IOS STATIC ANALYSIS REPORT

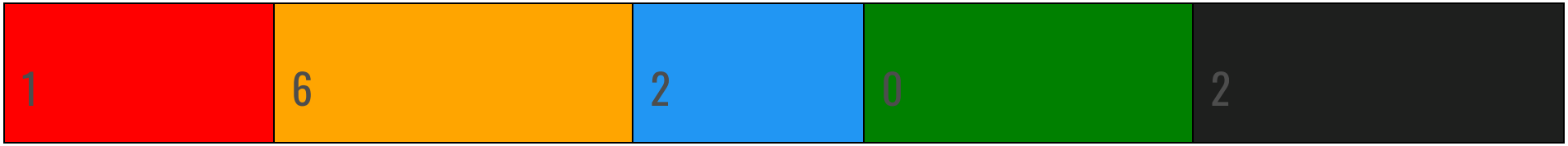
DVIA-v2 (2.0)

File Name:	DVIA-v2.ipa
Identifier:	com.highaltitudehacks.DVIAswiftv2

Scan Date:	Aug. 11, 2025, 11:13 a.m.
App Security Score:	42/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	3/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT



FILE INFORMATION

File Name: DVIA-v2.ipa
Size: 9.2MB
MD5: b919e84e7d35f68e16b6cd05d8e3b1ce
SHA1: 1dd38869cb0a5b9bdb57a46341547e1cc0dac8ca
SHA256: dabf92a5ca1cc00221fa3a12f1b58f1095da5698ea4dcb92ab0c64699cff6d5f

APP INFORMATION

App Name: DVIA-v2
App Type: Swift
Identifier: com.highaltitudehacks.DVIAswiftv2
SDK Name: iphoneos17.0
Version: 2.0
Build: 1
Platform Version: 17.0
Min OS Version: 12.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

Arch: ARM64
Sub Arch: CPU_SUBTYPE_ARM64_ALL
Bit: 64-bit
Endian: <

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
com.highaltitudehacks.DVIAswiftv2	dvia dviaswift

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	INFO	REASON IN MANIFEST
NSCameraUsageDescription	dangerous	Access the Camera.	To demonstrate the misuse of Camera, please grant it permission once.
NSFaceIDUsageDescription	normal	Access the ability to authenticate with Face ID.	The app needs FaceID permission

APP TRANSPORT SECURITY (ATS)

HIGH: **1** | WARNING: **0** | INFO: **0** | SECURE: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Transport Security AllowsArbitraryLoads is allowed	high	App Transport Security restrictions are disabled for all network connections. Disabling ATS means that unsecured HTTP connections are allowed. HTTPS connections are also allowed, and are still subject to default server trust evaluation. However, extended security checks like requiring a minimum Transport Layer Security (TLS) protocol version—are disabled. This setting is not applicable to domains listed in NSExceptionDomains.

IPA BINARY CODE ANALYSIS

HIGH: **0** | WARNING: **3** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
1	Binary makes use of insecure API(s)	warning	**CWE:** CWE-676: Use of Potentially Dangerous Function **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may contain the following insecure API(s) _fopen , _memcpy , _printf , _sscanf , _strcpy , _strlen , _strncpy
2	Binary makes use of the insecure Random function(s)	warning	**CWE:** CWE-330: Use of Insufficiently Random Values **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-6	The binary may use the following insecure Random function(s) _random
3	Binary makes use of Logging function	info	**CWE:** CWE-532: Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	The binary may use _NSLog function for logging.
4	Binary makes use of malloc function	warning	**CWE:** CWE-789: Uncontrolled Memory Allocation **OWASP Top 10:** M7: Client Code Quality **OWASP MASVS:** MSTG-CODE-8	The binary may use _malloc function instead of calloc
5	Binary uses WebView Component.	info	**OWASP MASVS:** MSTG-CODE-9	The binary may use UIWebView Component.

IPA BINARY ANALYSIS

PROTECTION	STATUS	SEVERITY	DESCRIPTION
NX	False	info	The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.
PIE	True	info	The binary is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.

