



QUALYS SECURITY CONFERENCE 2020

The Need to Shift Left and What It Means to Security

Alex Mandernack
Security Solution Architect
Product Management
Qualys, Inc

Traditional World

Each app team
builds their
own image
(CentOS v1, v2,
v3)

Deploy application
(1, 2, 3)

Inefficiencies,
slows things down,
no standardization
across teams,
repetition in
security workflows

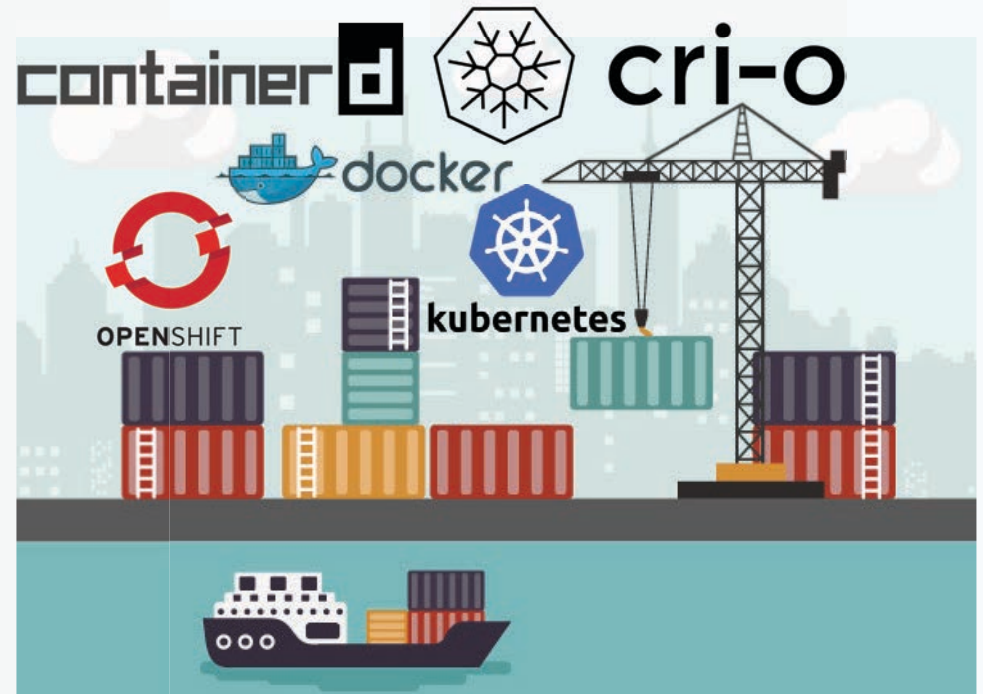
PenTest report to Dev
(t0+1Mo)

- Dev team dealing with out of date findings
- Not machine readable
- Repeated work across apps 1, 2, 3 (OS level vulns)
- Not doing it often enough due to cost, efficient reasons

Scan in production
(VM, WAS, PC etc.)

- Findings for app 1, 2, 3
- Separate patching workflows for running production workloads (v1, v2, v3)

The Driver: Scale, Elasticity & DevOps Pipeline



The background is a solid blue color with a pattern of small white dots arranged in a grid. Three of these dots are highlighted with a red glow, indicating a specific point of interest or a threat. The text is centered in the middle of the image, overlaid on a semi-transparent blue rectangular area.

Can Security
Teams do
Better?

