



ASSIGNMENT 2

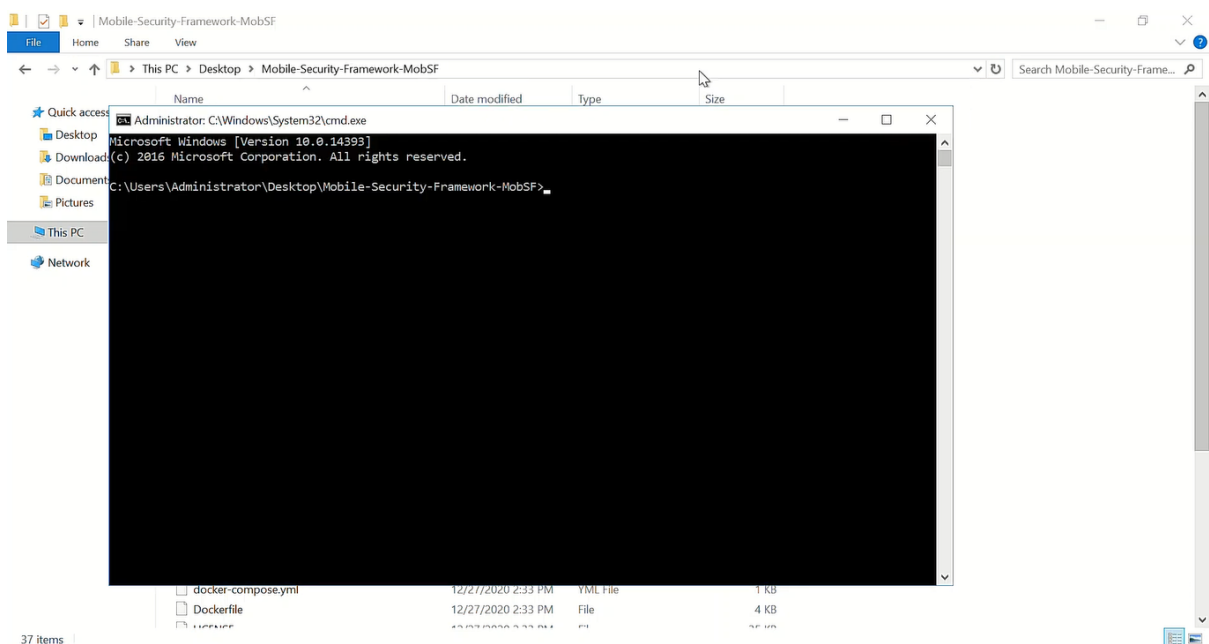
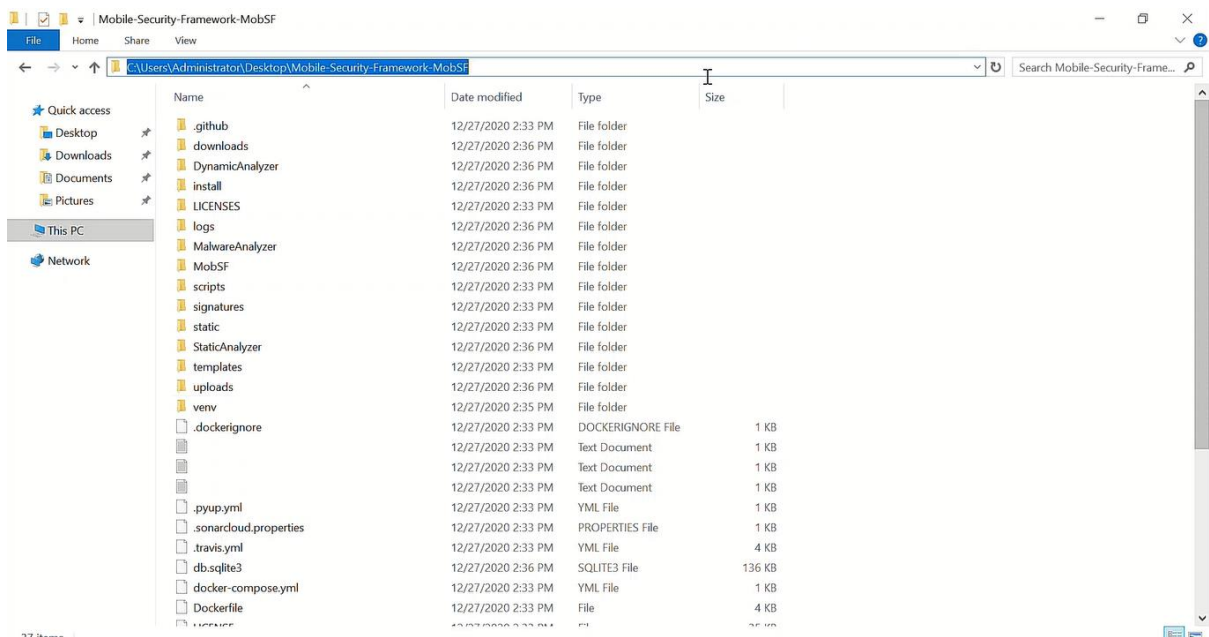
IE3112 - Mobile Security

Rodrigo K. A. M.
IT19001180

Part 01

STATIC AND DYNAMIC ANALYSIS OVER ANDROID PACKAGE FILE (APK)

