本ドキュメントは、Syhunt Mobile バージョン **6.8.0.0**で作成されています。

対応言語

言語	カバレッジタイプ
Objective-C、C、C++ (iOS)	SAST
Java (JEE、Android)	SAST
JavaScript環境(Node.js、Express.js、Koa.js)	SAST
JavaScript クライアントサイド (Angular & AngularJS)	SAST
Swift (iOS)	SAST
TypeScript(アンギュラー)	SAST

Objective-C、CおよびC++のためのコードチェック

チェックの合計136

チェック名	リスク	CWE
任意のファイル操作		
任意のファイル書き込み(Zip Slip)	高	22
任意のファイル操作の脆弱性	高	73
リソース・インジェクション	高	99
APIの誤用・悪用について		
バイオメトリクス認証操作の正当性の欠落	低	
SMSの利用状況	情報	
認証の失敗		
ポリシー評価チェックの欠落		
Touch IDの制限(生体認証)が不十分です。	中	287
不十分な認証処理	高	
安全でないクレデンシャル初期化	高	
リクエストホストチェックの欠落	高	
バイオメトリックローカル認証の使用方法	情報	287

チェック名	リスク	CWE
壊れた暗号		
安全でないハッシュアルゴリズム	中	328
空の暗号鍵	高	321
空のHMAC秘密鍵（Crypto）	高	321
弱いPBE鍵の生成	高	321
安全でないPBE反復	高	916
ユーザー定義の塩	高	328
安全でない初期化ベクター（暗号）	高	329
安全でない暗号化モードと初期化ベクトル	高	330
安全でない暗号化モード	高	327
不適切な暗号鍵のサイズ	高	326
安全でない暗号化アルゴリズム	中	327
コードインジェクション		
JavaScriptのコードインジェクション（WebView）	高	95
アンセーフ・リフレクション	高	470
サービス拒否		
バッファオーバーフロー（フォーマット）	高	120
安全でないレガシー C関数の使用	中	676
バッファオーバーフロー	高	
バッファオーバーフロー	高	
ハードコードされた機密情報		
ハードコードされたURI	情報	
保護されていないデータベースや資産	高	521
ハードコードされた暗号鍵	高	321
安全でない通信		
信頼できないHTTPS証明書の受理	高	
安全でないCookieの作成	低	1004
弱いSSLプロトコル（デフォルト）	中	326
脆弱なSSLプロトコル	中	326

チェック名	リスク	CWE
安全でない HTTP URL	情報	319
安全でないデータ保存		
同期されたクレデンシャル	中	
安全でないファイル保存（保護機能の欠落）	中	311
安全でないファイル保存（保護が不十分な可能性あり）	情報	311
暗号化されていないデータベース	高	311
安全でない画像ストレージ	低	311
HTTPキャッシュストレージが誤って無効化されている	高	311
安全でないHTTPレスポンスの保存	中	311
安全でないHTTPセッションの保存	中	311
キーチェーンの安全でない保存（保護機能の欠落）	高	359
外部アクセス可能なキーホルダー	高	359
キーチェーンの安全な保存（保護が不十分な可能性あり）	情報	311
安全でないストレージ（パスコードポリシーの未徹底）	中	311
キーチェーンの安全でない保存（不特定のアクセスポリシー）	中	
不適切なパスワード保護	高	261
機密情報の安全な保管	中	256
機密情報の暗号化保存	高	312
ドキュメントに保存された機密データ	高	359
情報開示		
情報漏えい	低	497
保護されていないデータベース	高	521
ジオロケーションデータのロギング	中	359
ジオロケーションデータの強制送信	中	359
安全でないパスワード入力欄	中	359
不十分なクレデンシャル削除	高	359
機密情報のログ取得	高	
機密情報の安全な送信	中	359
JSONインジェクション		

チェック名	リスク	CWE
JSONインジェクション	高	91
ログフォージング		
ログ偽造の脆弱性	低	117
バッドプラクティス		
リクエストキャッシュの使用状況	情報	
Switchステートメントにデフォルトがない	低	
Jmp関数の使用	中	
安全でない文字列から数値への変換	低	
ループ内でのフロートの使用	低	
強制的にアプリケーションを終了させる	情報	382
Gotoステートメントの使用法	低	
誤ったテンポラリファイルやディレクトリの作成	中	
過度なキャッチフレーズ	低	396
offsetof マクロの使用法	低	
コマンドの実行		
コマンド実行の脆弱性	高	78
セキュリティの誤設定		
欠落コンテンツ検証(IPC)	中	501
広すぎるクッキーの作成	低	2827
永続的なクッキーの作成	情報	539
SQLインジェクション		
SQLインジェクションの脆弱性	高	89
制御不能なフォーマット文字列		
制御不能なフォーマット文字列	中	134
XPathインジェクション		
XPathインジェクションの脆弱性	高	91
クロスサイトスクリプティング(XSS)		
クロスサイトスクリプティング(WebView XSS)	高	79

