Pipeline Security a Catalyst for DevSecOps

Presented by:

Ravi Lachhman

Evangelist / Harness

Gets told no a lot

Had lots of outages

harness

APPDYNAMICS

MESOSPHERE

Red Hat

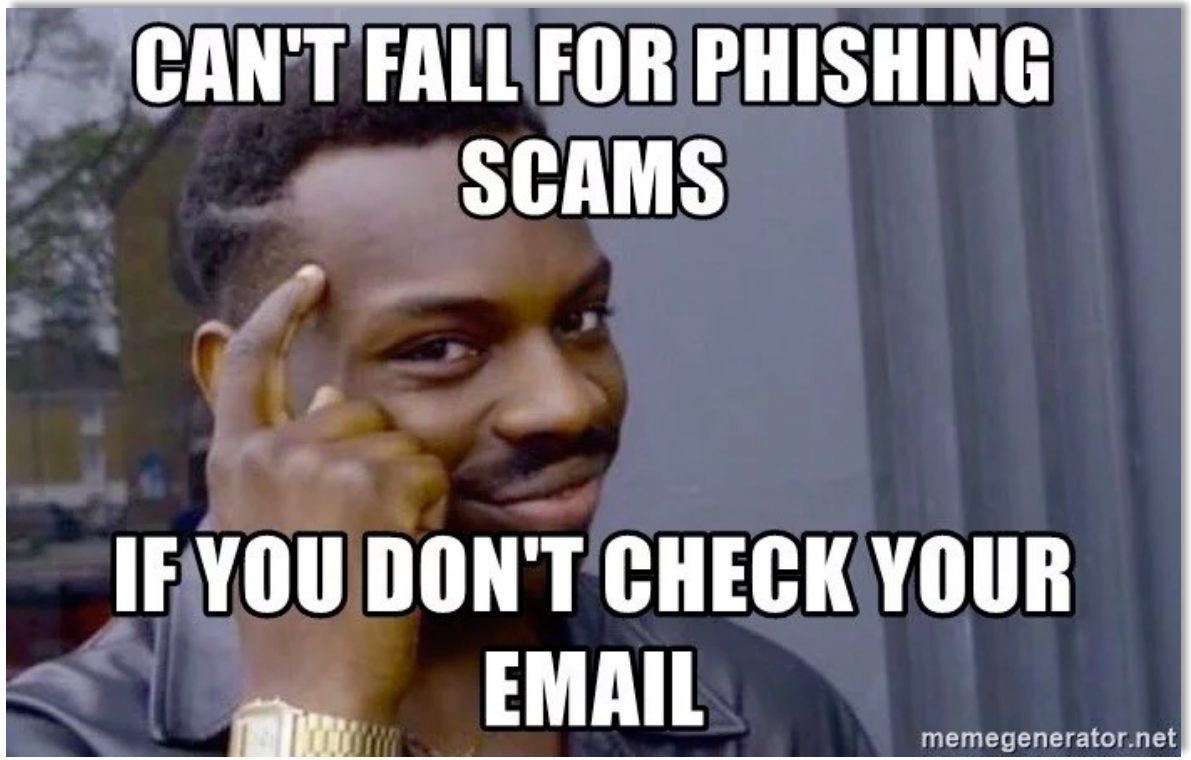
IBM

What are we talking about today?

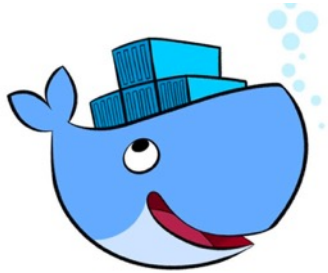
- Security, everyone’s responsibility?!
- Shift left into DevSecOps
- Build security into your CI/CD Pipelines

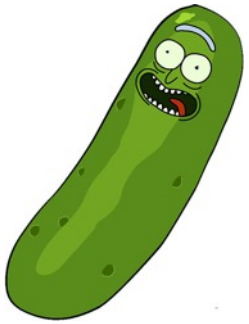
Security?

Well Duh!


CAN'T FALL FOR PHISHING SCAMS
IF YOU DON'T CHECK YOUR EMAIL
memegenerator.net

Which Ones do you Trust?

Application is Always Trusted

Why so?