Static Analysis

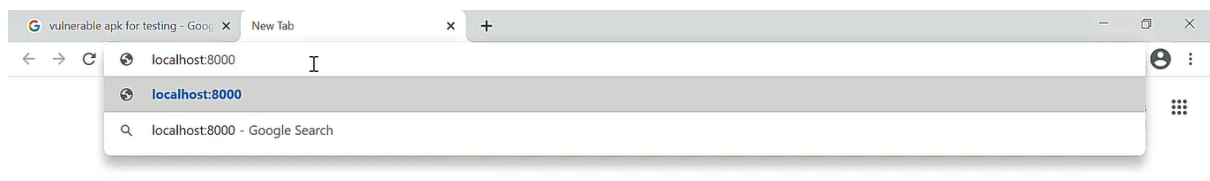


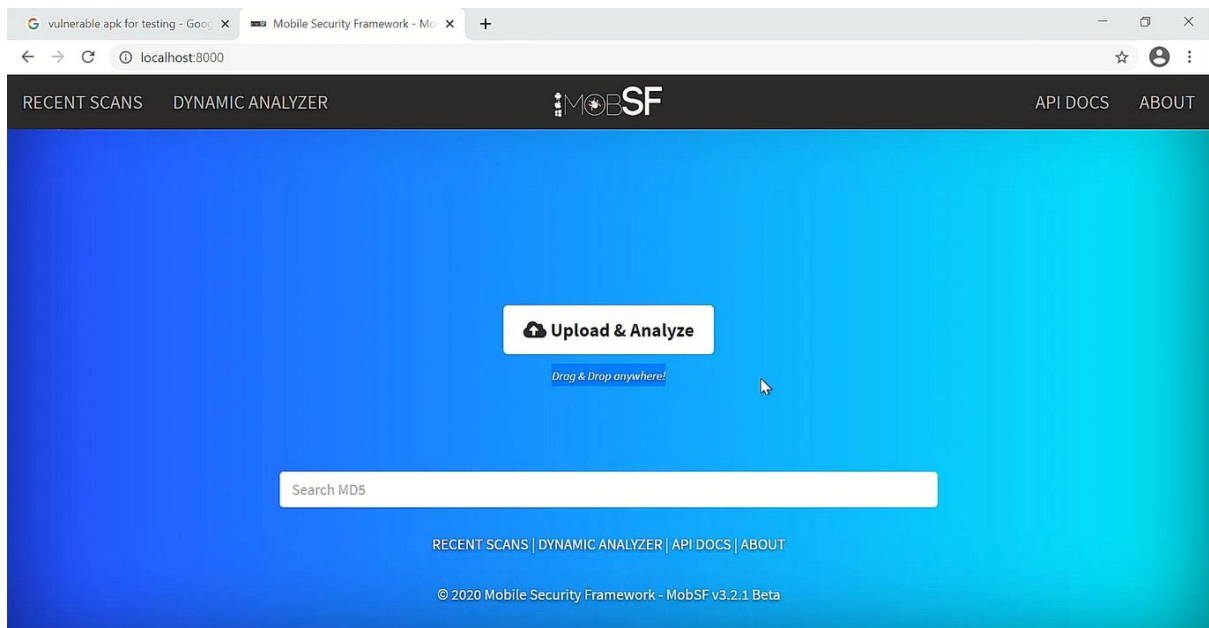
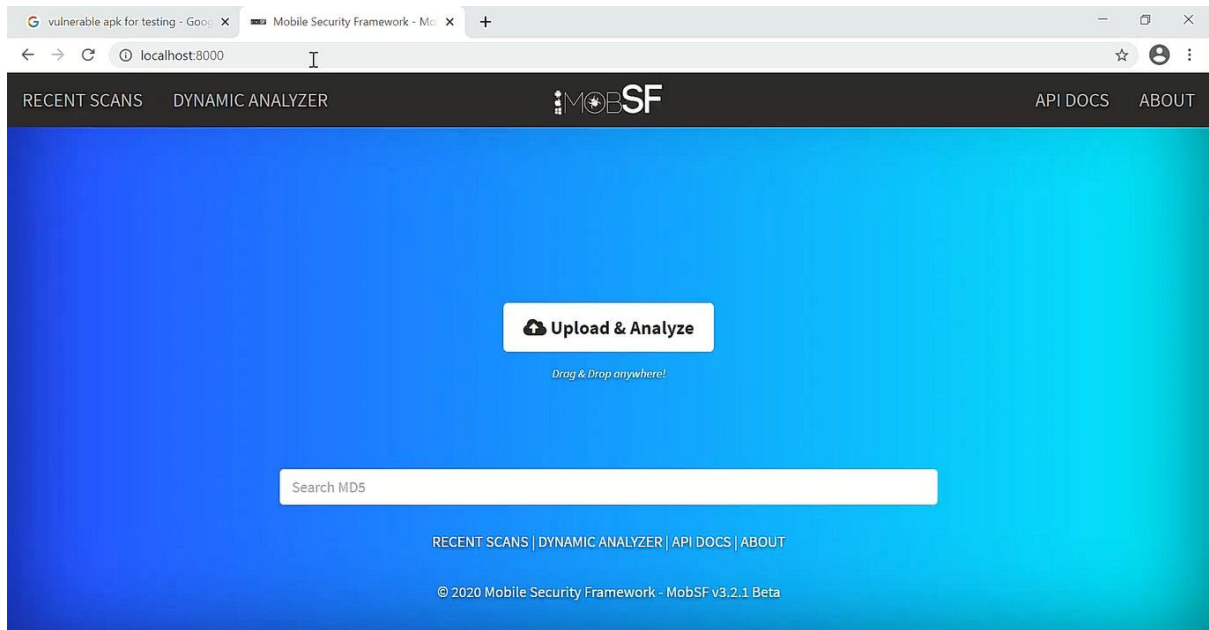
```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.


C:\Users\Administrator\Desktop\Mobile-Security-Framework-MobSF>run.bat
```

```
waitress-serve --listen="0.0.0.0:8000" --threads=10 --channel-timeout=3600 MobSF.wsgi:application
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop\Mobile-Security-Framework-MobSF>run.bat
Serving on http://EC2AMAZ-S02IE47:8000
```







PENTESTER LAND
OFFENSIVE INFOSEC

- Home
- AMA
- Challenges
- Cheatsheets
- Conference notes
- The 5 Hacking NewsLetter
- The Bug Hunter Podcast
- Tips & Tricks


List of intentionally vulnerable Android apps

12 Oct 2018 • [Cheatsheets](#)

This is just a quick blog post to share a list of intentionally vulnerable Android apps that you can use for training. Some are less known than others and I had to dig a little to find them (especially the new ones), so I'm sharing them in case you want to work on your mobile hacking skills.

They are sorted by "last update" date:

App	Last updated	Type of app	Vulnerabilities (not exhaustive)
Android InsecureBankv2	Oct 01,	Web &	Broken crypto Insecure data storage Poor authentication Untrusted input Reverse engineering




PENTESTER LAND
OFFENSIVE INFOSEC

- Home
- AMA
- Challenges
- Cheatsheets
- Conference notes
- The 5 Hacking NewsLetter
- The Bug Hunter Podcast
- Tips & Tricks

App	Last updated	Type of app	Vulnerabilities (not exhaustive)
Android InsecureBankv2	Jul 15, 2018	Native (Java)	<ul style="list-style-type: none"> Weak authorization mechanism Local Encryption issues Vulnerable Activity Components Root Detection and Bypass Emulator Detection and Bypass Insecure Content Provider access Insecure Webview implementation Weak Cryptography implementation Application Patching Sensitive Information in Memory Insecure Logging mechanism Android Pasteboard vulnerability Application Debuggable Android keyboard cache issues Android Backup vulnerability Runtime Manipulation Insecure SDCard storage Insecure HTTP connections Parameter Manipulation Hardcoded secrets Username Enumeration issue Developer Backdoors Weak change password implementation

pentester.land/cheatsheets/2018/10/12/list-of-intentionally-vulnerable-android-apps.html



PENTESTER LAND
OFFENSIVE INFOSEC

- Home
- AMA
- Challenges
- Cheatsheets
- Conference notes
- The 5 Hacking NewsLetter
- The Bug Hunter Podcast
- Tips & Tricks

