



ANDROID STATIC ANALYSIS REPORT



 Binar (5.1.2)

File Name: Binar_5.1.2_apkcombo.com.apk

Package Name: com.binaracademy.app

Scan Date: May 17, 2022, 3:11 p.m.






App Security Score: 34/100 (HIGH RISK)

Grade:



Trackers Detection: 8/428

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
6	13	2	0	2

FILE INFORMATION

File Name: Binar_5.1.2_apkcombo.com.apk

Size: 24.34MB

MD5: 60e3d6ebc368bd9fdc4e49e6fbd86d72

SHA1: 769ff30839b2617ef0e94a4e65086771ab8b26e6

SHA256: 1ebcf486c966a359158f1f47db77553bb8995967d7d4965a47fb84466588f734

APP INFORMATION

App Name: Binar

Package Name: com.binaracademy.app

Main Activity: id.co.binar.ui.splashscreen.SplashScreenActivity

Target SDK: 30

Min SDK: 23

Max SDK:

Android Version Name: 5.1.2

Android Version Code: 59

APP COMPONENTS

Activities: 57

Services: 13

Receivers: 6

Providers: 6

Exported Activities: 3

Exported Services: 2

Exported Receivers: 2

Exported Providers: 1

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: True

Found 1 unique certificates

Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2020-01-27 13:57:06+00:00

Valid To: 2050-01-27 13:57:06+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xed17f248c114ba51ddc0a92979083e00343cc0df

Hash Algorithm: sha256

md5: 6b6f58dcc465d6f7837252c247db7a05

sha1: 781075afabb5909dc3a234df7343ccca4e0bb7df

sha256: 37ae59108d1bab5ecb8b44f10ed8e8f5bd45b6724238ffb4b6d4a2f951c709a6

sha512: 307e16da8b1f9ec151bbfc73aa85fa54306da8c4950bd89ae6f662289ac1a22074ccd5cd510f11e497e674302441e0fe4d2e790f045fc0c9345879eccd555edb

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 8bb5d699cd517a297cb5f98d8cbb2d9fbdabc9d456261fec1418da6372592c3b

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
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.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check Build.TAGS check SIM operator check network operator name check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MODEL check Build.MANUFACTURER check network operator name check
	Compiler	r8 without marker (suspicious)

ACTIVITY	INTENT
id.co.binar.ui.splashscreen.SplashScreenActivity	Schemes: binar://, https://, http://, Hosts: j5478.app.link, j5478-alternate.app.link, @string/host_name, stg-app.binaracademy.com, Path Prefixes: @string/deeplink_route_home, @string/deeplink_route_profile, /profile, @string/deeplink_route_premium_all, @string/deeplink_route_premium, @string/deeplink_route_payment_status, @string/deeplink_route_course, @string/deeplink_route_insight_home, @string/deeplink_route_dana_cita,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.binaracademy.app,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
2	Activity (id.co.binar.ui.prevent_android_5.PreventAndroid5Activity) is not Protected. [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.
3	Activity (id.co.binar.ui.main_route.activity.MainActivity) is not Protected. An intent-filter exists.	warning	An Activity 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 Activity is explicitly exported.
4	Content Provider (com.facebook.FacebookContentProvider) is not Protected. [android:exported=true]	high	A Content Provider is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (id.co.binar.service.FcmService) is not Protected. An intent-filter exists.	warning	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.
6	Broadcast Receiver (id.co.binar.util.extension.IsDownloadComplete) is not Protected. [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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service 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	Activity (com.facebook.CustomTabActivity) is not Protected. [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.
9	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]	warning	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.

