# Lab Exercise 22

# Checking Vulnerabilities Using Trivy

**Objective:** To scan container images for vulnerabilities using Trivy to identify and mitigate security risks and ensure that containerized applications are secure

**Tools required:** Trivy

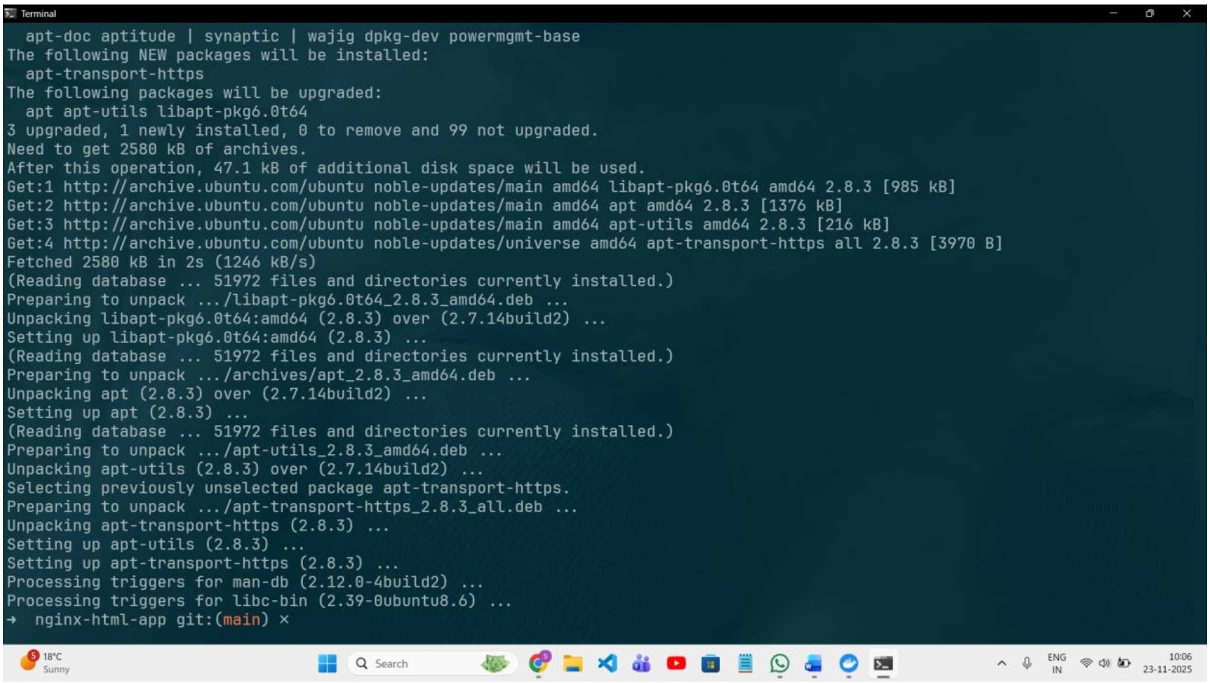
**Prerequisites:** None

Steps to be followed:

1. Install Trivy
2. Scan the vulnerabilities using Trivy

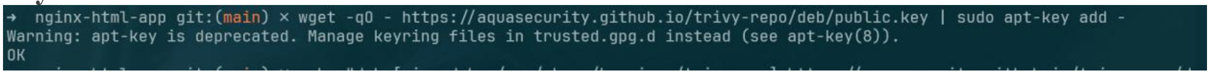
## Step 1: Install Trivy

1.1 Run the following command to install tools for secure downloads, HTTPS repositories, encryption key management, and system version identification:
**sudo apt-get install wget apt-transport-https gnupg lsb-release**