App Name	Date	Platform	Vulnerabilities
Android InsecureBankv2	Jul 15, 2018	Native (Java)	<ul style="list-style-type: none"> Weak Authorization mechanism Local Encryption issues Vulnerable Activity Components Root Detection and Bypass Emulator Detection and Bypass Insecure Content Provider access Insecure Webview implementation Weak Cryptography implementation Application Patching Sensitive Information in Memory Insecure Logging mechanism Android Pasteboard vulnerability Application Debuggable Android keyboard cache issues Android Backup vulnerability Runtime Manipulation Insecure SDCard storage Insecure HTTP connections Parameter Manipulation Hardcoded secrets Username Enumeration issue Developer Backdoors Weak change password implementation

github.com/dineshshetty/Android-InsecureBankv2

Why GitHub? Team Enterprise Explore Marketplace Pricing

Search Sign in Sign up

dineshshetty / Android-InsecureBankv2

Watch 47 Star 789 Fork 276

Code Issues 5 Pull requests 2 Actions Projects Security Insights

master 1 branch 4 tags

Go to file Code

dineshshetty Merge pull request #19 from ronaldyho/patch-1 3c8cc3a on Nov 21, 2019 82 commits

File	Commit Message	Time
.idea	Updated attacker apps to Android 3.1.3	3 years ago
AndroLabServer	Merge pull request #19 from ronaldyho/patch-1	13 months ago
InsecureBankv2	Updated apk file	2 years ago
Spoilers	Updated Code	6 years ago
Walkthroughs	Added additional steps (Thank you bugwrangler@git)	4 years ago
wip-attackercode	Updated attacker apps to Android 3.1.3	3 years ago
.gitignore	updated .gitignore	4 years ago
InsecureBankv2.apk	Updated apk file	2 years ago

About

Vulnerable Android application for developers and security enthusiasts to learn about Android insecurities

Readme

MIT License

Releases 4

2.3.1 Latest on Mar 5, 2019

+ 3 releases

github.com/dineshshetty/Android-InsecureBankv2/releases

File/Folder	Description	Updated
.idea	Updated attacker apps to Android 3.1.3	3 years ago
AndroLabServer	Merge pull request #19 from ronaldyho/patch-1	13 months ago
InsecureBankv2	Updated apk file	2 years ago
Spoilers	Updated Code	6 years ago
Walkthroughs	Added additional steps (Thank you bugwrangler@git	4 years ago
wip-attackercode	Updated attacker apps to Android 3.1.3	3 years ago
.gitignore	updated .gitignore	4 years ago
InsecureBankv2.apk	Updated apk file	2 years ago
LICENSE	Minor Updates	6 years ago
README.markdown	Updated python note	2 years ago
Thumbs.db	updated code files	6 years ago
Usage Guide.pdf	Updated Guide	2 years ago

learn about Android insecurities

- Readme
- MIT License

Releases 4

2.3.1 **Latest**
on Mar 5, 2019

[+ 3 releases](#)

Packages

No packages published

Contributors 3

- dineshshetty Dinesh Shetty
- anantshri Anant Shrivastava
- ronaldyho Dark Cowling

README.markdown

InsecureBankv2 Readme

github.com/dineshshetty/Android-InsecureBankv2/releases

dineshshetty / Android-InsecureBankv2

Watch 47 Star 789 Fork 276

Code Issues 5 Pull requests 2 Actions Projects Security Insights

Releases Tags

Latest release

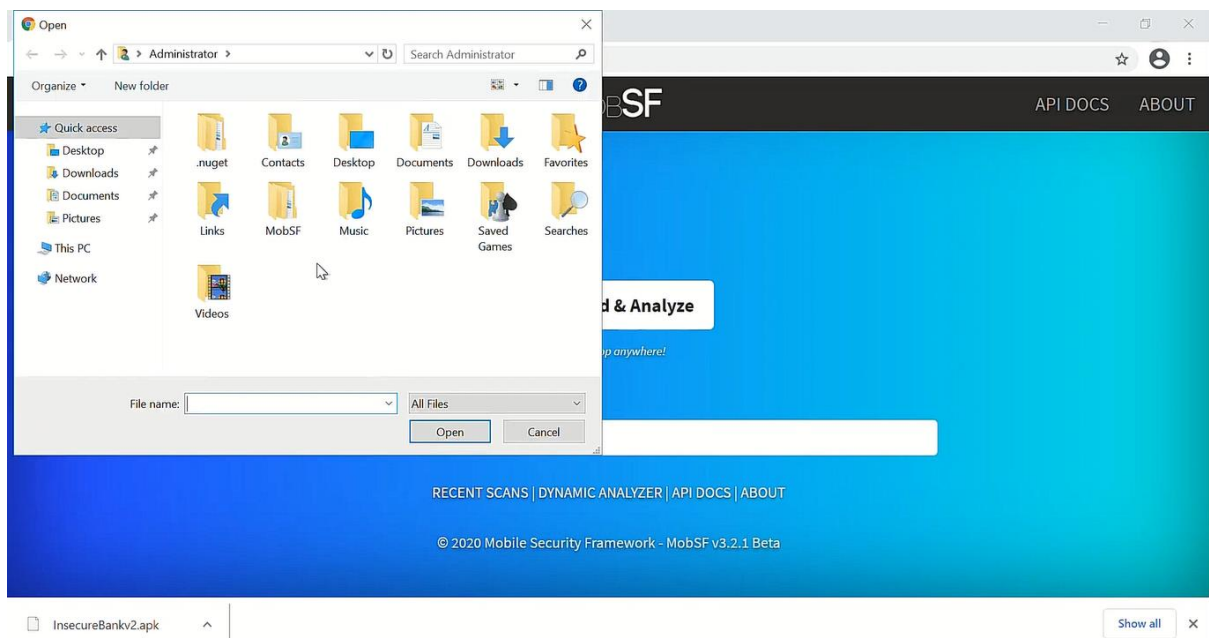
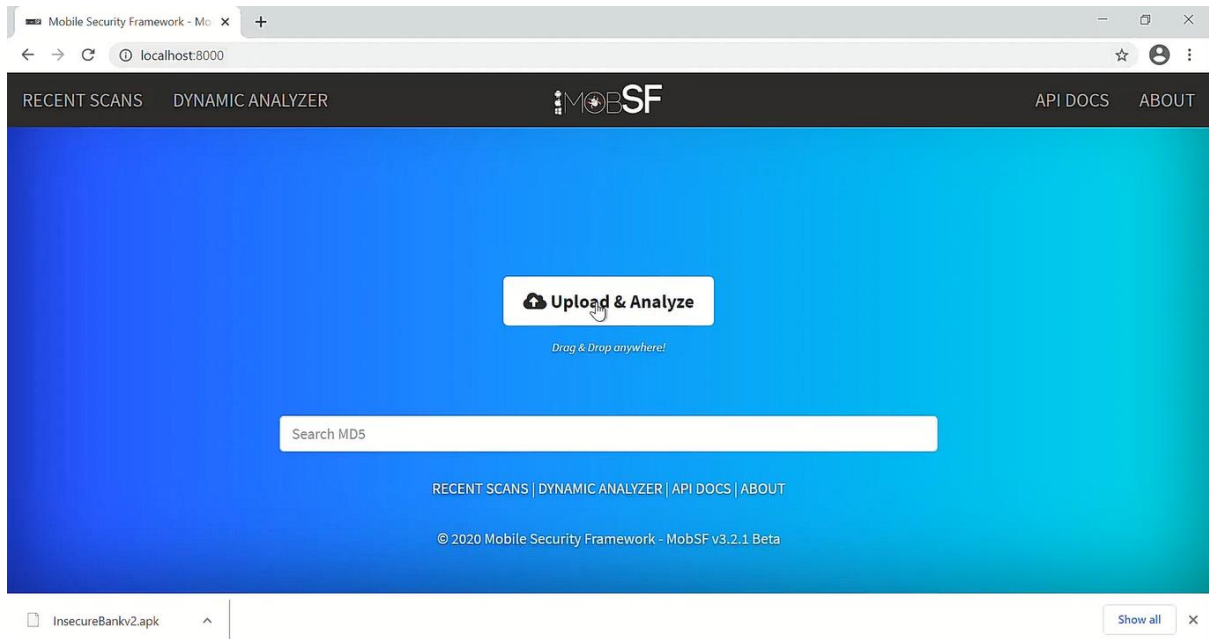
2.3.1
7f1ec32

