

CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2024

JUNE 26-27 | SEATTLE, WA #CNSCon

Scan, Patch, VEX!

Using Open Source Tools to Manage Vulnerabilities in Containers

Toddy Mladenov, Microsoft
Itay Shakury, Aqua Security

Who are we?



Toddy Mladenov
Principal Product Manager
Cloud-Native + Ecosystem



Itay Shakury
VP Open Source
Aqua Security

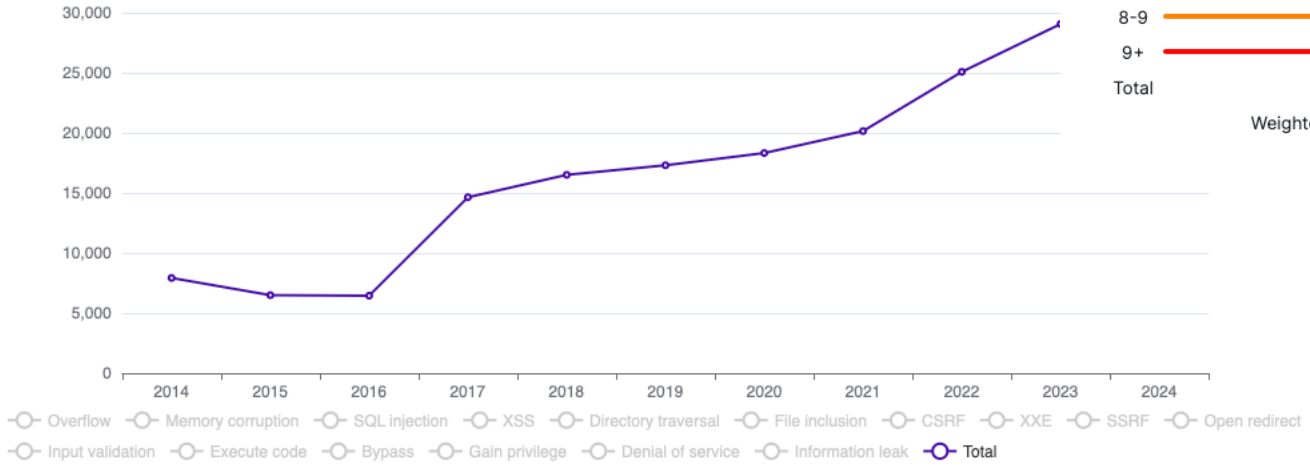
There are many vulnerabilities
You know it…
You need to deal with it

Distribution of vulnerabilities by CVSS scores

CVSS Score Range	Vulnerabilities
0-1	5274
1-2	138
2-3	928
3-4	2256
4-5	14681
5-6	29972
6-7	29158
7-8	44845
8-9	21120
9+	32818
Total	181190

Weighted Average CVSS Score: 7.5

Vulnerabilities by type & year



Images credit: https://cvedetails.com

Customer Story



So, you want to build a python application…




```
[ toddysm@tsm-mbp-msft ~ ] trivy image toddysm/python:3.12.2 | grep Total
2024-06-17T10:23:10-07:00       INFO    Vulnerability scanning is enabled
2024-06-17T10:23:10-07:00       INFO    Secret scanning is enabled
2024-06-17T10:23:10-07:00       INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-06-17T10:23:10-07:00       INFO    Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-06-17T10:23:10-07:00       INFO    Detected OS     family="debian" version="12.5"
2024-06-17T10:23:10-07:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=429
2024-06-17T10:23:10-07:00       INFO    Number of language-specific files       num=1
2024-06-17T10:23:10-07:00       INFO    [python-pkg] Detecting vulnerabilities...
Total: 1574 (UNKNOWN: 16, LOW: 533, MEDIUM: 867, HIGH: 151, CRITICAL: 7)
[ toddysm@tsm-mbp-msft ~ ] trivy image --ignore-unfixed toddysm/python:3.12.2 | grep Total
2024-06-17T10:23:23-07:00       INFO    Vulnerability scanning is enabled
2024-06-17T10:23:23-07:00       INFO    Secret scanning is enabled
2024-06-17T10:23:23-07:00       INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-06-17T10:23:23-07:00       INFO    Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-06-17T10:23:23-07:00       INFO    Detected OS     family="debian" version="12.5"
2024-06-17T10:23:23-07:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=429
2024-06-17T10:23:23-07:00       INFO    Number of language-specific files       num=1
2024-06-17T10:23:23-07:00       INFO    [python-pkg] Detecting vulnerabilities...
Total: 98 (UNKNOWN: 6, LOW: 5, MEDIUM: 63, HIGH: 24, CRITICAL: 0)
[ toddysm@tsm-mbp-msft ~ ]
```