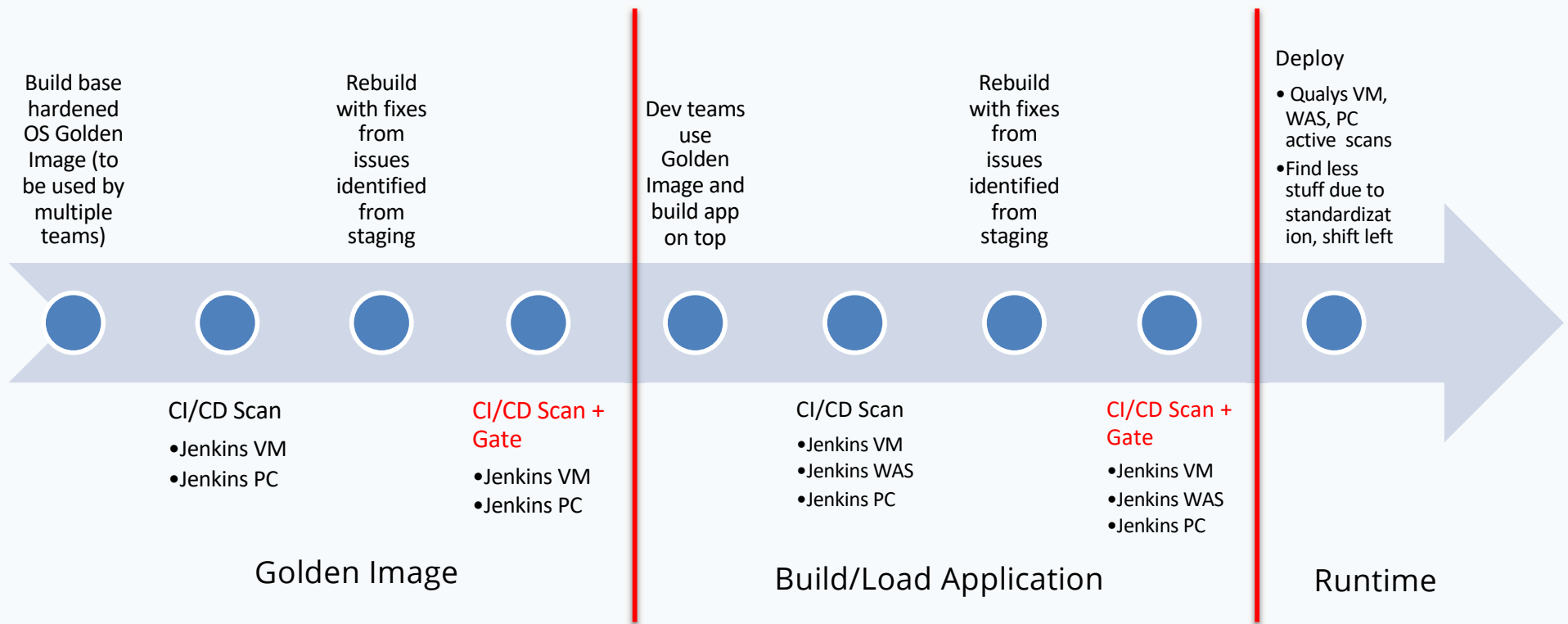
Shifting Security to the Left

- Developers and security teams must think about security, sooner
- Get security tools into the process earlier
- Automate! Leverage API's, CI plugins
- Golden images
- Scan in the CI pipeline
 - Vulnerability gates in the pipeline
 - Vulnerability information at the fingertips of Dev

The New Role of the Security Team

- Must not be a roadblock
- Provide security tooling that is self-service for DevOps, Dev
 - CI Plugins
 - APIs
 - Scripting
- Verify and audit the process
 - Dashboards/live data
 - Trending

Shift Left with Qualys!