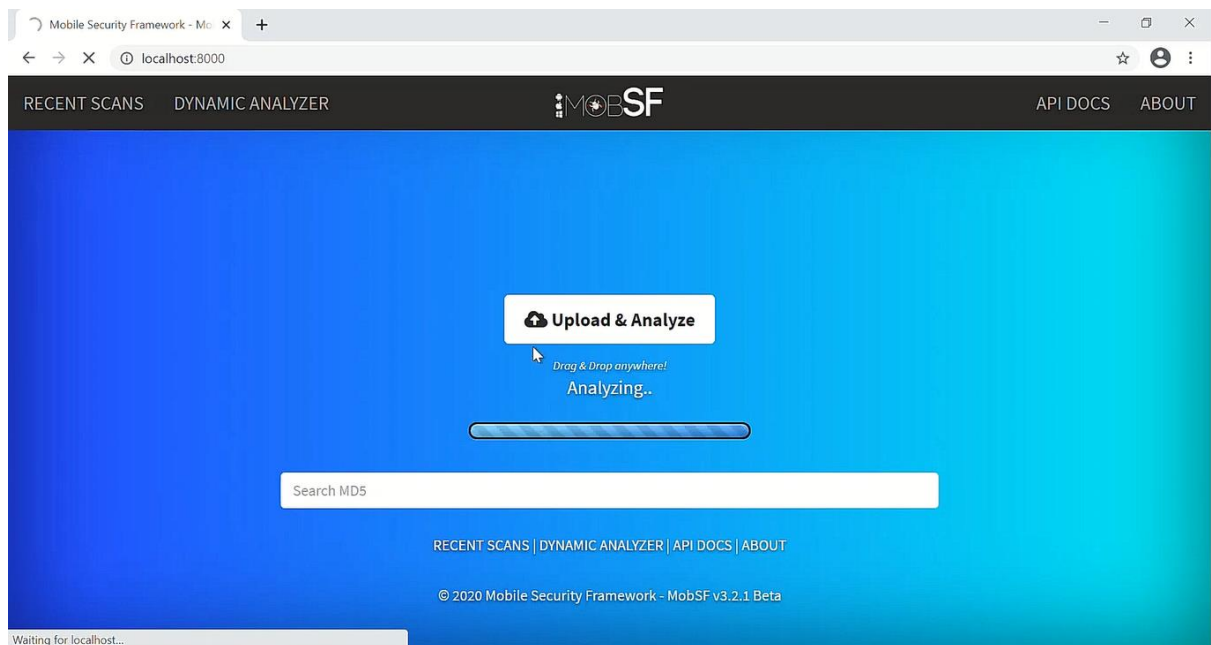
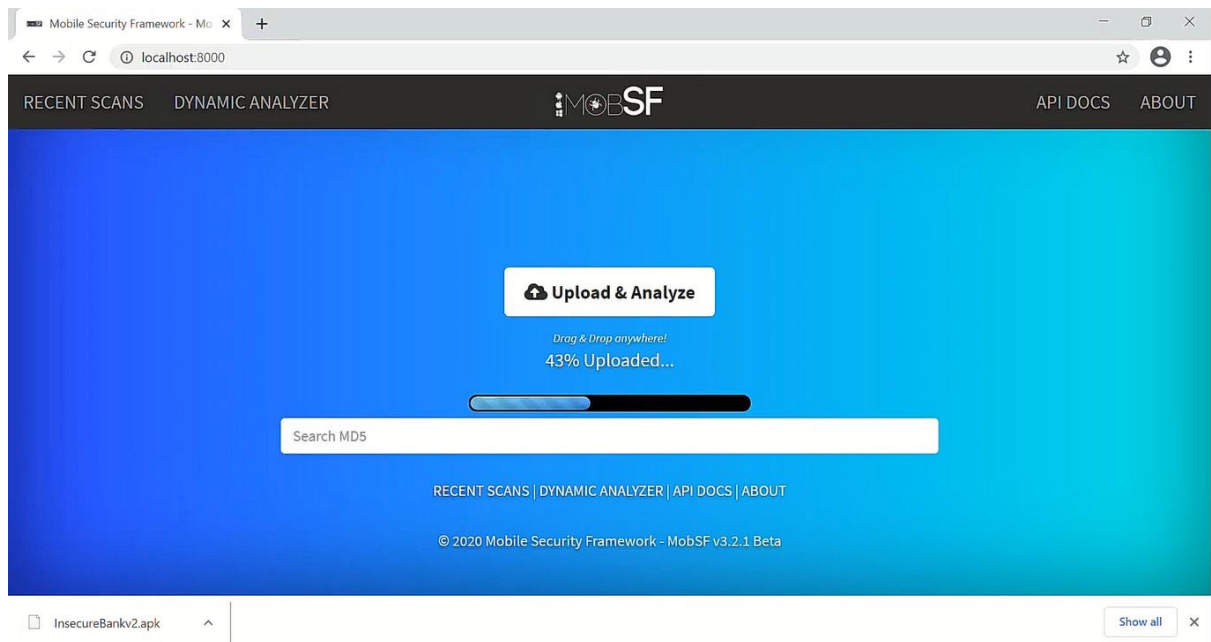
2.3.1
dineshshetty released this on Mar 5, 2019 - 8 commits to master since this release