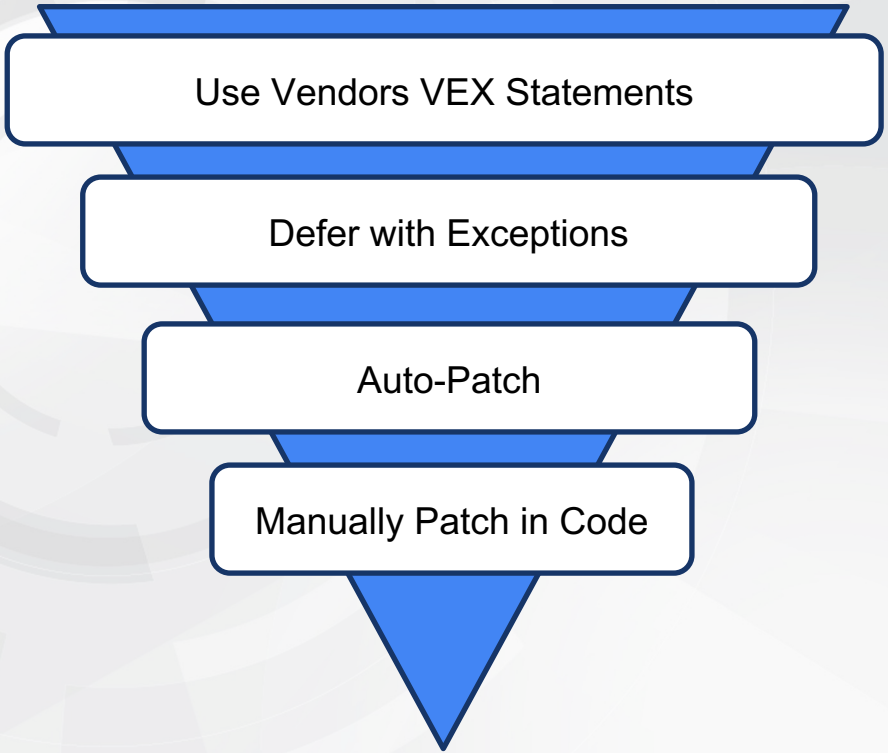
… and add your custom code



Flask

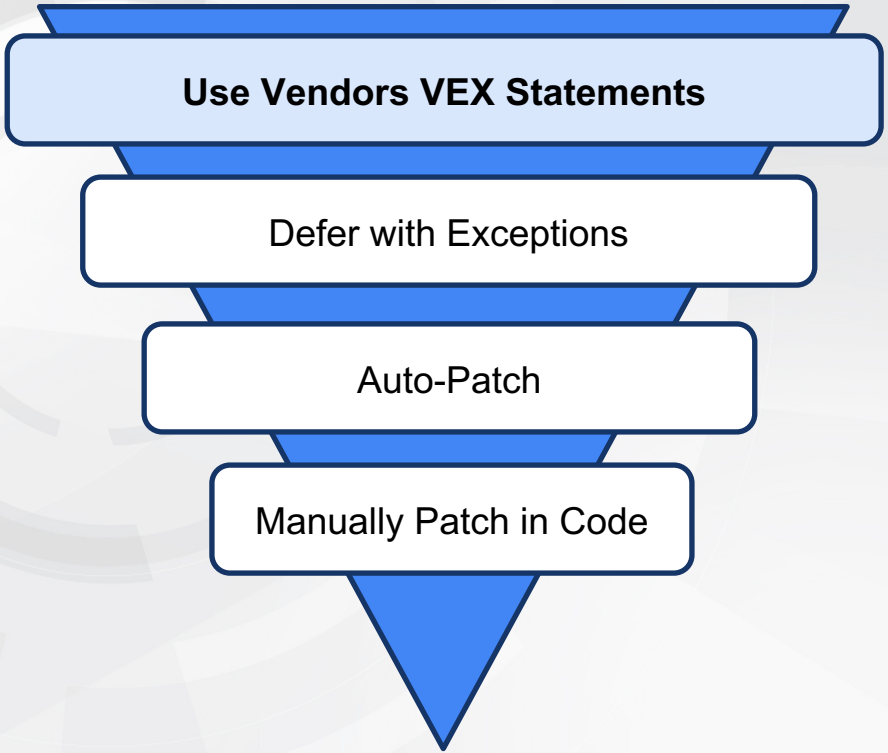
```
[ toddysm@tsm-mbp-msft ~ ] trivy image ghcr.io/toddysm/flasksample:1.0 | grep Total
2024-06-17T10:28:05-07:00       INFO    Vulnerability scanning is enabled
2024-06-17T10:28:05-07:00       INFO    Secret scanning is enabled
2024-06-17T10:28:05-07:00       INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-06-17T10:28:05-07:00       INFO    Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-06-17T10:28:05-07:00       INFO    Detected OS     family="debian" version="12.5"
2024-06-17T10:28:05-07:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=429
2024-06-17T10:28:06-07:00       INFO    Number of language-specific files       num=1
2024-06-17T10:28:06-07:00       INFO    [python-pkg] Detecting vulnerabilities...
Total: 1574 (UNKNOWN: 16, LOW: 533, MEDIUM: 867, HIGH: 151, CRITICAL: 7)
2024-06-17T10:28:06-07:00       INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.
Total: 7 (UNKNOWN: 0, LOW: 1, MEDIUM: 3, HIGH: 3, CRITICAL: 0)