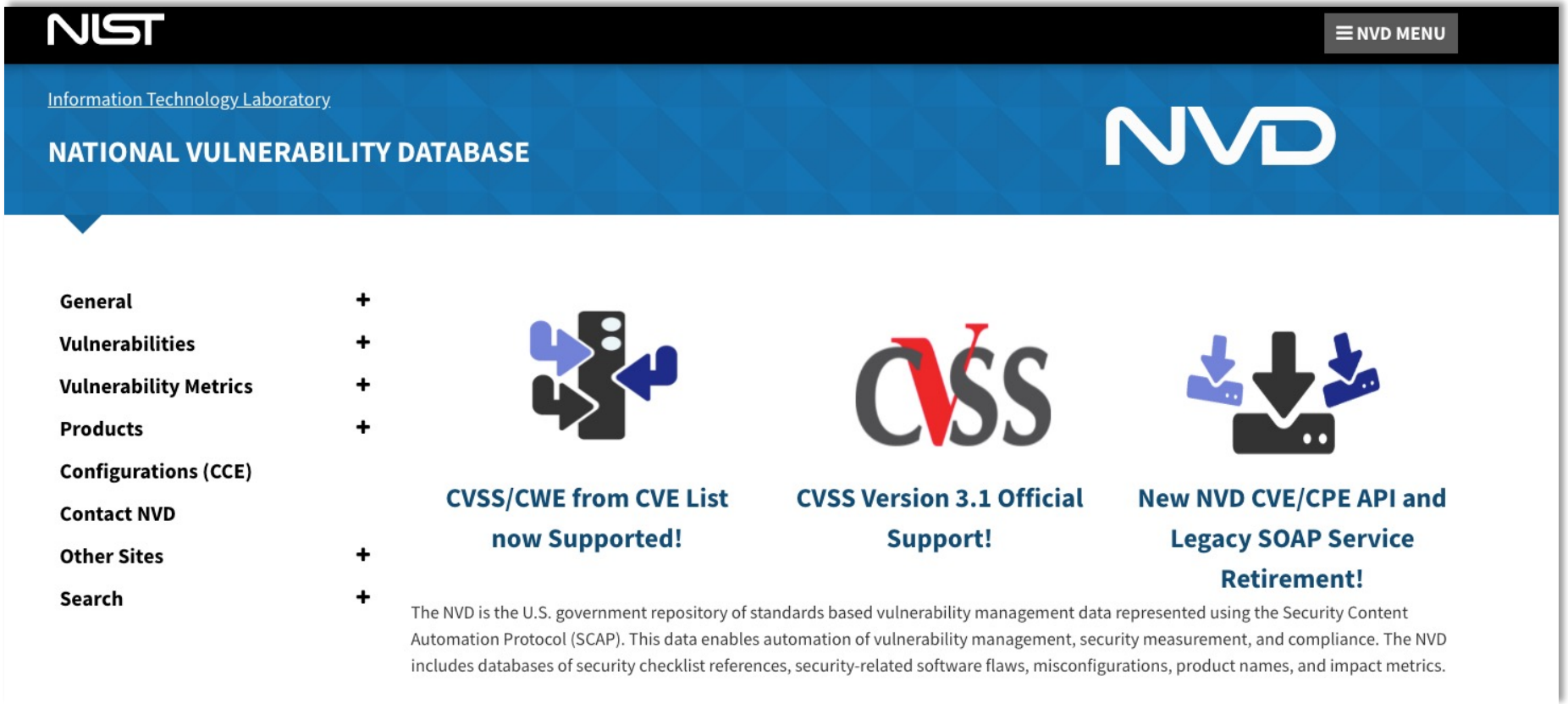
Our Domain

Shift Left to DevSecOps

Some Terms


R&M
stands for
Rick and Morty
ABBREVIATIONS
Abbreviations.com

National Vulnerability Database [NVD]