Updated Code to work with AndroidStudio 3.3.2

Assets 4

- AndroLabServer.zip 8.66 KB
- InsecureBankv2.apk 3.3 MB
- Source code (zip)
- Source code (tar.gz)





```
waitress-serve --listen="0.0.0.0:8000" --threads=10 --channel-timeout=3600 MobSF.wsgiapplication
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\Desktop\Mobile-Security-Framework-MobSF>run.bat
Serving on http://EC2AMAZ-SD2IE47:8000

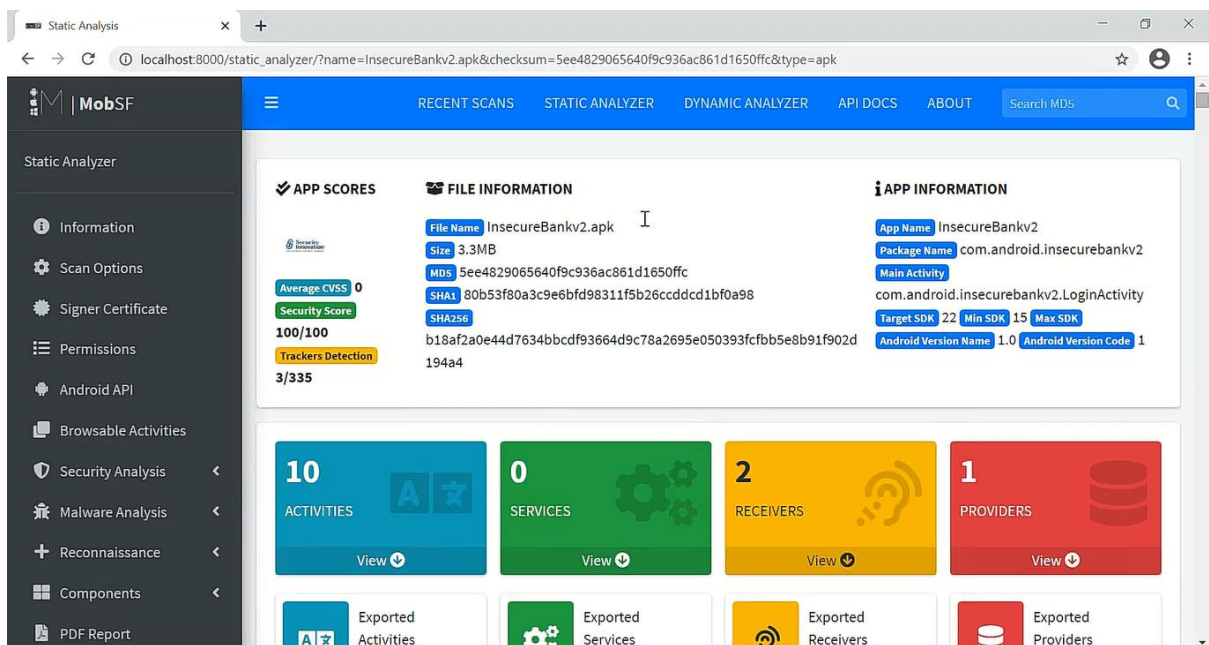
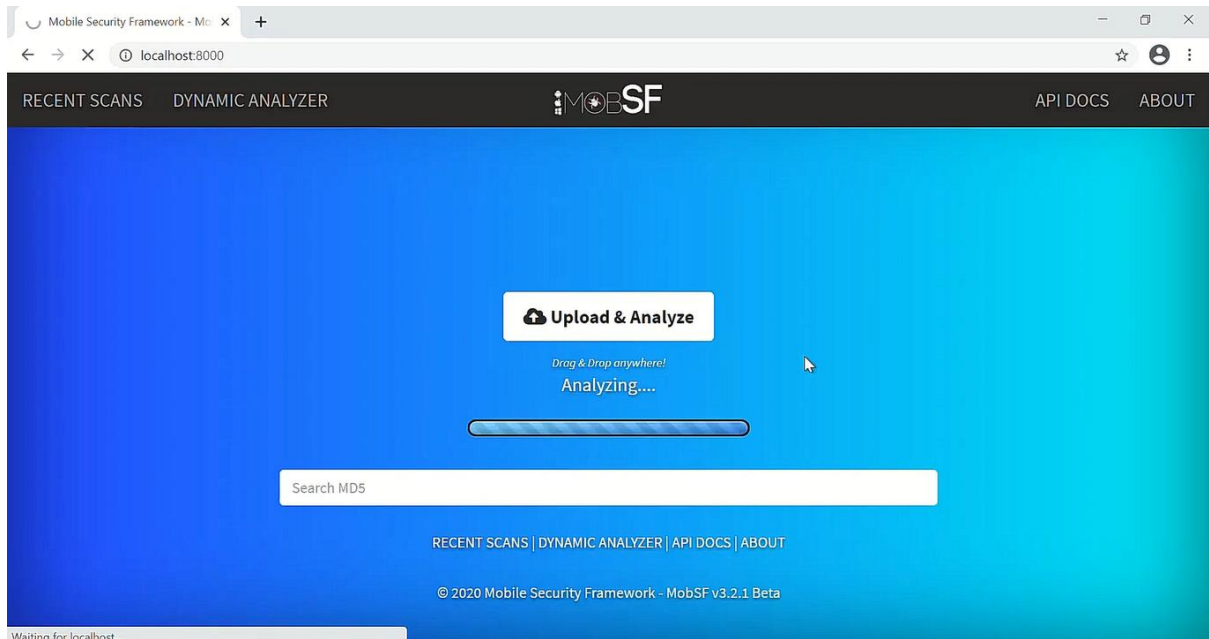
MobSF 3.2

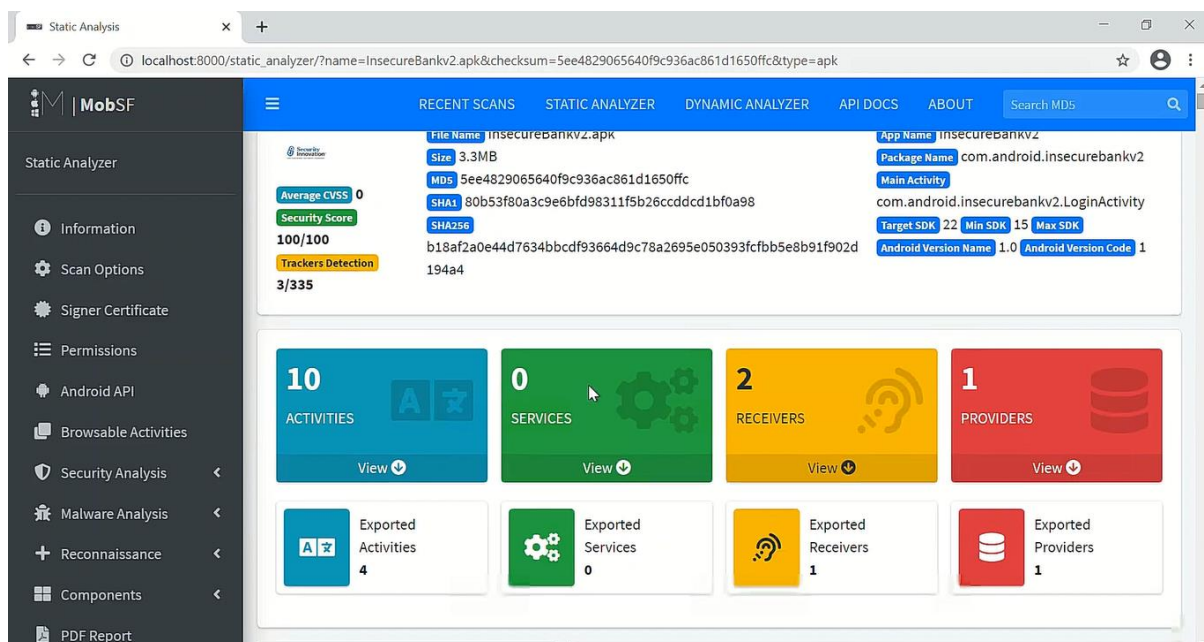
[INFO] 27/Dec/2020 14:39:33 - Mobile Security Framework v3.2.1 Beta
REST API Key: 870772acc6ea349893d4e221fa33caef4eafce04cdaa1ead2967dd52d94a66ea
[INFO] 27/Dec/2020 14:39:33 - OS: Windows
[INFO] 27/Dec/2020 14:39:33 - Platform: Windows-10-10.0.14393-SP0
[INFO] 27/Dec/2020 14:39:33 - Dist:
[INFO] 27/Dec/2020 14:39:33 - MobSF Basic Environment Check
[WARNING] 27/Dec/2020 14:39:33 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic Analysis.
[INFO] 27/Dec/2020 14:39:33 - Checking for Update.
[INFO] 27/Dec/2020 14:39:33 - No updates available.
[INFO] 27/Dec/2020 14:41:04 - MIME Type: application/vnd.android.package-archive FILE: insecurebankv2.apk
[INFO] 27/Dec/2020 14:41:04 - Performing Static Analysis of Android APK
[INFO] 27/Dec/2020 14:41:04 - Starting Analysis on : InsecureBankv2.apk
[INFO] 27/Dec/2020 14:41:04 - Generating Hashes
[INFO] 27/Dec/2020 14:41:04 - Unzipping
[INFO] 27/Dec/2020 14:41:04 - APK Extracted
[INFO] 27/Dec/2020 14:41:04 - Getting Hardcoded Certificates/Keystores
[INFO] 27/Dec/2020 14:41:04 - Getting AndroidManifest.xml from APK
[INFO] 27/Dec/2020 14:41:04 - Converting AXML to XML
[INFO] 27/Dec/2020 14:41:18 - Parsing AndroidManifest.xml
[INFO] 27/Dec/2020 14:41:18 - Fetching icon path
[INFO] 27/Dec/2020 14:41:19 - Extracting Manifest Data
[INFO] 27/Dec/2020 14:41:19 - Fetching Details from Play Store: com.android.insecurebankv2
[INFO] 27/Dec/2020 14:41:19 - Manifest Analysis Started
[INFO] 27/Dec/2020 14:41:19 - Binary Analysis Started
[INFO] 27/Dec/2020 14:41:19 - Reading Code Signing Certificate
[INFO] 27/Dec/2020 14:41:19 - Running APKID 2.1.1