[ toddysm@tsm-mbp-msft ~ ] trivy image --ignore-unfixed ghcr.io/toddysm/flasksample:1.0 | grep Total
2024-06-17T10:28:22-07:00       INFO    Vulnerability scanning is enabled
2024-06-17T10:28:22-07:00       INFO    Secret scanning is enabled
2024-06-17T10:28:22-07:00       INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-06-17T10:28:22-07:00       INFO    Please see also https://aquasecurity.github.io/trivy/v0.52/docs/scanner/secret/#recommendation for faster secret detection
2024-06-17T10:28:23-07:00       INFO    Detected OS     family="debian" version="12.5"
2024-06-17T10:28:23-07:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=429
2024-06-17T10:28:23-07:00       INFO    Number of language-specific files       num=1
2024-06-17T10:28:23-07:00       INFO    [python-pkg] Detecting vulnerabilities...
2024-06-17T10:28:23-07:00       INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.
Total: 98 (UNKNOWN: 6, LOW: 5, MEDIUM: 63, HIGH: 24, CRITICAL: 0)
Total: 7 (UNKNOWN: 0, LOW: 1, MEDIUM: 3, HIGH: 3, CRITICAL: 0)
[ toddysm@tsm-mbp-msft ~ ]
```

Finding the actionable items



Demo
(where do we start?)