Objective-C、C、C++のヘッダに対するコードチェック

チェックの合計1

チェック名	リスク	CWE
情報開示		
安全でないパスワード入力欄	中	359

Java用コードチェック

小切手合計315

チェック名	リスク	CWE
任意のファイル操作		
任意のファイル操作の脆弱性	高	73
任意のファイル書き込み(ZIP)	高	22
不適切なファイルアクセス権限	情報	276
認証の失敗		
クッキーへの機密情報の保存を禁止する	高	
機密情報の安全な保管	中	256
安全でないFacebookログインの処理	中	
非推奨のFingerprintManager APIの使用法	中	
BiometricPrompt認証失敗時の対応	中	
BiometricPromptのエラー処理欠落	中	
Missing BiometricPrompt Acquired の取り扱いについて	中	
Googleサインインエラー処理の欠落	中	
バイオメトリクス能力チェックの欠落	中	
壊れた暗号		
安全でないランダム性	高	338
OAEPを使用しないRSAアルゴリズムの使用(暗号化)	中	780
安全でない乱数生成	中	335
安全でない暗号鍵の比較	中	
安全でない暗号化モード	高	327
弱い乱数生成	中	330
ユーザー確認(暗号化)の欠落	中	

チェック名	リスク	CWE
unlockedDeviceRequired フラグの欠落（Crypto）	中	
安全でない暗号化アルゴリズム	中	327
安全でない暗号化モード	高	327
不適切な暗号鍵のサイズ	高	326
SecureRandomの不適切なシード	中	338
予測可能な乱数生成	中	338
安全でないSHA1 PRNG	中	328
安全でない暗号化モードと初期化ベクトル	高	330
暗号アルゴリズムのカスタム使用について	情報	
安全でないハッシュアルゴリズム	中	328
コードインジェクション		
コードインジェクション	高	94
アンセーフ・リフレクション	高	470
コードインジェクション（JavaBean）	高	15
安全でないURIのレンダリング（WebView）	高	
JavaScriptのコードインジェクション（WebView）	高	94
デバッグのエントリーポイント		
残っているデバッグエントリーポイント（メソッド）	中	489
サービス拒否		
外部プロセスブロック	中	
正規表現インジェクション	中	400
ファイル内包		
ファイルインクルード脆弱性	高	22
ハードコードされた機密情報		
ハードコードされたURI	情報	
保護されていないデータベースや資産	高	521
HTTPヘッダインジェクション		
HTTPヘッダ・インジェクションの脆弱性	中	113

チェック名	リスク	CWE
HTTPレスポンスの分割		
HTTPレスポンス分割の脆弱性	中	113
安全でない通信		
非推奨のJava HttpClientの使用について	中	
安全でないHTTPSクライアントの使用	中	319
安全でないHTTP接続	情報	319
安全でない HTTP URL	情報	319
インセキュアソケットデータ交換	中	311
安全でないSMTP接続	中	297
不適切なホスト検証	中	295
安全でない認証方法	高	522
安全でないCookieの作成	低	1004
脆弱なSSLプロトコル	中	326
情報開示		
情報漏えい	低	497
エラーメッセージの情報露出	低	209
デバッグチェックコールの欠落	低	
安全でない一時的なファイルのクリーンアップ	低	377
外部ストレージの使用状況	情報	
外部ストレージに保存された機密データ	高	
機密情報のログ取得	高	
安全でないコンテンツコンテキストモード	中	
グローバル放送におけるセンシティブデータ	高	
ジオロケーションデータの強制送信	中	359
保護されていないデータベース	高	521
残っているデバッグコード	低	489
JSONインジェクション		
安全でない非直列化(Jackson)	高	502
LDAPインジェクション		

チェック名	リスク	CWE
LDAPインジェクションの脆弱性	高	90
保護されていないLDAPトランザクション	高	521
ログフォージング		
ログ偽造の脆弱性	低	117
バッドプラクティス		
メモリーリーク(静止画コレクション)	低	
Java Array定数の使用	情報	582
安全でないデフォルトのソケットファクトリの使用	中	319
インポッシブル・アレイ キャスト	低	704
NumberFormatExceptionの欠落したキャッチ	低	248
安全でないNaN比較	低	
精度の損失(BigDecimal)	低	
汎用例外のThrowsの宣言	情報	397
NullPointerException の Catch Clause	低	396
ロックシンクロ	低	
安全でないThreadGroupメソッドの使用方法	低	362
スレッドの強制終了	低	705
欠落ファイル削除エラー処理	低	
安全でないResultSetメソッドの使用方法	低	
不適切なオブジェクトの最終化	低	586
過度なキャッチフレーズ	低	396
オブジェクトクラス比較の不足	低	
安全でないファイナライザーメソッドの使用	中	
アンリリースドロック(デッドロック)	低	833
Switchステートメントにデフォルトがない	低	
強制的なJVMの終了	情報	382
スレッドデッドロック	中	
安全でない同期方法	中	
不正な16進数変換	高	704