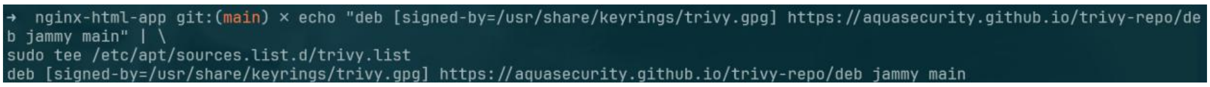
```
  apt-doc aptitude | synaptic | wajig dpkg-dev powermgmt-base
The following NEW packages will be installed:
  apt-transport-https
The following packages will be upgraded:
  apt apt-utils libapt-pkg6.0t64
3 upgraded, 1 newly installed, 0 to remove and 99 not upgraded.
Need to get 2580 kB of archives.
After this operation, 47.1 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libapt-pkg6.0t64 amd64 2.8.3 [985 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apt amd64 2.8.3 [1376 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apt-utils amd64 2.8.3 [216 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/universe amd64 apt-transport-https all 2.8.3 [3970 B]
Fetched 2580 kB in 2s (1246 kB/s)
(Reading database ... 51972 files and directories currently installed.)
Preparing to unpack .../libapt-pkg6.0t64_2.8.3_amd64.deb ...
Unpacking libapt-pkg6.0t64:amd64 (2.8.3) over (2.7.14build2) ...
Setting up libapt-pkg6.0t64:amd64 (2.8.3) ...
(Reading database ... 51972 files and directories currently installed.)
Preparing to unpack .../archives/apt_2.8.3_amd64.deb ...
Unpacking apt (2.8.3) over (2.7.14build2) ...
Setting up apt (2.8.3) ...
(Reading database ... 51972 files and directories currently installed.)
Preparing to unpack .../apt-utils_2.8.3_amd64.deb ...
Unpacking apt-utils (2.8.3) over (2.7.14build2) ...
Selecting previously unselected package apt-transport-https.
Preparing to unpack .../apt-transport-https_2.8.3_all.deb ...
Unpacking apt-transport-https (2.8.3) ...
Setting up apt-utils (2.8.3) ...
Setting up apt-transport-https (2.8.3) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
➜  nginx-html-app git:(main) ✗
```

1.2 Run the following command to download the Trivy repository's public key and add it to the system's trusted keys, ensuring secure package verification:
**wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -**



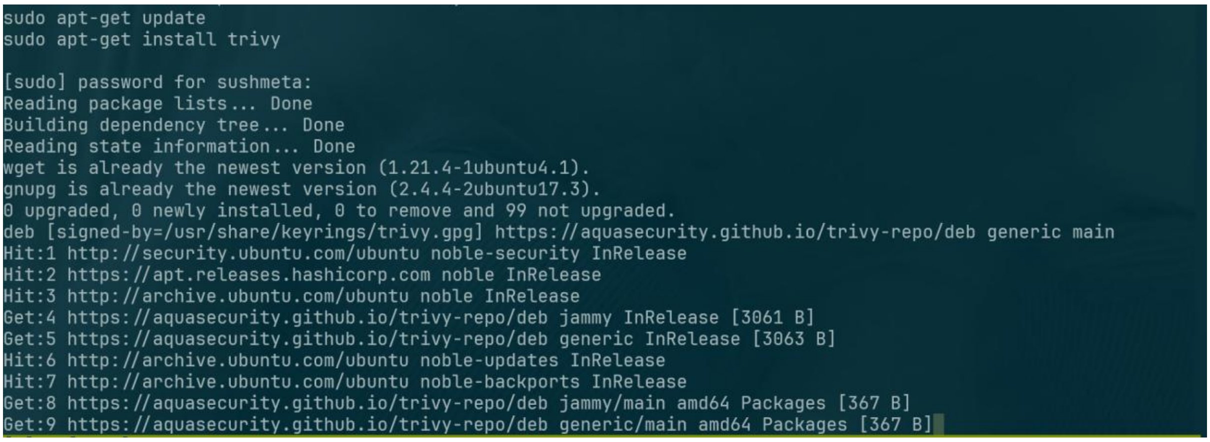
```
→  nginx-html-app git:(main) × wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
```

1.3 Run the following command to add the Trivy repository to the system's sources list, enabling the installation of Trivy packages tailored to the Ubuntu version:
**echo deb https://aquasecurity.github.io/trivy-repo/deb $(lsb_release -sc) main | sudo tee -a /etc/apt/sources.list.d/trivy.list**



