ANDROID STATIC ANALYSIS REPORT

SABBMobile (3.4.0)

File Name:	com.sabb.mobilebanking_30400_apps.evozi.com.apk
Package Name:	com.sabb.mobilebanking
Average CVSS Score:	6.6
App Security Score:	25/100 (HIGH RISK)
Trackers Detection:	2/405
Scan Date:	Oct. 7, 2021, 1:39 p.m.

FILE INFORMATION

File Name: com.sabb.mobilebanking_30400_apps.evozi.com.apk
Size: 32.87MB
MD5: 6616f9a3c905ffbb52df40989a38745f
SHA1: 02c8c5202fe117c7eb6f37ebdc85930d46ffa82d
SHA256: 62cbadbea339aa404d85a613687a5b30c041d720d2ca2e8dabb2c37ac4865f14

APP INFORMATION

App Name: SABBMobile
Package Name: com.sabb.mobilebanking
Main Activity: com.sabb.mobilebanking.MainActivity
Target SDK: 29
Min SDK: 16
Max SDK:
Android Version Name: 3.4.0
Android Version Code: 30400

APP COMPONENTS

Activities: 2
Services: 6
Receivers: 6
Providers: 3
Exported Activities: 1
Exported Services: 4
Exported Receivers: 3
Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=HS, ST=HSBC, L=HSBC, O=HSBC, OU=HSBC, CN=HSBC
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2012-04-26 12:10:50+00:00
Valid To: 2149-03-19 12:10:50+00:00
Issuer: C=HS, ST=HSBC, L=HSBC, O=HSBC, OU=HSBC, CN=HSBC
Serial Number: 0x271f7b96
Hash Algorithm: sha256
md5: 7677dc9b6dac7ecd5bd620ab2e852881
sha1: 5f432709857de074ed38f2e7acb57e3363579910
sha256: 1f3c6481453dfc5f41edfee201ddce476aa0aa605f6d8e3259c252f46a0a092f
sha512:

9f501fde9ba91b9a946de2ad278f220340826907507cdd514447e9b46494daeef3f88d2849524c3d196e89accb7d250e0a75b2e54763d749d9f88634a61c7315

PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 333a049d358a323911c11741a35374b097072c76c7c54ceb4c506cb1052f3f20

STATUS	DESCRIPTION
secure	Application is signed with a code signing certificate
warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android <7.0

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.RECEIVE_SMS	dangerous	receive SMS	Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

PERMISSION	STATUS	INFO	DESCRIPTION
com.sabb.mobilebanking.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.sec.android.provider.badge.permission.READ	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.sec.android.provider.badge.permission.WRITE	normal	Show notification count on app	Show notification count or badge on application launch icon for samsung phones.
com.htc.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.htc.launcher.permission.UPDATE_SHORTCUT	normal	Show notification count on app	Show notification count or badge on application launch icon for htc phones.
com.sonyericsson.home.permission.BROADCAST_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for sony phones.
com.anddoes.launcher.permission.UPDATE_COUNT	normal	Show notification count on app	Show notification count or badge on application launch icon for apex.
com.majeur.launcher.permission.UPDATE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for solid.
com.huawei.android.launcher.permission.CHANGE_BADGE	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
com.huawei.android.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.

PERMISSION	STATUS	INFO	DESCRIPTION
com.huawei.android.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for huawei phones.
android.permission.READ_APP_BADGE	normal	show app notification	Allows an application to show app icon badges.
com.oppo.launcher.permission.READ_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
com.oppo.launcher.permission.WRITE_SETTINGS	normal	Show notification count on app	Show notification count or badge on application launch icon for oppo phones.
me.everything.badger.permission.BADGE_COUNT_READ	unknown	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
Build.TAGS check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>dx</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Broadcast Receiver (nl.xservices.plugins.ShareChooserPendingIntent) is not Protected. An intent-filter exists.	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
2	Activity (com.adobe.phonegap.push.PushHandlerActivity) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.sabb.mobilebanking.permission.PushHandlerActivity [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
3	Service (com.adobe.phonegap.push.FCMService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
4	Service (com.adobe.phonegap.push.PushInstanceIDListenerService) is not Protected. An intent-filter exists.	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Service is explicitly exported.
5	Service (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