PROTECTION	STATUS	SEVERITY	DESCRIPTION
STACK CANARY	True	info	This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.
ARC	True	info	The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.
RPATH	True	warning	The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.
CODE SIGNATURE	True	info	This binary has a code signature.
ENCRYPTED	False	warning	This binary is not encrypted.
SYMBOLS STRIPPED	False	warning	Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

DYNAMIC LIBRARY & FRAMEWORK BINARY ANALYSIS

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
1	Payload/DVIA-v2.app/Frameworks/Parse.framework/Parse	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	False warning This binary is not encrypted.	False warning Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
2	Payload/DVIA-v2.app/Frameworks/Realm.framework/Realm	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	False warning This binary is not encrypted.	False warning Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
3	Payload/DVIA-v2.app/Frameworks/Bolts.framework/Bolts	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	False warning This binary is not encrypted.	False warning Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

NO	DYLIB/FRAMEWORK	NX	STACK CANARY	ARC	RPATH	CODE SIGNATURE	ENCRYPTED	SYMBOLS STRIPPED
4	Payload/DVIA-v2.app/Frameworks/RealmSwift.framework/RealmSwift	False info The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. However iOS never allows an app to execute from writeable memory. You do not need to specifically enable the 'NX bit' because it's always enabled for all third-party code.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	True info The binary is compiled with Automatic Reference Counting (ARC) flag. ARC is a compiler feature that provides automatic memory management of Objective-C objects and is an exploit mitigation mechanism against memory corruption vulnerabilities.	True warning The binary has Runpath Search Path (@rpath) set. In certain cases an attacker can abuse this feature to run arbitrary executable for code execution and privilege escalation. Remove the compiler option -rpath to remove @rpath.	True info This binary has a code signature.	False warning This binary is not encrypted.	False warning Debug Symbols are available. To strip debugging symbols, set Strip Debug Symbols During Copy to YES, Deployment Postprocessing to YES, and Strip Linked Product to YES in project's build settings.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
crl.apple.com	ok	**IP:** 17.253.61.206 **Country:** United States of America **Region:** Arizona **City:** Mesa **Latitude:** 33.422272 **Longitude:** -111.822639 **View:** Google Map
api.parse.com	ok	**IP:** 57.144.152.141 **Country:** United States of America **Region:** California **City:** Palo Alto **Latitude:** 37.441879 **Longitude:** -122.143021 **View:** Google Map
damnvulnerableiosapp.com	ok	**IP:** 15.197.225.128 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.example.com	ok	**IP:** 42.99.140.192 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.digicert.com1	ok	No Geolocation information available.
www.apple.com	ok	**IP:** 23.15.129.45 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.youtube.com	ok	**IP:** 142.250.4.136 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.org0	ok	No Geolocation information available.
realm.io	ok	**IP:** 13.35.202.27 **Country:** India **Region:** Telangana **City:** Hyderabad **Latitude:** 17.375280 **Longitude:** 78.474442 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
google.com	ok	**IP:** 74.125.130.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 172.217.194.103 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
highaltitudehacks.com	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.digicert.com	ok	**IP:** 45.60.125.229 **Country:** United States of America **Region:** California **City:** Redwood City **Latitude:** 37.532440 **Longitude:** -122.248833 **View:** Google Map
www.thejuniperfund.org	ok	**IP:** 198.185.159.144 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.734699 **Longitude:** -74.005898 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
cfg.flurry.com	ok	**IP:** 180.222.114.11 **Country:** India **Region:** Maharashtra **City:** Mumbai **Latitude:** 19.014410 **Longitude:** 72.847939 **View:** Google Map
www.google-analytics.com	ok	**IP:** 172.217.194.102 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
cacerts.digicert.com	ok	**IP:** 23.210.96.161 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map
www.example.net0	ok	No Geolocation information available.
ssl.google-analytics.com	ok	**IP:** 74.125.68.97 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
data.flurry.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
example.com	ok	**IP:** 96.7.128.198 **Country:** United States of America **Region:** California **City:** El Segundo **Latitude:** 33.919182 **Longitude:** -118.416473 **View:** Google Map
ocsp.apple.com	ok	**IP:** 17.253.61.204 **Country:** United States of America **Region:** Arizona **City:** Mesa **Latitude:** 33.422272 **Longitude:** -111.822639 **View:** Google Map
crl3.digicert.com	ok	**IP:** 23.210.96.161 **Country:** Germany **Region:** Berlin **City:** Berlin **Latitude:** 52.524368 **Longitude:** 13.410530 **View:** Google Map
www.example.edu	ok	**IP:** 42.99.140.160 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map
www.example.org	ok	**IP:** 42.99.140.210 **Country:** Japan **Region:** Tokyo **City:** Tokyo **Latitude:** 35.689507 **Longitude:** 139.691696 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api.login.yahoo.com	ok	**IP:** 106.10.248.157 **Country:** Singapore **Region:** Singapore **City:** Singapore **Latitude:** 1.289670 **Longitude:** 103.850067 **View:** Google Map
goo.gl	ok	**IP:** 64.233.170.138 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ocsp.digicert.com0m	ok	No Geolocation information available.
twitter.com	ok	**IP:** 162.159.140.229 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.mixpanel.com	ok	**IP:** 35.190.25.25 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
certs.apple.com	ok	**IP:** 17.253.61.196 **Country:** United States of America **Region:** Arizona **City:** Mesa **Latitude:** 33.422272 **Longitude:** -111.822639 **View:** Google Map
github.com	ok	**IP:** 20.205.243.166 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map