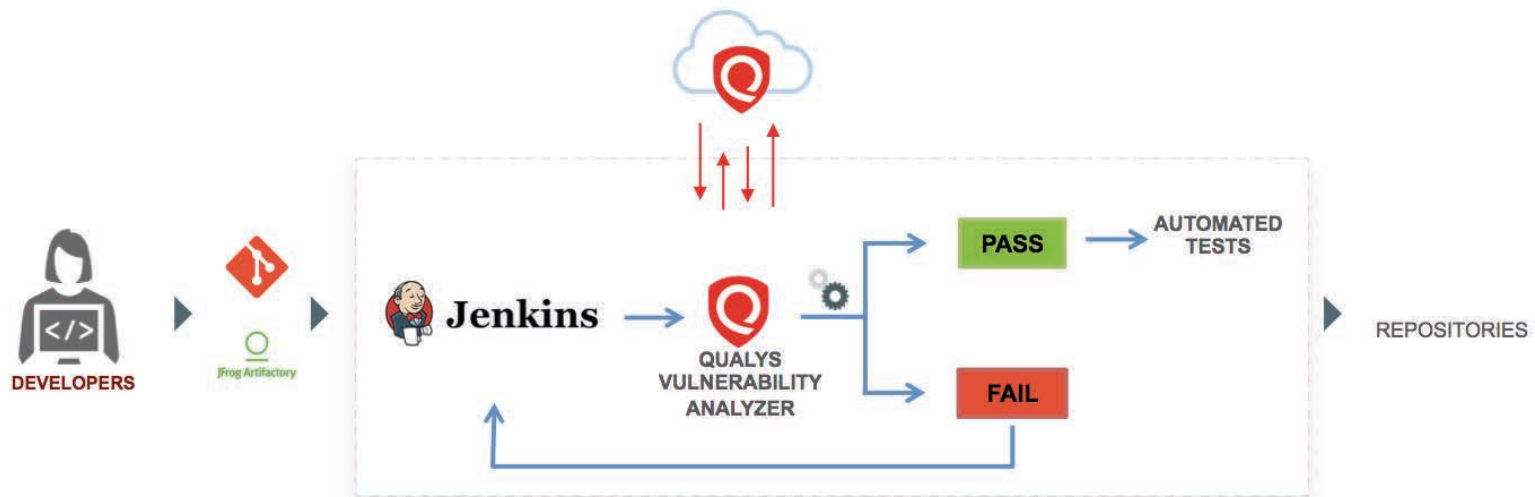
Qualys Jenkins Plugin

Available on the Jenkins Marketplace

- Vulnerability Management
- Container Security
- Web Application Scanning
- API Security



Secure the CI Pipeline



Jenkins Vulnerability Management Plugin

The screenshot displays the Jenkins Vulnerability Management Plugin interface. The top navigation bar shows the Jenkins logo, a search bar, and a 'log out' button. The main header indicates the current view is 'Qualys Report for 10.113.197.71'. The left sidebar contains a 'Qualys' logo and a 'Summary' section with a 'Vulnerabilities' link. The main content area is titled 'QUALYS VULNERABILITY ANALYZER RESULTS' and shows a 'Scan Build Status: FAILED' and 'Scan Status: Finished'. A 'Results Summary' box provides details: Type: API, Launch Date: 05/21/2019 10:18:39, Network: Global Default Network, Total Duration: 00:04:09, and Scan Target: 10.113.197.71. Below this, a table shows the 'Criteria Evaluation' with a red 'X' for QIDs, a green checkmark for CVEs, and a red 'X' for CVSS. A note indicates 'Excluded QIDs: 11' and 'Considered potential vulnerabilities'. The main table lists 13 vulnerabilities with columns for QID, Title, CVE ID, Severity, CVSSv2 Base Score, CVSSv3 Base Score, Category, PCI Vuln?, Type, and Bug Traq ID. The table shows various vulnerabilities related to SSH and RPC services. The bottom of the page indicates 'Showing 1 to 10 of 13 entries' and 'Page generated: May 21, 2019 12:04:45 PM UTC Jenkins ver. 2.164.2'.

Jenkins

test_pipeline #4 Qualys Report for 10.113.197.71

Qualys

Summary

Vulnerabilities

QUALYS VULNERABILITY ANALYZER RESULTS

Scan Build Status: **FAILED**

Scan Status: Finished

Scan Name: test_pipeline_jenkins_build_4_2019-05-21-10-18-26

Results Summary

Type: API

Launch Date: 05/21/2019 10:18:39

Network: Global Default Network

Total Duration: 00:04:09

Scan Target: 10.113.197.71

Criteria Evaluation	QIDs	CVEs	CVSS
	✗	✓	✗

*Excluded QIDs: 11

*Considered potential vulnerabilities.

QID	Title	CVE ID	Severity	CVSSv2 Base Score	CVSSv3 Base Score	Category	PCI Vuln?	Type	Bug Traq ID
11	Hidden RPC Services	-	2	5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	-	RPC	yes	Confirmed	-
36003	TCP Test-Services	-	2	5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	-	General remote service	yes	Confirmed	-
36623	OpenSSH Xauth Command Injection Vulnerability	CVE-2016-31115	3	5.5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	6.4	General remote service	yes	Potential	84314
36679	OpenSSH Multiple Vulnerabilities	CVE-2015-5600, CVE-2015-6563, CVE-2015-6564	4	8.5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	-	General remote service	yes	Potential	75990, 91787, 92012, 76317
36692	OpenSSH 7.4 Not Installed Multiple Vulnerabilities	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2016-8858	4	7.5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	7.8	General remote service	yes	Potential	84315, 24968, 94972, 94977, 94978, 93776
36725	OpenSSH Information Disclosure and Denial of Service Vulnerability	CVE-2016-0777, CVE-2016-0778	3	4.6 (AV/NIAC/H/AU/N/C:P/I/N/A/N)	8.1	General remote service	yes	Potential	80695, 80698
36726	OpenSSH Username Enumeration Vulnerability	CVE-2016-15473	3	5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	5.3	General remote service	yes	Potential	105140
36736	SSH Server Public Key Too Small	-	2	5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	5.3	General remote service	yes	Confirmed	-
36739	Deprecated SSH Cryptographic Settings	-	2	9.4 (AV/NIAC/LAU/N/C:P/I/N/A/N)	9.1	General remote service	yes	Confirmed	-
42413	OpenSSH LoginGraceTime Denial of Service Vulnerability	CVE-2010-5107	3	5 (AV/NIAC/LAU/N/C:P/I/N/A/N)	-	General remote service	no	Potential	58162, 58162