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

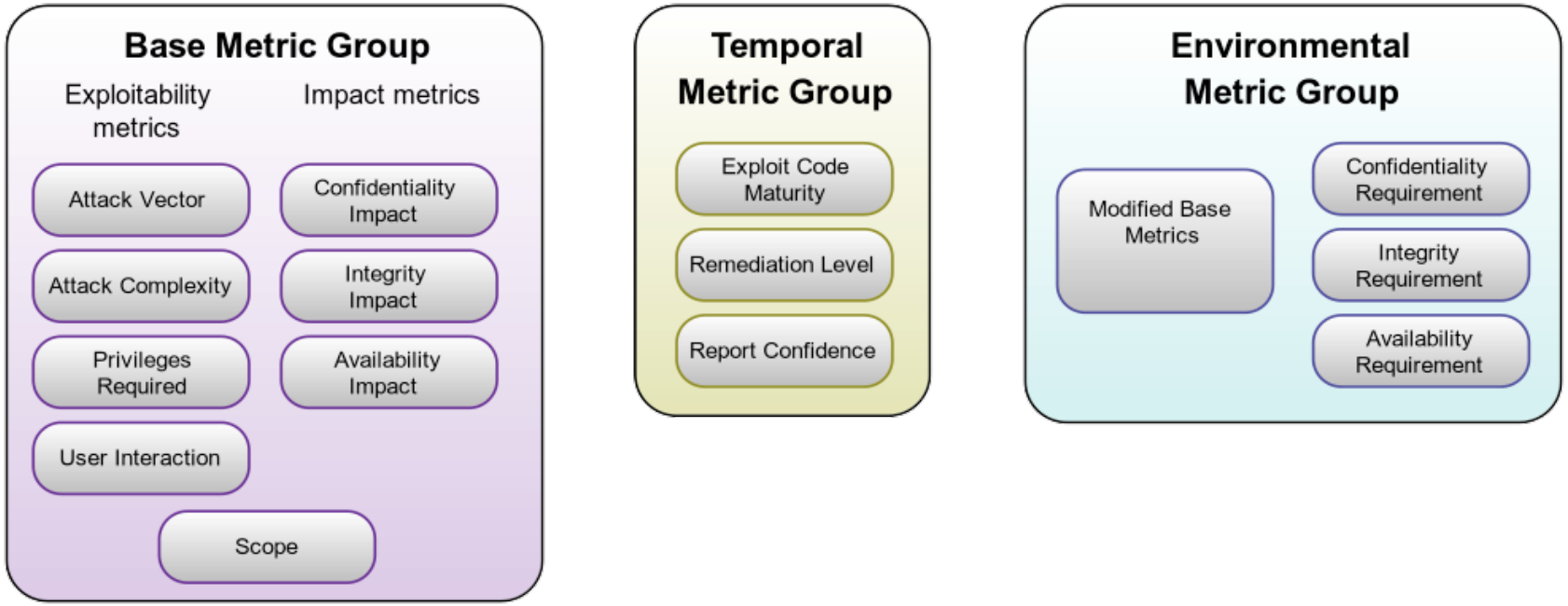
Severity

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


OWASP
Top 10

