This document was generated by Syhunt Mobile **version 6.8.0.0**.

Supported Languages

Language	Coverage Type
Objective-C, C & C++ (iOS)	SAST
Java (JEE, Android)	SAST
JavaScript Environments (Node.js, Express.js & Koa.js)	SAST
JavaScript Client-Side (Angular & AngularJS)	SAST
Swift (iOS)	SAST
TypeScript (Angular)	SAST

Code Checks for Objective-C, C & C++

Total Checks: **136**

Check Name	Risk	CWE
Arbitrary File Manipulation		
Arbitrary File Write (Zip Slip)	high	22
Arbitrary File Manipulation Vulnerability	high	73
Resource Injection	high	99
API Misuse & Abuse		
Missing Biometric Auth Operation Justification	low	
SMS Usage	info	
Broken Authentication		
Missing Policy Evaluation Check	low	
Insufficient Touch ID Restriction (Biometric Auth)	medium	287
Insufficient Authentication Handling	high	
Insecure Credential Initialization	high	
Missing Request Host Check	high	

Check Name	Risk	CWE
Biometric LocalAuthentication Usage	info	287
Broken Cryptography		
Insecure Hashing Algorithm	medium	328
Empty Cryptographic Key	high	321
Empty HMAC Secret Key (Crypto)	high	321
Weak PBE Key Generation	high	321
Insecure PBE Iteration	high	916
User-Defined Salt	high	328
Insecure Initialization Vector (Crypto)	high	329
Insecure Cryptographic Mode and Initialization Vector	high	330
Insecure Cryptographic Mode	high	327
Inadequate Cryptographic Key Size	high	326
Insecure Cryptographic Algorithm	medium	327
Code Injection		
JavaScript Code Injection (WebView)	high	95
Unsafe Reflection	high	470
Denial of Service		
Buffer Overflow (Format)	high	120
Use of Insecure Legacy C Function	medium	676
Buffer Overflow	high	
Buffer Overflow	high	
Hardcoded Sensitive Information		
Hardcoded URI	info	
Unprotected Database or Asset	high	521
Hardcoded Cryptographic Key	high	321
Insecure Communication		

Check Name	Risk	CWE
Untrusted HTTPS Certificate Acceptance	high	
Insecure Cookie Creation	low	1004
Weak SSL Protocol (Default)	medium	326
Weak SSL Protocol	medium	326
Insecure HTTP URL	info	319
Insecure Data Storage		
Synchronized Credential	medium	
Insecure File Storage (Missing Protection)	medium	311
Insecure File Storage (Possibly Insufficient Protection)	info	311
Unencrypted Database	high	311
Insecure Image Storage	low	311
HTTP Cache Storage Incorrectly Disabled	high	311
Insecure HTTP Response Storage	low	311
Insecure HTTP Session Storage	low	311
Insecure Storage in Keychain (Missing Protection)	high	359
Externally Accessible Keychain	high	359
Insecure Storage in Keychain (Possibly Insufficient Protection)	info	311
Insecure Storage (Unenforced Passcode Policy)	medium	311
Insecure Storage in Keychain (Unspecified Access Policy)	medium	
Inadequate Password Protection	high	261
Insecure Storage of Sensitive Information	medium	256
Cleartext Storage of Sensitive Information	high	312
Sensitive Data Stored in Documents	high	359
Information Disclosure		
Information Leak	low	497
Unprotected Database	high	521

Check Name	Risk	CWE
Logging of Geolocation Data	medium	359
Forced Geolocation Data Transmission	medium	359
Insecure Password Input Field	medium	359
Insufficient Credential Removal	high	359
Logging of Sensitive Information	high	
Insecure Transmission of Sensitive Information	medium	359
JSON Injection		
JSON Injection	high	91
Log Forging		
Log Forging Vulnerability	low	117
Bad Practices		
Request Cache Usage	info	
Missing Default in Switch Statement	low	
Use of Jmp Function	medium	
Insecure String To Number Conversion	low	
Use of Float in Loop	low	
Forcible Application Termination	info	382
Goto Statement Usage	low	
Incorrect Temp File or Directory Creation	medium	
Overly-General Catch Clause	low	396
offsetof Macro Usage	low	
Command Execution		
Command Execution Vulnerability	high	78
Security Misconfiguration		
Missing Content Validation (IPC)	medium	501
Overly Broad Cookie Creation	low	287

Check Name	Risk	CWE
Persistent Cookie Creation	info	539
SQL Injection		
SQL Injection Vulnerability	high	89
Uncontrolled Format String		
Uncontrolled Format String	medium	134
XPath Injection		
XPath Injection Vulnerability	high	91
Cross-Site Scripting (XSS)		
Cross-Site Scripting (WebView XSS)	high	79