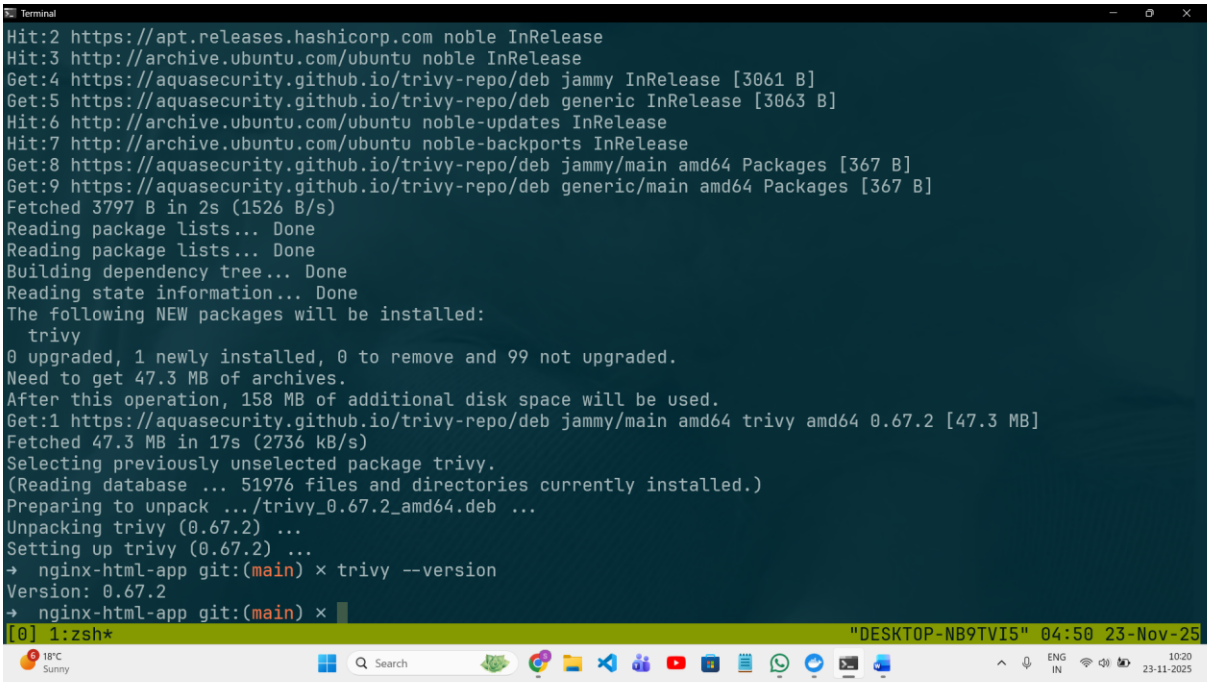
```
→  nginx-html-app git:(main) × echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/de
b jammy main" | \
sudo tee /etc/apt/sources.list.d/trivy.list
deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb jammy main
```

1.4 Run the following command to update the system's package lists, ensuring the latest information on available software and updates from all configured repositories:
**sudo apt-get update**



```
sudo apt-get update
sudo apt-get install trivy

[sudo] password for sushmeta:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wget is already the newest version (1.21.4-1ubuntu4.1).
gnupg is already the newest version (2.4.4-2ubuntu17.3).
0 upgraded, 0 newly installed, 0 to remove and 99 not upgraded.
deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb generic main
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 https://apt.releases.hashicorp.com noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble InRelease
Get:4 https://aquasecurity.github.io/trivy-repo/deb jammy InRelease [3061 B]
Get:5 https://aquasecurity.github.io/trivy-repo/deb generic InRelease [3063 B]
Hit:6 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:7 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Get:8 https://aquasecurity.github.io/trivy-repo/deb jammy/main amd64 Packages [367 B]
Get:9 https://aquasecurity.github.io/trivy-repo/deb generic/main amd64 Packages [367 B]
```