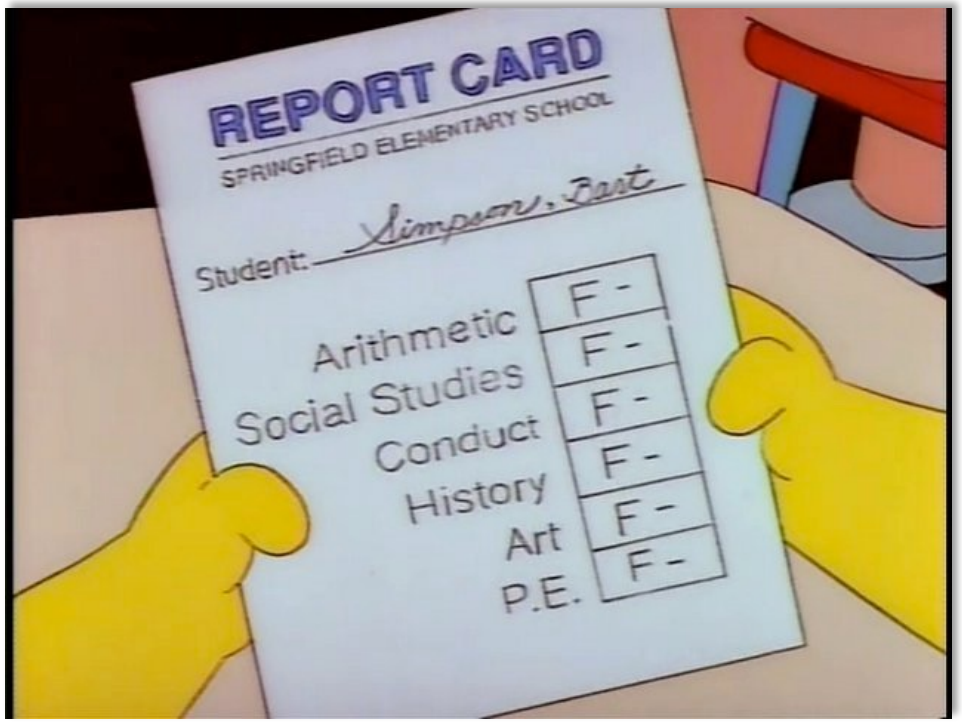

WEBGOAT

Shifting Left

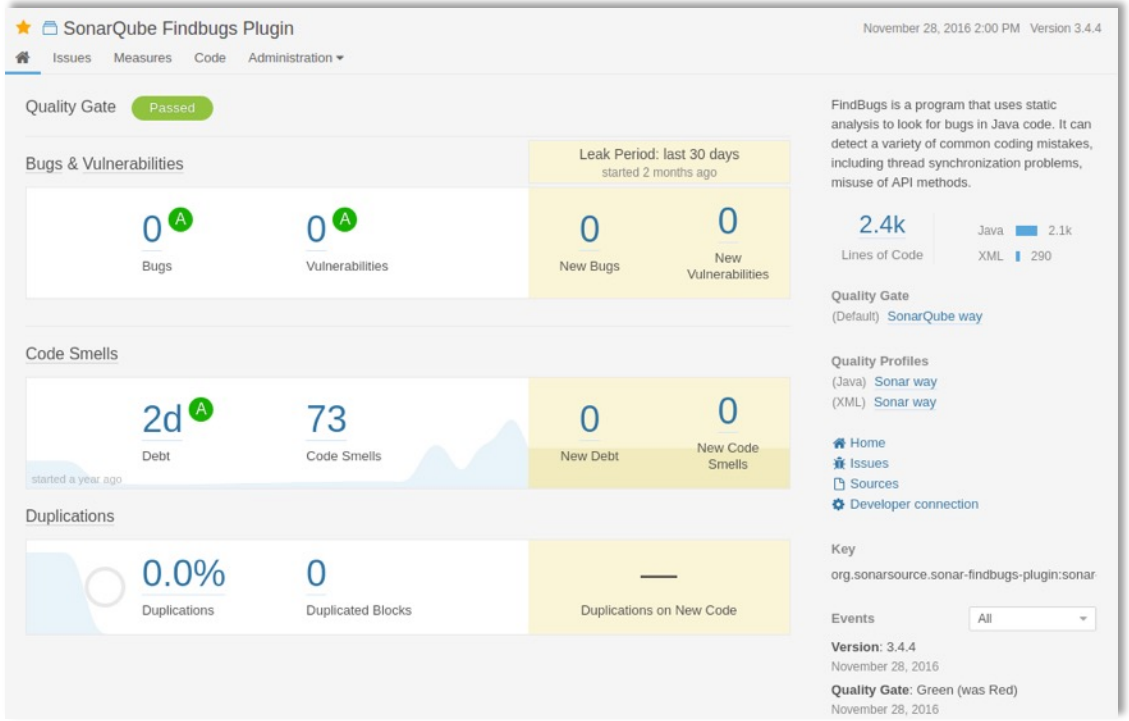
DevSecOps

```
@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");
```

