IOS STATIC ANALYSIS REPORT

DVIA (1.3)

File Name:	DamnVulnerableiOSApp.ipa
Identifier:	com.highaltitudehacks.dvia
Scan Date:	Oct. 23, 2025, 6:37 p.m.
App Security Score:	73/100 (LOW RISK)
Grade:	A

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
0	2	2	1	1

FILE INFORMATION

File Name: DamnVulnerableiOSApp.ipa
Size: 5.53MB
MD5: 6b27b725e021afbc15c0e6574732af2a
SHA1: 7525a037f65b43891a49052091e63322ed12dd15
SHA256: a8c6cafcbf915f876f72b9221dd3fd35a1279abd27c54b3c2d19df14d750ef19

APP INFORMATION

App Name: DVIA
App Type: Objective C
Identifier: com.highaltitudehacks.dvia
SDK Name: iphoneos8.1
Version: 1.3
Build: 1.0
Platform Version: 8.1
Min OS Version: 7.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

Arch: ARM
Sub Arch: CPU_SUBTYPE_ARM_V7
Bit: 32-bit
Endian: <

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
None None	dvia

APP TRANSPORT SECURITY (ATS)

NO	ISSUE	SEVERITY	DESCRIPTION

IPA BINARY CODE ANALYSIS

HIGH: **0** | WARNING: **2** | 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) _memcpy , _sscanf , _stat , _strlen
2	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.
3	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
4	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	False	info	The binary does not have Runpath Search Path (@rpath) set.
CODE SIGNATURE	True	info	This binary has a code signature.
ENCRYPTED	False	warning	This binary is not encrypted.
SYMBOLS STRIPPED	True	info	Debug Symbols are stripped

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
api.twitter.com	ok	**IP:** 172.66.0.227 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
developer.apple.com	ok	**IP:** 17.253.39.131 **Country:** Sweden **Region:** Stockholms lan **City:** Stockholm **Latitude:** 59.332581 **Longitude:** 18.064899 **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
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
google.com	ok	**IP:** 173.194.220.101 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
twitter-oauth.callback	ok	No Geolocation information available.
api.parse.com	ok	**IP:** 157.240.205.1 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
www.google.co.uk0	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
clients1.google.com	ok	**IP:** 209.85.233.113 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.22.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.google.co.uk	ok	**IP:** 64.233.161.94 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.apple.com	ok	**IP:** 23.196.53.50 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
www.google.co.uk0h	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
ns.adobe.com	ok	No Geolocation information available.
pki.google.com	ok	**IP:** 142.251.1.100 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

✉ EMAILS

EMAIL	FILE
y@k9.8_z 5of@й.du r6@0.ălirlsf1 i@b.r8 5@6.kfv f4pf2@f.bxp	DamnVulnerableIOSApp.app/DamnVulnerableIOSApp

SCAN LOGS

Timestamp	Event	Error

2025-10-23 18:37:21	iOS Binary (IPA) Analysis Started	OK
2025-10-23 18:37:21	Generating Hashes	OK
2025-10-23 18:37:21	Extracting IPA	OK
2025-10-23 18:37:21	Unzipping	OK
2025-10-23 18:37:21	iOS File Analysis and Normalization	OK
2025-10-23 18:37:21	iOS Info.plist Analysis Started	OK
2025-10-23 18:37:21	Finding Info.plist in iOS Binary	OK
2025-10-23 18:37:21	Fetching Details from App Store: com.highaltitudehacks.dvia	OK
2025-10-23 18:37:21	Searching for secrets in plist files	OK
2025-10-23 18:37:21	Starting Binary Analysis	OK
2025-10-23 18:37:21	Dumping Classes from the binary	OK

2025-10-23 18:37:21	Running jtool against the binary for dumping classes	OK
2025-10-23 18:37:24	Library Binary Analysis Started	OK
2025-10-23 18:37:24	Framework Binary Analysis Started	OK
2025-10-23 18:37:24	Extracting String Metadata	OK
2025-10-23 18:37:24	Extracting URL and Email from IPA	OK
2025-10-23 18:37:24	Performing Malware check on extracted domains	OK
2025-10-23 18:37:26	Fetching IPA icon path	OK
2025-10-23 18:37:27	Detecting Trackers from Domains	OK
2025-10-23 18:37:27	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.