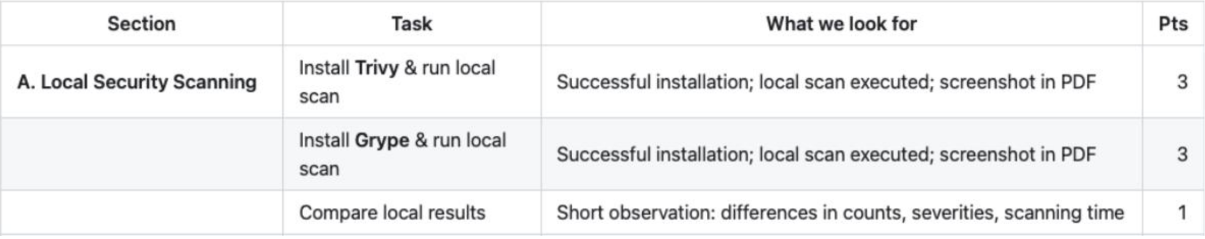
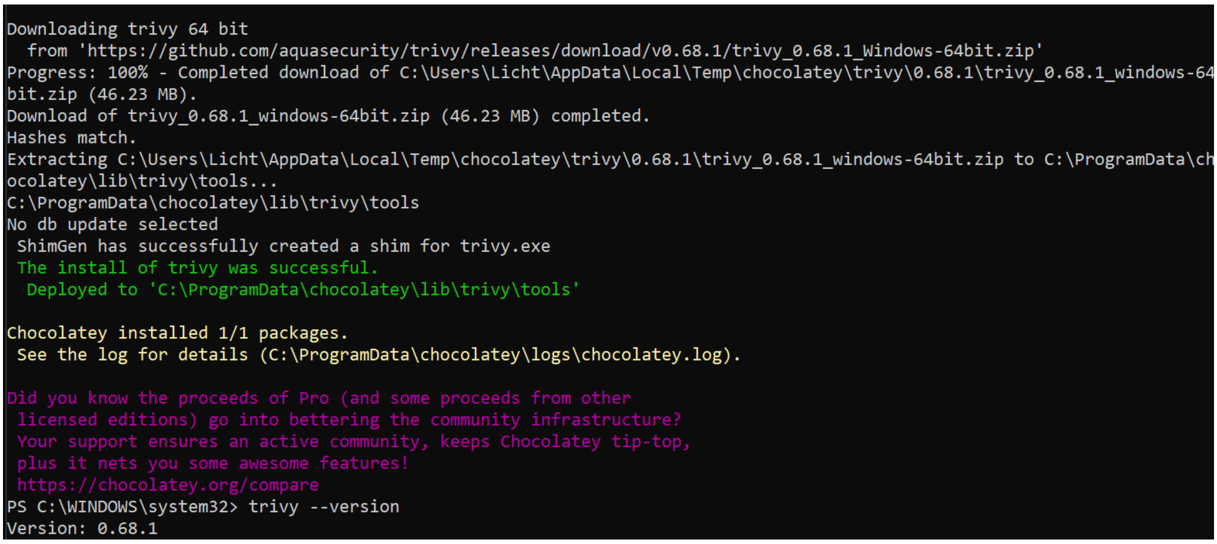
CICD Exercise04 Lichtenberger



Section	Task	What we look for	Pts
A. Local Security Scanning	Install **Trivy** & run local scan	Successful installation; local scan executed; screenshot in PDF	3
	Install **Grype** & run local scan	Successful installation; local scan executed; screenshot in PDF	3
	Compare local results	Short observation: differences in counts, severities, scanning time	1

Download und Install von Trivy

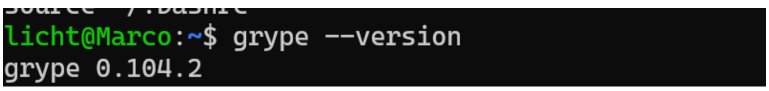


```
Downloading trivy 64 bit
  from 'https://github.com/aquasecurity/trivy/releases/download/v0.68.1/trivy_0.68.1_Windows-64bit.zip'
Progress: 100% - Completed download of C:\Users\Licht\AppData\Local\Temp\chocolatey\trivy\0.68.1\trivy_0.68.1_windows-64
bit.zip (46.23 MB).
Download of trivy_0.68.1_windows-64bit.zip (46.23 MB) completed.
Hashes match.
Extracting C:\Users\Licht\AppData\Local\Temp\chocolatey\trivy\0.68.1\trivy_0.68.1_windows-64bit.zip to C:\ProgramData\ch
ocolatey\lib\trivy\tools...
C:\ProgramData\chocolatey\lib\trivy\tools
No db update selected
 ShimGen has successfully created a shim for trivy.exe
 The install of trivy was successful.
  Deployed to 'C:\ProgramData\chocolatey\lib\trivy\tools'

Chocolatey installed 1/1 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).

Did you know the proceeds of Pro (and some proceeds from other
 licensed editions) go into bettering the community infrastructure?
 Your support ensures an active community, keeps Chocolatey tip-top,
 plus it nets you some awesome features!
 https://chocolatey.org/compare
PS C:\WINDOWS\system32> trivy --version
Version: 0.68.1
```