Finding the actionable items



Current Behavior

`gradle v8.0.1` adds the `testng-6.3.1.jar` plugin. According to https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4065, the security vulnerability is patched in `testng-7.7.0.jar`

I would appreciate if the `testng` plugin is patched in an upcoming release.



ljacomet commented on Apr 27, 2023 — Member

The version 6.3.1 of TestNG does not have the necessary code to produce the path traversal. It does not extract files out of the archive. Instead, processing is done in place.
The PR that introduced the issue is in versions `[6.13, 7.6.1]`:

- **Extracting out unrelated logic from TestNG class.** testng-team/testng#1596

Second, that CVE has a very inflated score in my opinion:

- Only `.xml`, `.yaml` and `.yml` files can be extracted that way, not any file. The scope could be extended if custom `org.testng.xml.ISuiteParser` are available on the classpath.
- Second, this happens when running a supposedly malicious test JAR. If you have such a malicious JAR, chances are that the test execution itself will be compromised, which is *directly remote code execution* then, including attempting to write any content to any file on disk. But managing to do that JAR injection and only attempt to exploit the path traversal problem seems quite unlikely.
- It feels like the vulnerability has been rated as if TestNG was used in a webapp that accepts random archives and not as a testing library used by developers and build tools. While there might be a webapp out there doing just that, it is not the common usage scenario.

I'll try to follow up to get the vulnerability score revised.

While the above means Gradle is not vulnerable, we still plan to update TestNG at some point, see:

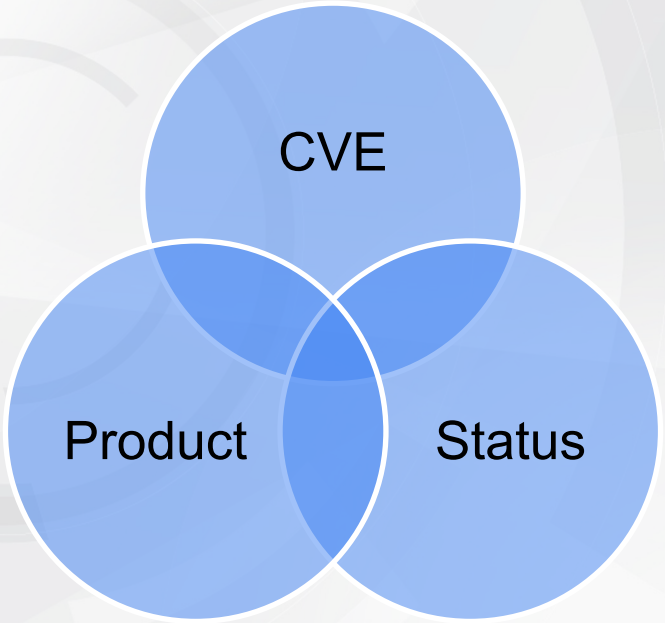
- **Update bundled TestNG to a recent version** #24930

I will close this issue as the CVE is not applicable.

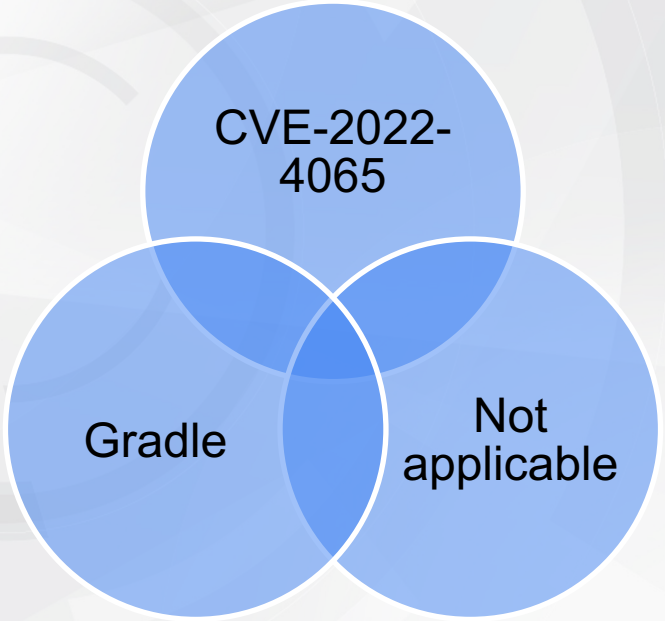
👍 5

ljacomet closed this as not planned on Apr 27, 2023

Vulnerability eXploitability Exchange (VEX)



