Cyberspect Quick Start

Abbott Laboratories | January 2023

Contents

Overview

Cyberspect is a cloud hosted mobile application security scanning solution used by Abbott Laboratories. It provides a self-service workflow to upload mobile applications, scan them for security vulnerabilities and compliance concerns, and deliver reports containing the results.
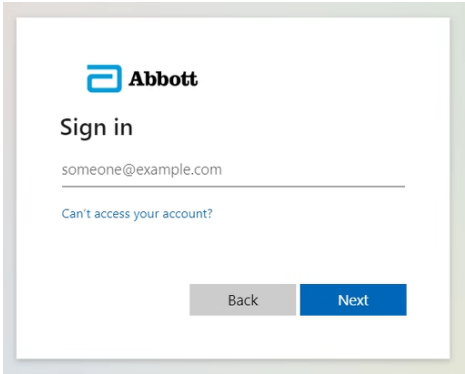
Requesting Access

To request access to the Cyberspect solution:

- Login to IIQ: https://iiq.abbott.com/identityiq/home.jsf
- Request Access to the Mobile Security Platform group (**APP-Cyberspect-Users**)

Login

- Browse to https://abbott.cyberspect.io
- You will need to login using your Abbott domain credentials.

- NOTE: If you pause at the login page for more than 15 minutes, you may receive a 401 Authorization Required error when attempting to login. If this occurs, please refresh the page, and try again.

Scanning a Mobile App

To upload and scan a mobile application package and/or source code for a mobile app, use the following steps:

Fill out the required fields displayed above with the information applicable to the mobile application.

- **Application Name**: The name of the mobile application as it appears (or will appear) in the applicable app store.
- **Version**: The version of the mobile application.
- **Production or Preproduction**: The release status of the mobile application.
- **Division**: The Abbott Labs organizational division applicable to the mobile application.
- **Country**: Select Global if the application is used worldwide, or one or more countries.
- **Data Privacy Classification**: Choose the appropriate classification for the mobile application from Abbott's Information Classification Policy.
- **Data Privacy Attributes**: Choose one or more data privacy attributes:
    - PII: Personal Information
    - PHI: Health Information
    - PIFI: Financial Information
    - GEO: Geolocation Data
    - CTI: Consumer Tracking Info
    - C18: Data of Children Under 18
    - ABT: Abbott Personnel Info

- **Mobile App File**: The mobile application package file (.apk, .ipa) to scan.
- **Source Code File**: Including a .zip file containing the source code for the mobile application is optional, but if included will result in more accurate results.

Click the **Upload & Analyze** button to upload the file(s) and start the scanning process.

Recent Scanned Apps

🚀 Recent Scanned Apps

HASH / DATE	APPLICATION	FILE	TYPE	ACTIONS
a2158b2ed410e882ab2e52b273ca8a66 Dec 14, 2022 8:58 PM RELEASE	**AMDPG - 1.0** AMDPG - 1.1.0.4 com.oneabbott.BTS101AMDPG	com.oneabbott.BTS101AMDPG-1.1.0.4.apk	🤖	👁 Scan Details 👤 Scorecard 🔗 Dependencies 🗑 📄
5c6e037bc9fe9ba42372a5175896f62e Dec 14, 2022 8:56 PM RELEASE	**Octofy - 1.0** Octofy - 1.0.0.2 com.hrsgsolutionsOct.twa	Octofy_1.0.0.2_Apkpure.apk	🤖	👁 Scan Details 👤 Scorecard 🔗 Dependencies 🗑 📄

After submitting a mobile application to analyze you will be taken to the Recent Scanned Apps page. This page will also show any mobile applications that you have previously scanned. The Application column will display a gray circle with the words "No Icon" and a "scan in progress" label while the scan is being performed. The static analysis details for an application could take a few minutes to be available depending on the size and complexity of the mobile application. Once complete, you will see additional information and can view more detail using the buttons on the far right.

Viewing Scan Results

To view the scan results, click a button in the Actions column on the right to view Static Details, Scorecard, or Dependencies information.

Static Analyzer Details

This page includes a lot of information about the mobile application, not all of which is security related. The Security Scorecard (which you can access from this page using the Security Scorecard button) includes a summarized list of all security findings and is generally what you want to focus on, but the detail on this page may provide further context when addressing any security concerns.

For example, if the scan is for an Android based application you can access and view the decompiled Java source code from this page. This page also allows you to determine what information embedded in the mobile application will be publicly accessible to others who may use similar tools to extract the contents.