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	p5/p.java p5/m.java p5/q.java p5/r.java p5/n.java p5/o.java
				u2/h.java v0/f.java ra/b.java wm/c.java r2/i.java t9/e.java com/journeyapps/barcodescanner/b.java r7/l.java io/branch/referral/f.java u8/a.java d0/g.java zn/a.java u2/i.java tc/e.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java v0/a.java m4/k.java h0/e.java o7/a.java j6/b.java h6/e.java com/clevertap/android/sdk/displayunits/model/CleverTapDisplayUnit.java a3/h.java ru/rambler/libs/swipe_layout/SwipeLayout.java i6/a.java l0/h.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	org/greenrobot/eventbus/a.java a.java n0/g.java j7/r.java l0/d.java j6/h.java v0/t.java m6/o.java m1/a.java j7/u.java o0/f.java o0/g.java t9/k.java g3/l.java j7/v.java c7/d.java l5/g.java c1/a.java e1/c.java j7/s.java j7/n.java v4/c.java l0/e.java d0/s.java o3/a.java t9/a.java v0/o.java z2/a.java p2/d.java v0/b.java z1/f.java com/bumptechnology/load/resource/bitmap/g.java j7/e.java nc/a.java n6/d.java io/branch/referral/o.java r7/t.java y9/d.java id/co/binar/util/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				t6/b.java t6/c.java e1/t.java p2/e.java w2/a.java qa/a.java r7/q.java n0/e.java v0/n.java r7/a.java io/branch/referral/BranchJsonConfig.jav a oa/a.java j6/g.java r2/k.java com/bumptechnology/load/resource/bit map/i.java k6/d.java a3/b.java x1/a.java n4/a.java o0/l.java z5/c.java a3/l.java com/journeyapps/barcodescanner/Cam eraPreview.java com/clevertap/android/sdk/s.java v2/j.java l0/r.java com/bumptechnology/load/engine/Glide Exception.java o0/h.java r2/b.java c0/c.java com/clevertap/android/sdk/ab_testing/ CTVar.java r7/p.java com/midtrans/sdk/corekit/core/Logger. java t9/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o0/d.java r6/m.java y1/x.java r7/n.java v4/t.java k6/c.java t9/i.java jn/a.java n/m.java f8/b.java s8/c.java a3/i.java z0/c.java n/k.java d8/d.java t8/a.java
3	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	r0/g.java com/journeyapps/barcodescanner/b.java a id/co/binar/util/a.java
4	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	q3/i.java
5	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	um/a.java
6	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	o7/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
7	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptechnology/load/engine/h.java
8	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	gm/a.java fm/a.java fa/c.java
9	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	fa/c.java

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 generate no asymmetric cryptographic keys.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['location', 'network connectivity', 'camera'].
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 does not encrypt files 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_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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
12	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
13	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
14	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.
15	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['RFC 5280 certificate validation and certificate path validation'].
16	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.
17	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
--------	--------	-------------

DOMAIN	STATUS	GEOLOCATION
developers.facebook.com	ok	IP: 157.240.205.1 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api2.branch.io	ok	IP: 65.9.49.125 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
klikbca.com	ok	IP: 202.6.211.8 Country: Indonesia Region: Jawa Barat City: Utama Latitude: -7.321600 Longitude: 108.382103 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.midtrans.com	ok	IP: 104.17.2.81 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
static.wizrocket.com	ok	IP: 65.9.49.23 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map
schemas.android.com	ok	No Geolocation information available.
www.youtube.com	ok	IP: 142.250.181.238 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
docs.google.com	ok	IP: 142.250.186.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
app.midtrans.com	ok	IP: 104.17.2.81 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
storage.googleapis.com	ok	IP: 142.250.185.208 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
play.google.com	ok	IP: 142.250.185.174 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
blog.binaracademy.com	ok	IP: 35.247.154.208 Country: Singapore Region: Singapore City: Singapore Latitude: 1.289670 Longitude: 103.850067 View: Google Map

DOMAIN	STATUS	GEOLOCATION
binar-academy-eng.firebaseio.com	ok	IP: 35.201.97.85 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
ibank.bankmandiri.co.id	ok	IP: 103.139.82.21 Country: Indonesia Region: Jawa Barat City: Bekasi Latitude: -6.234900 Longitude: 106.989601 View: Google Map
promo.vt-stage.info	ok	No Geolocation information available.
cdn.branch.io	ok	IP: 54.230.99.89 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map
hangout.betas.in	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ibank.bni.co.id	ok	IP: 104.75.65.101 Country: Sweden Region: Stockholms lan City: Stockholm Latitude: 59.332581 Longitude: 18.064899 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
https://binar-academy-eng.firebaseio.com	info App talks to a Firebase Database.