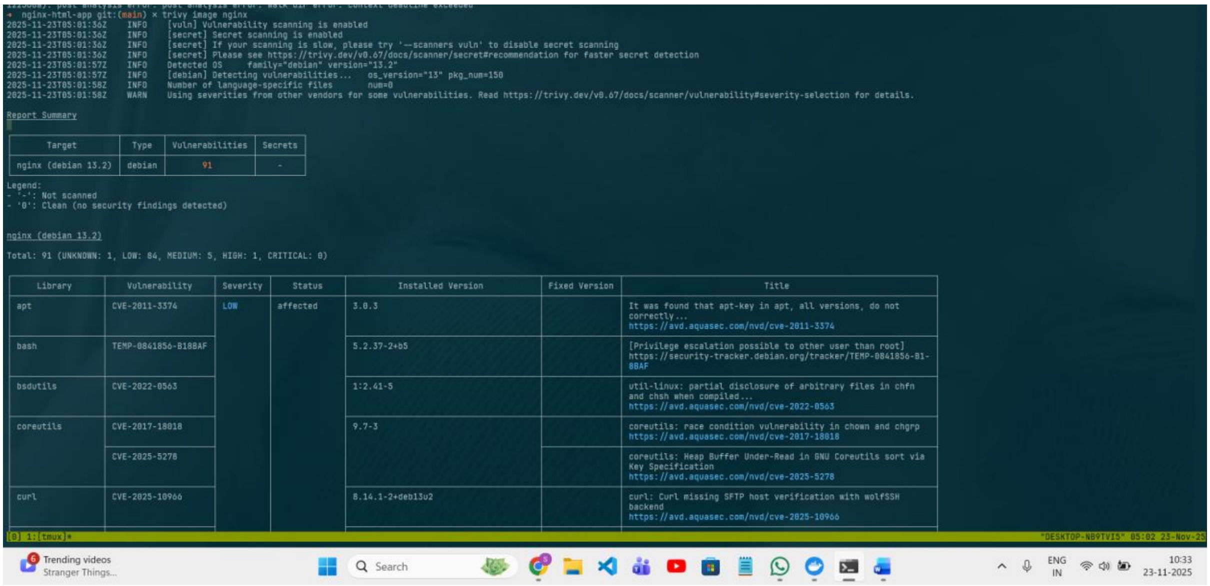
1.5 Run the following command to install Trivy, a security scanner for containers, directly from the configured repository:
**sudo apt-get install trivy**



```
Hit:2 https://apt.releases.hashicorp.com noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble InRelease
Get:4 https://aquasecurity.github.io/trivy-repo/deb jammy InRelease [3061 B]
Get:5 https://aquasecurity.github.io/trivy-repo/deb generic InRelease [3063 B]
Hit:6 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:7 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Get:8 https://aquasecurity.github.io/trivy-repo/deb jammy/main amd64 Packages [367 B]
Get:9 https://aquasecurity.github.io/trivy-repo/deb generic/main amd64 Packages [367 B]
Fetched 3797 B in 2s (1526 B/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  trivy
0 upgraded, 1 newly installed, 0 to remove and 99 not upgraded.
Need to get 47.3 MB of archives.
After this operation, 158 MB of additional disk space will be used.
Get:1 https://aquasecurity.github.io/trivy-repo/deb jammy/main amd64 trivy amd64 0.67.2 [47.3 MB]
Fetched 47.3 MB in 17s (2736 kB/s)
Selecting previously unselected package trivy.
(Reading database ... 51976 files and directories currently installed.)
Preparing to unpack .../trivy_0.67.2_amd64.deb ...
Unpacking trivy (0.67.2) ...
Setting up trivy (0.67.2) ...
→  nginx-html-app git:(main) × trivy --version
Version: 0.67.2
→  nginx-html-app git:(main) ×
[0] 1:zsh*                                               "DESKTOP-NB9TVIS" 04:50 23-Nov-25
```