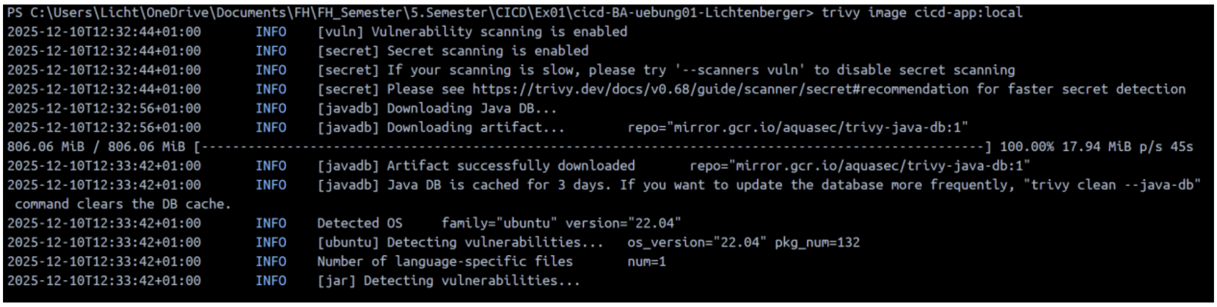
Grype ebenfalls erfolgreich installiert:



```
source ~/.bashrc
licht@Marco:~$ grype --version
grype 0.104.2
```

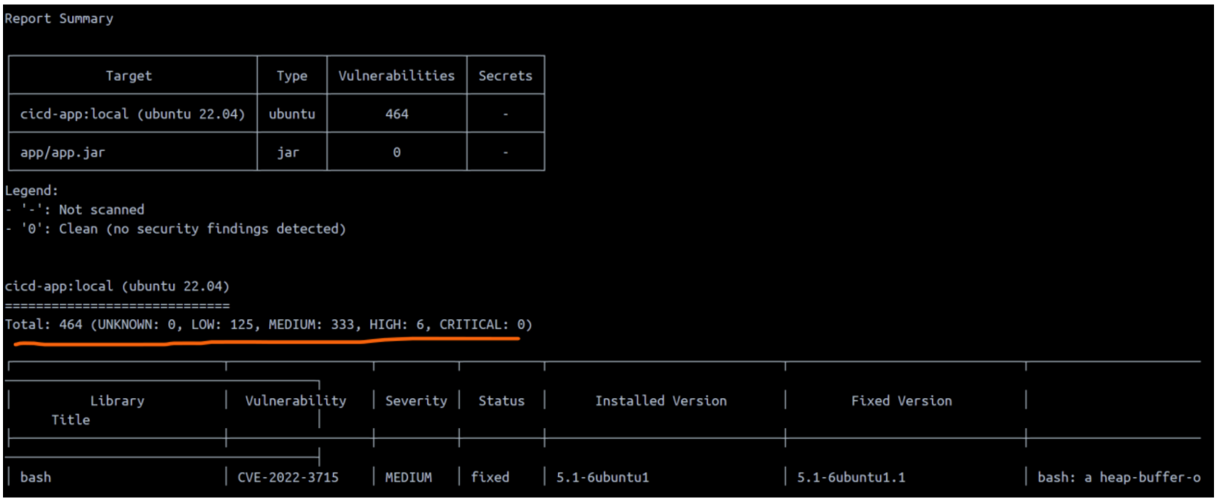
Scan:

Trivy Scan Local



```
PS C:\Users\Licht\OneDrive\Documents\FH\FH_Semester\5.Semester\CICD\Ex01\cicd-BA-uebung01-Lichtenberger> trivy image cicd-app:local
2025-12-10T12:32:44+01:00       INFO    [vuln] Vulnerability scanning is enabled
2025-12-10T12:32:44+01:00       INFO    [secret] Secret scanning is enabled
2025-12-10T12:32:44+01:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-12-10T12:32:44+01:00       INFO    [secret] Please see https://trivy.dev/docs/v0.68/guide/scanner/secret#recommendation for faster secret detection
2025-12-10T12:32:56+01:00       INFO    [javadb] Downloading Java DB...
2025-12-10T12:32:56+01:00       INFO    [javadb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-java-db:1"
806.06 MiB / 806.06 MiB [----------------------------------------------------------------------------------------------] 100.00% 17.94 MiB p/s 45s
2025-12-10T12:33:42+01:00       INFO    [javadb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-java-db:1"
2025-12-10T12:33:42+01:00       INFO    [javadb] Java DB is cached for 3 days. If you want to update the database more frequently, "trivy clean --java-db"
 command clears the DB cache.
2025-12-10T12:33:42+01:00       INFO    Detected OS     family="ubuntu" version="22.04"
2025-12-10T12:33:42+01:00       INFO    [ubuntu] Detecting vulnerabilities...   os_version="22.04" pkg_num=132
2025-12-10T12:33:42+01:00       INFO    Number of language-specific files       num=1
2025-12-10T12:33:42+01:00       INFO    [jar] Detecting vulnerabilities...
```

Results: veraltete Ubuntu version 22.04 wirft viele viele Vulnerabilities.



