

Koolspan_TrustCall_Android Scan Report

Project Name	Koolspan_TrustCall_Android
Scan Start	Monday, June 29, 2020 11:49:14 AM
Preset	All
Scan Time	-04h:-50m:-59s
Lines Of Code Scanned	120335
Files Scanned	1226
Report Creation Time	Monday, June 29, 2020 12:50:33 PM
Online Results	http://checkmarx.igapp.com/CxWebClient/ViewerMain.aspx?scanid=1211861&projectid=80404
Team	Users
Checkmarx Version	8.9.0.210 HF14
Scan Type	Full
Source Origin	LocalPath
Density	1/100 (Vulnerabilities/LOC)
Visibility	Public

Filter Settings

Severity

Included: High, Medium, Low, Information

Excluded: None

Result State

Included: Confirmed, Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Excluded: None

Assigned to

Included: All

Categories

Included:

Uncategorized	All
Custom	All
PCI DSS v3.2	All
OWASP Top 10 2013	All
STIG	All
FISMA 2014	All
NIST SP 800-53	All
OWASP Top 10 2017	All
OWASP Mobile Top 10 2016	All
NIAP 1.2 - Alpha	All

Excluded:

Uncategorized	None
Custom	None
PCI DSS v3.2	None

OWASP Top 10 2013	None
STIG	None
FISMA 2014	None
NIST SP 800-53	None
OWASP Top 10 2017	None
OWASP Mobile Top 10 2016	None
NIAP 1.2 - Alpha	None

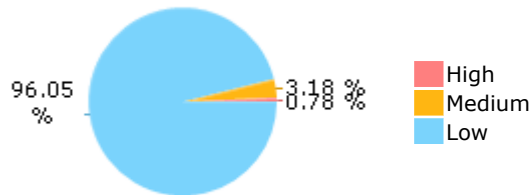
Results Limit

A limit was not defined

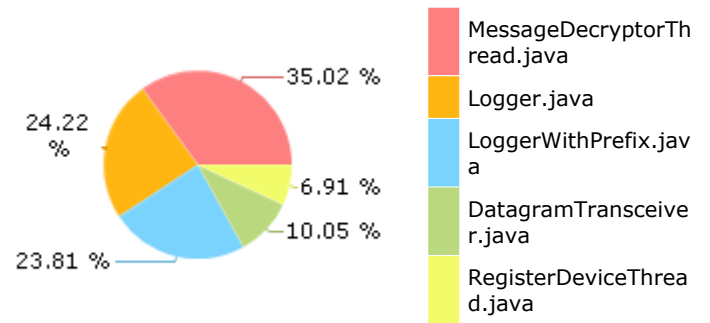
Selected Queries

Selected queries are listed in [Result Summary](#)

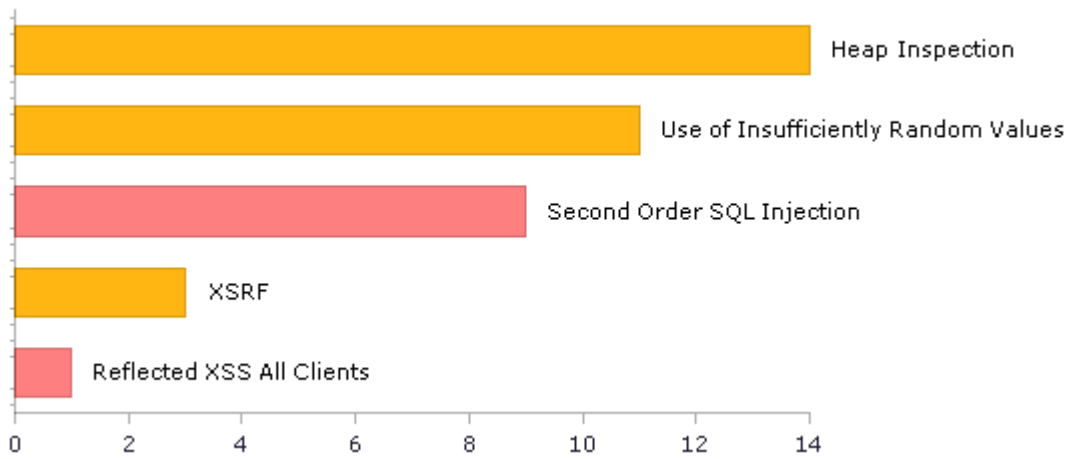
Result Summary



Most Vulnerable Files



Top 5 Vulnerabilities



Scan Summary - OWASP Top 10 2017

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2017](#)

