



Pipeline Security a Catalyst for DevSecOps



Presented by:

Ravi Lachhman

Evangelist / Harness

Gets told no a lot

Had lots of outages



MESOSPHERE



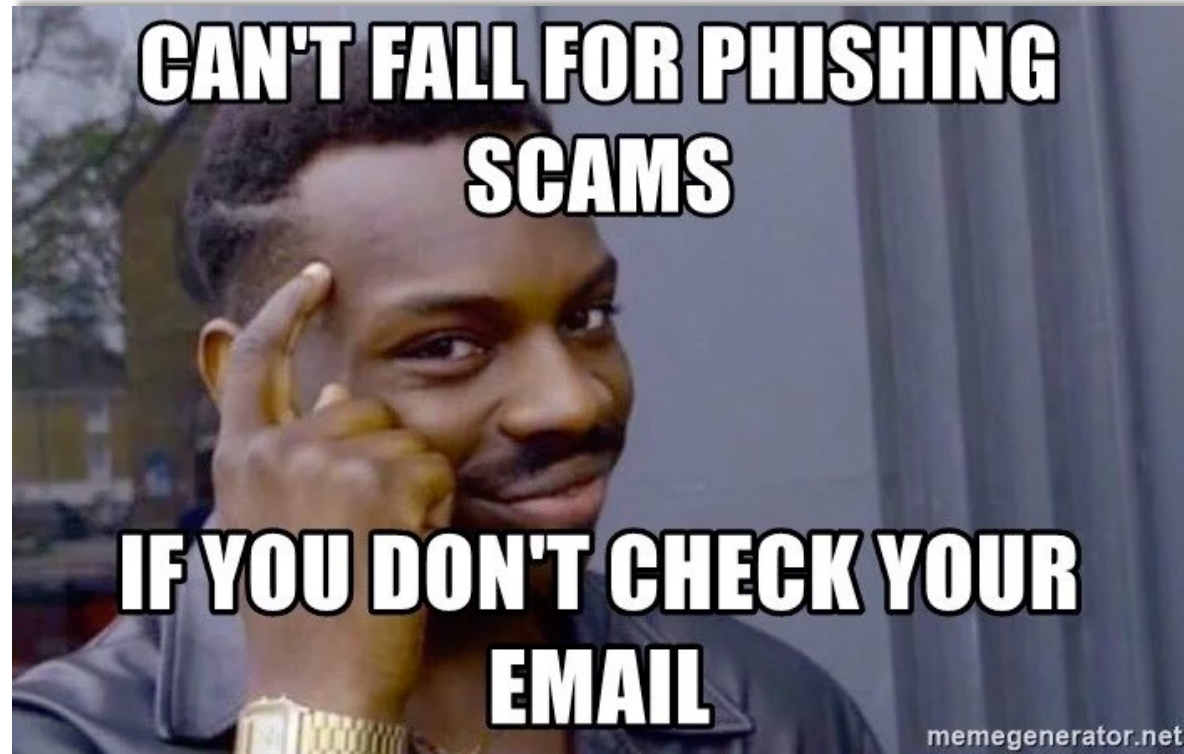
What are we talking about today?

- Security, everyone's responsibility?!
- Shift left into DevSecOps
- Build security into your CI/CD Pipelines

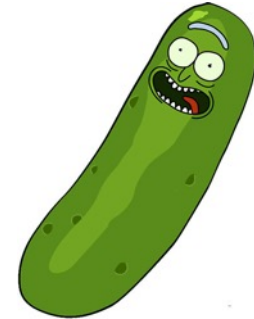
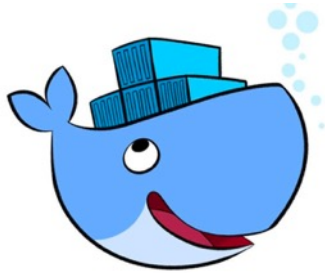
Security?



Well Duh!



Which Ones do you Trust?



Application is Always Trusted



Why so?



