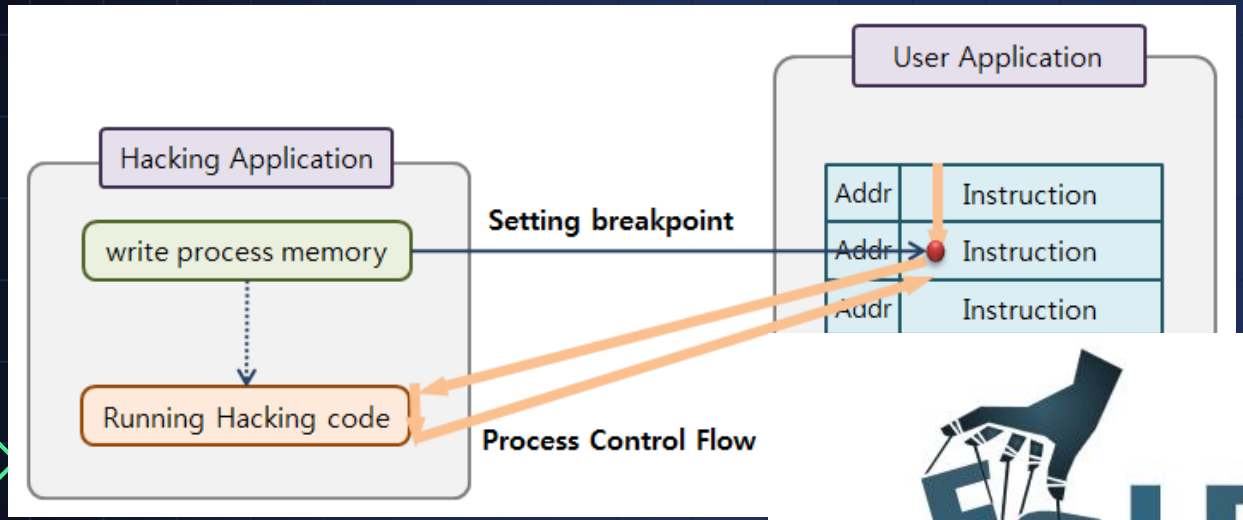
Consideraciones de Análisis





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

Consideraciones de Análisis



Mobile Helper Framework

```python
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"
        ]
    ),
```

```python
            "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=[
```

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	✅	✅	✅	❌	
Automaticall						
Extracts a						
Ex						
Detect if the resources are compressed.		❌	Hermes ✅	❌	❌	XALZ ✅
Detect if the app is split		❌	❌	❌	❌	❌

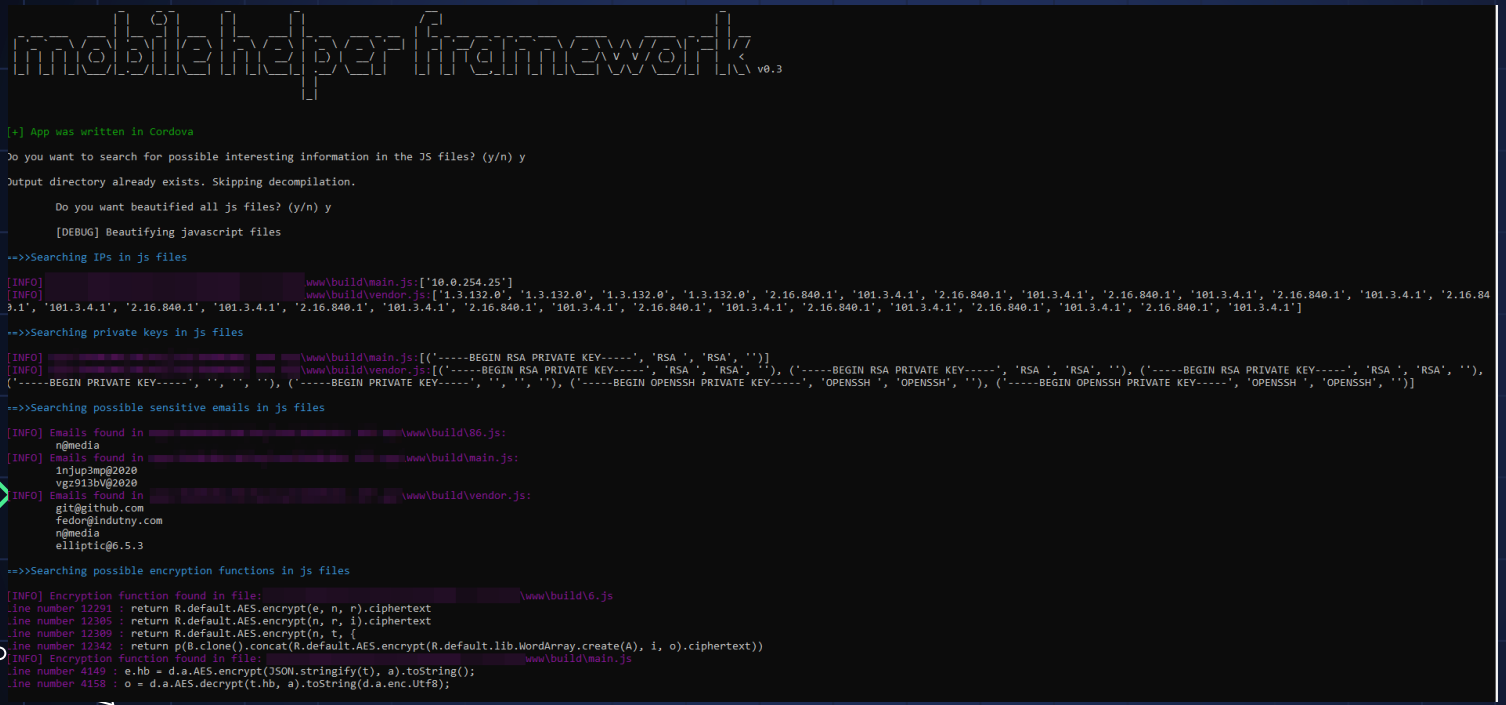
`Split APKs` is a technique used by Android to reduce the size of an application and allow users to download and use only the necessary parts of the application.

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

Ejemplo - Codova



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

==>>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\mcdonals_REACT\assets\index.android.bundle:["
```

Ejemplo - Xamarin


```
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
      Windo
      Windo
      Linux,

Possible main

DLL Compresed
```

```
[+] 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
AIRBUS A350-1000
1000
A350
git push
AIRBUS A350-1000
1000
A350
git add .

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

Exported Activities
com.pollocampero.pc_gt_mobile.MainActivity
org.apache.cordova.firebase.DynamicLinkActivity
com.facebook.CustomTabActivity

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

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

Exported Providers
com.facebook.FacebookContentProvider

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