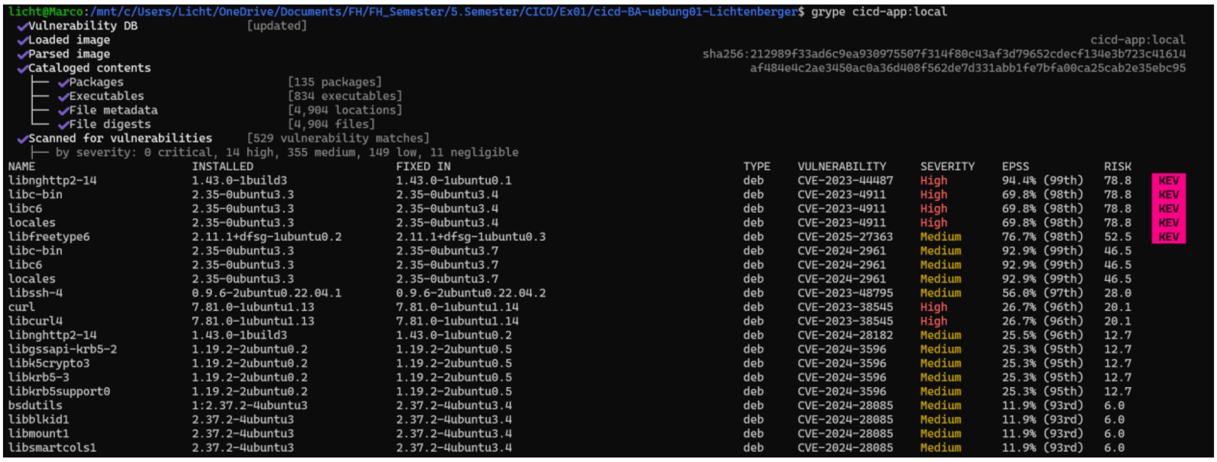
```
Report Summary

┌────────────────────────────────┬────────┬─────────────────┬─────────┐
│             Target             │  Type  │ Vulnerabilities │ Secrets │
├────────────────────────────────┼────────┼─────────────────┼─────────┤
│ cicd-app:local (ubuntu 22.04)  │ ubuntu │       464       │    -    │
├────────────────────────────────┼────────┼─────────────────┼─────────┤
│ app/app.jar                    │  jar   │        0        │    -    │
└────────────────────────────────┴────────┴─────────────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


cicd-app:local (ubuntu 22.04)
=============================
Total: 464 (UNKNOWN: 0, LOW: 125, MEDIUM: 333, HIGH: 6, CRITICAL: 0)

┌───────────────────────────┬───────────────────┬──────────┬────────┬──────────────────────────────┬──────────────────────────────┬──────────────────
│          Library          │   Vulnerability   │ Severity │ Status │      Installed Version       │        Fixed Version         │
   Title                    │
├───────────────────────────┼───────────────────┼──────────┼────────┼──────────────────────────────┼──────────────────────────────┼──────────────────
│ bash                      │ CVE-2022-3715     │ MEDIUM   │ fixed  │ 5.1-6ubuntu1                 │ 5.1-6ubuntu1.1               │ bash: a heap-buffer-o
```