Our Domain



Shift Left to DevSecOps



Some Terms

R&M

..... stands for

Rick and Morty



Abbreviations.com

National Vulnerability Database [NVD]

The screenshot shows the NVD website interface. At the top left is the NIST logo and the text 'Information Technology Laboratory'. At the top right is a 'NVD MENU' button. Below this is a blue header with 'NATIONAL VULNERABILITY DATABASE' on the left and 'NVD' on the right. A left-hand navigation menu lists: General, Vulnerabilities, Vulnerability Metrics, Products, Configurations (CCE), Contact NVD, Other Sites, and Search, each with a plus sign. The main content area features three announcements: 1) 'CVSS/CWE from CVE List now Supported!' with an icon of a server and arrows; 2) 'CVSS Version 3.1 Official Support!' with the CVSS logo; 3) 'New NVD CVE/CPE API and Legacy SOAP Service Retirement!' with an icon of a server and download arrows. A paragraph at the bottom explains the NVD's role as a U.S. government repository for vulnerability data.

NIST Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE **NVD**

- General +
- Vulnerabilities +
- Vulnerability Metrics +
- Products +
- Configurations (CCE)
- Contact NVD
- Other Sites +
- Search +

CVSS/CWE from CVE List now Supported!

CVSS Version 3.1 Official Support!

New NVD CVE/CPE API and Legacy SOAP Service Retirement!

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Common Vulnerabilities and Exposures [CVE]

CVE-2018-1002105 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection.

Source: MITRE

[+View Analysis Description](#)

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:

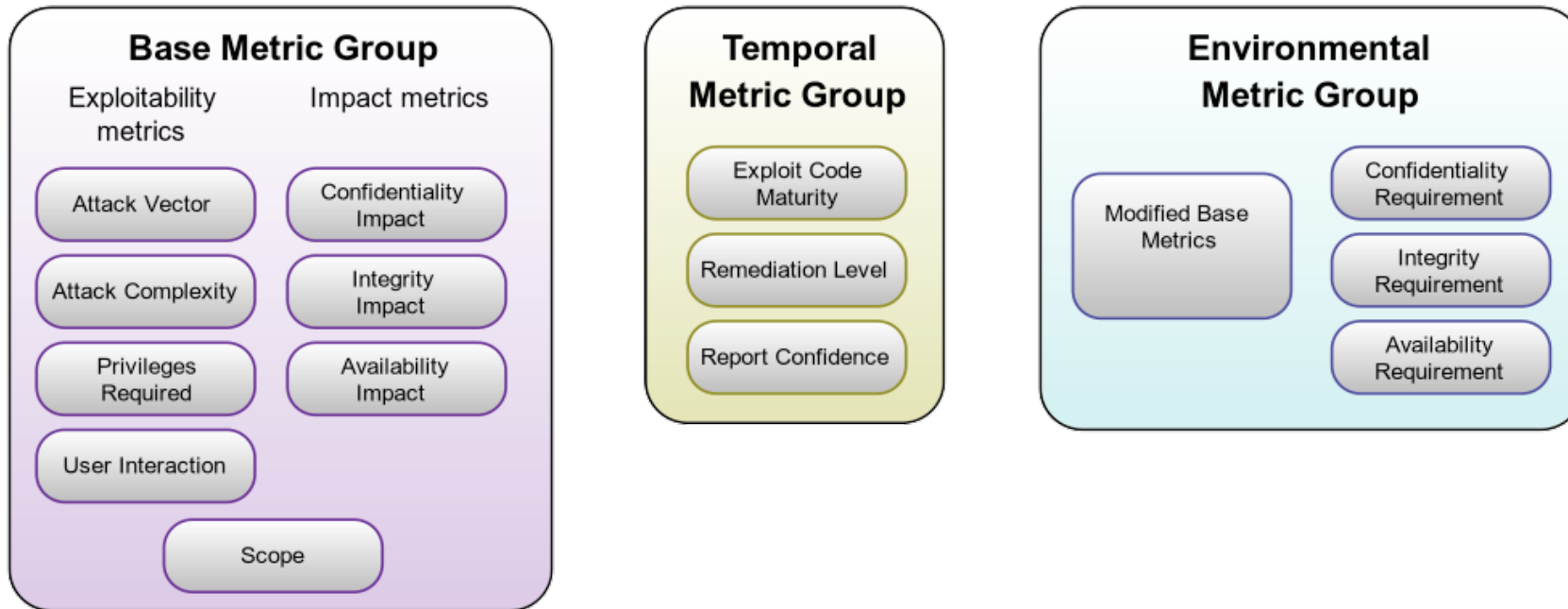


CNA: Kubernetes

Base Score: 9.8 CRITICAL

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Common Vulnerability Scoring System [CVSS]