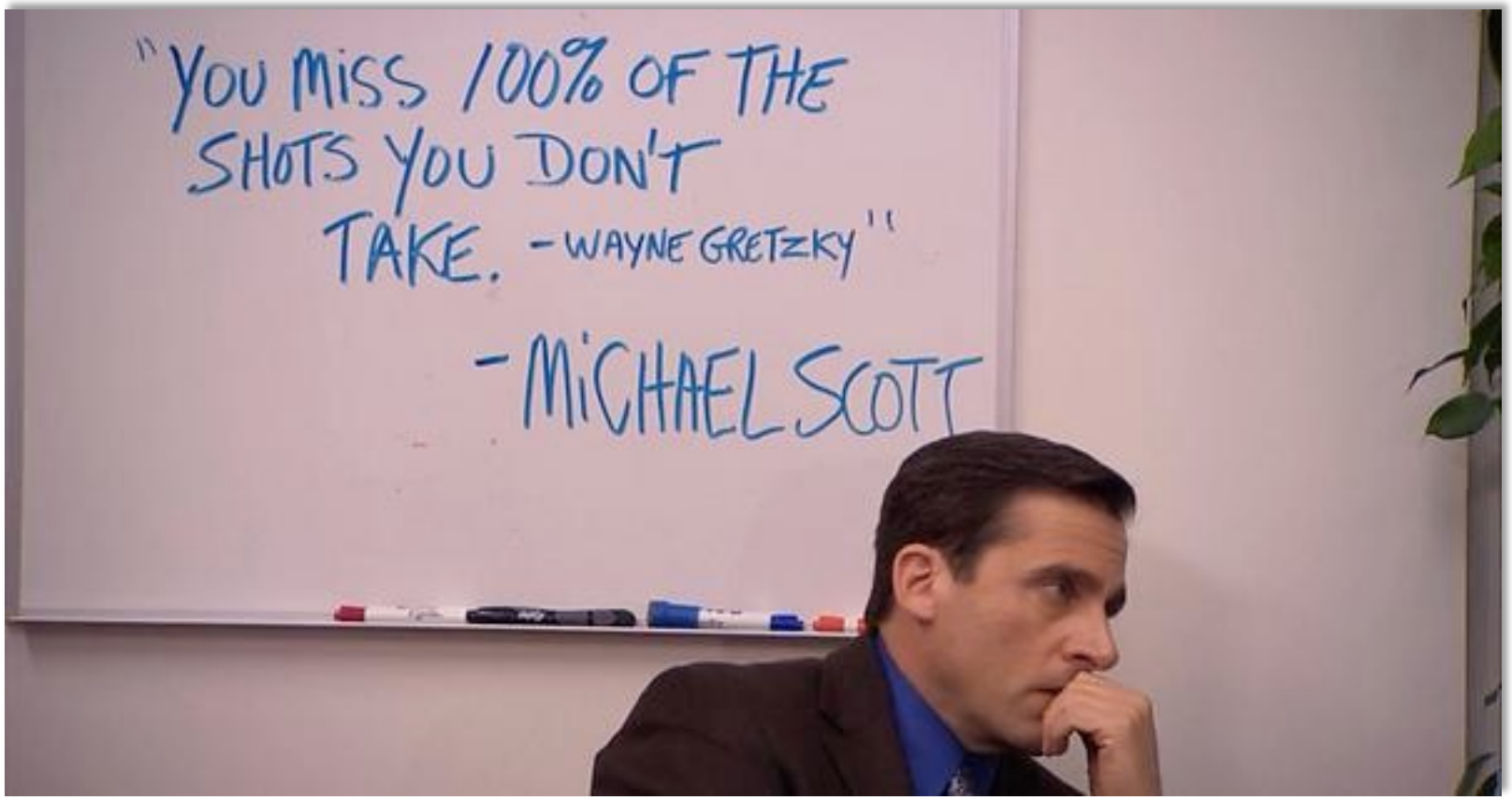
Static Analysis [SAST]



Or



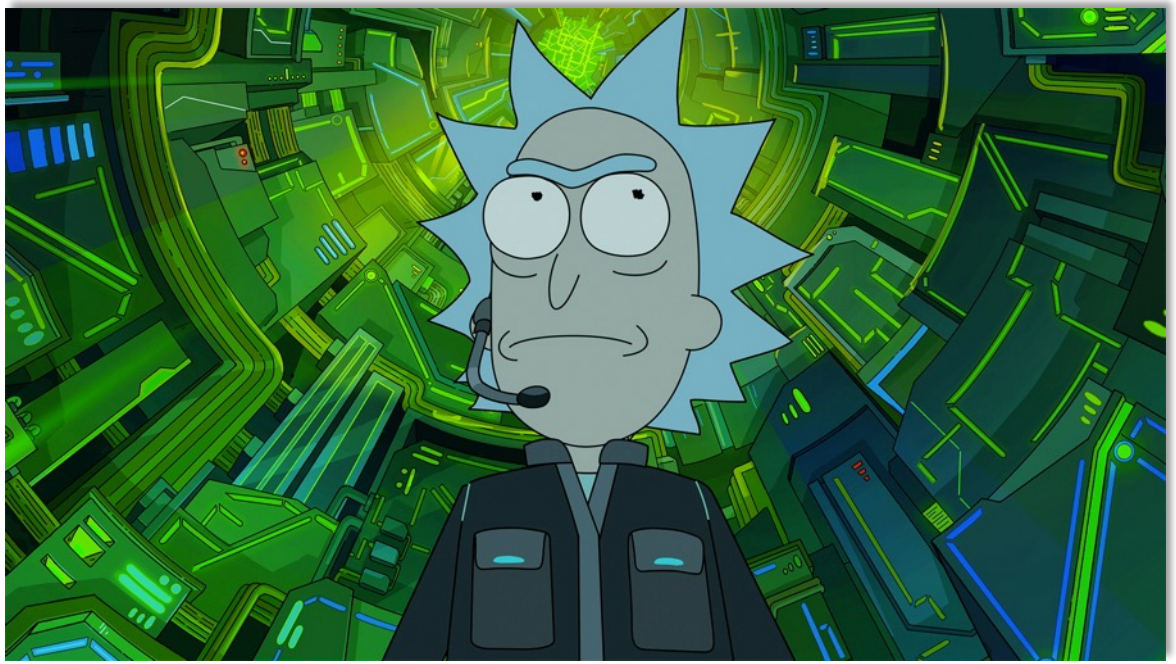
Dynamic Analysis [DAST]



