



IOS STATIC ANALYSIS REPORT



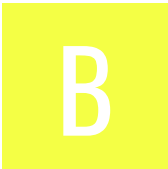
🍏 ImpactGuruDonor (1.6.929)

File Name:	withoutssl_ImpactGuruDonor.ipa
Identifier:	com.impactguru.donor-react-app
Scan Date:	June 23, 2026, 8:32 a.m.

App Security Score:

42/100 (MEDIUM RISK)

Grade:



Trackers Detection:

2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	6	2	0	6

FILE INFORMATION

File Name: withoutssl_ImpactGuruDonor.ipa
Size: 45.62MB
MD5: 43a39ad8a972da35f7dd84d81ec1de64

SHA1: 70a3e82cb44938a2fb15f965b028379e55fc1648
SHA256: 6c8825aed1ae81a741f673d2aa072e909083aaa42430297a3c84c829cf7deb9d

i APP INFORMATION

App Name: ImpactGuruDonor
App Type: Swift
Identifier: com.impactguru.donor-react-app
SDK Name: iphoneos26.2
Version: 1.6.929
Build: 96
Platform Version: 26.2
Min OS Version: 15.1
Supported Platforms: iPhoneOS,

Ad BINARY INFORMATION

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

#CUSTOM URL SCHEMES

URL NAME	SCHEMES
None	fb1000563233479492
None Editor	com.googleusercontent.apps.157774533426-a9klq5740mofd439hnes714v2k14jk4t
com.impactguru.donar-react-app Editor	igdonorapp
None	razorpay
com.impactguru.donor-react-app Editor	impactguru.com
com.impactguru.donor-react-app Editor	impactguru

≡ APPLICATION PERMISSIONS

PERMISSIONS	STATUS	INFO	REASON IN MANIFEST
NSCameraUsageDescription	dangerous	Access the Camera.	Camera permissions are required to set a profile picture, personalising the user experience and capture photos for specific tasks, unlocking rewards and enhancing user engagement in our Donor App
NSContactsUsageDescription	dangerous	Access Contacts.	Grant permission to the app to access your contacts, enabling you to effortlessly refer it to your friends and connections
NSHealthShareUsageDescription	dangerous	Read Health Data.	To enable users to track fitness-related data such as step counts and calories burned. The collected information is solely used within the app to provide users with insights into their fitness activities. It is also used to determine eligibility and reward users who successfully complete fitness challenges.
NSHealthUpdateUsageDescription	dangerous	Write Health Data.	To enable users to track fitness-related data such as step counts and calories burned. The collected information is solely used within the app to provide users with insights into their fitness activities. It is also used to determine eligibility and reward users who successfully complete fitness challenges.
NSLocationWhenInUseUsageDescription	dangerous	Access location information when app is in the foreground.	
NSMotionUsageDescription	dangerous	Access the device's accelerometer.	In order to count steps I need an access to your pedometer
NSPhotoLibraryUsageDescription	dangerous	Access the user's photo library.	Photo gallery permissions are required to set a profile picture, personalising the user experience and upload photos for specific tasks, unlocking rewards and enhancing user engagement in our Donor App

 APP TRANSPORT SECURITY (ATS)

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	Insecure local networking is allowed	high	App Transport Security restrictions are disabled for requests made from local networking without affecting your URLSession connections. This setting is not applicable to domains listed in NSExceptionDomains.

</> IPA BINARY CODE ANALYSIS

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

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 , _stat , _strcpy , _strlen , _strncat , _strncpy , _vsprintf

NO	ISSUE	SEVERITY	STANDARDS	DESCRIPTION
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