OWASP



OWASP

Open Web Application
Security Project



Shifting Left

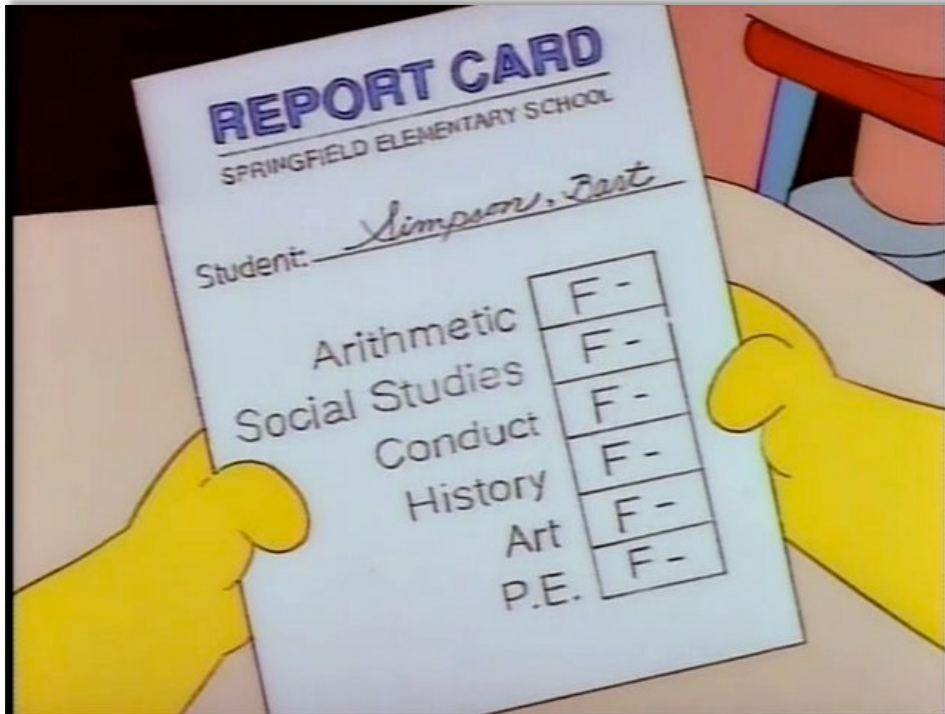


DevSecOps

```
@Override
public void apply(Project project) {
    PluginContainer plugins = project.getPlugins();
    plugins.apply(DeployedPlugin.class);
    plugins.apply(JavaLibraryPlugin.class);
    plugins.apply(ConventionsPlugin.class);
    plugins.apply(InternalDependencyManagementPlugin.class);
    StarterMetadata starterMetadata = project.getTasks().create("starterMetadata", StarterMetadata.class);
    ConfigurationContainer configurations = project.getConfigurations();
    Configuration runtimeClasspath = configurations.getByName(JavaPlugin.RUNTIME_CLASSPATH_CONFIGURATION_NAME);
    starterMetadata.setDependencies(runtimeClasspath);
    File destination = new File(project.getBuildDir(), "starter-metadata.properties");
```



Static Analysis [SAST]



Or

SonarQube Findbugs Plugin
November 28, 2016 2:00 PM Version 3.4.4

Issues Measures Code Administration

Quality Gate **Passed**

Bugs & Vulnerabilities

Leak Period: last 30 days started 2 months ago

0 Bugs 0 Vulnerabilities

0 New Bugs 0 New Vulnerabilities

Code Smells

2d Debt 73 Code Smells

0 New Debt 0 New Code Smells

Duplications

0.0% Duplications 0 Duplicated Blocks

— Duplications on New Code

FindBugs is a program that uses static analysis to look for bugs in Java code. It can detect a variety of common coding mistakes, including thread synchronization problems, misuse of API methods.