RASPs

Your Pipelines

Your Pipelines

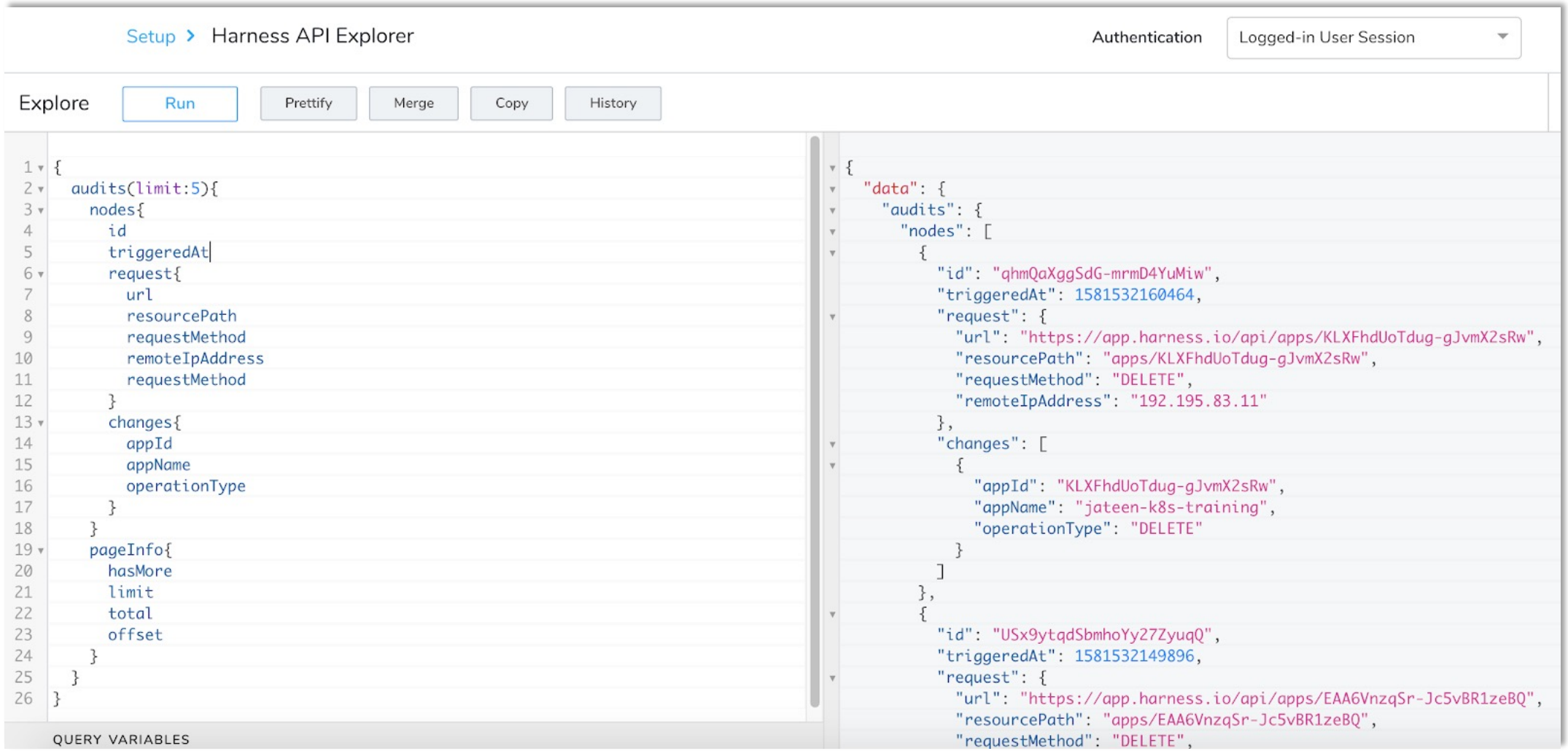


Least Privilege

Role Based Access

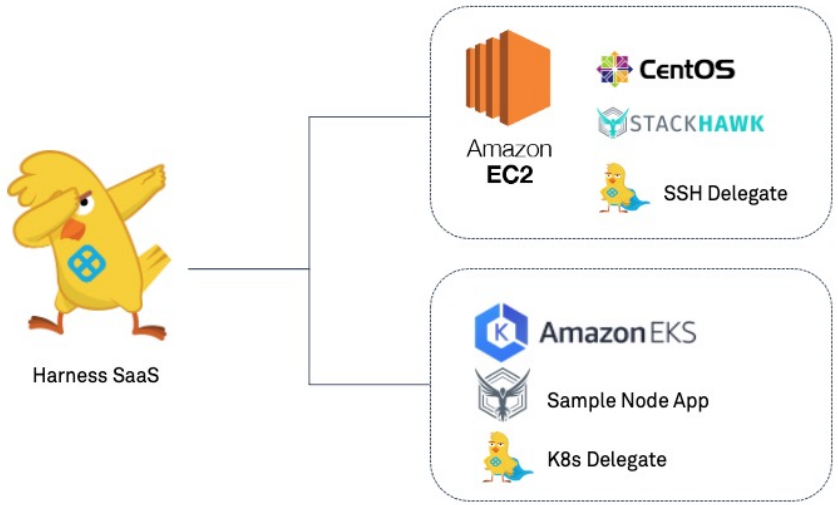
Secrets

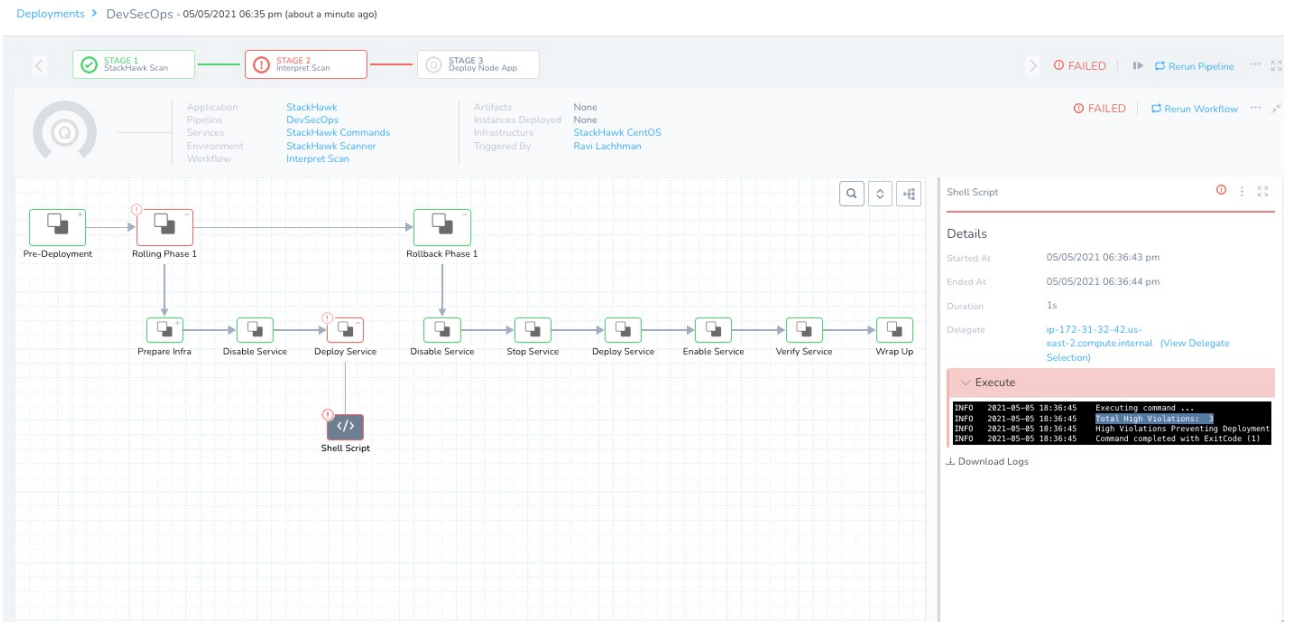
Audit Trail