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	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/ImpactGuruDonor.app/Frameworks/Smartech.framework/Smartech	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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/ImpactGuruDonor.app/Frameworks/FBSDKGamingServicesKit.framework/FBSDKGamingServicesKit	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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/ImpactGuruDonor.app/Frameworks/hermes.framework/hermes	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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.	False info The binary does not have Runpath Search Path (@rpath) set.	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/ImpactGuruDonor.app/Frameworks/FBAEMKit.framework/FBAEMKit	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
5	Payload/ImpactGuruDonor.app/Frameworks/Razorpay.framework/Razorpay	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
6	Payload/ImpactGuruDonor.app/Frameworks/FBSDKShareKit.framework/FBSDKShareKit	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
7	Payload/ImpactGuruDonor.app/Frameworks/SmartPush.framework/SmartPush	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
8	Payload/ImpactGuruDonor.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
9	Payload/ImpactGuruDonor.app/Frameworks/RazorpayCore.framework/RazorpayCore	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	False high This binary does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option - fstack-protector-all to enable stack canaries.	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
10	Payload/ImpactGuruDonor.app/Frameworks/RazorpayStandard.framework/RazorpayStandard	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
11	Payload/ImpactGuruDonor.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
12	Payload/ImpactGuruDonor.app/Frameworks/FBSDKLoginKit.framework/FBSDKLoginKit	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
13	Payload/ImpactGuruDonor.app/Frameworks/Clarity.framework/Clarity	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	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
----	-------	----------	-----------	-------

 FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://impact-guru-1280.firebaseio.com

! OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
d2aq6dqxahe4ka.cloudfront.net	IP: 13.224.163.28 Country: Hong Kong Region: Hong Kong City: Hong Kong
certs.apple.com	IP: 17.253.85.137 Country: Hong Kong Region: Hong Kong City: Hong Kong
crl.apple.com	IP: 17.253.85.141 Country: Hong Kong Region: Hong Kong City: Hong Kong
cdn.razorpay.com	IP: 13.225.103.118 Country: Hong Kong Region: Hong Kong City: Hong Kong
cdn.branch.io	IP: 13.224.163.113 Country: Hong Kong Region: Hong Kong City: Hong Kong

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
dev.branch.io	ok	No Geolocation information available.
api-adservices.apple.com	ok	IP: 17.188.23.85 Country: United States of America Region: California City: Cupertino Latitude: 37.316605 Longitude: -122.046486 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.i18next.com	ok	IP: 104.18.40.47 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
whitehat.impactguru.com.dropbox.android.permission.access	ok	No Geolocation information available.
api-safetrack.branch.io	ok	IP: 108.158.245.25 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
help.branch.io	ok	IP: 104.18.20.218 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
iid.googleapis.com	ok	IP: 216.239.38.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
bnc.lt	ok	IP: 18.66.78.44 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
api3-eu.branch.io	ok	IP: 18.66.63.56 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
wa.me	ok	IP: 57.144.41.32 Country: United States of America Region: California City: Palo Alto Latitude: 37.441879 Longitude: -122.143021 View: Google Map
console.firebase.google.com	ok	IP: 192.178.173.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
.app-analytics-services-att.com	ok	No Geolocation information available.
www.google.com	ok	IP: 142.251.153.119 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
helpx.adobe.com	ok	IP: 23.48.245.155 Country: India Region: Delhi City: New Delhi Latitude: 28.635759 Longitude: 77.224449 View: Google Map
plus.google.com	ok	IP: 142.250.193.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
d2aq6dqxahe4ka.cloudfront.net	ok	IP: 13.224.163.28 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map

DOMAIN	STATUS	GEOLOCATION
firebaseremoteconfigrealtime.googleapis.com	ok	IP: 216.239.34.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
razorpay.com	ok	IP: 18.66.78.93 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
www.whitehat.com	ok	IP: 172.67.185.205 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
firebase-settings.crashlytics.com	ok	IP: 192.178.158.94 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
stage1.igstg.com	ok	IP: 172.67.191.34 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
npms.io	ok	IP: 104.21.49.221 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
api.razorpay.com	ok	IP: 13.126.148.6 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 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
lumberjack.razorpay.com	ok	IP: 13.234.245.177 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map
ocsp.apple.com	ok	IP: 17.253.18.201 Country: Brazil Region: Sao Paulo City: Sao Paulo Latitude: -23.547501 Longitude: -46.636108 View: Google Map
firebase.google.com	ok	IP: 142.250.134.139 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
firebaseLogging.googleapis.com	ok	IP: 216.239.38.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map