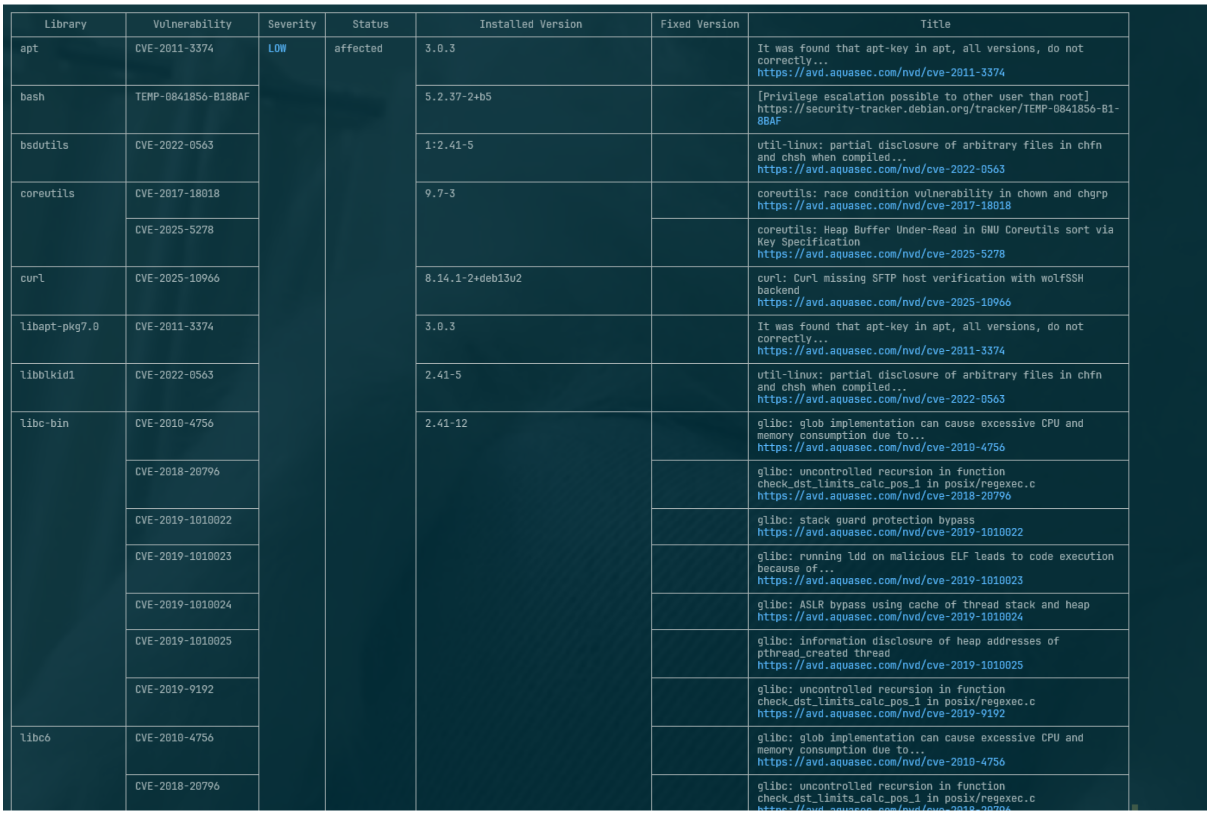
## Step 2: Scan the vulnerabilities using Trivy

2.1 Run the following command to scan the NGINX container image with Trivy for vulnerabilities and security issues:
**trivy image nginx**