2.4k Lines of Code

Java 2.1k XML 290

Quality Gate (Default) SonarQube way

Quality Profiles (Java) Sonar way (XML) Sonar way

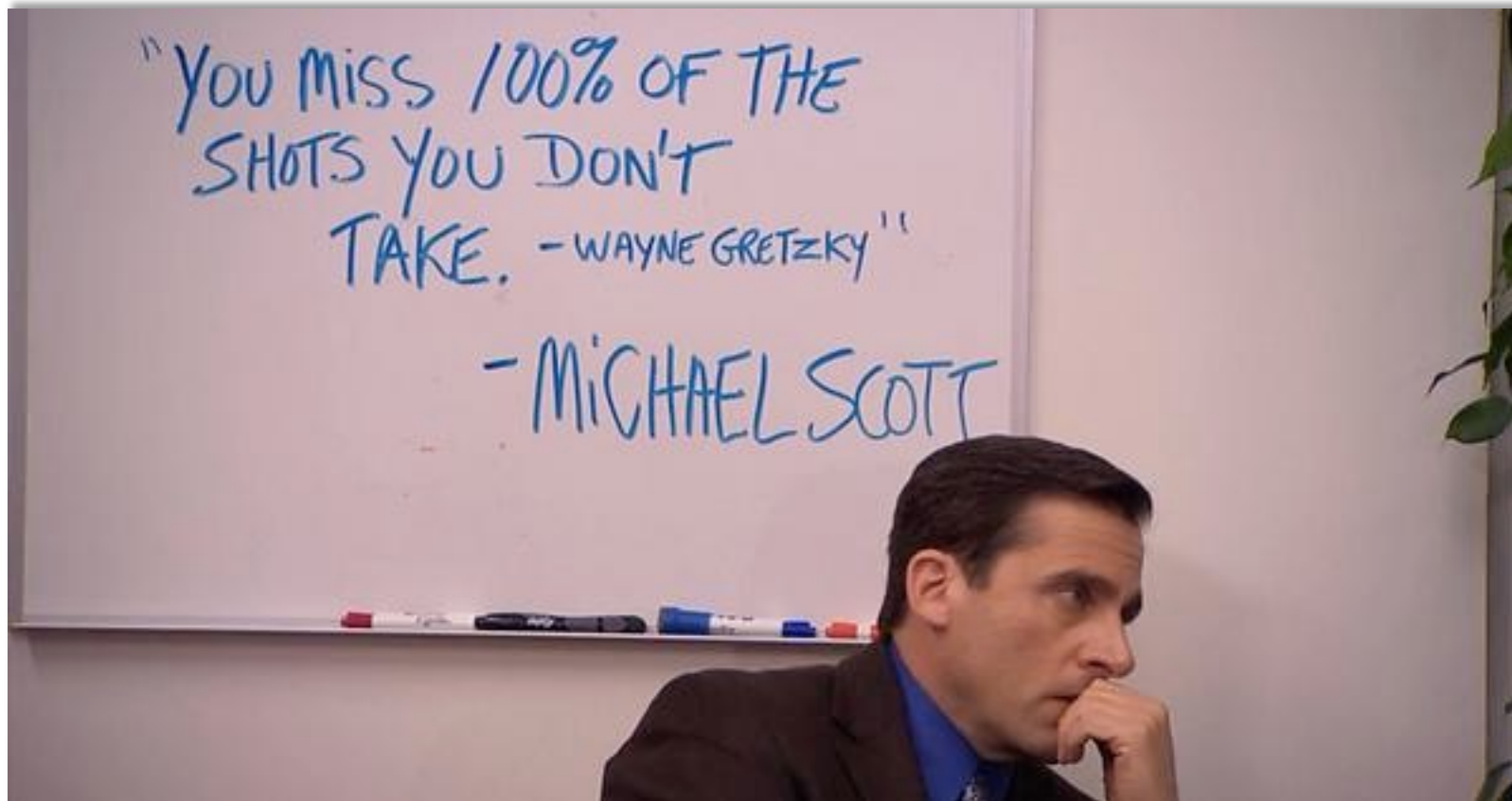
Home Issues Sources Developer connection

Key org.sonarsource.sonar-findbugs-plugin:sonar

Events All

Version: 3.4.4
November 28, 2016
Quality Gate: Green (was Red)
November 28, 2016

Dynamic Analysis [DAST]