Category	Threat Agent	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	85	16
A2-Broken Authentication	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	9	8
A3-Sensitive Data Exposure	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	24	23
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	202	198
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	557	99
A7-Cross-Site Scripting (XSS)*	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	6	1
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Top 10 2013

Further details and elaboration about vulnerabilities and risks can be found at: [OWASP Top 10 2013](https://owasp.org/Top10)

Category	Threat Agent	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact	Issues Found	Best Fix Locations
A1-Injection	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	20	9
A2-Broken Authentication and Session Management	EXTERNAL, INTERNAL, USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	305	304
A3-Cross-Site Scripting (XSS)*	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	6	1
A4-Insecure Direct Object References	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	5	2
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	513	55
A6-Sensitive Data Exposure	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	21	20
A7-Missing Function Level Access Control	EXTERNAL, INTERNAL, USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	197	196
A8-Cross-Site Request Forgery (CSRF)*	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with Known Vulnerabilities	EXTERNAL, USERS, AUTOMATED TOOLS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Scan Summary - PCI DSS v3.2

Category	Issues Found	Best Fix Locations
PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection	14	4
PCI DSS (3.2) - 6.5.2 - Buffer overflows	0	0
PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage	7	6
PCI DSS (3.2) - 6.5.4 - Insecure communications	26	26
PCI DSS (3.2) - 6.5.5 - Improper error handling	974	516
PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS)	6	1
PCI DSS (3.2) - 6.5.8 - Improper access control	557	549
PCI DSS (3.2) - 6.5.9 - Cross-site request forgery*	0	0
PCI DSS (3.2) - 6.5.10 - Broken authentication and session management	10	9

* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Scan Summary - FISMA 2014

Category	Description	Issues Found	Best Fix Locations
Access Control	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	46	45
Audit And Accountability	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	318	318
Configuration Management	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	551	93
Identification And Authentication	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	354	312
Media Protection	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	11	10
System And Communications Protection	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	122	43

Scan Summary - NIST SP 800-53

Category	Issues Found	Best Fix Locations
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	374	372
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	65	7
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	1	1
SC-13 Cryptographic Protection (P1)	14	14
SC-17 Public Key Infrastructure Certificates (P1)	0	0
SC-18 Mobile Code (P2)	0	0
SC-23 Session Authenticity (P1)*	51	9
SC-28 Protection of Information at Rest (P1)	7	7
SC-4 Information in Shared Resources (P1)	8	2
SC-5 Denial of Service Protection (P1)	248	245
SC-8 Transmission Confidentiality and Integrity (P1)	2	1
SI-10 Information Input Validation (P1)	33	17
SI-11 Error Handling (P2)	794	336
SI-15 Information Output Filtering (P0)*	6	1
SI-16 Memory Protection (P1)	20	20

* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Mobile Top 10 2016

Category	Description	Issues Found	Best Fix Locations
M1-Improper Platform Usage*	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage*	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication*	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication*	This category captures notions of authenticating the end user or bad session management. This can include: -Failing to identify the user at all when that should be required -Failure to maintain the user's identity when it is required -Weaknesses in session management	0	0
M5-Insufficient Cryptography*	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category is for issues where cryptography was attempted, but it wasn't done correctly.	0	0
M6-Insecure Authorization*	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality*	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that's running on the mobile device.	32	12
M8-Code Tampering*	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or	0	0

	modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.		
M9-Reverse Engineering*	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	7	7
M10-Extraneous Functionality*	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Scan Summary - Custom