DOMAIN	STATUS	GEOLOCATION
accounts.google.com	ok	IP: 192.178.158.84 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
rnfirebase.io	ok	IP: 104.21.62.204 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
www.facebook.com	ok	IP: 57.144.40.1 Country: United States of America Region: California City: Palo Alto Latitude: 37.441879 Longitude: -122.143021 View: Google Map
graph.facebook.com	ok	IP: 57.144.48.141 Country: United States of America Region: California City: Palo Alto Latitude: 37.441879 Longitude: -122.143021 View: Google Map
developers.facebook.com	ok	IP: 57.144.48.141 Country: United States of America Region: California City: Palo Alto Latitude: 37.441879 Longitude: -122.143021 View: Google Map
77a84256-2401-46ee-a801-edcecb4efe94.mock.pstmn.io	ok	IP: 172.64.152.13 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.clarity.ms	ok	IP: 74.162.106.40 Country: United States of America Region: Florida City: Orlando Latitude: 28.558441 Longitude: -81.356186 View: Google Map
certs.apple.com	ok	IP: 17.253.85.137 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
example.invalid	ok	No Geolocation information available.
www.apple.com	ok	IP: 2.20.157.47 Country: Italy Region: Lombardia City: Milan Latitude: 45.464272 Longitude: 9.189510 View: Google Map
impact4.igstg.com	ok	IP: 172.67.191.34 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
device-provisioning.googleapis.com	ok	IP: 216.239.34.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
observablender-phone-android.permission.bluetooth	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
api3.branch.io	ok	IP: 108.158.245.48 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
static.razorpay.com	ok	No Geolocation information available.
momentjs.com	ok	IP: 104.17.63.214 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
dev.to	ok	IP: 151.101.2.217 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
fpn.netcoresmartech.com	ok	IP: 65.2.207.233 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map
app-analytics-services-att.com	ok	IP: 142.250.67.14 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
tools.ietf.org	ok	IP: 104.16.44.99 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map

DOMAIN	STATUS	GEOLOCATION
fcmtoken.googleapis.com	ok	IP: 216.239.32.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
react.dev	ok	IP: 76.76.21.98 Country: United States of America Region: California City: Walnut Latitude: 34.015400 Longitude: -117.858223 View: Google Map
dummyapiverylong-dummy.google.com	ok	No Geolocation information available.
reactnative.dev	ok	IP: 52.74.6.109 Country: Singapore Region: Singapore City: Singapore Latitude: 1.289670 Longitude: 103.850067 View: Google Map
whitehatapi.impactguru.com	ok	IP: 104.20.20.6 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
play.google.com	ok	IP: 142.250.193.142 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
api2.netcoresmartech.com	ok	IP: 13.200.139.176 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map

DOMAIN	STATUS	GEOLOCATION
app-analytics-services.com	ok	IP: 192.178.174.102 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
crl.apple.com	ok	IP: 17.253.85.141 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
reactnavigation.org	ok	IP: 172.67.138.49 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
itunes.apple.com	ok	IP: 2.20.156.28 Country: Italy Region: Lombardia City: Milan Latitude: 45.464272 Longitude: 9.189510 View: Google Map
ns.adobe.com	ok	No Geolocation information available.
cpn.netcoresmartech.com	ok	IP: 23.55.108.25 Country: India Region: Delhi City: New Delhi Latitude: 28.635759 Longitude: 77.224449 View: Google Map
whitehatapi.impactguru.com.android.voicemail.permission.write	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
docs.swmansion.com	ok	IP: 104.26.8.117 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
firebaseinstallations.googleapis.com	ok	IP: 216.239.32.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
fakeurl.com	ok	No Geolocation information available.
api-safetrack-eu.branch.io	ok	IP: 18.66.63.84 Country: United States of America Region: Washington City: Seattle Latitude: 47.627499 Longitude: -122.346199 View: Google Map
fb.gg	ok	IP: 57.144.40.141 Country: United States of America Region: California City: Palo Alto Latitude: 37.441879 Longitude: -122.143021 View: Google Map
purl.org	ok	IP: 207.241.225.157 Country: United States of America Region: California City: San Francisco Latitude: 37.781734 Longitude: -122.459435 View: Google Map
www.npmjs.com	ok	IP: 104.17.134.117 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

