# Docker Image Security Vulnerabilities Scan

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | Paul Kenny  BSc. (Hons) Computing | | Gradle, Docker, Java, Groovy, SQL, Git, Linux, HTML5, CSS 3, JavaScript, Bootstrap | |  |

## Project Overview

|  |
| --- |
| The goal of this project is to develop a Gradle Plugin for IBM to allow developers to run a security vulnerabilities scan on a Docker Image. This plugin will scan the chosen image for third party Java Framework dependencies, in the form of jar files, and cross reference these dependencies with a database of known security vulnerabilities. If security vulnerabilities are found, the plugin will relay the results back to the developer as a HTML report which will contain the security vulnerabilities, in the form of the Common Vulnerabilities & Exposures (CVE) entries, for each dependency found.  The system is a three-tier architecture using an AWS RDS MySQL instance as its data layer, a Gradle Plugin to scan the Docker Image and query the database, and a HTML 5/JavaScript based results interface.  Traditionally, at IBM, a Java application is wrapped in a Docker Image prior to being deployed as a Docker Container. The source code has been scanned for known security vulnerabilities as part of the Jenkins development pipeline. However, this process does not identify whether the Docker Image contains vulnerabilities. This application will ensure that the developer is aware of security vulnerabilities present in the new Docker Image. |
|  |