EMAILS

EMAIL	FILE
info@binar.co vinda@gmail.com name@email.com binar@email.com budi@utomo.com sabrina@hotmail.com	Android String Resource

TRACKERS

TRACKER	CATEGORIES	URL
Branch	Analytics	https://reports.exodus-privacy.eu.org/trackers/167
CleverTap	Analytics, Profiling, Location	https://reports.exodus-privacy.eu.org/trackers/174
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Places		https://reports.exodus-privacy.eu.org/trackers/69
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"ISSUE_TRACKER_API_KEY" : "eqBTHdEAfobg/zeTi8d5gw=="
"PREFERENCE_PASSWORD" : "19098756823e327465789342"

POSSIBLE SECRETS
"branch_key" : "key_live_odXnleHroce2kculMIO2hkgnCCbtHM9V"
"branch_key_test" : "key_test_ff0plaKxdih0bbFiNkR7ckicEukENN3x"
"certificate" : "Sertifikat"
"clevertap_project_token" : "216-5a6"
"firebase_database_url" : "https://binar-academy-eng.firebaseio.com"
"google_api_key" : "AlzaSyDHv4op-rn5W-DZVC7ZBjgV3ld3W77k4UQ"
"google_crash_reporting_api_key" : "AlzaSyDHv4op-rn5W-DZVC7ZBjgV3ld3W77k4UQ"
"lengkapi" : "Lengkapi"
"password" : "Password"
"share_certificate" : "Bagikan"
"com_facebook_device_auth_instructions" : "facebook.com/deviceXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
"com_facebook_device_auth_instructions" : "XXfacebook.com/device>XXXXXXXXXXXXXXXXXX"
"com_facebook_device_auth_instructions" : "XXXfacebook.com/deviceXXXXXXXXXXXX"
"com_facebook_device_auth_instructions" : "XXfacebook.com/device>XXXXXXXXXXXXXXXXXX"

Title: Binar

Score: 4.428571 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** 6.0 and up **Category:** Education **Play Store URL:** [com.binaracademy.app](https://play.google.com/store/apps/details?id=com.binaracademy.app)

Developer Details: Binar Academy, 7125299661105225216, Jalan BSD Grand Boulevard, Sampora, BSD, Tangerang, Banten 15345, BSD Green Office Park, Tangerang, Banten 12730, ID, <https://binar.co.id/>, info@binar.co.id,

Release Date: Feb 20, 2020 **Privacy Policy:** [Privacy link](#)

Description:

Selamat Datang di Binar Academy! Dengan belajar di Binar, kesempatan kamu berkarier di industri digital lebih terbuka lebar. Kenal lebih dekat dengan Binar Academy, kamu cukup install aplikasinya. Di sini, kamu akan mendapat pengalaman belajar digital yang lengkap, interaktif, dan mudah diakses. Mulai dari Binar Bootcamp, Binar Insight, informasi promo, hingga akses materi secara gratis bisa kamu dapatkan di aplikasi Binar Academy. Sekarang, kamu bisa belajar sambil ngakak bareng BinarGO! BinarGO! adalah produk terbaru Binar Academy, yang bakal jadi solusi asyik buat kamu yang suka belajar mandiri. Materinya dibawakan lewat video seru yang bikin kamu berasa lagi nonton Netflix, ditambah bahan bacaan dan quiz yang relevan. Kamu bisa atur waktu belajar, kapan pun dan di mana pun kamu mau. Kamu juga bisa cobain banyak materi gratisnya, di dalam aplikasi Binar Academy. Yuk cobain sekarang! Gambaran singkat tentang produk Binar Academy: Binar Bootcamp Yang awam bakal diajarin sampai paham selama 4/6 bulan. Kalau udah lulus Binar Bootcamp, kamu bisa dibantu cari kerja lewat Job Connect! Binar Insight Roketkan karier digitalmu dengan belajar langsung bareng expert dari unicorn dan industry leaders di Indonesia dalam webinar berserial. Beli bundle lebih murah, dapatkan materi, recording, dan kesempatan networking langsung di dalam sesi Binar Insight! Promo Hayoo.. siapa sih yang nggak suka promo? Temukan berbagai promo menarik eksklusif hanya di aplikasi! Tunggu apalagi? Biar cepat tanggap, yuk pelajari lengkap. Ayo install aplikasi Binar Academy sekarang! KENALAN YUK! Instagram: @academybinar Twitter: @academybinar Facebook: facebook.com/binaracademy Web: binaracademy.com Contact us at info@binar.co.id.

Report Generated by - MobSF v3.5.2 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).