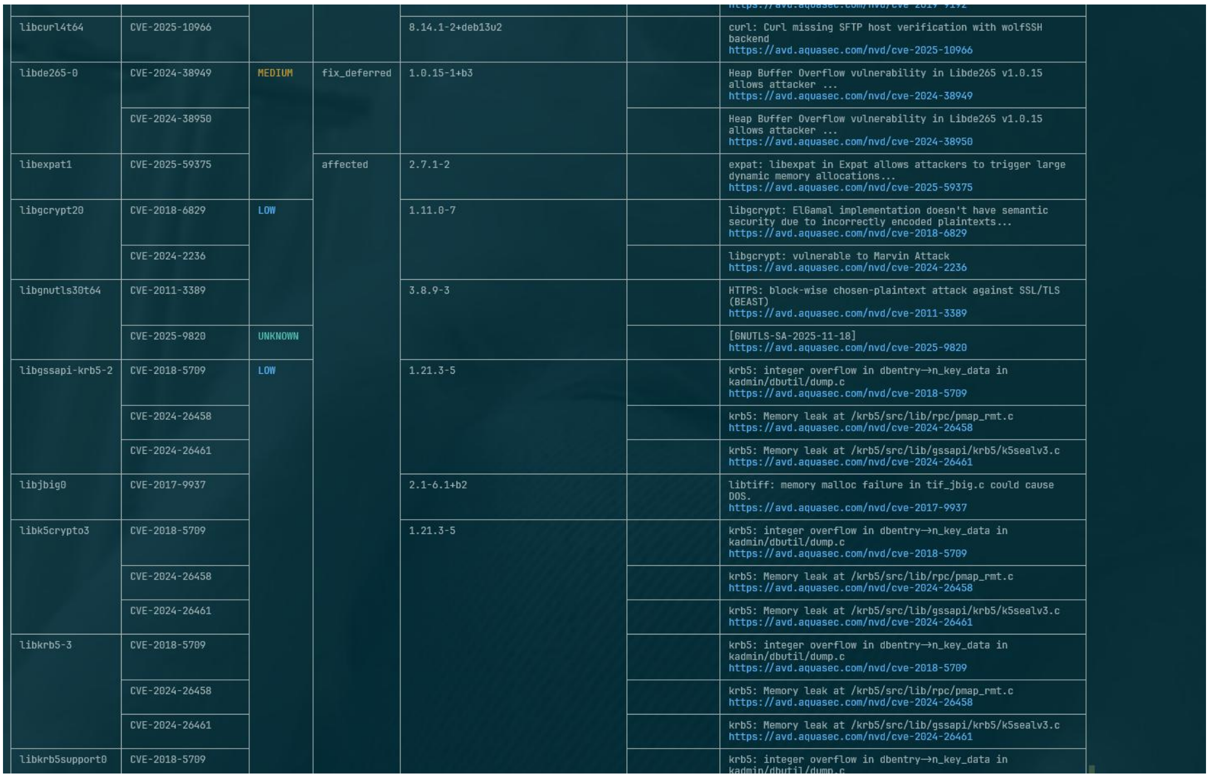


```
→  nginx-html-app git:(main) × trivy image nginx
2025-11-23T05:01:36Z    INFO    [vuln] Vulnerability scanning is enabled
2025-11-23T05:01:36Z    INFO    [secret] Secret scanning is enabled
2025-11-23T05:01:36Z    INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-23T05:01:36Z    INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-23T05:01:57Z    INFO    Detected OS     family="debian" version="13.2"
2025-11-23T05:01:57Z    INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-23T05:01:58Z    INFO    Number of language-specific files       num=0
2025-11-23T05:01:58Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.

Report Summary

┌─────────────────────┬────────┬─────────────────┬─────────┐
│       Target        │  Type  │ Vulnerabilities │ Secrets │
├─────────────────────┼────────┼─────────────────┼─────────┤
│ nginx (debian 13.2) │ debian │       91        │    -    │
└─────────────────────┴────────┴─────────────────┴─────────┘
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


nginx (debian 13.2)

Total: 91 (UNKNOWN: 1, LOW: 84, MEDIUM: 5, HIGH: 1, CRITICAL: 0)

┌───────────┬─────────────────────┬──────────┬──────────┬──────────────────────────┬───────────────┬───────────────────────────────────────────────────────────────┐
│  Library  │    Vulnerability    │ Severity │  Status  │    Installed Version     │ Fixed Version │                             Title                             │
├───────────┼─────────────────────┼──────────┼──────────┼──────────────────────────┼───────────────┼───────────────────────────────────────────────────────────────┤
│ apt       │ CVE-2011-3374       │ LOW      │ affected │ 3.0.3                    │               │ It was found that apt-key in apt, all versions, do not        │
│           │                     │          │          │                          │               │ correctly...                                                  │
│           │                     │          │          │                          │               │ https://avd.aquasec.com/nvd/cve-2011-3374                     │
├───────────┼─────────────────────┤          │          ├──────────────────────────┼───────────────┼───────────────────────────────────────────────────────────────┤
│ bash      │ TEMP-0841856-B18BAF │          │          │ 5.2.37-2+b5              │               │ [Privilege escalation possible to other user than root]       │
│           │                     │          │          │                          │               │ https://security-tracker.debian.org/tracker/TEMP-0841856-B1-  │
│           │                     │          │          │                          │               │ 8BAF                                                          │
├───────────┼─────────────────────┤          │          ├──────────────────────────┼───────────────┼───────────────────────────────────────────────────────────────┤
│ bsdutils  │ CVE-2022-0563       │          │          │ 1:2.41-5                 │               │ util-linux: partial disclosure of arbitrary files in chfn     │
│           │                     │          │          │                          │               │ and chsh when compiled...                                     │
│           │                     │          │          │                          │               │ https://avd.aquasec.com/nvd/cve-2022-0563                     │
├───────────┼─────────────────────┤          │          ├──────────────────────────┼───────────────┼───────────────────────────────────────────────────────────────┤
│ coreutils │ CVE-2017-18018      │          │          │ 9.7-3                    │               │ coreutils: race condition vulnerability in chown and chgrp    │
│           │                     │          │          │                          │               │ https://avd.aquasec.com/nvd/cve-2017-18018                    │
│           ├─────────────────────┤          │          │                          ├───────────────┼───────────────────────────────────────────────────────────────┤
│           │ CVE-2025-5278       │          │          │                          │               │ coreutils: Heap Buffer Under-Read in GNU Coreutils sort via   │
│           │                     │          │          │                          │               │ Key Specification                                             │
│           │                     │          │          │                          │               │ https://avd.aquasec.com/nvd/cve-2025-5278                     │
├───────────┼─────────────────────┤          │          ├──────────────────────────┼───────────────┼───────────────────────────────────────────────────────────────┤
│ curl      │ CVE-2025-10966      │          │          │ 8.14.1-2+deb13u2         │               │ curl: Curl missing SFTP host verification with wolfSSH        │
│           │                     │          │          │                          │               │ backend                                                       │
│           │                     │          │          │                          │               │ https://avd.aquasec.com/nvd/cve-2025-10966                    │
[0] 1:[tmux]*                                                                                                              "DESKTOP-NB9TVIS" 05:02 23-Nov-25
```