DOMAIN	STATUS	GEOLOCATION
impact3.igstg.com.apple.health-caret-back-circle-outline	ok	No Geolocation information available.
cdn.razorpay.com	ok	IP: 13.225.103.118 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
open.spotify.com	ok	IP: 151.101.107.42 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
whitehatapi.impactguru.com.evernote-addcompilersafegetandset	ok	No Geolocation information available.
firebaseappcheck.googleapis.com	ok	IP: 216.239.32.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
impact-guru-1280.firebaseio.com	ok	IP: 34.120.206.254 Country: United States of America Region: Missouri City: Kansas City Latitude: 39.099731 Longitude: -94.578568 View: Google Map
butler.razorpay.com	ok	IP: 13.126.148.6 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map

DOMAIN	STATUS	GEOLOCATION
goo.gl	ok	IP: 192.178.158.113 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
cdn.branch.io	ok	IP: 13.224.163.113 Country: Hong Kong Region: Hong Kong City: Hong Kong Latitude: 22.285521 Longitude: 114.157692 View: Google Map
fb.me	ok	IP: 57.144.48.1 Country: United States of America Region: California City: Palo Alto Latitude: 37.441879 Longitude: -122.143021 View: Google Map
www.impactguru.com	ok	IP: 104.20.20.6 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api.netcoresmartech.com	ok	IP: 44.193.86.235 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
lumberjack-metrics.razorpay.com	ok	IP: 13.234.245.177 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map

DOMAIN	STATUS	GEOLOCATION
clarity.microsoft.com	ok	IP: 13.107.9.158 Country: United Kingdom of Great Britain and Northern Ireland Region: England City: London Latitude: 51.508530 Longitude: -0.125740 View: Google Map
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
redux.js.org	ok	IP: 52.74.6.109 Country: Singapore Region: Singapore City: Singapore Latitude: 1.289670 Longitude: 103.850067 View: Google Map
firebaseremoteconfig.googleapis.com	ok	IP: 216.239.34.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
.app-analytics-services.com	ok	No Geolocation information available.
carepalsecure3.igstg.com	ok	IP: 104.21.60.36 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
api2.netcorecloud.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
www.googleapis.com	ok	IP: 216.239.34.223 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
github.com	ok	IP: 20.207.73.82 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
whitehat.impactguru.com.android.voicemail.permission.read	ok	No Geolocation information available.
branch.app.link	ok	IP: 99.86.30.93 Country: India Region: Delhi City: Delhi Latitude: 28.666670 Longitude: 77.216667 View: Google Map
api.igstg.com	ok	IP: 13.127.57.28 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map
www.googleadservices.com	ok	IP: 142.250.193.130 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
apps.apple.com	ok	IP: 2.20.156.28 Country: Italy Region: Lombardia City: Milan Latitude: 45.464272 Longitude: 9.189510 View: Google Map

DOMAIN	STATUS	GEOLOCATION
psegment.netcoresmartech.com	ok	IP: 15.207.230.166 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map