Category	Issues Found	Best Fix Locations
Must audit	0	0
Check	0	0
Optional	0	0

Scan Summary - STIG

Category	Issues Found	Best Fix Locations
CAT I: APP3250_1 The Designer will ensure unclassified sensitive data transmitted through a commercial or wireless network is protected using NIST-certified cryptography*	0	0
CAT I: APP3310 The Designer will ensure the application does not display account passwords as clear text*	7	7
CAT I: APP3405 The Designer will ensure the application supports detection and/or prevention of communication session hijacking*	0	0
CAT I: APP3510 The Designer will ensure the application validates all input	45	17
CAT I: APP3540_1 The Designer will ensure the application is not vulnerable to SQL injection*	20	9
CAT I: APP3560 The Designer will ensure the application does not contain format string vulnerabilities	0	0
CAT I: APP3570 The Designer will ensure the application does not allow command injection	0	0
CAT I: APP3580 The Designer will ensure the application does not have XSS vulnerabilities*	6	1
CAT I: APP3590_1 The Designer will ensure the application does not have buffer overflows	9	4
CAT II: APP2060_4 The Designer will not use unsafe functions documented in the project coding standards*	0	0
CAT II: APP3050 The Designer will ensure the application does not contain source code that is never invoked during operation except for software components and libraries from approved third-party products which may include un-invoked code	5	5
CAT II: APP3100 The Designer will ensure the application removes temporary storage of files and cookies when the application is terminated	3	3
CAT II: APP3120 The Designer will ensure the application is not subject to error handling vulnerabilities	976	518
CAT II: APP3150_1 The Designer will ensure the application uses FIPS 140-2 validated cryptographic modules if the application implements encryption key exchange digital signature and hash functionality	13	13
CAT II: APP3230_1 The Designer will ensure the application properly clears or overwrites all memory blocks used to process sensitive data if required by the information owner	0	0
CAT II: APP3585 The Designer will ensure the application does not have CSRF vulnerabilities*	0	0
CAT II: APP3590_2 The Designer will ensure the application does not use functions known to be vulnerable to buffer overflows	9	4
CAT II: APP3630_1 The Designer will ensure the application is not vulnerable to race conditions	20	20
CAT II: APP3630_3 The Designer will ensure a multi-threaded application uses thread safe functions when threads are accessing the same object or data	8	2
CAT II: APP3630_4 The Designer will ensure global resources are locked before being accessed by the application	0	0
CAT II: APP3690_2 The Designer will ensure the audit trail is protected against modification or deletion except by the application and auditors	13	3

* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Scan Summary - NIAP 1.2 - Alpha