Vulnerability eXploitability Exchange (VEX)



VEX Standards



- OpenVEX (OSSF)
- CSAF (OASIS)
- CycloneDX VEX (OWASP)
- ...



OpenVEX

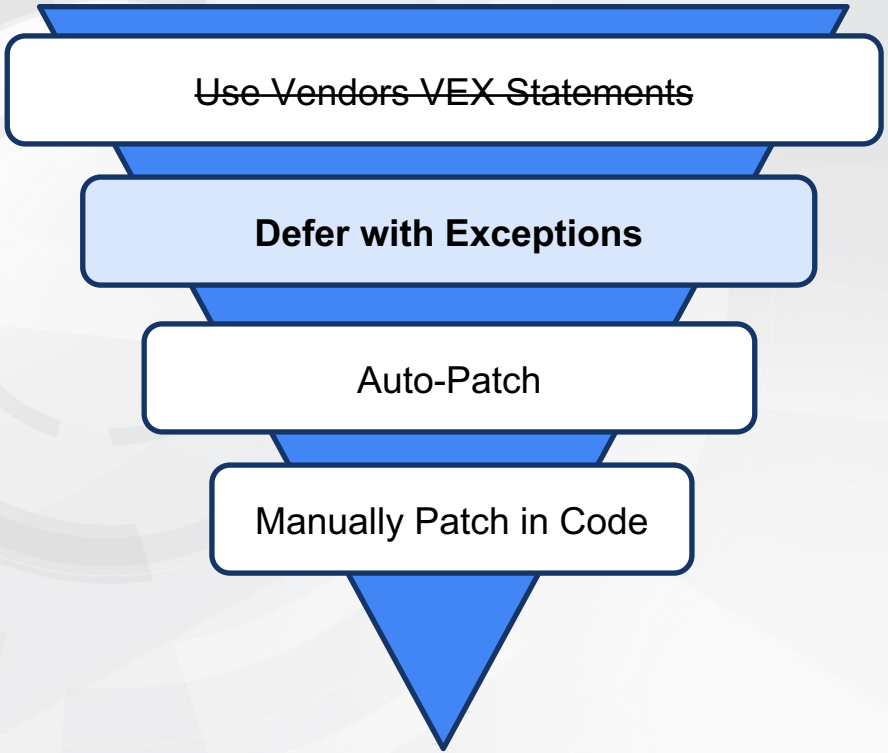
A simplified Vulnerability Exploitability eXchange implementation

90 followers https://openvex.dev Verified


```
{
  "@context": "https://openvex.dev/ns/v0.2.0",
  "@id": "https://openvex.dev/docs/example/vex-9fb3463de1b57",
  "author": "Wolfi J Inkinson",
  "role": "Document Creator",
  "timestamp": "2023-01-08T18:02:03.647787998-06:00",
  "version": 1,
  "statements": [
    {
      "vulnerability": {
        "name": "CVE-2023-12345"
      },
      "products": [
        {"@id": "pkg:apk/wolfi/git@2.39.0-r1?arch=armv7"},
        {"@id": "pkg:apk/wolfi/git@2.39.0-r1?arch=x86_64"}
      ],
      "status": "fixed"
    }
  ]
}
```