NO	ISSUE	SEVERITY	DESCRIPTION
6	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementInstallReferrerReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	high	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
8	Service (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	IP Address disclosure	warning	CVSS V2: 4.3 (medium) CWE: CWE-200 Information Exposure OWASP MASVS: MSTG-CODE-2	com/vasco/digipass/sdk/utils/utilities/obfuscated/cp.java com/vasco/digipass/sdk/utils/utilities/obfuscated/cf.java com/vasco/digipass/sdk/utils/utilities/obfuscated/bz.java com/vasco/digipass/sdk/utils/utilities/obfuscated/cn.java com/vasco/digipass/sdk/utils/utilities/obfuscated/ch.java com/vasco/digipass/sdk/utils/utilities/obfuscated/cu.java com/vasco/digipass/sdk/utils/utilities/obfuscated/cd.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CVSS V2: 7.5 (high) CWE: CWE-532 Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/appdynamics/eumagent/runtime/p000private/bk.java com/appdynamics/eumagent/runtime/p000private/w.java com/appdynamics/eumagent/runtime/p000private/t.java com/appdynamics/eumagent/runtime/p000private/ay.java com/sabb/mobilebanking/MainActivity.java com/adobe/phonegap/push/PushInstanceIDListenerService.java com/appdynamics/eumagent/runtime/p000private/aj.java com/appdynamics/eumagent/runtime/logging/ADLog.java com/adobe/phonegap/push/BackgroundActionButtonHandler.java com/adobe/phonegap/push/PushHandlerActivity.java com/appdynamics/eumagent/runtime/p000private/ac.java com/sdk/plugin/sdkPlugin/DigipassUtil.java com/appdynamics/eumagent/runtime/Instrumentation.java com/appdynamics/eumagent/runtime/p000private/ce.java de/niklasmerz/cordova/fingerprint/FingerprintAuthenticationDialogFragment.java com/appdynamics/eumagent/runtime/p000private/k.java com/adobe/phonegap/push/FCMService.java com/appdynamics/eumagent/runtime/p000private/bn.java com/appdynamics/eumagent/runtime/p000private/e.java com/appdynamics/eumagent/runtime/p000private/ax.java com/appdynamics/eumagent/runtime/p000private/al.java com/adobe/phonegap/push/PushPlugin.java com/adobe/phonegap/push/PushDismissedHandler.java com/appdynamics/eumagent/runtime/p000private/bt.java me/leolin/shortcutbadger/ShortcutBadger.java uk/co/workingedge/phonegap/plugin/LaunchReview.java de/niklasmerz/cordova/fingerprint/Fingerprint.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CVSS V2: 5.9 (medium) CWE: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	com/appdynamics/eumagent/runtime/p000private/ai.java com/appdynamics/eumagent/runtime/p000private/ae.java com/appdynamics/eumagent/runtime/p000private/ah.java
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CVSS V2: 7.4 (high) CWE: CWE-312 Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/appdynamics/eumagent/runtime/AgentConfiguration.java com/adobe/phonegap/push/PushConstants.java com/appdynamics/eumagent/runtime/Instrumentation.java com/sdk/plugin/sdkPlugin/SDK_Properties.java com/adobe/phonegap/push/FCMService.java com/vasco/digipass/managers/constants/VDS_ManagerConstants.java
5	This App may have root detection capabilities.	secure	CVSS V2: 0 (info) OWASP MASVS: MSTG-RESILIENCE-1	com/sabb/mobilebanking/MainActivity.java
6	The App uses an insecure Random Number Generator.	warning	CVSS V2: 7.5 (high) CWE: CWE-330 Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/adobe/phonegap/push/FCMService.java
7	MD5 is a weak hash known to have hash collisions. سهولة الاختراق	warning	CVSS V2: 7.4 (high) CWE: CWE-327 Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/appdynamics/eumagent/runtime/p000private/be.java
8	App can read/write to External Storage. Any App can read data written to External Storage.	high	CVSS V2: 5.5 (medium) CWE: CWE-276 Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	nl/xservices/plugins/SocialSharing.java
9	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	CVSS V2: 0 (info) OWASP MASVS: MSTG-STORAGE-10	nl/xservices/plugins/SocialSharing.java
10	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CVSS V2: 7.4 (high) CWE: CWE-649 Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	de/niklasmerz/cordova/fingerprint/Fingerprint.java