RASPs



Your Pipelines



Your Pipelines



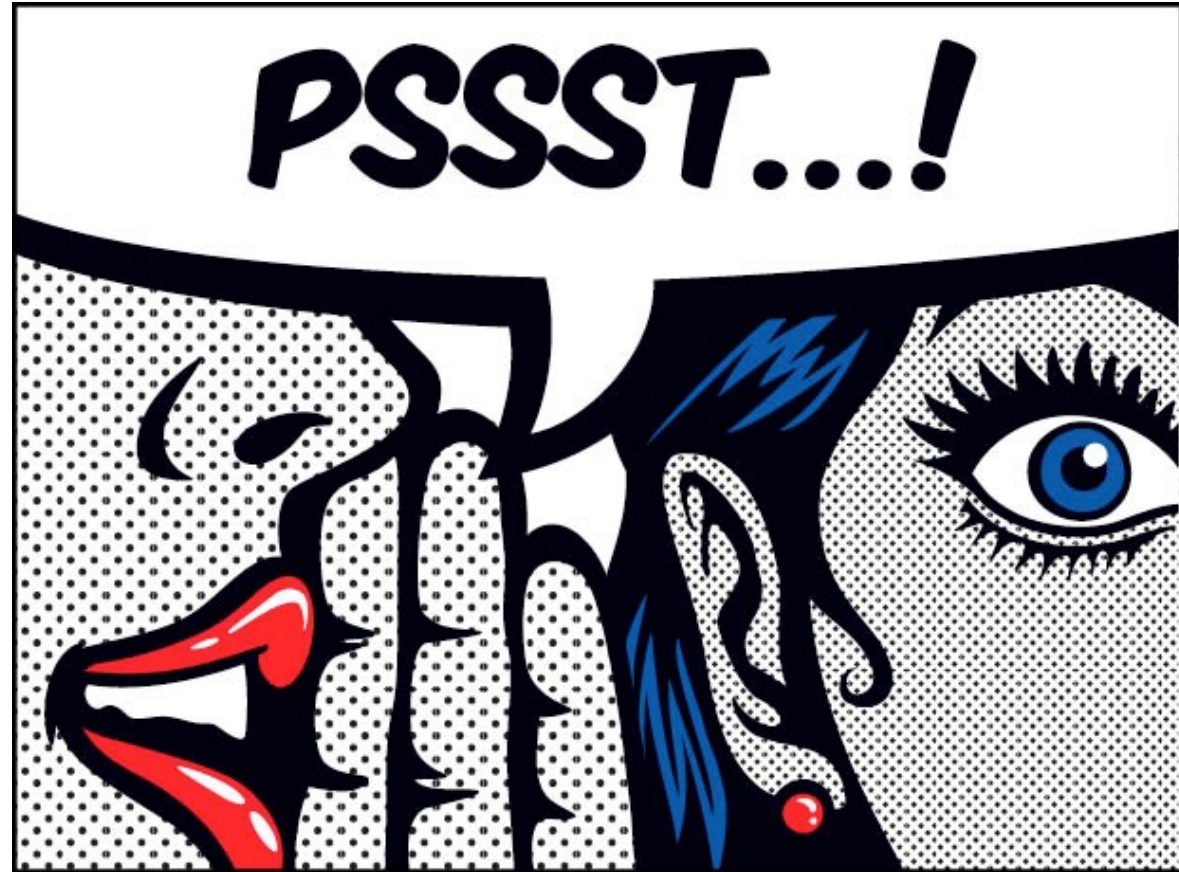
Least Privilege



Role Based Access



Secrets



Audit Trail

Setup > Harness API Explorer Authentication Logged-in User Session

Explore Run Prettify Merge Copy History

```
1 {
2   audits(limit:5){
3     nodes{
4       id
5       triggeredAt
6     }
7     request{
8       url
9       resourcePath
10      requestMethod
11      remoteIpAddress
12      requestMethod
13    }
14    changes{
15      appId
16      appName
17      operationType
18    }
19  }
20  pageInfo{
21    hasMore
22    limit
23    total
24    offset
25  }
26 }
```

