IOS STATIC ANALYSIS REPORT

DVIA-v2 (2.0)

File Name:	DVIA-v2-swift.ipa
Identifier:	com.highaltitudehacks.DVIAswiftv2
Scan Date:	Feb. 20, 2022, 11:45 a.m.
App Security Score:	21/100 (CRITICAL RISK)
Grade:	F
Trackers Detection:	1/421

FINDINGS SEVERITY

HIGH	WARNING	INFO	✓ SECURE
4	3	2	0

FILE INFORMATION

File Name: DVIA-v2-swift.ipa
Size: 19.37MB
MD5: 35469622303ba10a2195557a3ad1810a
SHA1: 85174824d6cd7c83df98c518247acf8a14b28882
SHA256: a0efb217f3dd018a4fbea7b2d63db7da4e21d5d7cdc20bd4a72a8a5b57e98817

APP INFORMATION

App Name: DVIA-v2
App Type: Swift
Identifier: com.highaltitudehacks.DVIAswiftv2
SDK Name: iphoneos11.2
Version: 2.0
Build: 1
Platform Version: 11.2
Min OS Version: 10.0
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	DESCRIPTION	REASON IN MANIFEST
NSCameraUsageDescription	dangerous	Access the Camera.	To demonstrate the misuse of Camera, please grant it permission once.

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION
1	App Transport Security AllowsArbitraryLoads	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

	is allowed		disabled. This setting is not applicable to domains listed in NSExceptionDomains.

IPA BINARY CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
1	Binary makes use of insecure API(s)	high	**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) _memcpy , _fopen , _strncpy , _strlen , _strcpy , _printf
2	Binary makes use of the insecure Random function(s)	high	**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	high	**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	True	info	The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.
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.
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	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.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
		IP: 23.59.85.8 **Country:** Poland

www.apple.com	ok	**Region:** Mazowieckie **City:** Warsaw **Latitude:** 52.229771 **Longitude:** 21.011780 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.129 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
goo.gl	ok	**IP:** 142.250.186.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
		IP: 104.18.11.39

cacerts.digicert.com	ok	**Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
highaltitudehacks.com	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
damnvulnerableiosapp.com	ok	**IP:** 160.153.63.197 **Country:** United States of America **Region:** Arizona **City:** Scottsdale **Latitude:** 33.601974 **Longitude:** -111.887917 **View:** Google Map
ocsp.digicert.com0m	ok	No Geolocation information available.
www.youtube.com	ok	**IP:** 142.250.180.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.example.org	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map

www.google-analytics.com	ok	**IP:** 142.250.203.142 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.digicert.com1	ok	No Geolocation information available.
www.digicert.com	ok	**IP:** 45.60.123.229 **Country:** France **Region:** Ile-de-France **City:** Paris **Latitude:** 48.853409 **Longitude:** 2.348800 **View:** Google Map
www.example.com	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
crl.apple.com	ok	**IP:** 17.253.123.202 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map
www.example.edu	ok	**IP:** 93.184.216.34 **Country:** United States of America **Region:** Virginia **City:** Ashburn

		Latitude: 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.example.net0	ok	No Geolocation information available.
crl3.digicert.com	ok	**IP:** 93.184.220.29 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **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
www.example.org0	ok	No Geolocation information available.
ssl.google-analytics.com	ok	**IP:** 142.250.180.200 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ocsp.apple.com	ok	**IP:** 17.253.123.201 **Country:** Russian Federation **Region:** Moskva **City:** Moscow **Latitude:** 55.752220 **Longitude:** 37.615559 **View:** Google Map

EMAILS

EMAIL	FILE
test123@gmail.com defaultrealm@host.com prateek@damnvulnerableiosapp.com ij@2.ssi ț9@.ηq	DVIA-v2.app/DVIA-v2
defaultrealm@host.com test123@gmail.com	IPA Strings Dump

TRACKERS

TRACKER	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

Report Generated by - MobSF v3.5.0 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.