Code Checks for Objective-C, C & C++ Headers

Total Checks: **1**

Check Name	Risk	CWE
Information Disclosure		
Insecure Password Input Field	medium	359

Code Checks for Java

Total Checks: **315**

Check Name	Risk	CWE
Arbitrary File Manipulation		
Arbitrary File Manipulation Vulnerability	high	73
Arbitrary File Write (ZIP)	high	22
Inappropriate File Access Permissions	info	276
Broken Authentication		
Insegure Storage of Sensitive Information in Cookie	high	
Insecure Storage of Sensitive Information	medium	256
Insecure Facebook Login Handling	medium	

Check Name	Risk	CWE
Deprecated FingerprintManager API Usage	medium	
Missing BiometricPrompt Auth Failure Handling	medium	
Missing BiometricPrompt Error Handling	medium	
Missing BiometricPrompt Acquired Handling	medium	
Missing Google Sign In Error Handling	medium	
Missing Biometric Capability Check	medium	
Broken Cryptography		
Insecure Randomness	high	338
Use of RSA Algorithm without OAEP (Crypto)	medium	780
Insecure Random Number Generation	medium	335
Insecure Cryptographic Key Comparison	medium	
Insecure Cryptographic Mode	high	327
Weak Random Number Generation	medium	330
Missing User Confirmation (Crypto)	medium	
Missing unlockedDeviceRequired Flag (Crypto)	medium	
Insecure Cryptographic Algorithm	medium	327
Insecure Cryptographic Mode	high	327
Inadequate Cryptographic Key Size	high	326
Improper Seed of SecureRandom	medium	338
Predictable Random Number Generation	medium	338
Insecure SHA1 PRNG	medium	328
Insecure Cryptographic Mode and Initialization Vector	high	330
Custom Cryptographic Algorithm Usage	info	
Insecure Hashing Algorithm	medium	328
Code Injection		
Code Injection	high	94

Check Name	Risk	CWE
Unsafe Reflection	high	470
Code Injection (JavaBean)	high	15
Insecure URI Rendering (WebView)	high	
JavaScript Code Injection (WebView)	high	94
Debug Entry Points		
Leftover Debug Entry Point (Method)	medium	489
Denial of Service		
External Process Block	medium	
Regular Expression Injection	medium	400
File Inclusion		
File Inclusion Vulnerability	high	22
Hardcoded Sensitive Information		
Hardcoded URI	info	
Unprotected Database or Asset	high	521
HTTP Header Injection		
HTTP Header Injection Vulnerability	medium	113
HTTP Response Splitting		
HTTP Response Splitting Vulnerability	medium	113
Insecure Communication		
Use of Deprecated Java HttpClient	medium	
Insecure HTTPS Client Usage	medium	319
Insecure HTTP Connection	info	319
Insecure HTTP URL	info	319
Insecure Socket Data Exchange	medium	311
Insecure SMTP Connection	medium	297
Improper Host Verification	medium	295

Check Name	Risk	CWE
Insecure Authentication Method	high	522
Insecure Cookie Creation	low	1004
Weak SSL Protocol	medium	326
Information Disclosure		
Information Leak	low	497
Error Message Information Exposure	low	209
Missing Debug Check Call	low	
Insecure Temporary File Cleanup	low	377
External Storage Usage	info	
Sensitive Data Stored in External Storage	high	
Logging of Sensitive Information	high	
Insecure Content Context Mode	medium	
Sensitive Data in Global Broadcast	high	
Forced Geolocation Data Transmission	medium	359
Unprotected Database	high	521
Leftover Debug Code	low	489
JSON Injection		
Unsafe Deserialization (Jackson)	high	502
LDAP Injection		
LDAP Injection Vulnerability	high	90
Unprotected LDAP Transaction	high	521
Log Forging		
Log Forging Vulnerability	low	117
Bad Practices		
Memory Leak (Static Collection)	low	
Use of Java Array Constant	info	582

Check Name	Risk	CWE
Use of Insecure, Default Socket Factories	medium	319
Impossible Array Cast	low	704
Missing Catch of NumberFormatException	low	248
Unsafe NaN Comparison	low	
Loss of Precision (BigDecimal)	low	
Declaration of Throws for Generic Exception	info	397
NullPointerException Catch Clause	low	396
Lock Synchronization	low	
Insecure ThreadGroup Method Usage	low	362
Forceful Thread Termination	low	705
Missing File Deletion Error Handling	low	
Unsafe ResultSet Method Usage	low	
Improper Object Finalization	low	586
Overly-General Catch Clause	low	396
Insufficient Object Class Comparison	low	
Unsafe Finalizer Method Usage	medium	
Unreleased Lock (Deadlock)	low	833
Missing Default in Switch Statement	low	
Forcible JVM Termination	info	382
Thread Deadlock	medium	
Unsafe Synchronization Method	medium	
Incorrect Hex Conversion	high	704
Command Execution		
Use of Relative Path in Command	medium	88
Command Execution Vulnerability	high	78
Insecure Stream Reading	medium	