Security Scorecard
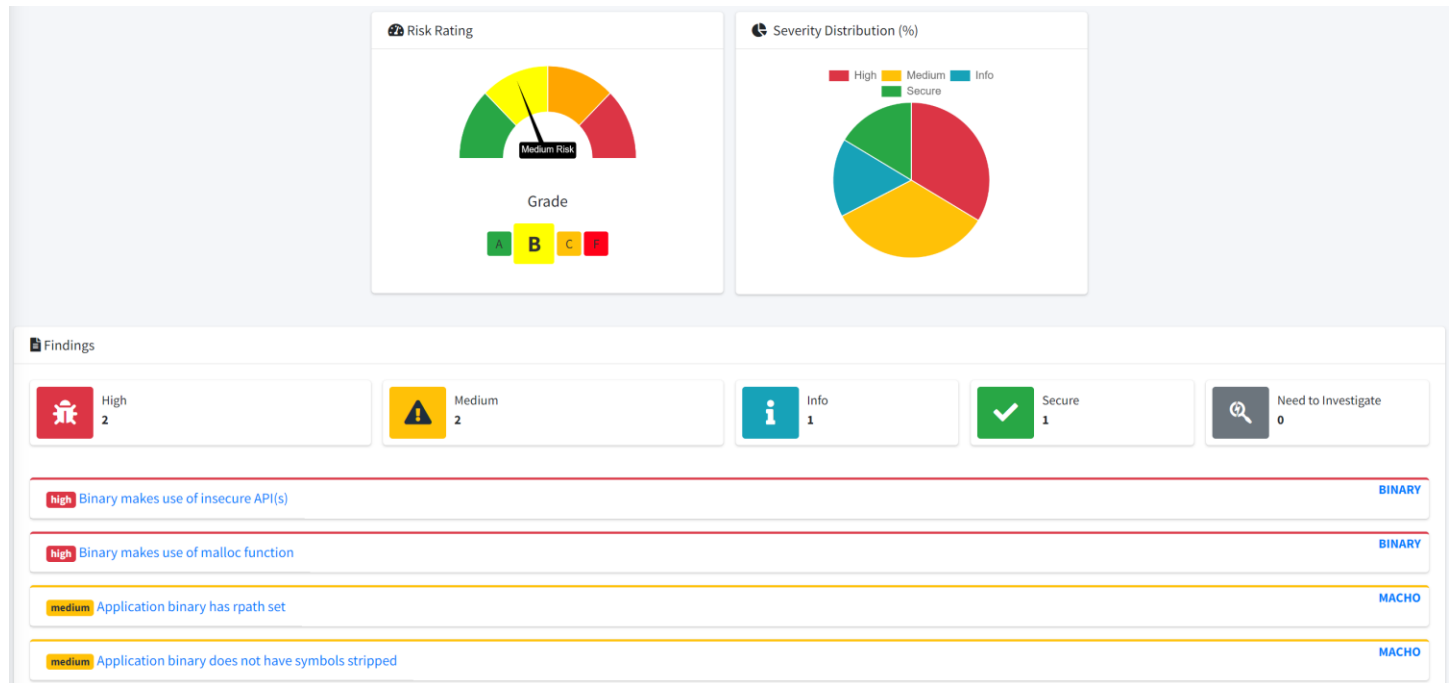
The Security Scorecard page includes a summarized view of all security relevant findings from the static analysis (SAST) scan. Clicking each of the rows that start with "high", "medium", "info", etc. will reveal more detail about the finding.
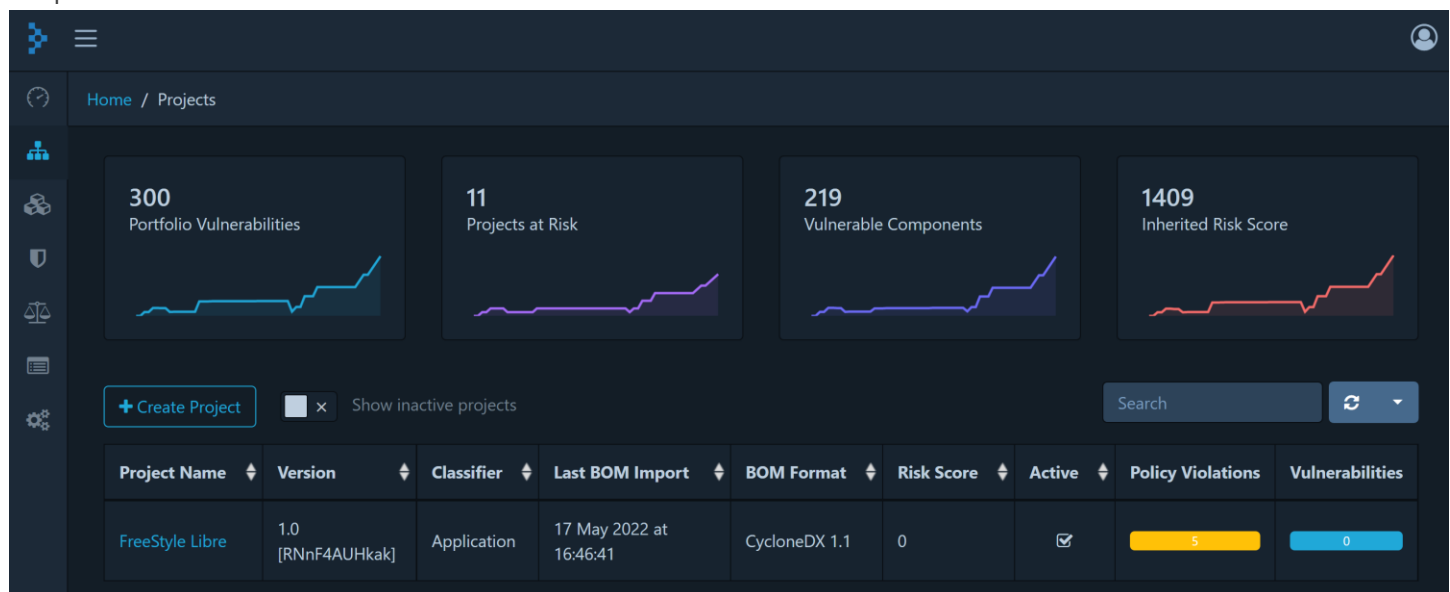
Dependencies