チェック名	リスク	CWE
コマンドの実行		
コマンドでの相対パスの使用	中	88
コマンド実行の脆弱性	高	78
インセキュアストリームリーディング	中	
セキュリティの誤設定		
安全でないデータベース接続	中	
パーミッションチェックにおける信頼できない入力	高	807
セキュリティマネージャーの停止	高	
広すぎるクッキーの作成	低	287
SQLインジェクション		
SQLインジェクションの脆弱性	高	89
SQLテーブルへの直接アクセス	低	
サーバーサイドリクエストフォージェリ		
サーバーサイドリクエストフォージェリ	中	918
CSRF保護機能無効	高	352
安全でないリクエストのマッピング	中	352
制御不能なフォーマット文字列		
制御不能なフォーマット文字列	中	134
無効なリダイレクト		
無効なリダイレクトの脆弱性	低	601
XMLインジェクション		
不適切なXMLパースモデル	低	
XXE制限の欠落	中	611
信頼できないデータの非直列化	高	502
XMLインジェクション	高	91
XXEインジェクション	高	611
XXE制限の欠落	低	611
XPathインジェクション		
XPathインジェクションの脆弱性	高	91

チェック名	リスク	CWE
クロスサイトスクリプティング(XSS)		
クロスサイトスクリプティング(XSS)の脆弱性	中	79
脆弱な検証方法(XSS)	中	625
クロスサイトスクリプティング(WebView XSS)	高	79

JavaScript環境（Node.js）のコードチェックについて

チェックの合計104

チェック名	リスク	CWE
任意のファイル操作		
任意のファイル操作の脆弱性	高	73
任意のファイル書き込み(ZIP)	高	22
壊れた暗号		
安全でないランダム性	高	338
安全でないハッシュアルゴリズム	中	328
安全でない暗号化アルゴリズム	中	327
バックドア		
リモートアクセス型トロイの木馬/バックドア	高	507
コードインジェクション		
コードインジェクション	高	94
サービス拒否		
正規表現インジェクション	中	400
ファイル内包		
ファイルインクルード脆弱性	高	22
ハードコードされた機密情報		
ハードコードされたURI	情報	
保護されていないデータベースや資産	高	521
HTTPヘッダインジェクション		
HTTPヘッダ・インジェクションの脆弱性	中	113
ホストヘッダーポイズニング	中	

チェック名	リスク	CWE
安全でない通信		
安全でないCookieの作成	低	1004
情報開示		
エラーメッセージの情報露出	低	209
機密情報 クライアント側	高	
機密情報のログ取得	高	
残っているデバッグコード	低	489
ログフォージング		
ログ偽造の脆弱性	低	117
NoSQLインジェクション		
NoSQLインジェクションの脆弱性	高	
コマンドの実行		
コマンド実行の脆弱性	高	78
セキュリティの誤設定		
ヘルメットを使用する	情報	
SSL検証を無効にする	中	295
安全でないコンテンツを許可する	高	
webSecurity 無効	高	
ノード統合を有効にしたレンダリング	高	94
許可されたクロスオリジンリソース共有	高	942
広すぎるクッキーの作成	低	287
SQLインジェクション		
SQLインジェクションの脆弱性	高	89
サーバーサイドリクエストフォージェリ		
サーバーサイドリクエストフォージェリ	中	918
無効なリダイレクト		
無効なリダイレクトの脆弱性	低	601
不完全な正規表現	低	
不完全なURLサブストリングのサニタイズ	低	20

チェック名	リスク	CWE
XMLインジェクション		
XXEインジェクション	高	611
XMLインジェクション	高	91
XPathインジェクション		
XPathインジェクションの脆弱性	高	91
クロスサイトスクリプティング(XSS)		
クロスサイトスクリプティング(XSS)の脆弱性	中	79

JavaScriptクライアントサイドのコードチェック

チェックの合計45

チェック名	リスク	CWE
壊れた暗号		
安全でないランダム性	高	338
安全でないハッシュアルゴリズム	中	328
コードインジェクション		
コードインジェクション	高	94
ハードコードされた機密情報		
ハードコードされたURI	情報	
保護されていないデータベースや資産	高	521
情報開示		
ローカルストレージの使用状況	情報	
ローカルストレージに保存された機密データ	高	
Web SQLデータベースの使用方法		
安全でないクロスウィンドウ通信	中	201
機密情報 クライアント側	高	
セキュリティの誤設定		
広すぎるクッキーの作成	低	287
安全でないURLのホワイトリスト	中	183
サーバーサイドリクエストフォージェリ		
クライアントサイドリクエストフォージェリ	中	