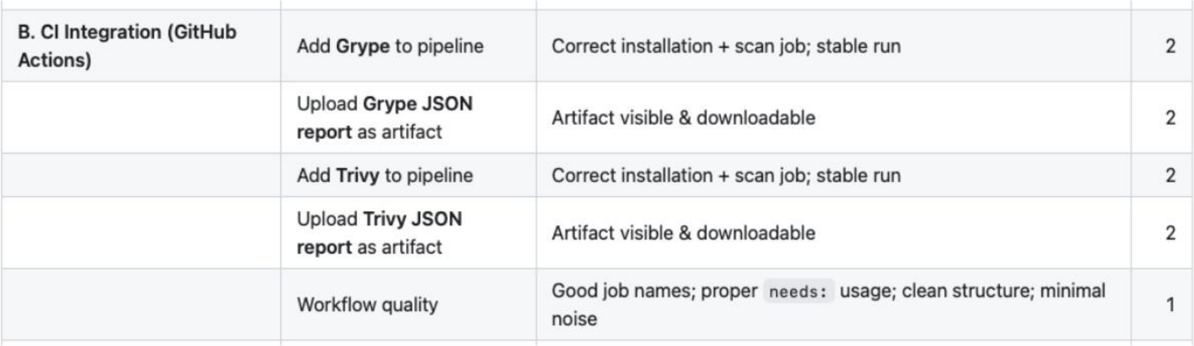
Grype Scan und Results: ebenfalls viele Vulnerabilities wegen veralteter version



```
licht@Marco:/mnt/c/Users/Licht/OneDrive/Documents/FH/FH_Semester/5.Semester/CICD/Ex01/cicd-BA-uebung01-Lichtenberger$ grype cicd-app:local
 ✔Vulnerability DB                [updated]
 ✔Loaded image                                                                                                cicd-app:local
 ✔Parsed image                                            sha256:212989f33ad6c9ea930975507f314f80c43af3d79652cdecf134e3b723c41614
 ✔Cataloged contents                                             af484e4c2ae3450ac0a36d408f562de7d331abb1fe7bfa00ca25cab2e35ebc95
   ├── ✔Packages                        [135 packages]
   ├── ✔Executables                     [834 executables]
   ├── ✔File metadata                   [4,904 locations]
   └── ✔File digests                    [4,904 files]
 ✔Scanned for vulnerabilities     [529 vulnerability matches]
   ├── by severity: 0 critical, 14 high, 355 medium, 149 low, 11 negligible
NAME                 INSTALLED                  FIXED IN                   TYPE  VULNERABILITY   SEVERITY  EPSS           RISK
libnghttp2-14        1.43.0-1build3             1.43.0-1ubuntu0.1          deb   CVE-2023-44487  High      94.4% (99th)   78.8   KEV
libc-bin             2.35-0ubuntu3.3            2.35-0ubuntu3.4            deb   CVE-2023-4911   High      69.8% (98th)   78.8   KEV
libc6                2.35-0ubuntu3.3            2.35-0ubuntu3.4            deb   CVE-2023-4911   High      69.8% (98th)   78.8   KEV
locales              2.35-0ubuntu3.3            2.35-0ubuntu3.4            deb   CVE-2023-4911   High      69.8% (98th)   78.8   KEV
libfreetype6         2.11.1+dfsg-1ubuntu0.2     2.11.1+dfsg-1ubuntu0.3     deb   CVE-2025-27363  Medium    76.7% (98th)   52.5   KEV
libc-bin             2.35-0ubuntu3.3            2.35-0ubuntu3.7            deb   CVE-2024-2961   Medium    92.9% (99th)   46.5
libc6                2.35-0ubuntu3.3            2.35-0ubuntu3.7            deb   CVE-2024-2961   Medium    92.9% (99th)   46.5
locales              2.35-0ubuntu3.3            2.35-0ubuntu3.7            deb   CVE-2024-2961   Medium    92.9% (99th)   46.5
libssh-4             0.9.6-2ubuntu0.22.04.1     0.9.6-2ubuntu0.22.04.2     deb   CVE-2023-48795  Medium    56.0% (97th)   28.0
curl                 7.81.0-1ubuntu1.13         7.81.0-1ubuntu1.14         deb   CVE-2023-38545  High      26.7% (96th)   20.1
libcurl4             7.81.0-1ubuntu1.13         7.81.0-1ubuntu1.14         deb   CVE-2023-38545  High      26.7% (96th)   20.1
libnghttp2-14        1.43.0-1build3             1.43.0-1ubuntu0.2          deb   CVE-2024-28182  Medium    25.5% (96th)   12.7
libgssapi-krb5-2     1.19.2-2ubuntu0.2          1.19.2-2ubuntu0.5          deb   CVE-2024-3596   Medium    25.3% (95th)   12.7
libk5crypto3         1.19.2-2ubuntu0.2          1.19.2-2ubuntu0.5          deb   CVE-2024-3596   Medium    25.3% (95th)   12.7
libkrb5-3            1.19.2-2ubuntu0.2          1.19.2-2ubuntu0.5          deb   CVE-2024-3596   Medium    25.3% (95th)   12.7
libkrb5support0      1.19.2-2ubuntu0.2          1.19.2-2ubuntu0.5          deb   CVE-2024-3596   Medium    25.3% (95th)   12.7
bsdutils             1:2.37.2-4ubuntu3          2.37.2-4ubuntu3.4          deb   CVE-2024-28085  Medium    11.9% (93rd)   6.0
libblkid1            2.37.2-4ubuntu3            2.37.2-4ubuntu3.4          deb   CVE-2024-28085  Medium    11.9% (93rd)   6.0
libmount1            2.37.2-4ubuntu3            2.37.2-4ubuntu3.4          deb   CVE-2024-28085  Medium    11.9% (93rd)   6.0
libsmartcols1        2.37.2-4ubuntu3            2.37.2-4ubuntu3.4          deb   CVE-2024-28085  Medium    11.9% (93rd)   6.0
```

Vergleich warum Grype mehr findet als Trivy

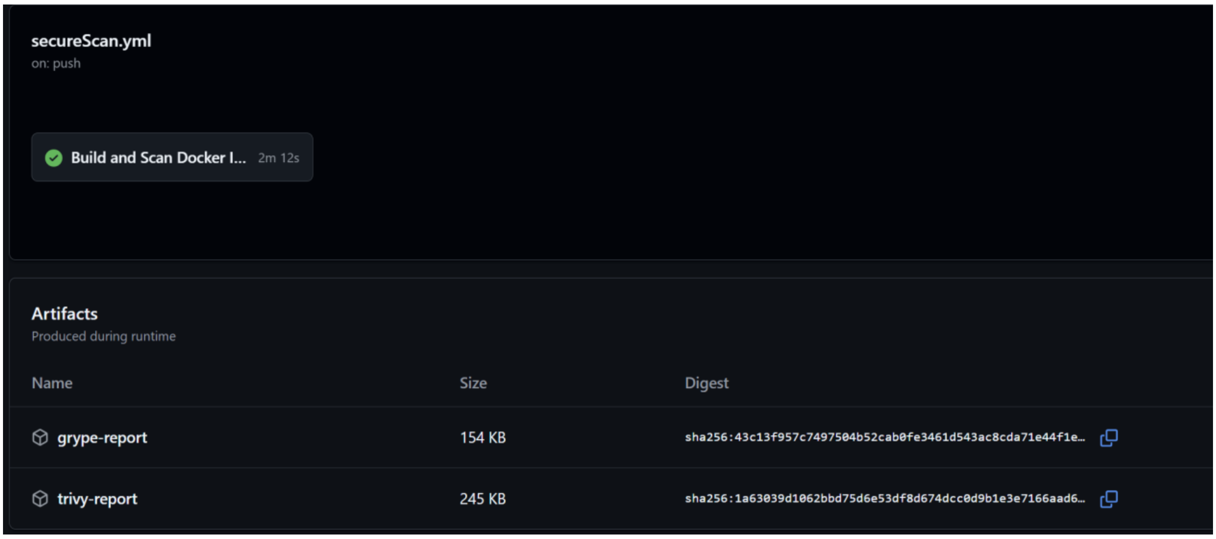
Grype zeigt mehr Vulnerabilities als Trivy, weil es tiefer scannt und mehr Quellen kombiniert: Es berücksichtigt zusätzlich ausführbare Dateien, Metadaten von Libraries und OS-Pakete, die Trivy teilweise überspringt, und nutzt eine umfassendere Datenbank aus Anchore und OS-CVEs. Trivy filtert dagegen manche Funde oder zählt nur bestimmte Pakete, wodurch die Zahl der erkannten Schwachstellen niedriger erscheint. Der Unterschied liegt also an **Scope, Datenbasis und Standardfilterung**, nicht an falschen Ergebnissen.