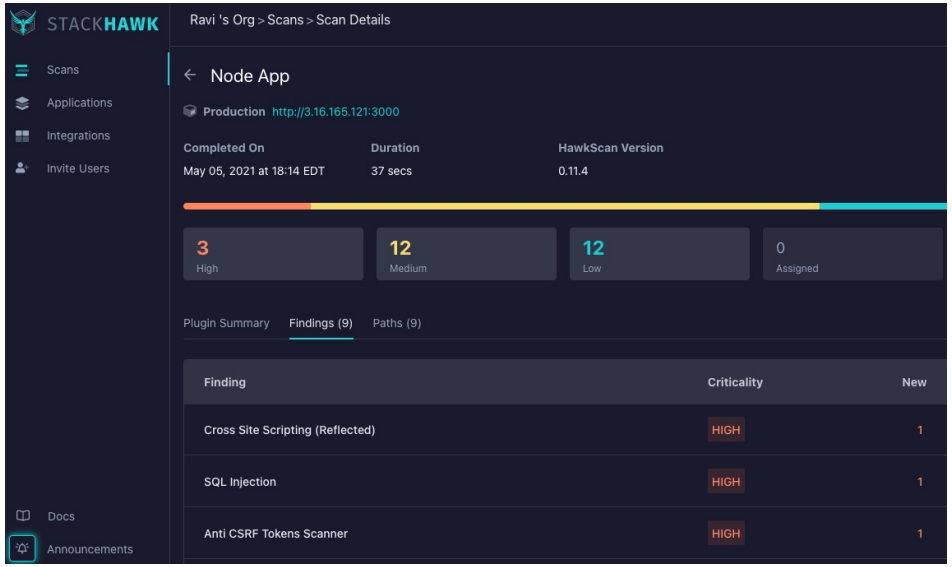

Setup > Harness API Explorer
Authentication
Logged-in User Session
Explore
Run
Prettify
Merge
Copy
History
{
audits(limit:5){
nodes{
id
triggeredAt
request{
url
resourcePath
requestMethod
remoteIpAddress
requestMethod
}