Category	Issues Found	Best Fix Locations
FCS_RBG_EXT.1.1 - The application shall [selection: use no DRBG functionality, invoke platform-provided DRBG functionality, implement DRBG functionality] for its cryptographic operations.*	0	0
FCS_STO_EXT.1.1 - The application shall [selection: not store any credentials, invoke the functionality provided by the platform to securely store [assignment: list of credentials] , implement functionality to securely store [assignment: list of credentials]] to non-volatile memory*	7	7
FDP_DEC_EXT.1.1 - The application shall restrict its access to [selection: no hardware resources, network connectivity, camera, microphone, location services, NFC, USB, Bluetooth, [assignment: list of additional hardware resources]] .	0	0
FDP_DEC_EXT.1.2 - The application shall restrict its access to [selection: no sensitive information repositories, address book, calendar, call lists, system logs, [assignment: list of additional sensitive information repositories]] .	0	0
FDP_NET_EXT.1.1 - The application shall restrict network communication to [selection: no network communication, user-initiated communication for [assignment: list of functions for which the user can initiate network communication] , respond to [assignment: list of remotely initiated communication] , [assignment: list of application-initiated network communication]] .*	296	296
FDP_DAR_EXT.1.1 - The application shall [selection: leverage platform-provided functionality to encrypt sensitive data, implement functionality to encrypt sensitive data, not store any sensitive data] in non-volatile memory.*	13	3
FMT_MEC_EXT.1.1 - The application shall invoke the mechanisms recommended by the platform vendor for storing and setting configuration option*	0	0
FMT_CFG_EXT.1.1 - The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials	0	0
FMT_CFG_EXT.1.2 - The application shall be configured by default with file permissions which protect it and its data from unauthorized access.	0	0
FMT_SMF.1.1 - The TSF shall be capable of performing the following management functions [selection: no management functions, enable/disable the transmission of any information describing the system s hardware, software, or configuration , enable/disable the transmission of any PII , enable/disable transmission of any application state (e.g. crashdump) information, enable/disable network backup functionality to [assignment: list of enterprise or commercial cloud backup systems] , [assignment: list of other management functions to be provided by the TSF]] .*	1	1
FPR_ANO_EXT.1.1 - The application shall [selection: not transmit PII over a network , require user approval before executing [assignment: list of functions that transmit PII over a network]] .	46	45
FPT_API_EXT.1.1 - The application shall use only documented platform APIs.	0	0
FPT_AEX_EXT.1.1 - The application shall not request to map memory at an explicit address except for [assignment: list of explicit exceptions] .	0	0
FPT_AEX_EXT.1.2 - The application shall [selection: not allocate any memory region with both write and execute permissions , allocate memory regions with write and execute permissions for only [assignment: list of functions performing just-in-time compilation]] .	0	0
FPT_AEX_EXT.1.3 - The application shall be compatible with security features provided by the platform vendor.	0	0
FPT_AEX_EXT.1.4 - The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.	0	0
FPT_AEX_EXT.1.5 - The application shall be compiled with stack-based buffer overflow protection enabled.	0	0
FPT_TUD_EXT.1.1 - The application shall [selection: provide the ability, leverage the platform] to check for updates and patches to the application software.	0	0
FPT_TUD_EXT.1.2 - The application shall be distributed using the format of the platform-supported package manager.	0	0

FPT_TUD_EXT.1.3 - The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.	0	0
FPT_TUD_EXT.1.4 - The application shall not download, modify, replace or update its own binary code	0	0
FPT_TUD_EXT.1.5 - The application shall [selection, at least one of: provide the ability, leverage the platform] to query the current version of the application software.	0	0
FPT_TUD_EXT.1.6 - The application installation package and its updates shall be digitally signed such that its platform can cryptographically verify them prior to installation	0	0
FPT_LIB_EXT.1.1 - The application shall be packaged with only [assignment: list of third-party libraries] .	0	0
FTP_DIT_EXT.1.1 - The application shall [selection: not transmit any data, not transmit any sensitive data, encrypt all transmitted sensitive data with [selection, at least one of: HTTPS, TLS, DTLS, SSH as conforming to the Extended Package for Secure Shell] , encrypt all transmitted data with [selection, at least one of: HTTPS, TLS, DTLS, SSH]] between itself and another trusted IT product.*	19	8
FCS_CKM.1.1(2) - The application shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [selection: 128 bit, 256 bit] .*	1	1
FCS_TLSC_EXT.2.1 - The application shall support mutual authentication using X.509v3 certificates.	0	0
FCS_RBG_EXT.2.1 - The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)] .	0	0
FCS_RBG_EXT.2.2 - The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [selection: a software-based noise source, no other noise source] with a minimum of [selection: 128 bits, 256 bits] of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.	0	0
FCS_CKM_EXT.1.1 - The application shall [selection: generate no asymmetric cryptographic keys, invoke platform-provided functionality for asymmetric key generation, implement asymmetric key generation] .	6	6
FCS_CKM.1.1(1) - The application shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [selection: [RSA schemes] using cryptographic key sizes of [2048- bit or greater] that meet the following: [selection: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 , ANSI X9.31-1998, Section 4.1] , [ECC schemes] using ["NIST curves" P-256, P-384 and [selection: P-521 , no other curves]] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4] , [FFC schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1]] .	0	0
FCS_COP.1.1(1) - The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode; and [selection: AES-GCM (as defined in NIST SP 800-38D), no other modes] and cryptographic key sizes 256-bit and [selection: 128-bit, no other key sizes] .	0	0
FCS_TLSC_EXT.1.2 - The application shall verify that the presented identifier matches the reference identifier according to RFC 6125.	0	0
FCS_TLSC_EXT.1.3 - The application shall establish a trusted channel only if the peer certificate is valid.*	0	0
FCS_TLSS_EXT.1.2 - The application shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and [selection: TLS 1.2, none] .	0	0
FCS_CKM.2.1 - The application shall [selection: invoke platform-provided functionality , implement functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [RSA-based key establishment schemes] that meets the following: [NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"] and [selection: [Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"] , [Finite field-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"] , No other schemes] .	0	0
FCS_COP.1.1(2) - The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [selection: SHA-1, SHA-256, SHA-384, SHA-512, no other algorithms] and message digest sizes [selection: 160, 256, 384, 512, no other message digest sizes] bits that meet the following: FIPS Pub 180-4	0	0
FCS_COP.1.1(3) - The application shall perform cryptographic signature services (generation and	0	0