EMAILS

EMAIL	FILE
defaultrealm@host.com test123@gmail.com j2@j.rj	DVIA-v2.app/DVIA-v2
defaultrealm@host.com test123@gmail.com	IPA Strings Dump
help@realm.io	Payload/DVIA-v2.app/Frameworks/Realm.framework/Realm

TRACKERS

TRACKER	CATEGORIES	URL
Flurry	Analytics, Advertisement	https://reports.exodus-privacy.eu.org/trackers/25
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48
MixPanel	Analytics	https://reports.exodus-privacy.eu.org/trackers/118

SCAN LOGS

Timestamp	Event	Error
2025-08-11 11:14:13	iOS Binary (IPA) Analysis Started	OK
2025-08-11 11:14:13	Generating Hashes	OK
2025-08-11 11:14:13	Extracting IPA	OK
2025-08-11 11:14:13	Unzipping	OK
2025-08-11 11:14:13	iOS File Analysis and Normalization	OK
2025-08-11 11:14:13	iOS Info.plist Analysis Started	OK
2025-08-11 11:14:13	Finding Info.plist in iOS Binary	OK

2025-08-11 11:14:13	Fetching Details from App Store: com.highaltitudehacks.DVIAswiftv2	OK
2025-08-11 11:14:13	Searching for secrets in plist files	OK
2025-08-11 11:14:13	Starting Binary Analysis	OK
2025-08-11 11:14:13	Dumping Classes from the binary	OK
2025-08-11 11:14:13	Running jtool against the binary for dumping classes	OK
2025-08-11 11:14:23	Library Binary Analysis Started	OK
2025-08-11 11:14:23	Framework Binary Analysis Started	OK
2025-08-11 11:14:23	Analyzing Payload/DVIA-v2.app/Frameworks/Parse.framework/Parse	OK
2025-08-11 11:14:23	Analyzing Payload/DVIA-v2.app/Frameworks/Realm.framework/Realm	OK
2025-08-11 11:14:24	Analyzing Payload/DVIA-v2.app/Frameworks/Bolts.framework/Bolts	OK
2025-08-11 11:14:24	Analyzing Payload/DVIA-v2.app/Frameworks/RealmSwift.framework/RealmSwift	OK
2025-08-11 11:14:24	Extracting String Metadata	OK

2025-08-11 11:14:24	Extracting URL and Email from IPA	OK
2025-08-11 11:14:28	Performing Malware check on extracted domains	OK
2025-08-11 11:14:30	Fetching IPA icon path	OK
2025-08-11 11:14:32	Detecting Trackers from Domains	OK
2025-08-11 11:14:32	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.