IOS STATIC ANALYSIS REPORT

iGoat-Swift (1.0)

File Name:	iGoat-Swift.ipa
Identifier:	OWASP.iGoat-Swift
Scan Date:	Feb. 20, 2022, 1:23 p.m.
App Security Score:	31/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	WARNING	INFO	✓ SECURE
4	2	2	1

FILE INFORMATION

File Name: iGoat-Swift.ipa
Size: 15.93MB
MD5: e73a7bf48e090a445febc06253a2ae60
SHA1: e560f00633d96a40f1d0f949ff3a854830e3af50
SHA256: 364273106c7fdb7b627bf7821a1539af4044025bf7190ebb760afb4b85c15a47

APP INFORMATION

App Name: iGoat-Swift
App Type: Swift
Identifier: OWASP.iGoat-Swift
SDK Name: iphoneos13.2
Version: 1.0
Build: 1
Platform Version: 13.2
Min OS Version: 10.0
Supported Platforms: iPhoneOS,

BINARY INFORMATION

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

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
com.iGoat.myCompany Editor	iGoat

APPLICATION PERMISSIONS

PERMISSIONS	STATUS	DESCRIPTION	REASON IN MANIFEST
NSFaceIDUsageDescription	normal	Access the ability to authenticate with Face ID.	iGoat would like to use FaceID to authenticate you.

APP TRANSPORT SECURITY (ATS)

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

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) _strncpy , _memcpy , _strlen , _fopen , _strcpy
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
			The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-

NX	True	info	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
ocsp.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.apple.com	ok	**IP:** 23.59.85.8 **Country:** Poland **Region:** Mazowieckie **City:** Warsaw **Latitude:** 52.229771 **Longitude:** 21.011780 **View:** Google Map
twitter.com	ok	**IP:** 104.244.42.193 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.773968 **Longitude:** -122.410446 **View:** Google Map
www.arxan.com	ok	**IP:** 204.16.106.105 **Country:** United States of America **Region:** California **City:** Brisbane **Latitude:** 37.688900 **Longitude:** -122.405098 **View:** Google Map
www.owasp.org	ok	**IP:** 104.22.26.77 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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

s3.us-east-2.amazonaws.com	ok	**IP:** 52.219.97.233 **Country:** United States of America **Region:** Ohio **City:** Columbus **Latitude:** 39.961182 **Longitude:** -82.998787 **View:** Google Map
www.igoatapp.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
www.linkedin.com	ok	**IP:** 13.107.42.14 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
www.paypal.com	ok	**IP:** 151.101.65.21 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
m.youtube.com	ok	**IP:** 142.250.201.206 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

www.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
www.krvw.com	ok	**IP:** 66.207.131.17 **Country:** United States of America **Region:** Pennsylvania **City:** Pittsburgh **Latitude:** 40.464062 **Longitude:** -79.947060 **View:** Google Map
www.paypalobjects.com	ok	**IP:** 192.229.221.25 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.034081 **Longitude:** -77.488503 **View:** Google Map
www.w3.org	ok	**IP:** 128.30.52.100 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **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

platform.twitter.com	ok	**IP:** 192.229.233.25 **Country:** United States of America **Region:** New Jersey **City:** Newark **Latitude:** 40.735661 **Longitude:** -74.172371 **View:** Google Map

EMAILS

EMAIL	FILE
ophychius@gmail.com	iGoat-Swift.app/rutger.html
mansi.sheth@gmail.com	iGoat-Swift.app/mansi.html
ken@krvw.com jcarter@arxan.com	iGoat-Swift.app/KRvWAssociates.html
swaroop.yermalkar@owasp.org paypal@owasp.org	iGoat-Swift.app/splash.html
frf3fg@f20f.pf h@f.a0 fs4pfs0@fs.0f h@f.0f x@f.n1 h@f-.0f 0f@f.jl0 fx@ftpfyf.5iqfzf h@f.eva fj4@fj20fj.xfj f@fin.qjf f@5.o1 f@f.lxf	iGoat-Swift.app/iGoat-Swift

johndoe@yap.com john@test.com	
swaroop.yermalkar@owasp.org	iGoat-Swift.app/Swaroop_Junard.html
swaroop.yermalkar@owasp.org	iGoat-Swift.app/Swaroop_anthony.html
swaroop.yermalkar@owasp.org	iGoat-Swift.app/Swaroop_Heefan.html
swaroop.yermalkar@owasp.org	iGoat-Swift.app/Swaroop.html
h@f.0f x@f.n1 john@test.com f@f.lxf 0f@f.jl0 h@f.eva h@f.a0 johndoe@yap.com fx@ftpfyf.5iqfzf fj4@fj20fj.xfj h@f-.0f f@fin.qjf	IPA Strings Dump

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.