B. CI Integration (GitHub Actions)	Add **Grype** to pipeline	Correct installation + scan job; stable run	2
	Upload **Grype JSON report** as artifact	Artifact visible & downloadable	2
	Add **Trivy** to pipeline	Correct installation + scan job; stable run	2
	Upload **Trivy JSON report** as artifact	Artifact visible & downloadable	2
	Workflow quality	Good job names; proper `needs:` usage; clean structure; minimal noise	1

Pipline hinzugefügt:

1. Zuerst wird das Dockerimage erstellt (build)
2. Danach Grype und Trivy Scans
3. Reports werden exportiert

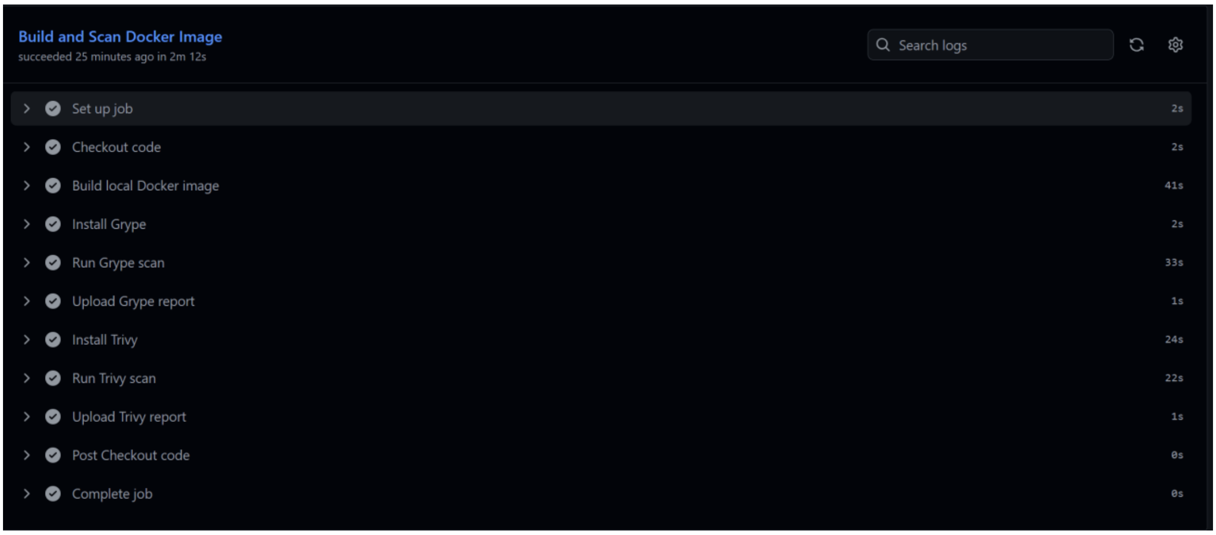


secureScan.yml
on: push

Build and Scan Docker I... 2m 12s

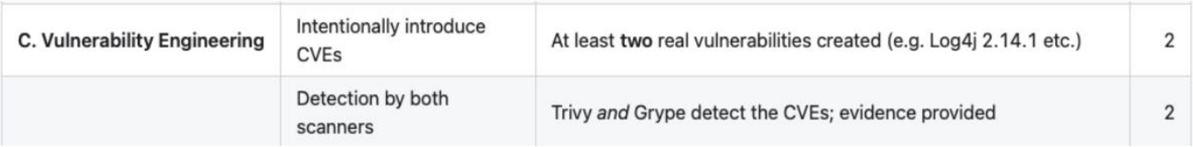
Artifacts
Produced during runtime

Name	Size	Digest
grype-report	154 KB	sha256:43c13f957c7497504b52cab0fe3461d543ac8cda71e44f1e…
trivy-report	245 KB	sha256:1a63039d1062bbd75d6e53df8d674dcc0d9b1e3e7166aad6…