It shows the results of a Trivy security scan, listing vulnerabilities in installed packages, their severity, and whether they are affected. It also includes details like the installed version and links for more information.



| Library | Vulnerability | Severity | Status | Installed Version | Fixed Version | Title |
|---|---|---|---|---|---|---|
| apt | CVE-2011-3374 | LOW | affected | 3.0.3 | | It was found that apt-key in apt, all versions, do not correctly...<br>https://avd.aquasec.com/nvd/cve-2011-3374 |
| bash | TEMP-0841856-B18BAF | | | 5.2.37-2+b5 | | [Privilege escalation possible to other user than root]<br>https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF |
| bsdutils | CVE-2022-0563 | | | 1:2.41-5 | | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled...<br>https://avd.aquasec.com/nvd/cve-2022-0563 |
| coreutils | CVE-2017-18018 | | | 9.7-3 | | coreutils: race condition vulnerability in chown and chgrp<br>https://avd.aquasec.com/nvd/cve-2017-18018 |
| | CVE-2025-5278 | | | | | coreutils: Heap Buffer Under-Read in GNU Coreutils sort via Key Specification<br>https://avd.aquasec.com/nvd/cve-2025-5278 |
| curl | CVE-2025-10966 | | | 8.14.1-2+deb13u2 | | curl: Curl missing SFTP host verification with wolfSSH backend<br>https://avd.aquasec.com/nvd/cve-2025-10966 |
| libapt-pkg7.0 | CVE-2011-3374 | | | 3.0.3 | | It was found that apt-key in apt, all versions, do not correctly...<br>https://avd.aquasec.com/nvd/cve-2011-3374 |
| libblkid1 | CVE-2022-0563 | | | 2.41-5 | | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled...<br>https://avd.aquasec.com/nvd/cve-2022-0563 |
| libc-bin | CVE-2010-4756 | | | 2.41-12 | | glibc: glob implementation can cause excessive CPU and memory consumption due to...<br>https://avd.aquasec.com/nvd/cve-2010-4756 |
| | CVE-2018-20796 | | | | | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c<br>https://avd.aquasec.com/nvd/cve-2018-20796 |
| | CVE-2019-1010022 | | | | | glibc: stack guard protection bypass<br>https://avd.aquasec.com/nvd/cve-2019-1010022 |
| | CVE-2019-1010023 | | | | | glibc: running ldd on malicious ELF leads to code execution because of...<br>https://avd.aquasec.com/nvd/cve-2019-1010023 |
| | CVE-2019-1010024 | | | | | glibc: ASLR bypass using cache of thread stack and heap<br>https://avd.aquasec.com/nvd/cve-2019-1010024 |
| | CVE-2019-1010025 | | | | | glibc: information disclosure of heap addresses of pthread_created thread<br>https://avd.aquasec.com/nvd/cve-2019-1010025 |
| | CVE-2019-9192 | | | | | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c<br>https://avd.aquasec.com/nvd/cve-2019-9192 |
| libc6 | CVE-2010-4756 | | | | | glibc: glob implementation can cause excessive CPU and memory consumption due to...<br>https://avd.aquasec.com/nvd/cve-2010-4756 |
| | CVE-2018-20796 | | | | | glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c<br>https://avd.aquasec.com/nvd/cve-2018-20796 |



