UrbanCode Deploy Integration with Appscan Enterprise

HCL DevOps Paragon

Don Weber

Shawn Varughese

Purpose

- After deploying an application, it is important to validate the installation.
  - Previously there was an integration with Rational Functional Tester for basic UI testing.
 - This demonstrates a security scan to validate the application

Topology

- UCD Server – Linux AWS Instance, 2 CPU, 8 GB RAM, 80 GB HDD
- ASE Server – Windows 2016 Server, 2 CPU, 8 GB RAM, 120 GB HDD

Application/Security Test

- UCD sample application is JPetStore
  - Tomcat modified from readonly to introduce an error.

- Security Policy
  - Quick and Light Scan with "The Vital Few" for a quick scan.
  - Report errors that are High or Critical
  - Introduced error is a High priority issue
  - Auto explore, should be a manual explore
  - Pre-defined scan

UCD AppScan Process
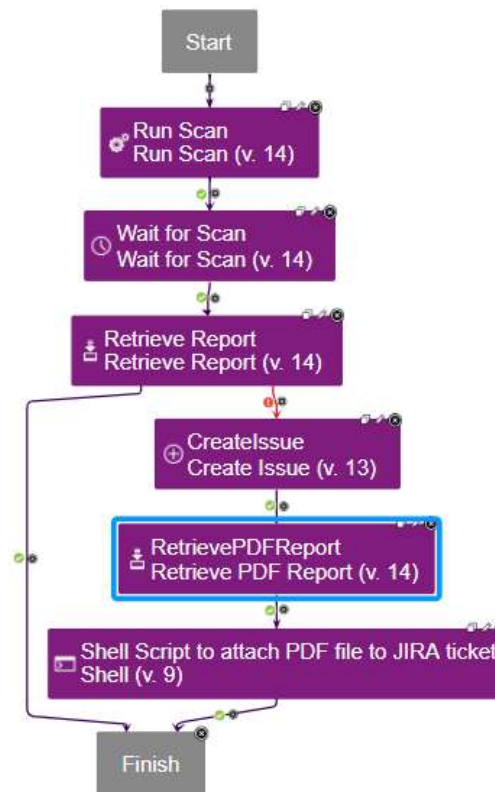
UCD AppScan Process

- Run the scan

- Wait for the scan to complete

- Get the scan results

- If High or Critical Issues found
  - Create JIRA Ticket
  - Retrieve PDF Report
  - Attach PDF to JIRA ticket

UCD AppScan Process more Details

- Post processing scripts are required for
    - Create Issue
    - Retrieve PDF Report

    - The purpose of the post processing script is to capture specific data from those steps (JIRA Ticket Number and Appscan file) which are then used to attach the Appscan report to the JIRA Ticket.

Tricks and Tips

- The plugin for AppScan Enterprise asks for the URL. This means https://dns-name, it does not mean https://dns-name:port/path

- The directory for the Retrieve PDF step should be a local predefined directory. /tmp/Appscan wasn't working, but /home/ucd/Appscan did.

- The parameters for JiraTicket and AppscanPDF are qualified by the step name, so those steps do not have white space.

Next Steps

- The JIRA ticket shows up in the backlog, but not on the Kanban board.
  - Not associated with an Epic
  - Not assigned

- The PDF report lacks detail. Need to get a better report.

- The Appscan process is stand alone, should be integrated into the deploy process