チェック名	リスク	CWE
無効なリダイレクト		
無効なリダイレクトの脆弱性	低	601
XPathインジェクション		
XPathインジェクションの脆弱性	高	91
クロスサイトスクリプティング(XSS) DOMベース		
クロスサイトスクリプティング(XSS)の脆弱性	中	79
SCE 無効	高	

Swiftのコードチェック

チェックの合計111

チェック名	リスク	CWE
任意のファイル操作		
任意のファイル書き込み(Zip Slip)	高	22
任意のファイル操作の脆弱性	高	73
リソース・インジェクション	低	99
APIの誤用・悪用について		
バイオメトリクス認証操作の正当性の欠落	情報	
SMSの利用状況	低	
認証の失敗		
ポリシー評価チェックの欠落		
Touch IDの制限(生体認証)が不十分です	中	287
不十分な認証処理	高	
安全でないクレデンシャル初期化	高	
リクエストホストチェックの欠落	高	
バイオメトリックローカル認証の使用方法	情報	287
壊れた暗号		
安全でないハッシュアルゴリズム	中	328
安全でない暗号化アルゴリズム	中	327
安全でないランダム性	高	338
空の暗号鍵	高	321

チェック名	リスク	CWE
空のHMAC秘密鍵（Crypto）	高	321
弱いPBE鍵の生成	高	321
安全でないPBE反復	高	916
ユーザー定義の塩	高	328
安全でない初期化ベクター（暗号）	高	329
安全でない暗号化モードと初期化ベクトル	高	330
安全でない暗号化モード	高	327
不適切な暗号鍵のサイズ	高	326
コードインジェクション		
JavaScriptのコードインジェクション（WebView）	高	95
安全でないURIのレンダリング（WebView）	高	
アンセーフ・リフレクション	高	470
サービス拒否		
正規表現インジェクション	中	400
ハードコードされた機密情報		
ハードコードされたURI	情報	
保護されていないデータベースや資産	高	521
ハードコードされた暗号鍵	高	321
ハードコードソルト	高	759
安全でない通信		
安全でないCookieの作成	低	1004
弱いSSLプロトコル（デフォルト）	中	326
脆弱なSSLプロトコル	中	326
安全でない HTTP URL	情報	319
安全でないデータ保存		
安全でないファイル保存（保護機能の欠落）	中	311
安全でないファイル保存（保護が不十分な可能性あり）	情報	311
暗号化されていないデータベース	高	311
安全でない画像ストレージ	低	311

チェック名	リスク	CWE
HTTPキャッシュストレージが誤って無効化されている	高	311
安全でないHTTPレスポンスの保存	低	311
キーチェーンの安全でない保存(保護機能の欠落)	高	359
外部アクセス可能なキーホルダー	高	359
キーチェーンの安全な保存(保護が不十分な可能性あり)	情報	311
安全でないストレージ(パスコードポリシーの未徹底)	中	311
キーチェーンの安全でない保存(不特定のアクセスポリシー)	中	
安全でないHTTPセッションの保存	低	311
不適切なパスワード保護	高	261
機密情報の安全な保管	中	256
機密情報の暗号化保存	高	312
ドキュメントに保存された機密データ	高	359
同期されたクレデンシャル	中	
情報開示		
保護されていないデータベース	高	521
ジオロケーションデータの強制送信	中	359
安全でないパスワード入力欄	中	359
不十分なクレデンシャル削除	高	359
機密情報の安全な送信	中	359
情報漏えい	低	497
ジオロケーションデータのロギング	中	359
機密情報のログ取得	高	
JSONインジェクション		
JSONインジェクション	高	91
ログフォージング		
ログ偽造の脆弱性	低	117
NoSQLインジェクション		
NoSQLインジェクションの脆弱性	高	
セキュリティの誤設定		

チェック名	リスク	CWE
欠落コンテンツ検証(IPC)	中	501
広すぎるクッキーの作成	低	287
永続的なクッキーの作成	情報	539
SQLインジェクション		
SQLインジェクションの脆弱性	高	89
XMLインジェクション		
XXEインジェクション	高	611
クロスサイトスクリプティング(XSS)		
クロスサイトスクリプティング(WebView XSS)	高	79

TypeScriptのコードチェック

チェックの合計13

チェック名	リスク	CWE
ハードコードされた機密情報		
ハードコードされたURI	情報	
保護されていないデータベースや資産	高	521
情報開示		
残っているデバッグコード	低	489
機密情報のログ取得	高	
クロスサイトリクエストフォージェリ		
クロスサイトリクエストフォージェリ	中	352
クロスサイトスクリプティング(XSS)		
クロスサイトスクリプティング(XSS)の脆弱性	中	79
安全でないHTTPクライアントの使用	中	