→ ما تحقق لا امان التشفير

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'location'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application implement functionality to encrypt sensitive data in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_CKM.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Asymmetric Key Generation	The application generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
12	FCS_COP.1.1(1)	Selection-Based Security Functional Requirements	Cryptographic Operation - Encryption/Decryption	The application perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode or AES-GCM (as defined in NIST SP 800-38D) and cryptographic key sizes 256-bit/128-bit.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
13	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
14	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
15	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA-256'] .
16	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
17	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
18	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.
19	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.
20	FPT_TUD_EXT.2.1	Selection-Based Security Functional Requirements	Integrity for Installation and Update	The application shall be distributed using the format of the platform-supported package manager.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
sabbmobile-prod-android.firebaseio.com	good	**IP:** 35.201.97.85 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.whatsapp.com	good	**IP:** 31.13.69.60 **Country:** Italy **Region:** Sicilia **City:** Palermo **Latitude:** 38.115822 **Longitude:** 13.359760 **View:** Google Map
flush.queue	good	No Geolocation information available.
mobile.eum-appdynamics.com	good	**IP:** 34.217.242.192 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
eum.sabb.com	good	**IP:** 193.27.7.152 **Country:** Saudi Arabia **Region:** Ar Riyad **City:** Riyadh **Latitude:** 24.687731 **Longitude:** 46.721851 **View:** Google Map
image.eum-appdynamics.com	good	**IP:** 54.148.179.96 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map

URLS

URL	FILE
data:image/ https://api.whatsapp.com/send?phone=	nl/xservices/plugins/SocialSharing.java
https://mobile.eum-appdynamics.com https://image.eum-appdynamics.com	com/appdynamics/eumagent/runtime/AgentConfiguration.java
javascript:(function()	com/appdynamics/eumagent/runtime/p000private/cp.java
http://flush.queue	com/appdynamics/cordova/plugin/ADEUMMobilePlugin.java
https://eum.sabb.com https://sabbmobile-prod-android.firebaseio.com	Android String Resource

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://sabbmobile-prod-android.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
someone@domain.com	nl/xservices/plugins/SocialSharing.java

TRACKERS

TRACKER	CATEGORIES	URL
Appdynamics	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/194
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"adeum_app_key" : "EUM-AAB-AUB"
"fingerprint_auth_dialog_title" : "Fingerprint Authentication"
"firebase_database_url" : "https://sabbmobile-prod-android.firebaseio.com"
"google_api_key" : "AIzaSyCfiHKQmHQwwJjsA-PvJOsZSQrCAgjsJn4"
"google_crash_reporting_api_key" : "AIzaSyCfiHKQmHQwwJjsA-PvJOsZSQrCAgjsJn4"
"fingerprint_auth_dialog_title" : "Fingeraftryk Login"
"fingerprint_auth_dialog_title" : "Authentifizierung"
"fingerprint_auth_dialog_title" : "□□□□"
"fingerprint_auth_dialog_title" : "Ελεγχος αποτυπώματος"
"fingerprint_auth_dialog_title" : "Authenticatie met vingerafdruk"

POSSIBLE SECRETS
"fingerprint_auth_dialog_title" : "Authentification par empreinte digitale"
"fingerprint_auth_dialog_title" : "Autenticación de Huellas Digitales"
"fingerprint_auth_dialog_title" : "Autenticazione impronta digitale"
"fingerprint_auth_dialog_title" : "Autenticação de impressão digital"
"fingerprint_auth_dialog_title" : "□□□□"

App Security Score Calculation

Every app is given an ideal score of 100 to begin with.
For every findings with severity high we reduce 15 from the score.
For every findings with severity warning we reduce 10 from the score.
For every findings with severity good we add 5 to the score.
If the calculated score is greater than 100, then the app security score is considered as 100.
And if the calculated score is less than 0, then the app security score is considered as 10.

Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

Report Generated by - MobSF v3.4.5 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.