| Library | Vulnerability | Severity | Status | Installed Version | Fixed Version | Title |
|---|---|---|---|---|---|---|
| | | | | | | https://avd.aquasec.com/nvd/cve-2019-9192 |
| libcurl4t64 | CVE-2025-10966 | | | 8.14.1-2+deb13u2 | | curl: Curl missing SFTP host verification with wolfSSH backend<br>https://avd.aquasec.com/nvd/cve-2025-10966 |
| libde265-0 | CVE-2024-38949 | MEDIUM | fix_deferred | 1.0.15-1+b3 | | Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ...<br>https://avd.aquasec.com/nvd/cve-2024-38949 |
| | CVE-2024-38950 | | | | | Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ...<br>https://avd.aquasec.com/nvd/cve-2024-38950 |
| libexpat1 | CVE-2025-59375 | | affected | 2.7.1-2 | | expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations...<br>https://avd.aquasec.com/nvd/cve-2025-59375 |
| libgcrypt20 | CVE-2018-6829 | LOW | | 1.11.0-7 | | libgcrypt: ElGamal implementation doesn't have semantic security due to incorrectly encoded plaintexts...<br>https://avd.aquasec.com/nvd/cve-2018-6829 |
| | CVE-2024-2236 | | | | | libgcrypt: vulnerable to Marvin Attack<br>https://avd.aquasec.com/nvd/cve-2024-2236 |
| libgnutls30t64 | CVE-2011-3389 | | | 3.8.9-3 | | HTTPS: block-wise chosen-plaintext attack against SSL/TLS (BEAST)<br>https://avd.aquasec.com/nvd/cve-2011-3389 |
| | CVE-2025-9820 | UNKNOWN | | | | [GNUTLS-SA-2025-11-18]<br>https://avd.aquasec.com/nvd/cve-2025-9820 |
| libgssapi-krb5-2 | CVE-2018-5709 | LOW | | 1.21.3-5 | | krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c<br>https://avd.aquasec.com/nvd/cve-2018-5709 |
| | CVE-2024-26458 | | | | | krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c<br>https://avd.aquasec.com/nvd/cve-2024-26458 |
| | CVE-2024-26461 | | | | | krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c<br>https://avd.aquasec.com/nvd/cve-2024-26461 |
| libjbig0 | CVE-2017-9937 | | | 2.1-6.1+b2 | | libtiff: memory malloc failure in tif_jbig.c could cause DOS.<br>https://avd.aquasec.com/nvd/cve-2017-9937 |
| libk5crypto3 | CVE-2018-5709 | | | 1.21.3-5 | | krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c<br>https://avd.aquasec.com/nvd/cve-2018-5709 |
| | CVE-2024-26458 | | | | | krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c<br>https://avd.aquasec.com/nvd/cve-2024-26458 |
| | CVE-2024-26461 | | | | | krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c<br>https://avd.aquasec.com/nvd/cve-2024-26461 |
| libkrb5-3 | CVE-2018-5709 | | | | | krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c<br>https://avd.aquasec.com/nvd/cve-2018-5709 |
| | CVE-2024-26458 | | | | | krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c<br>https://avd.aquasec.com/nvd/cve-2024-26458 |
| | CVE-2024-26461 | | | | | krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c<br>https://avd.aquasec.com/nvd/cve-2024-26461 |
| libkrb5support0 | CVE-2018-5709 | | | | | krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c |

By following these steps, you have successfully scanned container images for vulnerabilities using Trivy to identify and mitigate security risks and ensure the security of containerized applications.