QUERY VARIABLES

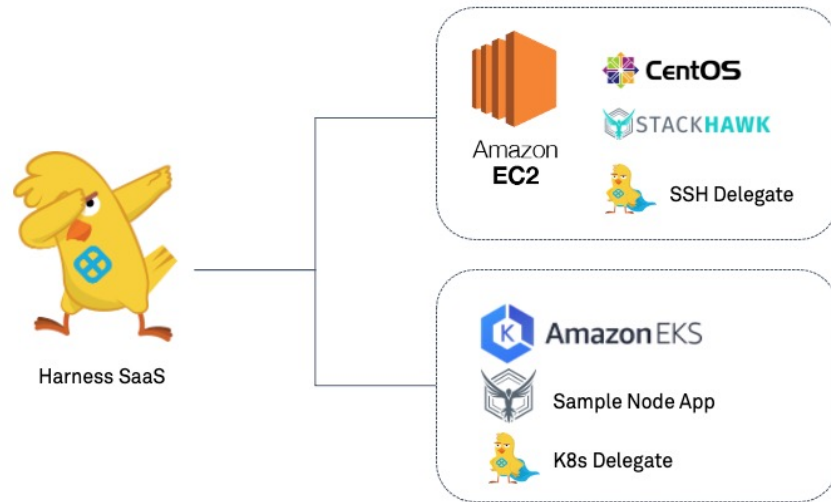
```
{
  "data": {
    "audits": {
      "nodes": [
        {
          "id": "qhmQaXggSdG-mrmD4YuMiw",
          "triggeredAt": 1581532160464,
          "request": {
            "url": "https://app.harness.io/api/apps/KLXFhdUoTdug-gJvmX2sRw",
            "resourcePath": "apps/KLXFhdUoTdug-gJvmX2sRw",
            "requestMethod": "DELETE",
            "remoteIpAddress": "192.195.83.11"
          },
          "changes": [
            {
              "appId": "KLXFhdUoTdug-gJvmX2sRw",
              "appName": "jateen-k8s-training",
              "operationType": "DELETE"
            }
          ]
        },
        {
          "id": "USx9ytqdSbmhoYy27ZyuqQ",
          "triggeredAt": 1581532149896,
          "request": {
            "url": "https://app.harness.io/api/apps/EAA6VnzqSr-Jc5vBR1zeBQ",
            "resourcePath": "apps/EAA6VnzqSr-Jc5vBR1zeBQ",
            "requestMethod": "DELETE",

```

Security Starts with YOU



Some Cool Examples



This screenshot shows a deployment pipeline for a Node application. The pipeline consists of several stages:

- STAGE 1:** StackHawk Scan (Successful)
- STAGE 2:** Interpret Scan (Failed)
- STAGE 3:** Deploy Node App (Skipped)

The pipeline steps include: Pre-Deployment, Rolling Phase 1, Rollback Phase 1, Prepare Infra, Disable Service, Deploy Service, Disable Service, Stop Service, Deploy Service, Enable Service, Verify Service, and Wrap Up. A Shell Script step is also present. The right-hand panel shows the details of the failed stage, including a shell script execution log with error messages.

The screenshot displays the StackHawk web interface for a scan of a Node application. The scan was completed on May 05, 2021, at 18:14 EDT, with a duration of 37 seconds. The scan results are summarized as follows:

- 3 High severity findings
- 12 Medium severity findings
- 12 Low severity findings
- 0 Assigned findings

The findings list includes:

Finding	Criticality	New
Cross Site Scripting (Reflected)	HIGH	1
SQL Injection	HIGH	1
Anti CSRF Tokens Scanner	HIGH	1

The screenshot shows the Nexus IQ server web interface displaying a Webgoat Build Report. The report is dated 2020-12-29 11:58:06 UTC-0500. The summary indicates:

- 112 VIOLATIONS Affecting 64 components
- 171 COMPONENTS 75% of all components identified
- 0 GRANDFATHERED violations

The report lists several high-severity findings (Severity 10, Security-Critical):

THREAT	POLICY	COMPONENT
10	Security-Critical	com.thoughtworks.xstream : xstream : 1.4.5
10	Security-Critical	io.undertow : undertow-core : 2.0.28.Final
10	Security-Critical	jQuery 1.6.4
10	Security-Critical	org.dom4j : dom4j : 2.1.1
10	Security-Critical	org.jruby : jruby-complete : 9.1.17.0
10	Security-Critical	org.springframework : spring-web : 5.2.2.RELEASE
10	Security-Critical	org.webjars jquery 1.10.2

Thanks!