[INFO] 27/Dec/2020 14:41:22 - Trackers Database is up-to-date
[INFO] 27/Dec/2020 14:41:22 - Detecting Trackers
```

```
waitress-serve --listen="0.0.0.0:8000" --threads=10 --channel-timeout=3600 MobSF.wsgiapplication
C:\Users\Administrator\Desktop\Mobile-Security-Framework-MobSF>run.bat
Serving on http://EC2AMAZ-SD2IE47:8000

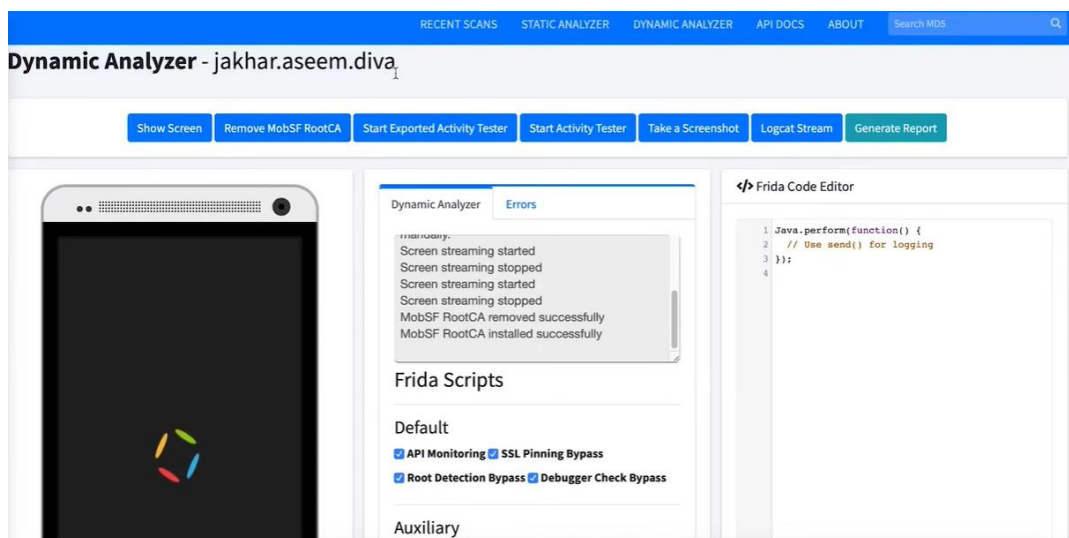
MobSF 3.2

[INFO] 27/Dec/2020 14:39:33 - Mobile Security Framework v3.2.1 Beta
REST API Key: 870772acc6ea349893d4e221fa33caef4eafce04cdaa1ead2967dd52d94a66ea
[INFO] 27/Dec/2020 14:39:33 - OS: Windows
[INFO] 27/Dec/2020 14:39:33 - Platform: Windows-10-10.0.14393-SP0
[INFO] 27/Dec/2020 14:39:33 - Dist:
[INFO] 27/Dec/2020 14:39:33 - MobSF Basic Environment Check
[WARNING] 27/Dec/2020 14:39:33 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic Analysis.
[INFO] 27/Dec/2020 14:39:33 - Checking for Update.
[INFO] 27/Dec/2020 14:39:33 - No updates available.
[INFO] 27/Dec/2020 14:41:04 - MIME Type: application/vnd.android.package-archive FILE: insecurebankv2.apk
[INFO] 27/Dec/2020 14:41:04 - Performing Static Analysis of Android APK
[INFO] 27/Dec/2020 14:41:04 - Starting Analysis on : InsecureBankv2.apk
[INFO] 27/Dec/2020 14:41:04 - Generating Hashes
[INFO] 27/Dec/2020 14:41:04 - Unzipping
[INFO] 27/Dec/2020 14:41:04 - APK Extracted
[INFO] 27/Dec/2020 14:41:04 - Getting Hardcoded Certificates/Keystores
[INFO] 27/Dec/2020 14:41:04 - Getting AndroidManifest.xml from APK
[INFO] 27/Dec/2020 14:41:04 - Converting AXML to XML
[INFO] 27/Dec/2020 14:41:18 - Parsing AndroidManifest.xml
[INFO] 27/Dec/2020 14:41:18 - Fetching icon path
[INFO] 27/Dec/2020 14:41:19 - Extracting Manifest Data
[INFO] 27/Dec/2020 14:41:19 - Fetching Details from Play Store: com.android.insecurebankv2
[INFO] 27/Dec/2020 14:41:19 - Manifest Analysis Started
[INFO] 27/Dec/2020 14:41:19 - Binary Analysis Started
[INFO] 27/Dec/2020 14:41:19 - Reading Code Signing Certificate
[INFO] 27/Dec/2020 14:41:19 - Running APKID 2.1.1
[INFO] 27/Dec/2020 14:41:22 - Trackers Database is up-to-date
[INFO] 27/Dec/2020 14:41:22 - Detecting Trackers
[INFO] 27/Dec/2020 14:41:25 - APK -> JAVA
[INFO] 27/Dec/2020 14:41:25 - Decompiling to Java with jadx
```