Build and Scan Docker Image
succeeded 25 minutes ago in 2m 12s

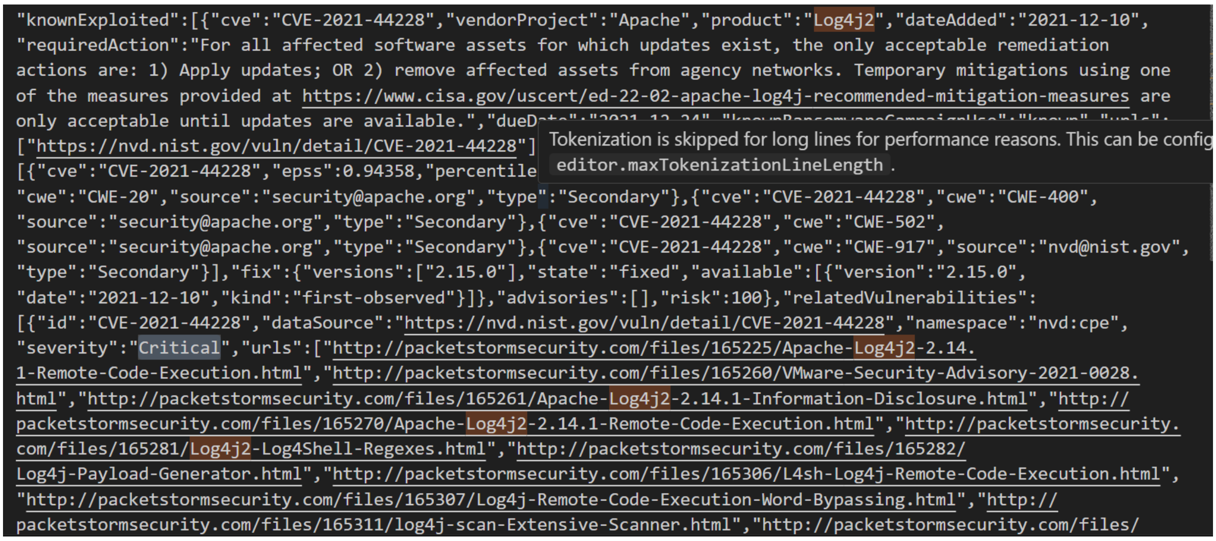
Set up job	2s
Checkout code	2s
Build local Docker image	41s
Install Grype	2s
Run Grype scan	33s
Upload Grype report	1s
Install Trivy	24s
Run Trivy scan	22s
Upload Trivy report	1s
Post Checkout code	0s
Complete job	0s



C. Vulnerability Engineering	Intentionally introduce CVEs	At least **two** real vulnerabilities created (e.g. Log4j 2.14.1 etc.)	2
	Detection by both scanners	Trivy *and* Grype detect the CVEs; evidence provided	2

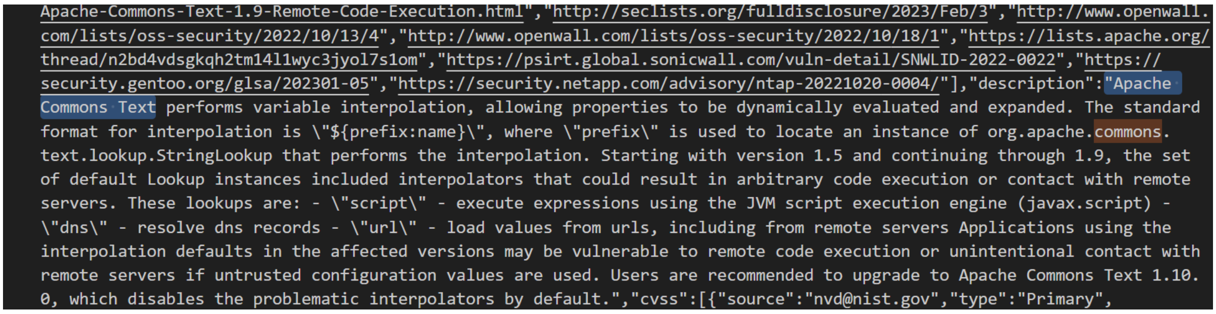
Grype:

Log4j2 eingebaut und gefunden



```
"knownExploited":[{"cve":"CVE-2021-44228","vendorProject":"Apache","product":"Log4j2","dateAdded":"2021-12-10",
"requiredAction":"For all affected software assets for which updates exist, the only acceptable remediation
actions are: 1) Apply updates; OR 2) remove affected assets from agency networks. Temporary mitigations using one
of the measures provided at https://www.cisa.gov/uscert/ed-22-02-apache-log4j-recommended-mitigation-measures are
only acceptable until updates are available.","dueD
["https://nvd.nist.gov/vuln/detail/CVE-2021-44228"]  Tokenization is skipped for long lines for performance reasons. This can be config
[{"cve":"CVE-2021-44228","epss":0.94358,"percentile  editor.maxTokenizationLineLength .
"cwe":"CWE-20","source":"security@apache.org","type":"Secondary"},{"cve":"CVE-2021-44228","cwe":"CWE-400",
"source":"security@apache.org","type":"Secondary"},{"cve":"CVE-2021-44228","cwe":"CWE-502",
"source":"security@apache.org","type":"Secondary"},{"cve":"CVE-2021-44228","cwe":"CWE-917","source":"nvd@nist.gov",
"type":"Secondary"}],"fix":{"versions":["2.15.0"],"state":"fixed","available":[{"version":"2.15.0",
"date":"2021-12-10","kind":"first-observed"}]},"advisories":[],"risk":100},"relatedVulnerabilities":
[{"id":"CVE-2021-44228","dataSource":"https://nvd.nist.gov/vuln/detail/CVE-2021-44228","namespace":"nvd:cpe",
"severity":"Critical","urls":["http://packetstormsecurity.com/files/165225/Apache-Log4j2-2.14.
1-Remote-Code-Execution.html","http://packetstormsecurity.com/files/165260/VMware-Security-Advisory-2021-0028.
html","http://packetstormsecurity.com/files/165261/Apache-Log4j2-2.14.1-Information-Disclosure.html","http://
packetstormsecurity.com/files/165270/Apache-Log4j2-2.14.1-Remote-Code-Execution.html","http://packetstormsecurity.
com/files/165281/Log4j2-Log4Shell-Regexes.html","http://packetstormsecurity.com/files/165282/
Log4j-Payload-Generator.html","http://packetstormsecurity.com/files/165306/L4sh-Log4j-Remote-Code-Execution.html",
"http://packetstormsecurity.com/files/165307/Log4j-Remote-Code-Execution-Word-Bypassing.html","http://
packetstormsecurity.com/files/165311/log4j-scan-Extensive-Scanner.html","http://packetstormsecurity.com/files/
```

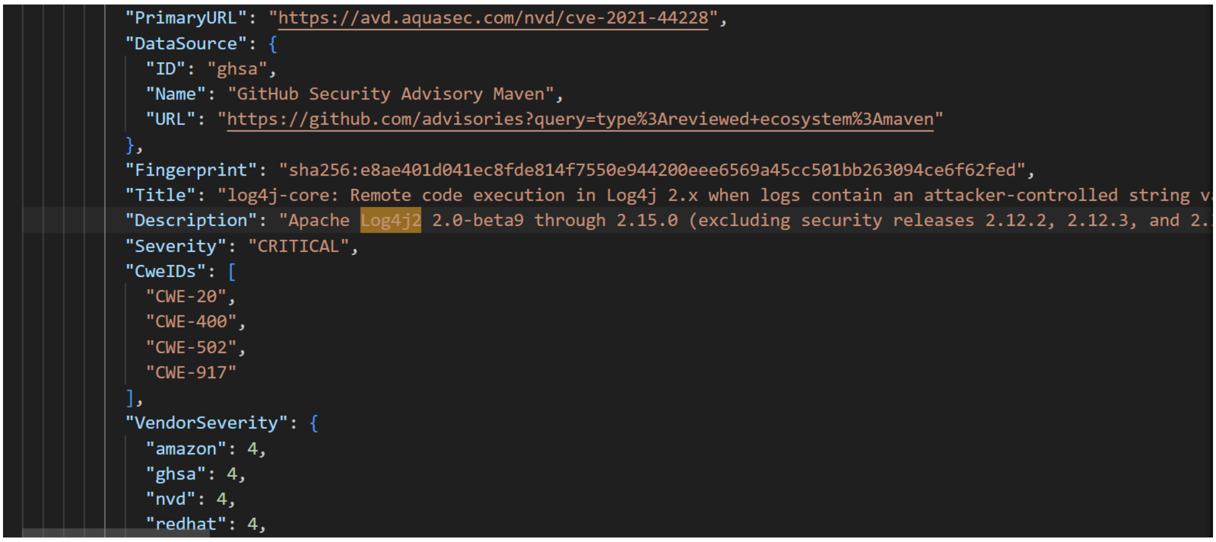
Apache commos-text: 1.9 eingebaut und gefunden



```
Apache-Commons-Text-1.9-Remote-Code-Execution.html","http://seclists.org/fulldisclosure/2023/Feb/3","http://www.openwall.
com/lists/oss-security/2022/10/13/4","http://www.openwall.com/lists/oss-security/2022/10/18/1","https://lists.apache.org/
thread/n2bd4vdsgkqh2tm14l1wyc3jyol7s1om","https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0022","https://
security.gentoo.org/glsa/202301-05","https://security.netapp.com/advisory/ntap-20221020-0004/"],"description":"Apache
Commons Text performs variable interpolation, allowing properties to be dynamically evaluated and expanded. The standard
format for interpolation is \"${prefix:name}\", where \"prefix\" is used to locate an instance of org.apache.commons.
text.lookup.StringLookup that performs the interpolation. Starting with version 1.5 and continuing through 1.9, the set
of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote
servers. These lookups are: - \"script\" - execute expressions using the JVM script execution engine (javax.script) -
\"dns\" - resolve dns records - \"url\" - load values from urls, including from remote servers Applications using the
interpolation defaults in the affected versions may be vulnerable to remote code execution or unintentional contact with
remote servers if untrusted configuration values are used. Users are recommended to upgrade to Apache Commons Text 1.10.
0, which disables the problematic interpolators by default.","cvss":[{"source":"nvd@nist.gov","type":"Primary",
```