Showing 1 to 10 of 13 entries

Previous 1 2 Next

Page generated: May 21, 2019 12:04:45 PM UTC Jenkins ver. 2.164.2


Jenkins WAS Plugin

The top screenshot displays the Jenkins interface for a Qualys WAS Scan. The scan ID is 23011099, and the status is **FINISHED**. The scan name is 'WASPluginFreestyle_2_jenkins_build_23_2019-02-14-17-14'. The scan report is available at [Click here to view Scan Report on Qualys Portal](#). The target URL is <http://google-gruyere.appspot.com/922324844025/>.

The bottom screenshot shows the 'QUALYS VULNERABILITIES RESULTS' table. The table has 10 entries, showing the QID, Title, URL, and whether the vulnerability is available unauthenticated.

QID	Title	URL	Available Unauthenticated?
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/feed?uid=%22%3E%3Cqss%20a%3DX166455440Y1Z%3E	Yes
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/login?uid=%3CEMBED%20SRC%3D%2F%2Flocalhost%2Fq.swf%20All%20owScriptAccess%3Dalways%3E%3C%2FEMBED%3E&pw=password	Yes
150001	Reflected Cross-Site Scripting (XSS) Vulnerabilities	http://google-gruyere.appspot.com/922324844025/snippets.gtl?uid=%20onEvent%3DX166495526Y1Z%20	Yes
150053	Login Form is Not Submitted Via HTTPS	http://google-gruyere.appspot.com/922324844025/saveprofile	Yes
150053	Login Form is Not Submitted Via HTTPS	http://google-gruyere.appspot.com/922324844025/login	Yes
150061	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/feed.gtl?uid=cheddar	Yes
150061	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/feed.gtl	Yes
150061	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/#	Yes
150061	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/	Yes
150061	X-Frame-Options header is not set	http://google-gruyere.appspot.com/922324844025/newaccount.gtl	Yes

Jenkins Container Security Plugin

 Jenkins

3


search

Jenkins

pipeline-project

#78

Qualys Report For e8d112ff7588

 Qualys


Build Summary

Vulnerabilities

Installed Software

Layers

BUILD REPORT - e8d112ff7588



Build Status: Failed

Image ID: e8d112ff7588

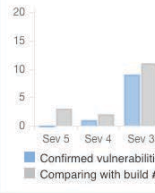
Tags: latest

Size: 828 MB


Build Summary

The vulnerabilities count by severity for image id e8d112ff7588 exceeded one of the configured threshold value :
Configured : Severity 1 > 0; Severity 2 > 0; Severity 3 > 0; Severity 4 > 0; Severity 5 > 0;
Found : Severity 1: 0, Severity 2: 1, Severity 3: 11, Severity 4: 2, Severity 5: 0

Vulnerability



Potential Vulner.



INSTALLED SOFTWARE

Show 10 entries

Search: QID=176259

Name	Installed Version	Fixed In Version
libmagickwand-dev	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickwand-6-headers	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-dev	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
libmagickcore-6-headers	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4
imagemagick-6.q16	8:6.9.7.4+dfsg-11+deb9u3	8:6.9.7.4+dfsg-11+deb9u4

Qualys Report For e8d112ff7588

ENABLE AUTO REFRESH



Demo

Qualys GitHub

Automation scripts

Reporting scripts

Open Source
community



<https://github.com/Qualys>



QUALYS SECURITY CONFERENCE 2020

Thank you

Alex Mandernack
amandernack@qualys.com