changes{
appId
appName
operationType
}
}
pageInfo{
hasMore
limit
total
offset
}
}
}
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",

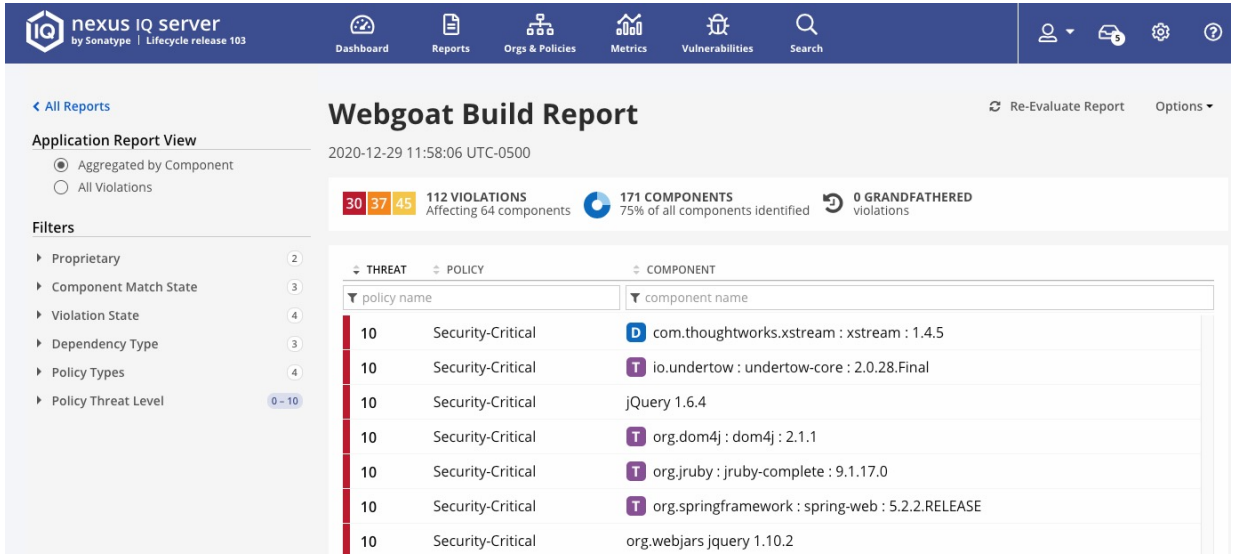
Security Starts with YOU

Some Cool Examples









Thanks!