Check Name	Risk	CWE
Security Misconfiguration		
Unsafe Database Connection	medium	
Untrusted Input in Permission Check	high	807
Deactivated Security Manager	high	
Overly Broad Cookie Creation	low	287
SQL Injection		
SQL Injection Vulnerability	high	89
Direct SQL Table Access	low	
Server-Side Request Forgery		
Server-Side Request Forgery	medium	918
CSRF Protection Disabled	high	352
Insecure Request Mapping	medium	352
Uncontrolled Format String		
Uncontrolled Format String	medium	134
Unvalidated Redirect		
Unvalidated Redirect Vulnerability	low	601
XML Injection		
Incorrect XML Parsing Model	low	
Missing XXE Restriction	medium	611
Deserialization of Untrusted Data	high	502
XML Injection	high	91
XXE Injection	high	611
Missing XXE Restriction	medium	611
XPath Injection		
XPath Injection Vulnerability	high	91
Cross-Site Scripting (XSS)		

Check Name	Risk	CWE
Cross-Site Scripting (XSS) Vulnerability	medium	79
Weak Validation Method (XSS)	medium	625
Cross-Site Scripting (WebView XSS)	high	79

Code Checks for JavaScript Environments (Node.js)

Total Checks: **104**

Check Name	Risk	CWE
Arbitrary File Manipulation		
Arbitrary File Manipulation Vulnerability	high	73
Arbitrary File Write (Zip Slip)	high	22
Broken Cryptography		
Insecure Randomness	high	338
Insecure Hashing Algorithm	medium	328
Insecure Cryptographic Algorithm	medium	327
Backdoors		
Remote Access Trojan/Backdoor	high	507
Code Injection		
Code Injection	high	94
Denial of Service		
Regular Expression Injection	medium	400
File Inclusion		
File Inclusion Vulnerability	high	22
Hardcoded Sensitive Information		
Hardcoded URI	info	
Unprotected Database or Asset	high	521
HTTP Header Injection		
HTTP Header Injection Vulnerability	medium	113

Check Name	Risk	CWE
Host Header Poisoning	medium	
Insecure Communication		
Insecure Cookie Creation	low	1004
Information Disclosure		
Error Message Information Exposure	low	209
Sensitive Information Client-Side	high	
Logging of Sensitive Information	high	
Leftover Debug Code	low	489
Log Forging		
Log Forging Vulnerability	low	117
NoSQL Injection		
NoSQL Injection Vulnerability	high	
Command Execution		
Command Execution Vulnerability	high	78
Security Misconfiguration		
Use Helmet	info	
SSL Verification Disabled	medium	295
Insecure Content Allowed	high	
webSecurity Disabled	high	
Rendering with Node Integration Enabled	high	94
Permissive Cross-Origin Resource Sharing	high	942
Overly Broad Cookie Creation	low	287
SQL Injection		
SQL Injection Vulnerability	high	89
Server-Side Request Forgery		
Server-Side Request Forgery	medium	918

Check Name	Risk	CWE
Unvalidated Redirect		
Unvalidated Redirect Vulnerability	low	601
Incomplete Regular Expression	low	
Incomplete URL Substring Sanitization	low	20
XML Injection		
XXE Injection	high	611
XML Injection	high	91
XPath Injection		
XPath Injection Vulnerability	high	91
Cross-Site Scripting (XSS)		
Cross-Site Scripting (XSS) Vulnerability	medium	79

Code Checks for JavaScript Client-Side

Total Checks: **45**

Check Name	Risk	CWE
Broken Cryptography		
Insecure Randomness	high	338
Insecure Hashing Algorithm	medium	328
Code Injection		
Code Injection	high	94
Hardcoded Sensitive Information		
Hardcoded URI	info	
Unprotected Database or Asset	high	521
Information Disclosure		
Local Storage Usage	info	
Sensitive Data Stored in Local Storage	high	
Web SQL Database Usage	medium	