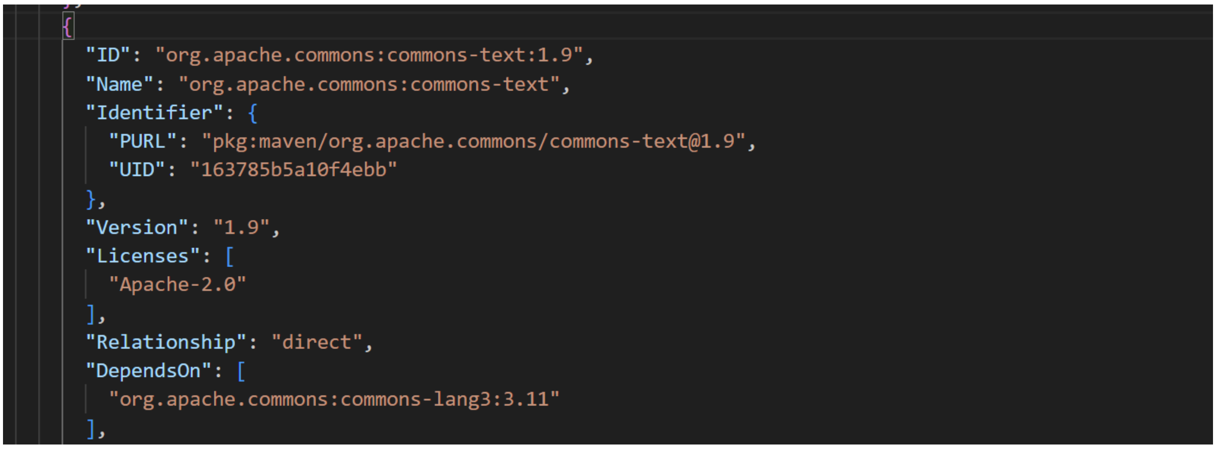
Trivity:

Log4j wurde erkannt von Trivity

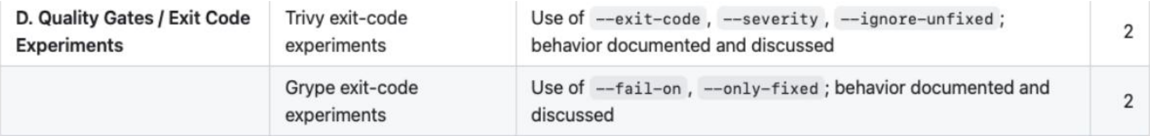


```
"PrimaryURL": "https://avd.aquasec.com/nvd/cve-2021-44228",
"DataSource": {
  "ID": "ghsa",
  "Name": "GitHub Security Advisory Maven",
  "URL": "https://github.com/advisories?query=type%3Areviewed+ecosystem%3Amaven"
},
"Fingerprint": "sha256:e8ae401d041ec8fde814f7550e944200eee6569a45cc501bb263094ce6f62fed",
"Title": "log4j-core: Remote code execution in Log4j 2.x when logs contain an attacker-controlled string v
"Description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.
"Severity": "CRITICAL",
"CweIDs": [
  "CWE-20",
  "CWE-400",
  "CWE-502",
  "CWE-917"
],
"VendorSeverity": {
  "amazon": 4,
  "ghsa": 4,
  "nvd": 4,
  "redhat": 4,
```

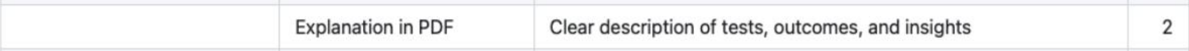
Apache commos-text: 1.9 eingebaut und gefunden



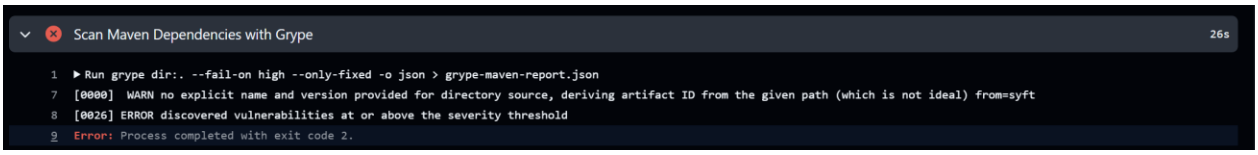
```
{
  "ID": "org.apache.commons:commons-text:1.9",
  "Name": "org.apache.commons:commons-text",
  "Identifier": {
    "PURL": "pkg:maven/org.apache.commons/commons-text@1.9",
    "UID": "163785b5a10f4ebb"
  },
  "Version": "1.9",
  "Licenses": [
    "Apache-2.0"
  ],
  "Relationship": "direct",
  "DependsOn": [
    "org.apache.commons:commons-lang3:3.11"
  ],
```



D. Quality Gates / Exit Code Experiments	Trivy exit-code experiments	Use of `--exit-code`, `--severity`, `--ignore-unfixed`; behavior documented and discussed	2
	Grype exit-code experiments	Use of `--fail-on`, `--only-fixed`; behavior documented and discussed	2



	Explanation in PDF	Clear description of tests, outcomes, and insights	2



Scan Maven Dependencies with Grype 26s

```
▶ Run grype dir:. --fail-on high --only-fixed -o json > grype-maven-report.json
[0000]  WARN no explicit name and version provided for directory source, deriving artifact ID from the given path (which is not ideal) from=syft
[0026] ERROR discovered vulnerabilities at or above the severity threshold
Error: Process completed with exit code 2.
```