verification) in accordance with a specified cryptographic algorithm [selection: RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4, ECDSA schemes using "NIST curves" P-256, P-384 and [selection: P-521, no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5] .		
FCS_COP.1.1(4) - The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-256 and [selection: SHA-1, SHA-384, SHA-512, no other algorithms] with key sizes [assignment: key size (in bits) used in HMAC] and message digest sizes 256 and [selection: 160, 384, 512, no other size] bits that meet the following: FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard.	0	0
FCS_TLSC_EXT.4.1 - The application shall present the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [selection: secp256r1, secp384r1, secp521r1] and no other curves.	0	0
FCS_TLSS_EXT.1.3 - The application shall generate key establishment parameters using RSA with size 2048 bits and [selection: 3072 bits, 4096 bits, no other sizes] and [selection: over NIST curves [selection: secp256r, secp384r] and no other curves, DiffieHellman parameters of size 2048 and [selection: 3072 bits, no other size] , no other]	0	0
FCS_TLSS_EXT.1.4 - The application shall support mutual authentication of TLS clients using X.509v3 certificates.	0	0
FCS_TLSS_EXT.1.5 - The application shall not establish a trusted channel if the peer certificate is invalid.	0	0
FCS_TLSS_EXT.1.6 - The application shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the peer.	0	0
FCS_DTLS_EXT.1.1 - The application shall implement the DTLS protocol in accordance with DTLS 1.2 (RFC 6347).	0	0
FCS_DTLS_EXT.1.2 - The application shall implement the requirements in TLS (FCS_TLSC_EXT.1) for the DTLS implementation, except where variations are allowed according to DTLS 1.2 (RFC 6347).	0	0
FCS_DTLS_EXT.1.3 - The application shall not establish a trusted communication channel if the peer certificate is deemed invalid.	0	0
FCS_HTTPS_EXT.1.1 - The application shall implement the HTTPS protocol that complies with RFC 2818.*	2	1
FCS_HTTPS_EXT.1.2 - The application shall implement HTTPS using TLS	0	0
FCS_TLSS_EXT.1.1 - The application shall [selection: invoke platform-provided TLS 1.2, implement TLS 1.2 (RFC 5246)] supporting the following cipher suites: Mandatory Cipher Suites: TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 Optional Cipher Suites: [selection: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, no other cipher suite] .	0	0
FCS_HTTPS_EXT.1.3 - The application shall notify the user and [selection: not FIA_X509_EXT.1.1 establish the connection , request application authorization to establish the connection , no other action] if the peer certificate is deemed invalid.	0	0
FIA_X509_EXT.1.1 - The application shall [selection: invoked platform-provided functionality , implement functionality] to validate certificates in accordance with the following rules:	0	0
FIA_X509_EXT.1.2 - The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.	0	0
FIA_X509_EXT.2.1 - The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: HTTPS , TLS , DTLS] .	0	0
FIA_X509_EXT.2.2 - When the application cannot establish a connection to determine the validity of a certificate, the application shall [selection: allow the administrator to choose whether to accept the certificate in these cases , accept the certificate , not accept the certificate] .	0	0