Check Name	Risk	CWE
Insecure Cross-Window Communication	medium	201
Sensitive Information Client-Side	high	
Security Misconfiguration		
Overly Broad Cookie Creation	low	287
Insecure URL Whitelist	medium	183
Server-Side Request Forgery		
Client-Side Request Forgery	medium	
Unvalidated Redirect		
Unvalidated Redirect Vulnerability	low	601
XPath Injection		
XPath Injection Vulnerability	high	91
Cross-Site Scripting (XSS) DOM-Based		
Cross-Site Scripting (XSS) Vulnerability	medium	79
SCE Disabled	high	

Code Checks for Swift

Total Checks: **111**

Check Name	Risk	CWE
Arbitrary File Manipulation		
Arbitrary File Write (Zip Slip)	high	22
Arbitrary File Manipulation Vulnerability	high	73
Resource Injection	high	99
API Misuse & Abuse		
Missing Biometric Auth Operation Justification	low	
SMS Usage	info	
Broken Authentication		
Missing Policy Evaluation Check	low	

Check Name	Risk	CWE
Insufficient Touch ID Restriction (Biometric Auth)	medium	287
Insufficient Authentication Handling	high	
Insecure Credential Initialization	high	
Missing Request Host Check	high	
Biometric LocalAuthentication Usage	info	287
Broken Cryptography		
Insecure Hashing Algorithm	medium	328
Insecure Cryptographic Algorithm	medium	327
Insecure Randomness	high	338
Empty Cryptographic Key	high	321
Empty HMAC Secret Key (Crypto)	high	321
Weak PBE Key Generation	high	321
Insecure PBE Iteration	high	916
User-Defined Salt	high	328
Insecure Initialization Vector (Crypto)	high	329
Insecure Cryptographic Mode and Initialization Vector	high	330
Insecure Cryptographic Mode	high	327
Inadequate Cryptographic Key Size	high	326
Code Injection		
JavaScript Code Injection (WebView)	high	95
Insecure URI Rendering (WebView)	high	
Unsafe Reflection	high	470
Denial of Service		
Regular Expression Injection	medium	400
Hardcoded Sensitive Information		
Hardcoded URI	info	

Check Name	Risk	CWE
Unprotected Database or Asset	high	521
Hardcoded Cryptographic Key	high	321
Hardcoded Salt	high	759
Insecure Communication		
Insecure Cookie Creation	low	1004
Weak SSL Protocol (Default)	medium	326
Weak SSL Protocol	medium	326
Insecure HTTP URL	info	319
Insecure Data Storage		
Insecure File Storage (Missing Protection)	medium	311
Insecure File Storage (Possibly Insufficient Protection)	info	311
Unencrypted Database	high	311
Insecure Image Storage	low	311
HTTP Cache Storage Incorrectly Disabled	high	311
Insecure HTTP Response Storage	low	311
Insecure Storage in Keychain (Missing Protection)	high	359
Externally Accessible Keychain	high	359
Insecure Storage in Keychain (Possibly Insufficient Protection)	info	311
Insecure Storage (Unenforced Passcode Policy)	medium	311
Insecure Storage in Keychain (Unspecified Access Policy)	medium	
Insecure HTTP Session Storage	low	311
Inadequate Password Protection	high	261
Insecure Storage of Sensitive Information	medium	256
Cleartext Storage of Sensitive Information	high	312
Sensitive Data Stored in Documents	high	359
Synchronized Credential	medium	

Check Name	Risk	CWE
Information Disclosure		
Unprotected Database	high	521
Forced Geolocation Data Transmission	medium	359
Insecure Password Input Field	medium	359
Insufficient Credential Removal	high	359
Insecure Transmission of Sensitive Information	medium	359
Information Leak	low	497
Logging of Geolocation Data	medium	359
Logging of Sensitive Information	high	
JSON Injection		
JSON Injection	high	91
Log Forging		
Log Forging Vulnerability	low	117
NoSQL Injection		
NoSQL Injection Vulnerability	high	
Security Misconfiguration		
Missing Content Validation (IPC)	medium	501
Overly Broad Cookie Creation	low	287
Persistent Cookie Creation	info	539
SQL Injection		
SQL Injection Vulnerability	high	89
XML Injection		
XXE Injection	high	611
Cross-Site Scripting (XSS)		
Cross-Site Scripting (WebView XSS)	high	79

Code Checks for TypeScript

Total Checks: **13**

Check Name	Risk	CWE
Hardcoded Sensitive Information		
Hardcoded URI	info	
Unprotected Database or Asset	high	521
Information Disclosure		
Leftover Debug Code	low	489
Logging of Sensitive Information	high	
Cross-Site Request Forgery		
Cross-Site Request Forgery	medium	352
Cross-Site Scripting (XSS)		
Cross-Site Scripting (XSS) Vulnerability	medium	79
Insecure HTTP Client Usage	medium	