IOS STATIC ANALYSIS REPORT

(1.0)

File Name:	igoat_ios.zip
Identifier:	com.swaroopsy.iGoat
Scan Date:	Dec. 4, 2025, 7:02 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	2	2	2	1

FILE INFORMATION

File Name: igoat_ios.zip
Size: 13.68MB
MD5: e018146bda5d7cb14ab45e7f265de8bd
SHA1: 89a8e8cfcfd6f1c543ef4b2dfe10c505ef404ac9
SHA256: 7e13dedd867e8023fd2cacdc84852917da73f94e6d5fd7cc480cdd7fb8418f1a

APP INFORMATION

App Name:
App Type: Objective-C
Identifier: com.swaroopsy.iGoat
SDK Name:
Version: 1.0
Build: 1
Platform Version:
Min OS Version:
Supported Platforms:

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

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION

CODE ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 2 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	User input in "loadHTMLString" will result in JavaScript Injection.	warning	CWE: CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') OWASP Top 10: M7: Client Code Quality OWASP MASVS: MSTG-PLATFORM-5	iGoat/iGoat/DetailViewController.m iGoat/iGoat/ExerciseIntroViewController.m iGoat/iGoat/HtmlViewController.m

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	iGoat/iGoat/BrokenCryptographyExerciseViewController.m iGoat/iGoat/DeviceLogsExerciseViewController.m iGoat/iGoat/KeychainExerciseViewController.m iGoat/iGoat/LocalDataStorageExerciseController.m iGoat/iGoat/NSObjectxSBJSON.m iGoat/iGoat/NSStringxSBJSON.m iGoat/iGoat/PlistStorageExerciseViewController.m iGoat/iGoat/PublicKeyPinningExerciseController.m iGoat/iGoat/RemoteAuthenticationExerciseController.m iGoat/iGoat/SBJsonParser.m iGoat/iGoat/ServerCommunicationExerciseController.m
3	This App may have Jailbreak detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	iGoat/iGoat/MethodSwizzlingExerciseController.m
4	App uses SQLite Database. Sensitive Information should be encrypted.	info	OWASP MASVS: MSTG-STORAGE-14	iGoat/iGoat/LocalDataStorageExerciseController.m iGoat/iGoat/SQLInjectionExerciseController.m
5	App allows self signed or invalid SSL certificates. App is vulnerable to MITM attacks.	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	iGoat/iGoat/PublicKeyPinningExerciseController.m

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
www.owasp.org	ok	**IP:** 172.66.157.115 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
code.google.com	ok	**IP:** 172.217.24.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
search.cpan.org	ok	**IP:** 151.101.209.55 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.krvw.com	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
ken@krvw.com sean@krvw.com	iGoat/iGoat/HtmlViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/SQLInjectionExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/main.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/Exercise.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/ExercisesViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/CutAndPasteExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/KeystrokeLoggingExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/iGoatAppDelegate.m

EMAIL	FILE
ken@krvw.com sean@krvw.com	iGoat/iGoat/InfoViewController.m
jcarter@arxan.com ken@krvw.com	iGoat/iGoat/PublicKeyPinningExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/AssetStore.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/DetailViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/StringAnalysisExerciseController.m
jcarter@arxan.com ken@krvw.com	iGoat/iGoat/MethodSwizzlingExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/RotationLimitingNavigationViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/RootViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/ExerciseViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/Utils.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/SQLInjectionArticlesViewController.m

EMAIL	FILE
ken@krvw.com sean@krvw.com	iGoat/iGoat/KeychainExerciseViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/ServerCommunicationExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/MasterViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/Asset.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/HintsViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/ExerciseIntroViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/RemoteAuthenticationExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/ExerciseContainerViewController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/BackgroundingExerciseController.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/AppDelegate.m
ken@krvw.com sean@krvw.com	iGoat/iGoat/LocalDataStorageExerciseController.m

EMAIL	FILE
ken@krvw.com sean@krvw.com	iGoat/iGoat/Category.m
ken@krvw.com sean@krvw.com	iGoat/iGoat.xcodeproj/Utils.m
ken@krvw.com sean@krvw.com	iGoat/iGoatTests/iGoatTests.m

HARDCODED SECRETS

POSSIBLE SECRETS
Key : username
User : admin
Password : Secret@123
Key : password
bbd85d235f7037c6a033a9690534391ffeacecc8
EhEKNQoVVBsuCwUYDGcfDRUAKRsEDB1nDg8HHiIdW1Q9KE8RBgYxCkEdHWcYAAcHYBtBFwEuDAoRBw==

SCAN LOGS

Timestamp	Event	Error
2025-12-04 07:02:30	Generating Hashes	OK
2025-12-04 07:02:30	Extracting ZIP	OK
2025-12-04 07:02:30	Unzipping	OK
2025-12-04 07:02:31	Detecting source code type	OK
2025-12-04 07:02:31	Source code type - ios	OK
2025-12-04 07:02:31	Redirecting to iOS Source Code Analyzer	OK
2025-12-04 07:02:31	Generating Hashes	OK
2025-12-04 07:02:31	iOS File Analysis and Normalization	OK
2025-12-04 07:02:32	iOS Info.plist Analysis Started	OK
2025-12-04 07:02:32	Finding Info.plist in iOS Source	OK

2025-12-04 07:02:32	Fetching Details from App Store: com.swaroopsy.iGoat	OK
2025-12-04 07:02:33	Searching for secrets in plist files	OK
2025-12-04 07:02:33	iOS Source Code Analysis Started	OK
2025-12-04 07:02:34	iOS Source Code Analysis Completed	OK
2025-12-04 07:02:34	iOS API Analysis Started	OK
2025-12-04 07:02:34	iOS API Analysis Completed	OK
2025-12-04 07:02:34	Extracting Emails and URLs from Source Code	OK
2025-12-04 07:02:34	Email and URL Extraction Completed	OK
2025-12-04 07:02:34	Performing Malware check on extracted domains	OK
2025-12-04 07:02:42	Finished Code Analysis, Email and URL Extraction	OK
2025-12-04 07:02:42	Extracting String values and entropies from Code	OK

2025-12-04 07:02:42	Fetching icon path	OK
2025-12-04 07:02:44	Detecting Trackers from Domains	OK
2025-12-04 07:02:44	Saving to Database	OK

Report Generated by - MobSF v4.4.3

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.