The Dependencies area allows you to view more details about third-party and open-source libraries used by the mobile application. This list of libraries is also referred to as a software bill of materials, or SBOM. This area of the system includes information about published security vulnerabilities and policy violations based on Abbott standards. To return to the Recent Scans area of the system, simply click the blue arrow looking icon in the upper left.

Third-party library details take longer to process and may not be available as soon as the Static Analyzer Details and Security Scorecard information are. Once all scanning has completed you should receive an email containing the results.

Note that the information displayed in the Dependencies area is updated daily as new information about published security vulnerabilities is made available.

Email Notification

Once the file(s) have been uploaded and the full scan is complete, the submitter will receive an email with attachments containing the Static Analysis (SAST) and Software Bill of Materials (SBOM) reports. The email will also include a document on how to read the scan results, and links to the web interface to view more information.

Be aware that if multiple users upload the same file, each user will be added to the recipient list for the email notification.

Monthly Scanning

Automatic monthly scanning is performed for mobile applications marked as Release; an activity performed by the Abbott Mobility Team. You may receive this email if you have been assigned to one or more of these release applications. The email message will look like that shown below and include the current high, warning, and info findings for each application, along with links to the web interface for more information.

Cyberspect Monthly Scan Results

noreply@cyberspect.io
To ● Brice Williams

↩ Reply   ↩ Reply All   → Forward   •••

Sun 1/1/2023 10:54 AM

ⓘ You forwarded this message on 1/1/2023 11:20 AM.

Monthly Scan Summary

Apps Scanned	Failed Scans	High Findings	Warnings	Info Findings	Avg Scan Time
9	1	18	22	25	54.84

Mobile Apps Scanned

App Name	Version	Scan Type	High	Warning	Info	Status	Scan Time	Scorecard	Dependencies
ConsentTool	1.0.3	IPA	4	8	8	Success	61.36	Scorecard	Dependencies
Nutritional Connection	1.1.2	IPA	2	1	1	Success	60.60	Scorecard	Dependencies
AbbWorld	1.4.1	IPA	3	1	1	Success	60.41	Scorecard	Dependencies
Field Toolkit	3.0.3	IPA	2	2	1	Success	60.46	Scorecard	Dependencies
Startup Toolkit	2.0.3	IPA	1	2	0	Success	60.41	Scorecard	Dependencies
AR Atheneum	1	IPA	4	1	1	Success	60.37	Scorecard	Dependencies
eHR India	1.2	IPA	2	1	0	Failed	8.99	Scorecard	Dependencies
Foodie	2.0.0	IPA	0	3	0	Success	60.45	Scorecard	Dependencies
Abbott	1.2	IPA	0	3	0	Success	60.51	Scorecard	Dependencies

Technical Support

For technical assistance please email cyberspectsupport@syslogicinc.com and include any information relevant to the issue or question you have.

Cyberspect Quick Start

https://cyberspect.com

© Copyright 2023 Cyberspect LLC

{cyberspect}®