EMAILS

EMAIL	FILE
q@k.k_ 3@9.rr defaultrealm@host.com	ImpactGuruDonor.app/ImpactGuruDonor
aultsystemfontsmtest@gmail.com 610@2611a.600 rtshouldsetresponder@fcm.googleapis timerdonationidgdgfh@gmail.com superstruct@0.11 611@2641a.n1 zack@root-two.com rice-skatingguestuser@impactguru.com support@branch.ios donorsupport@impactguru.com react-native-screens@3.30 info@impactguru.com	ImpactGuruDonor.app/main.jsbundle
2i@xfzxl.znxz1tcg	ImpactGuruDonor.app/assets/Src/Assets/Images/loader.gif
jx@9p.dh	ImpactGuruDonor.app/assets/Src/Assets/Images/NativePayments/pump-heart.gif
4@m-l.pmlu	ImpactGuruDonor.app/assets/Src/Assets/Images/NativePayments/rocket.gif
7w@-.ex	ImpactGuruDonor.app/assets/Src/Assets/Images/MatchingDonation/golden_heartbeat.gif
d@2m.jfqs	ImpactGuruDonor.app/assets/Src/Assets/Images/HomeScreen/coinGif.gif
jx@9p.dh	ImpactGuruDonor.app/assets/Src/Assets/Images/AppMatchingShareModal/red-heart.gif
defaultrealm@host.com	IPA Strings Dump
smartech@netcorecloud.com	Payload/ImpactGuruDonor.app/Frameworks/Smartech.framework/Smartech

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27

 HARDCODED SECRETS

POSSIBLE SECRETS
firebase_json_raw : eyJjcmFzaGx5dGljc19hdXRvX2NvbGxlY3Rpb25fZW5hYmxlZCI6IHRYdWUslCJwZXJmX2F1dG9fY29sbGVjdGlvb9l9bmFibGVkijogdHJ1ZSwgImNyYXNobHl0aWNzX2RIYnVnX2VuYWJsZWQiOiBmYWxzZX0=
FacebookClientToken : e70da268f5a0902de849ece6bad81548
API_KEY : AlzaSyCf7L6ugmgyM0inAv0UjtUOJmoMRCvgp8Y

 SCAN LOGS

Timestamp	Event	Error
2026-06-23 08:32:55	iOS Binary (IPA) Analysis Started	OK
2026-06-23 08:32:55	Generating Hashes	OK
2026-06-23 08:32:55	Extracting IPA	OK
2026-06-23 08:32:55	Unzipping	OK
2026-06-23 08:32:56	iOS File Analysis and Normalization	OK
2026-06-23 08:32:56	iOS Info.plist Analysis Started	OK

2026-06-23 08:32:56	Finding Info.plist in iOS Binary	OK
2026-06-23 08:32:56	Fetching Details from App Store: com.impactguru.donor-react-app	OK
2026-06-23 08:32:57	Failed to get app details	KeyError('sellerUrl')
2026-06-23 08:32:57	Searching for secrets in plist files	OK
2026-06-23 08:32:57	Starting Binary Analysis	OK
2026-06-23 08:32:57	Dumping Classes from the binary	OK
2026-06-23 08:32:57	Running jtool against the binary for dumping classes	OK
2026-06-23 08:33:57	Library Binary Analysis Started	OK
2026-06-23 08:33:58	Framework Binary Analysis Started	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/Smartech.framework/Smartech	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/FBSDKGamingServicesKit.framework/FBSDKGamingServicesKit	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/hermes.framework/hermes	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/FBAEMKit.framework/FBAEMKit	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/Razorpay.framework/Razorpay	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/FBSDKShareKit.framework/FBSDKShareKit	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/SmartPush.framework/SmartPush	OK

2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/FBSDKCoreKit.framework/FBSDKCoreKit	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/RazorpayCore.framework/RazorpayCore	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/RazorpayStandard.framework/RazorpayStandard	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/FBSDKCoreKit_Basics.framework/FBSDKCoreKit_Basics	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/FBSDKLoginKit.framework/FBSDKLoginKit	OK
2026-06-23 08:33:58	Analyzing Payload/ImpactGuruDonor.app/Frameworks/Clarity.framework/Clarity	OK
2026-06-23 08:33:59	Extracting String Metadata	OK
2026-06-23 08:33:59	Extracting URL and Email from IPA	OK
2026-06-23 08:34:09	Performing Malware check on extracted domains	OK
2026-06-23 08:34:22	Fetching IPA icon path	OK
2026-06-23 08:34:26	Detecting Trackers from Domains	OK
2026-06-23 08:34:27	Saving to Database	OK

Report Generated by - MobSF v4.5.0

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.

© 2026 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).