Demo

Finding the actionable items



Defering / Ignoring / Exceptions

Fix unavailable

Need more time

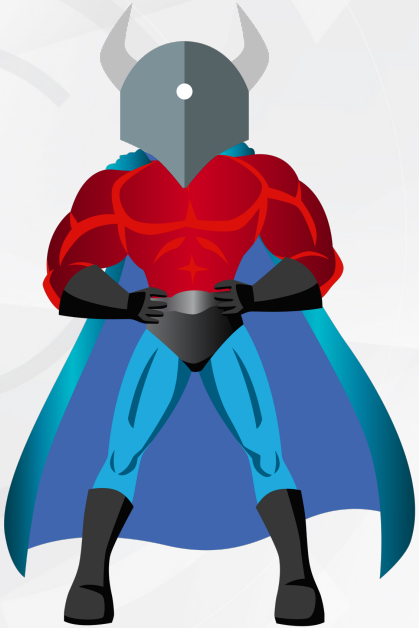


False positive

Low business impact

Trivy Ignore with Rego

- **Built-in Functions**
  - Comparison
  - Numbers
  - Aggregates
  - Arrays
  - Sets
  - Objects
  - Strings
  - Regex
  - Glob
  - Bitwise
  - Conversions
  - Units
  - Types
  - Encoding
  - Token Signing
  - Token Verification
  - Time
  - Cryptography
  - Graphs
  - GraphQL
  - HTTP
  - AWS
  - Net
  - UUID
  - Semantic Versions
  - Rego
  - OPA
  - Debugging
  - Tracing



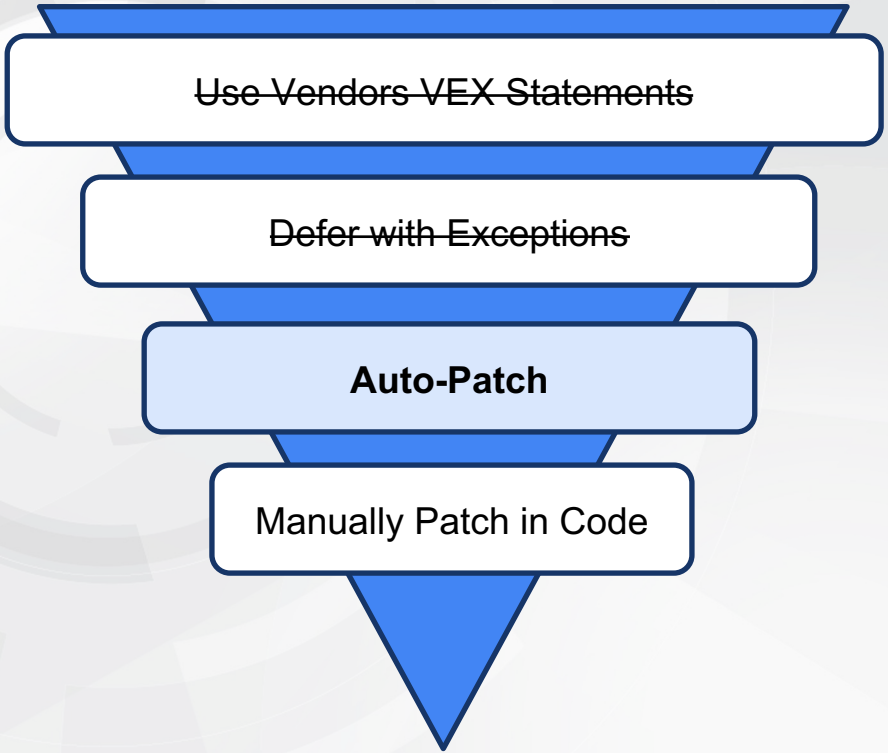
Policy Language

- **What is Rego?**
- Why use Rego?
- Learning Rego
- The Basics
- Scalar Values
- Strings
- Composite Values
- Variables
- References
- Comprehensions
- Rules
- Negation
- Universal Quantification (FOR ALL)
- Modules
- Future Keywords
- Some Keyword
- Every Keyword
- With Keyword
- Default Keyword
- Else Keyword
- Operators
- Built-in Functions
- Example Data
- Metadata
- Schema
- Strict Mode
- The rego.v1 Import
- Ecosystem Projects

