IBM Application Security On Cloud Plugin

Plugin Information
View IBM Application Security on Cloud on the plugin site for more information.

Older versions of this plugin may not be safe to use. Please review the following warnings before using an older version:

- Plain text password shown in job configuration form fields

Allows users to execute security scans in HCL AppScan on Cloud.

Prerequisites

An account at the HCL AppScan on Cloud service. You'll need to create an application on the service to associate your scans with.

Usage

This video demonstrates installation and configuration of the plugin.

1. Add your Application Security on Cloud credentials on the Jenkins **Credentials** page.
    - From the main Jenkins dashboard, click the **Credentials** link.
    - Add new global credentials.
    - In the **Kind** drop-down list, select **IBM Application Security on Cloud Credentials**.
    - Enter your API key details.
2. Add a **Run Security Test** build step to your Jenkins project configuration and enter the following information:
    - **Credentials:** Select the credentials you added to Jenkins in step 1 above.
    - **Application:** Select the application to associate the scan with. NOTE: You must create at least 1 application in the IBM Application Security on Cloud service or this field will be empty.
    - **Test Name:** Specify a name to use for the scan. This value will be used to distinguish this scan and its results from others.
    - **Test Type:** Select the type of scan to run from the available options.
        - **Dynamic Analyzer**
            - **Starting URL**: Enter the URL from where you want the scan to start exploring the site.
            - **Additional Options**: If selected, the following options are available.
                - **Scan Type**: Select whether your site is a Staging site (under development) or a Production site (live and in use).
                - **Login User** and **Login Password**: If your app requires login, enter valid user credentials so that Application Security on Cloud can log in to the site.
                - **Extra Field**: If your app requires a third credential, enter it in this field.
                - **Presence**: If your app is not on the internet, select your AppScan Presence from the list. Information about creating an AppScan Presence is available here.
                - **Scan File**: If you have an AppScan Standard scan file, enter its full path and file name in this field. To learn more about AppScan Standard scan files, see this topic.
        - **Mobile Analyzer**
            - **Application File**: Enter the full path and file name of the .apk or .ipa file that you want to scan.
            - **Additional Options**: If selected, the following options are available.
                - **Login User** and **Login Password**: If your app requires login, enter valid user credentials so that Application Security on Cloud can log in to the site.
                - **Extra Field**: If your app requires a third credential, enter it in this field.
                - **Presence**: If your app is not on the internet, select your AppScan Presence from the list. Information about creating an AppScan Presence is available here.
        - **Static Analyzer**
            - **Target**: Enter the full path to the directory that contains the files that you want to scan or enter the full path to an existing .irx file.
    - **Suspend job until security analysis completes:** If selected, the Jenkins job will pause until security analysis has completed and the results have been retrieved from the service. If unselected, the job will continue once the scan has been submitted to the analysis service.
    - **Fail job if:** If selected, the Jenkins job will fail if the finding count(s) exceed the specified thresholds (see below).
    - **Add Condition:** Allows you to add thresholds for the number of findings that will cause a build to fail. You can specify thresholds for total, high, medium, and/or low finding counts. If multiple conditions are added, they will be treated as though they are separated by a logical OR.

Additional Information

http://help.hcltechsw.com/appscan/ASoC/appseccloud_jenkins.html?query=jenkins

Release History

1.2.5 (August, 2019)

- Bug fixes.

1.2.4 (May, 2019)

- Update service url to cloud.appscan.com

1.2.3 (April, 2019)

- Support for "Normal" or "Optimized" DAST scans.

1.2.2 (October, 2018)

- Fail builds for noncompliance with application policies.
- Noncompliant issues reports.
- Open source only scans.
- Bug fixes.

1.2.1 (July, 2018)

- Update for JEP-200.

1.2.0 (July, 2018)

- Pipeline support
- Sort the application list alphabetically

1.1.3 (July, 2018)

- Allow ".scan" files in addition to ".scant" for dynamic scans.

1.1.2 (September, 2017)

- Bug fixes.

1.1.1 (May, 2017)

- Drop-down list for selecting a Presence for Mobile and Dynamic scans.
- Enter an existing .irx file in the Target field of a Static scan.

1.1 (February, 2017)

- Support for dynamic scanning.
- Additional options for mobile and dynamic scans.
- Authentication changed from username and password to API key.

1.0 (December, 2016)

- Initial release.