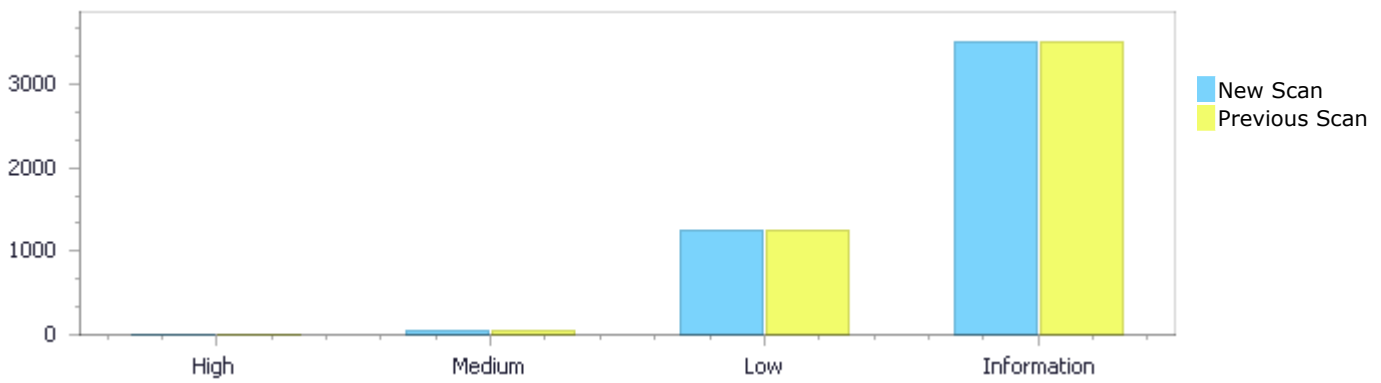
* Project scan results do not include all relevant queries. Presets and/or Filters should be changed to include all relevant standard queries.

Results Distribution By Status

Compared to project scan from 6/17/2020 3:32 PM

	High	Medium	Low	Information	Total
New Issues	0	0	1	0	1
Recurrent Issues	0	0	1,238	3,514	4,752
Total	0	0	1,239	3,514	4,753

Fixed Issues	0	0	1	1	2
--------------	---	---	---	---	---



Results Distribution By State

	High	Medium	Low	Information	Total
Confirmed	0	0	0	0	0
Not Exploitable	10	41	0	0	51
To Verify	0	0	1,239	3,514	4,753
Urgent	0	0	0	0	0
Proposed Not Exploitable	0	0	0	0	0
Total	10	41	1,239	3,514	4,804

Result Summary

Vulnerability Type	Occurrences	Severity
Second Order SQL Injection	9	High
Reflected XSS All Clients	1	High
Heap Inspection	14	Medium
Use of Insufficiently Random Values	11	Medium
XSRF	3	Medium

