

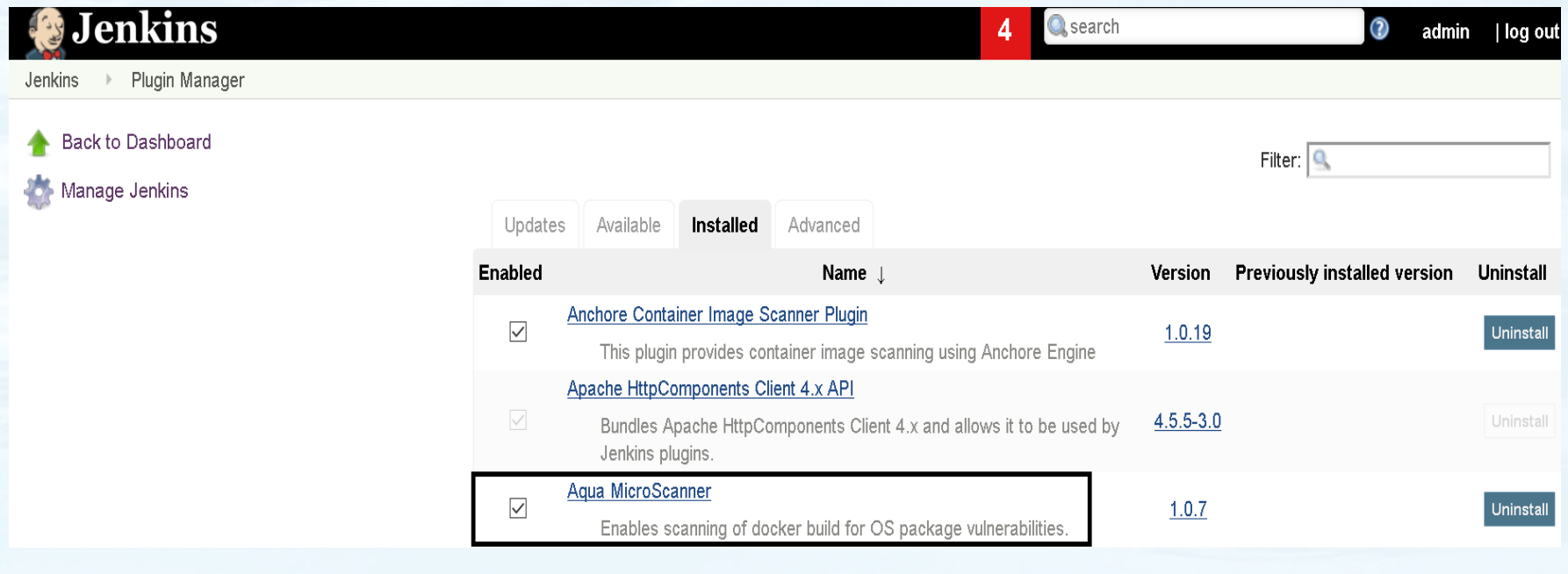
Container Security :Aqua



- A container image scanner looks at the software packages included in the image file system, and checks it against a (very long) list of packages with known vulnerabilities - typically the NVD
- MicroScanner uses the same vulnerability database as Aqua's best-in-class commercial scanner, so you're getting top-notch results

Setup Aqua Micro Scanner

- Register with your email.
- <https://microscanner.aquasec.com/signup>
- Install below highlighted pluggin



The screenshot shows the Jenkins Plugin Manager interface. The top navigation bar includes the Jenkins logo, a red notification badge with the number '4', a search bar, and user links for 'admin' and 'log out'. The main content area is titled 'Jenkins > Plugin Manager'. On the left, there are links for 'Back to Dashboard' and 'Manage Jenkins'. The main table displays installed plugins with columns for 'Enabled', 'Name', 'Version', 'Previously installed version', and 'Uninstall'. The 'Aqua MicroScanner' plugin is highlighted with a red box.

Enabled	Name ↓	Version	Previously installed version	Uninstall
<input checked="" type="checkbox"/>	Anchore Container Image Scanner Plugin This plugin provides container image scanning using Anchore Engine	1.0.19		Uninstall
<input checked="" type="checkbox"/>	Apache HttpComponents Client 4.x API Bundles Apache HttpComponents Client 4.x and allows it to be used by Jenkins plugins.	4.5.5-3.0		Uninstall
<input checked="" type="checkbox"/>	Aqua MicroScanner Enables scanning of docker build for OS package vulnerabilities.	1.0.7		Uninstall

Jenkins Configuration

- Insert token in global configuration of Jenkins

Manage Jenkins → Configure System

Aqua MicroScanner

Aqua MicroScanner token

.....



Fail scans if ca-certificate is missing.

☐

Create Jenkins Jobs

- Create a freestyle job and configure as shown below.

The screenshot shows the Jenkins configuration interface for a job named 'AQUASEC-SECURITY'. The browser address bar indicates the URL is '192.168.1.111/job/AQUASEC-SECURITY/configure'. The 'Build' tab is selected, and the 'Aqua MicroScanner' build step is configured. The configuration includes the following options:

- When high severity vulnerabilities are found:**
 - ☒ Generate report and PASS the build.
 - ☐ Generate report and FAIL the build.
- Output format:**
 - ☒ Output html report
 - ☐ Output json file
- Image to scan:**
 - Image Name:

At the bottom, the 'Post-build Actions' section is visible, and there are 'Save' and 'Apply' buttons.

Results

Jenkins > AQUASEC-SECURITY > #7 > Aqua Security Scanner

 Changes

 Console Output

 Edit Build Information

 Delete Build

 Aqua Security Scanner

 Previous Build

 Next Build

Scan Report: vulnerables/web-dvwa:latest

From Local Docker Engine

Risk Vulnerabilities Sensitive Data Malware



Image Is Allowed

Image scanned on September 2, 2019 15:28

Image Overview

 0 High  4 Medium  2 Low  32 Negligible