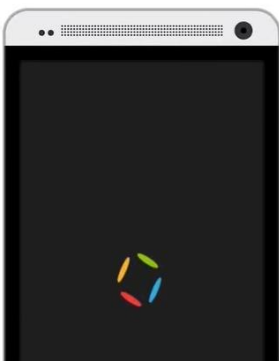


Dynamic Analysis



Dynamic Analyzer - jakhar.aseem.diva

Show Screen
Remove MobSF RootCA
Start Exported Activity Tester
Start Activity Tester
Take a Screenshot
Logcat Stream
Generate Report



Dynamic AnalyzerErrors

Screen streaming stopped
Screen streaming started
Screen streaming stopped
MobSF RootCA removed successfully
MobSF RootCA installed successfully
Starting Exported Activity tester...

Frida Scripts

Default
☒ API Monitoring
☒ SSL Pinning Bypass
☒ Root Detection Bypass
☒ Debugger Check Bypass

Auxiliary

Frida Code Editor

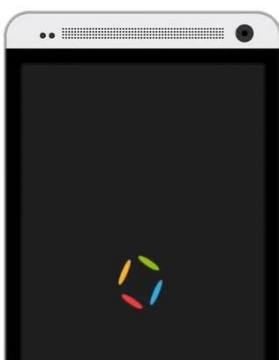
```

1 Java.perform(function() {
2   // Use send() for logging
3 });
4

```

Dynamic Analyzer - jakhar.aseem.diva

Show Screen
Remove MobSF RootCA
Start Exported Activity Tester
Start Activity Tester
Take a Screenshot
Logcat Stream
Generate Report



Dynamic AnalyzerErrors

Screen streaming stopped
Screen streaming started
Screen streaming stopped
MobSF RootCA removed successfully
MobSF RootCA installed successfully
Starting Exported Activity tester...
Exported Activity testing completed.

Frida Scripts

Default
☒ API Monitoring
☒ SSL Pinning Bypass
☒ Root Detection Bypass
☒ Debugger Check Bypass

Auxiliary

Frida Code Editor

```

1 Java.perform(function() {
2   // Use send() for logging
3 });
4

```

Frida Logs - jakhar.aseem.diva

Data refreshed in every 10 seconds.

```

Loaded Frida Script - ssl_pinning_bypass
Loaded Frida Script - api_monitor
Loaded Frida Script - root_bypass
Loaded Frida Script - debugger_check_bypass
[SSL Pinning Bypass] ConscryptFileDescriptorSocket.verifyCertificateChain() not found
[SSL Pinning Bypass] okhttp CertificatePinner not found
[SSL Pinning Bypass] okhttp CertificatePinner not found
[SSL Pinning Bypass] DataTheorem trustkit not found
[SSL Pinning Bypass] Appcelerator PinningTrustManager not found
[SSL Pinning Bypass] Apache Cordova SSLCertificateChecker not found
[SSL Pinning Bypass] Wultra CertStore.validateFingerprint not found
[API Monitor] Cannot find com.android.okhttp.internal.http.HttpURLConnectionImpl.getInputStream

```

100

android.app.Activity.startActivity(Activity.java:4475)

```

[*] java.lang.reflect.TypeVariable
[*] android.text.TextUtils$TruncateAt
[*] java.lang.ref.SoftReference
[*] java.io.File$PathStatus
[*] java.util.logging.Handler
[*] android.view.Choreographer$CallbackQueue
[*] java.io.File
[*] android.content.pm.FeatureGroupInfo
[*] sun.util.logging.PlatformLogger$Level
[*] javax.crypto.Cipher$NeedToSet
[*] android.icu.text.DateFormatSymbols$CapitalizationContextUsage
[*] java.lang.String
[*] android.widget.TextView$ChangeWatcher
[*] sun.security.x509.NetscapeCertTypeExtension$MapEntry
[*] java.lang.Void
[*] android.net.Network
[*] android.os.PatternMatcher
[*] android.graphics.PorterDuff$Mode
[*] android.os.MessageQueue$IdleHandler
[*] java.util.concurrent.TimeUnit
[*] android.text.InputFilter
[*] android.icu.impl.UCharacterProperties$BinaryProperty
[*] java.security.cert.X509Certificate
[*] java.lang.annotation.Annotation
[*] android.graphics.Bitmap$Config
[*] android.content.pm.Signature
[*] java.lang.reflect.Type
[*] sun.security.pkcs.SignerInfo
[*] javax.security.cert.X509Certificate
[*] com.android.org.conscrypt.OpenSSLX509CertPath$Encoding
[*] android.graphics.Paint$Style
[*] java.text.DateFormatsField

```

Dynamic Analyzer

Information

Frida API Monitor

Binder

Device Data

Exported Activity Tester

Activity Tester

Screenshots

Malware Analysis

Reconnaissance

File Analysis

Download / Print Report

BINDER

Search:

CLASS	METHOD
android.app.Activity	startActivity Arguments: [{"handle": "0x1008fe", "weakRef": 1170}, None] Called From: android.app.Activity.startActivity(Activity.java:4475)
android.app.Activity	startActivity Arguments: [{"handle": "0x2008f2", "weakRef": 1168}] Called From: jakhar.aseem.diva.MainActivity.startChallenge(MainActivity.java:50)
android.app.Activity	startActivity Arguments: [{"handle": "0x20096e", "weakRef": 1465}, None] Called From: android.app.Activity.startActivity(Activity.java:4475)
android.app.Activity	startActivity

Dynamic Analyzer

Information

Frida API Monitor

Binder

Device Data

Exported Activity Tester

Activity Tester

Screenshots

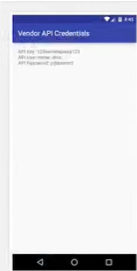
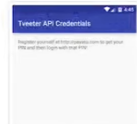
Malware Analysis