Download of Code Without Integrity Check	2	Medium
Improper Restriction of XXE Ref	2	Medium
Privacy Violation	2	Medium
Process Control	2	Medium
SSRF	2	Medium
CGI Stored XSS	1	Medium
Unchecked Input for Loop Condition	1	Medium
Use of a One Way Hash without a Salt	1	Medium
Information Exposure Through an Error Message	512	Low
Improper Resource Access Authorization	296	Low
Improper Exception Handling	148	Low
Stored Log Forging	52	Low
Incorrect Permission Assignment For Critical Resources	43	Low
Improper Resource Shutdown or Release	30	Low
Portability Flaw Locale Dependent Comparison	26	Low
Race Condition Format Flaw	20	Low
Log Forging	13	Low
Private Array Returned From A Public Method	10	Low
Integer Overflow	9	Low
Integer Underflow	9	Low
Unsynchronized Access To Shared Data	8	Low
Reversible One Way Hash	7	Low
Use Of Hardcoded Password	7	Low
Heuristic CGI Stored XSS	6	Low
Use of Broken or Risky Cryptographic Algorithm	6	Low
Public Data Assigned to Private Array	5	Low
Public Static Final References Mutable Object	4	Low
Stored Absolute Path Traversal	4	Low
Creation of Temp File With Insecure Permissions	3	Low
Leaving Temporary File	3	Low
Creation of Temp File in Dir with Incorrect Permissions	2	Low
Improper Exception Handling	2	Low
Insufficiently Protected Credentials	2	Low
Just One of Equals and Hash code Defined	2	Low
Divide By Zero	1	Low
Exposure of System Data	1	Low
Hardcoded AWS Credentials	1	Low
Heuristic SQL Injection	1	Low
Improper Transaction Handling	1	Low
Not Using a Random IV with CBC Mode	1	Low
Relative Path Traversal	1	Low
Uncontrolled Memory Allocation	1	Low
Use Of getenv	1	Low
Use of RSA Algorithm without OAEP	1	Low
Dead Code	1491	Information
Unused Variable	549	Information
Incorrect Block Delimitation	331	Information
Declaration Of Catch For Generic Exception	232	Information
Exposure of Resource to Wrong Sphere	192	Information
Insufficient Logging of Exceptions	123	Information
Empty Methods	67	Information
Expression is Always False	61	Information
Reliance On Untrusted Inputs In Security Decision	51	Information

Expression is Always True	44	Information
Input Not Normalized	40	Information
Public Static Field Not Marked Final	35	Information
Detection of Error Condition Without Action	32	Information
Unchecked Error Condition	32	Information
Uncontrolled Recursion	29	Information
Confusing Naming	25	Information
Missing Default Case In Switch Statement	23	Information
ESAPI Banned API	20	Information
Dynamic SQL Queries	19	Information
Declaration of Throws for Generic Exception	18	Information
Insufficient Logging of Database Actions	18	Information
Unclosed Objects	18	Information
Incorrect Conversion between Numeric Types	14	Information
Exposure of Resource to Wrong Sphere	11	Information
Use of Wrong Operator in String Comparison	11	Information
Potentially Serializable Class With Sensitive Data	7	Information
Leftover Debug Code	5	Information
Access Specifier Manipulation	3	Information
Portability Flaw In File Separator	3	Information
Improper Initialization	2	Information
Missing XML Validation	2	Information
Omitted Break Statement In Switch	2	Information
Use of Wrong Operator in String Comparison	2	Information
Array Declared Public Final and Static	1	Information
Not Static Final Logger	1	Information

10 Most Vulnerable Files

High and Medium Vulnerabilities

File Name	Issues Found
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/database/text/TextMessagesTable.java	8
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/common/transport/relayserver/RelayServerTransport.java	5
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/trustcall/databases/GroupChatSessionTable.java	4
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/MissingResources/src/MissingResources.java	4
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/config/TrustCallConfig.java	4
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/trustcall/activities/preferences/RelayServerSettingsActivity.java	4

trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/trustchip/unilateral/TDKUnilateralEncryptionHelper.java	3
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/text/service/SmsReceivedReceiver.java	3
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/trustcall/fragments/ConversationFragment.java	2
trustcall-master-igapp-e7838f91e22e806ecc04f2a2f3f35a7d92f53173/TrustCallAndroid/app/src/main/java/com/koolspan/text/service/TextMessageReencryptThread.java	2

Scanned Languages

Language	Hash Number	Change Date
Java	9842271496725627	2/14/2020
JavaScript	6861800560848663	2/14/2020
Groovy	3797911323776204	2/14/2020
Common	5160037751448622	2/14/2020