📖 https://aquasecurity.github.io/trivy/v0.52/docs/configuration/filtering

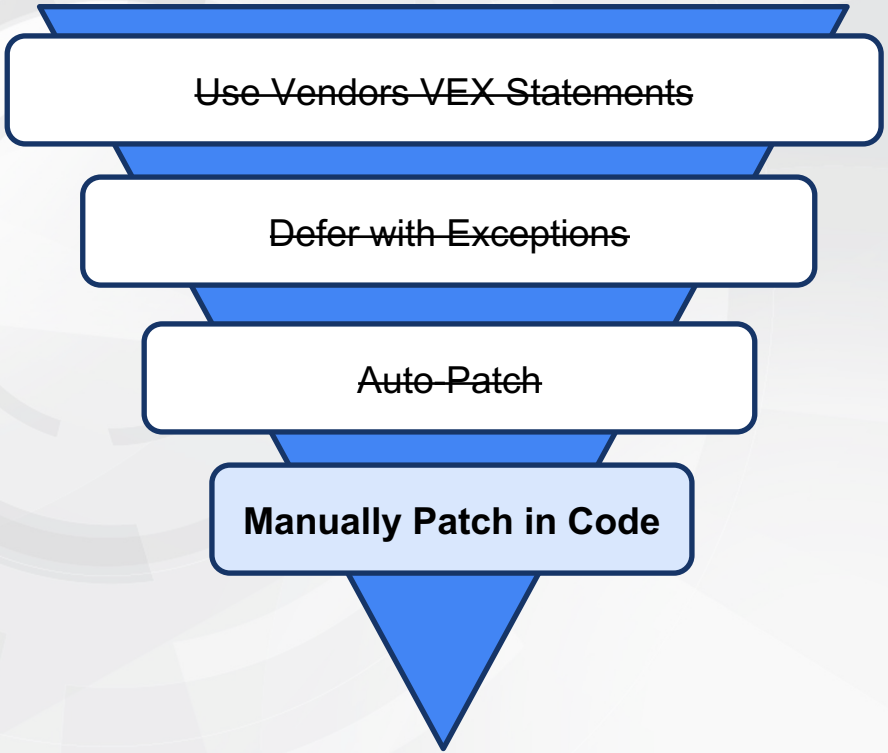
Demo

Finding the actionable items



Demo

Finding the actionable items



```
~ ❯ trivy -q image --severity CRITICAL,HIGH localhost:5000/flasksample:1.0

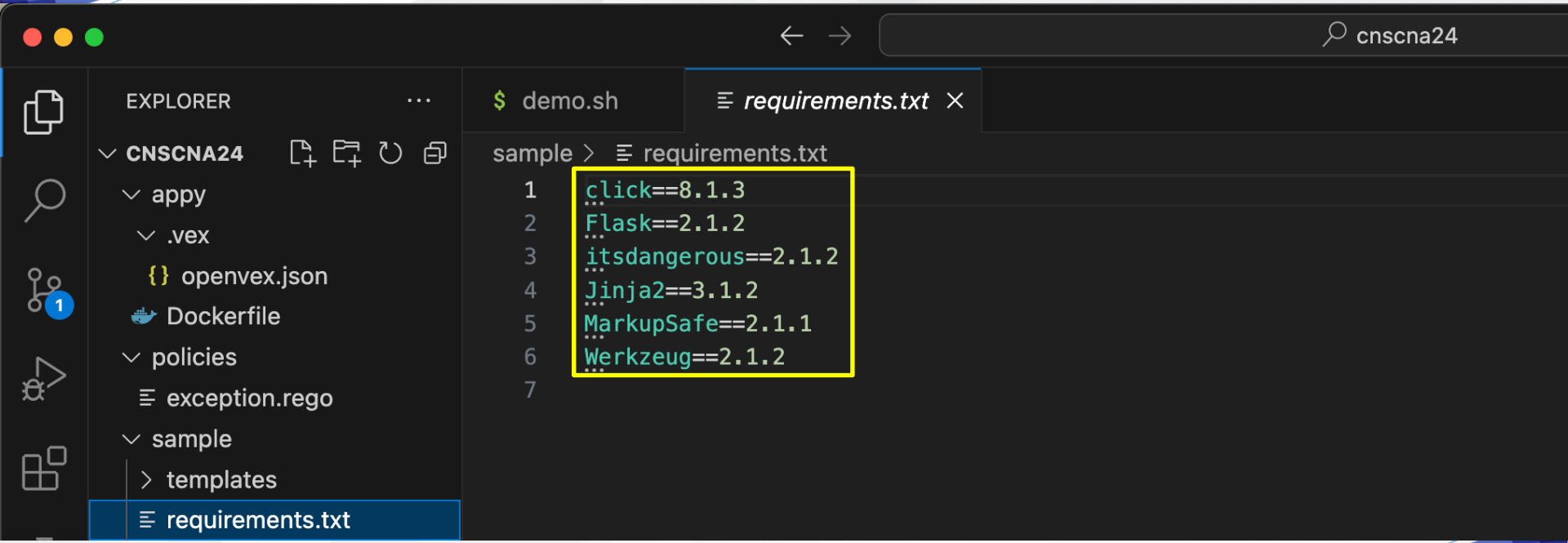
localhost:5000/flasksample:1.0 (debian 12.5)

Total: 158 (HIGH: 151, CRITICAL: 7)
```

Python (python-pkg)

Total: 3 (HIGH: 3, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
Flask (METADATA)	CVE-2023-30861	HIGH	fixed	2.1.2	2.3.2, 2.2.5	flask: Possible disclosure of permanent session cookie due to missing Vary: Cookie... https://avd.aquasec.com/nvd/cve-2023-30861
Werkzeug (METADATA)	CVE-2023-25577				2.2.3	python-werkzeug: high resource usage when parsing multipart form data with many fields... https://avd.aquasec.com/nvd/cve-2023-25577
	CVE-2024-34069				3.0.3	python-werkzeug: user may execute code on a developer's machine https://avd.aquasec.com/nvd/cve-2024-34069


cnscna24
EXPLORER
CNSCNA24
appy
.vex
openvex.json
Dockerfile
policies
exception.rego
sample
templates
requirements.txt
demo.sh
requirements.txt