Reconnaissance

File Analysis

Download / Print Report

EXPORTED ACTIVITY TESTER

	jakhar.aseem.diva.APICredsActivity
	jakhar.aseem.diva.APICreds2Activity

DOMAIN MALWARE CHECK		
DOMAIN	STATUS	GEOLOCATION
goo.gl	good	IP: 172.217.13.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
crt.sca1b.amazontrust.com	good	IP: 13.225.189.111 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map
ocsp.sca1b.amazontrust.com	good	IP: 13.225.189.165 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807

CLIPBOARD DUMP	
:	:
:	[INFO] 29/Feb/2020 20:48:38 - Connecting to Android
:	:ssl_pinning_bypass
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] Loaded Frida Script - api_monitor
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] Loaded Frida Script - root_bypass
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] Loaded Frida Script - debugger
:	:nscriptFileDescriptorSocket.verifyCertificateChain() not found
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] [SSL Pinning Bypass] okhttp CertificatePinner not found
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] [SSL Pinning Bypass] okhttp3 CertificatePinner not found
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] [SSL Pinning Bypass] DataTheorem trustkit not found
:	[DEBUG] 29/Feb/2020 20:58:21 - [Frida] [SSL Pinning Bypass] Appcelerator PinningTrustManager not found
:	[DEBUG] 29/Feb/2020 20:58:22 - [Frida] [SSL Pinning Bypass] Apache Cordova SSLCertificateChecker not found
:	[DEBUG] 29/Feb/2020 20:58:22 - [Frida] [SSL Pinning Bypass] Wultra CertStore.validateFingerprint not found
:	[DEBUG] 29/Feb/2020 20:58:22 - [Frida] [API Monitor] Cannot fi
URLS	
	http://goo.gl/8rd3yj
	http://crt.sca1b.amazontrust.com/sca1b.crt
	http://ocsp.sca1b.amazontrust.com
	http://crl.sca1b.amazontrust.com/sca1b.crl

SQLITE DATABASE	
	data/data/jakhar.aseem.diva/databases/sqli
	data/data/jakhar.aseem.diva/databases/ids
	data/data/jakhar.aseem.diva/databases/divanotes.db
	data/data/jakhar.aseem.diva/app_webview/Web Data
XML FILES	
	data/data/jakhar.aseem.diva/shared_prefs/jakhar.aseem.diva_preferences.xml
	data/data/jakhar.aseem.diva/shared_prefs/WebViewChromiumPrefs.xml
OTHER FILES	
	data/data/jakhar.aseem.diva/ufinfo1130876619tmp

jakhar.aseem.diva_preferences.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="password">qweqe</string>
  <string name="user">qweqe</string>
  <string name="App Restrictions">AAAAAA==5#10; </string>
</map>
```

DOMAIN MALWARE CHECK		
DOMAIN	STATUS	GEOLOCATION
goo.gl	good	IP: 172.217.13.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
crt.scalb.amazontrust.com	good	IP: 13.225.189.111 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839 Longitude: -73.587807 View: Google Map
ocsp.scalb.amazontrust.com	good	IP: 13.225.189.165 Country: Canada Region: Quebec City: Montreal Latitude: 45.508839

OTHER FILES	
data/data/jakhar.aseem.diva/uiinfo1130876619tmp	
data/data/jakhar.aseem.diva/uiinfo1313625354tmp	
data/data/jakhar.aseem.diva/databases/divanotes.db-journal	
data/data/jakhar.aseem.diva/databases/sqlite-journal	
data/data/jakhar.aseem.diva/databases/ids2-journal	
data/data/jakhar.aseem.diva/app_webview/webview_data.lock	
data/data/jakhar.aseem.diva/app_webview/metrics_guid	
data/data/jakhar.aseem.diva/app_webview/Web Data-journal	
data/data/jakhar.aseem.diva/app_webview/GPUCache/index	
data/data/jakhar.aseem.diva/app_webview/GPUCache/index-dir/the-real-index	

Part 02

DECENTRALIZED APPS

dApps is an abbreviation of the phrase Decentralized Applications. DeFi (Decentralized Finance) depends heavily on dApps. To understand DeFi's capabilities we need to grasp the concept behind dApps. dApp sub programs designed to function within decentralized networks. These networks can be blockchains, tor networks or Distributed Ledger Technologies (DLT). The key component of these protocols is their decentralized nature. There is no central authority corporations or agency that monitors and approves the business functions of these applications. dApps requires very little human intervention instead these platforms integrate advanced smart contracts to streamline their business systems. Smart contracts are pre programmed protocols that initiate upon receiving crypto to their address. Importantly smart contracts can handle a huge variety of tasks from customer approval to making payments. Today there are more DeFi apps than ever. These applications are already saving businesses and customers time and money. In fact, DeFi platforms have begun to emerge across nearly every financial sector as the DeFi sector expands it is important to understand what characteristics all dApps have in common.

DeFi application should be open source. Open source coding refers to the fact that the coding is made public. In this way anyone can audit it and validate its functionality security and capabilities. Open source codes are far more stable and secure than private codes because of this community interaction. Additionally it provides more confidence in the platform because users can rest assured that no hidden malicious coding is operating in the background.

DeFi provides the world with new levels of transparency. Since most DeFi apps function on public blockchains such as Ethereum all transactions are publicly available. In fact all activity on the blockchain is public. The main difference in this approach versus a traditional bank account is that the accounts are not tied to anyone directly instead accounts are pseudo anonymous and only list a numerical address. While the accounts are not directly linked to anyone's name in particular there are ways for researchers to figure out who owns them if required. Programs such as block explorers can help people track and trace decentralized transactions of their non privacy focused coins.

dApps represent an expansion in the way developers envision financial platforms (global audience). Anyone from around the world can participate in DeFi platforms. We just need a

smartphone with internet access, and us can enter the DeFi community in minutes. Consequently, DeFi apps have the ability to provide the unbanked of the world with access to financial services for the first time in recorded history. This openness is a huge upgrade from the current banking system that leaves around 40 percent of the global population without any form of banking. Importantly when WE think of unbanked populations it is easy to picture a village somewhere in the tropics or desert. But the reality is much different. For example, a recent study found that 25 percent of US households remain unbanked. It is in these locations that defeat has an immediate effect.

The DeFi sector functions without gatekeepers as such anyone can develop a DeFi application and offer it to the world (permissionless). Additionally, anyone can participate in DeFi dApps without concern of approval. This strategy is a far cry from today's financial system which requires potential users to traverse a myriad of regulatory verification systems before they can participate in the global economy.

Another pillar of the DeFi community is interoperability. Interoperability is critical because it ensures that as more developers enter the space all the previous work is not lost instead users can stack their DeFi products to expand their exposure to this new age economy. For example, it is common for a single user to utilize stable coins decentralized exchanges and wallets together. This strategy is possible due to the seamless integration DeFi applications possess.

Due to the open nature of the DeFi environment developers are able to exercise more flexibility in their platforms. Users gain considerable options through the integration of third party application integrations as well. In fact, users can even choose to build their own interfaces if they find the current options insufficient. dApps have a long way to go and the path to financial revolution has already begun. Whether governments like it or not dApps are here to stay and evolve us.