sample > requirements.txt
1 click==8.1.3
2 Flask==2.1.2
3 itsdangerous==2.1.2
4 Jinja2==3.1.2
5 MarkupSafe==2.1.1
6 Werkzeug==2.1.2
7

Learnings

PURL matching for container images

- ~~docker.io/python~~
- ~~library/python~~
- ~~python:3.12.2~~
- python
  - Which?
- python@version
  - ~~python@3.12.2~~
  - ~~python@imageID~~
  - python@repoDigest
  - python@anotherRepoDigest?tag=3.12.2
- Version ranges 🫠

`pkg:deb/debian/curl@7.50.3-1`

Where to find VEX?

- In container registry
  - Which registry: multi registries, mirroring, air-gapped
  - Which image: oci references are per-digest
  - Non-containers: packages, binaries
- Vendor provided
  - Manual
  - Non-standardized
  - Non-accessible
- In source repository
  - Manual
  - Not everything is OSS



Other Learnings

- VEX document integrity and authenticity
- Tools are not a magic bullet
- Data is sparse
- It is an honor system
- Others??



CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2024

JUNE 26-27 | SEATTLE, WA #CNSCon

Scan, Patch, VEX!

Using Open Source Tools to Manage Vulnerabilities in Containers

Toddy Mladenov, Microsoft
Itay Shakury, Aqua Security