Lab Exercise 22- Docker Image Vulnerability Scanning Using Trivy (Windows)

Objective

By the end of this lab, you will be able to:

- Install and configure **Trivy** on Windows
- Scan **Docker images** for vulnerabilities
- Interpret scan reports and take remediation actions

Prerequisites

- Windows 10/11 (with **Docker Desktop** installed and running)
- Internet access (Trivy downloads vulnerability databases)
- Basic familiarity with Docker CLI commands

Step 1: Verify Docker Setup

Before using Trivy, make sure Docker is working correctly.

```
docker --version

docker run hello-world
```

Expected Output:

Docker runs successfully and displays the “Hello from Docker!” message.

Output:

```
C:\Users\namit\nginx-html-app>docker --version
Docker version 28.3.2, build 578ccf6

C:\Users\namit\nginx-html-app>docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
17eec7bbc9d7: Pull complete
Digest: sha256:f7931603f70e13dbd844253370742c4fc4202d290c80442b2e68706d8f33ce26
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
 $ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
 https://hub.docker.com/

For more examples and ideas, visit:
 https://docs.docker.com/get-started/


C:\Users\namit\nginx-html-app>
```

Step 2: Install Trivy on Windows

Manual Installation

1. Go to the official GitHub releases page:

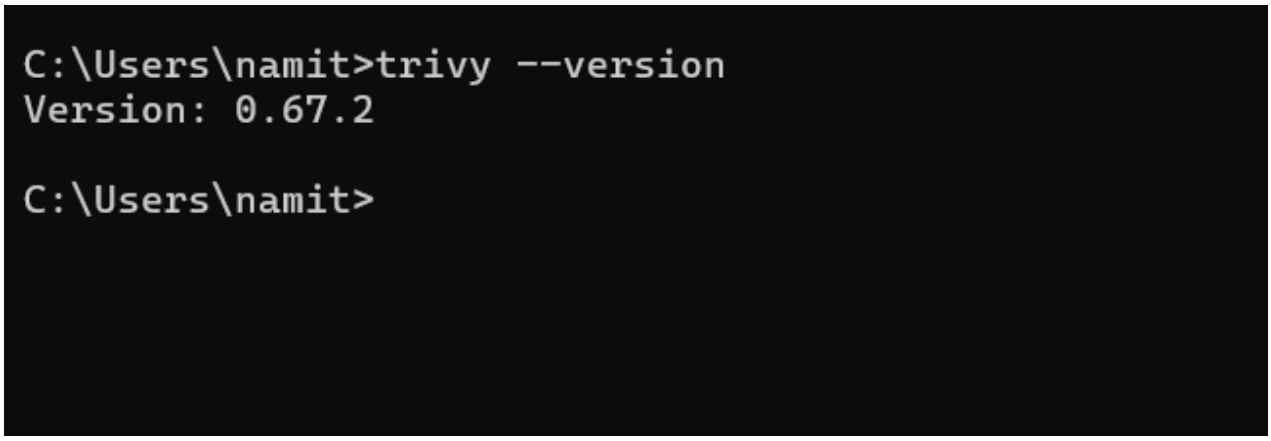
   https://github.com/aquasecurity/trivy/releases
2. Download the Windows ZIP file (trivy_x.x.x_windows_amd64.zip)
3. Extract it (e.g., to C:\trivy)
4. Add that folder to your **System PATH** environment variable

Verify Installation

Open **PowerShell** and run:

```
trivy --version
```

Output:



Step 3: Pull a Docker Image

Let's pull an image that we'll scan:

```
docker pull nginx:latest
```

Check it's downloaded:

```
docker images
```

```
C:\Users\namit>docker images
REPOSITORY       TAG       IMAGE ID       CREATED          SIZE
nginx-html-app   latest    752e523d02e9   38 minutes ago   225MB
nginx            latest    1beed3ca46ac   13 days ago      225MB
hello-world      latest    f7931603f70e   3 months ago     20.3kB

C:\Users\namit>
```

Step 4: Scan Docker Image with Trivy

Now, run a vulnerability scan on the image:

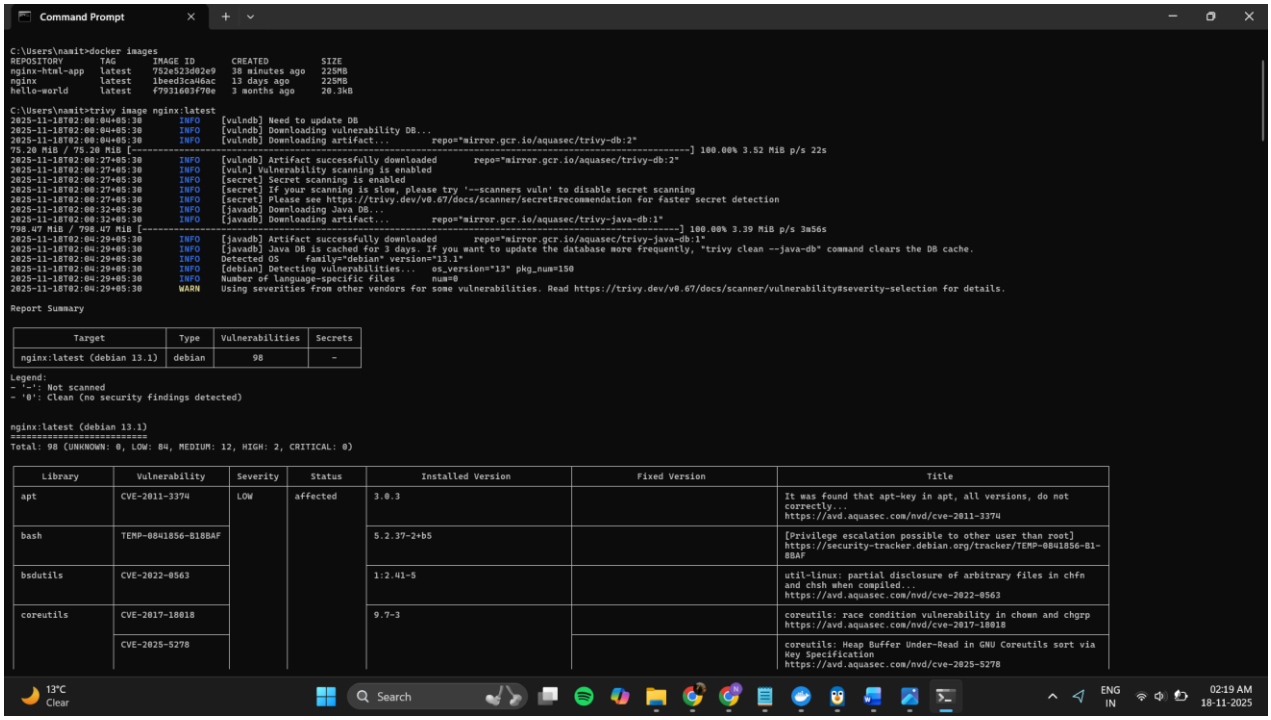
```
trivy image nginx:latest
```

Explanation:

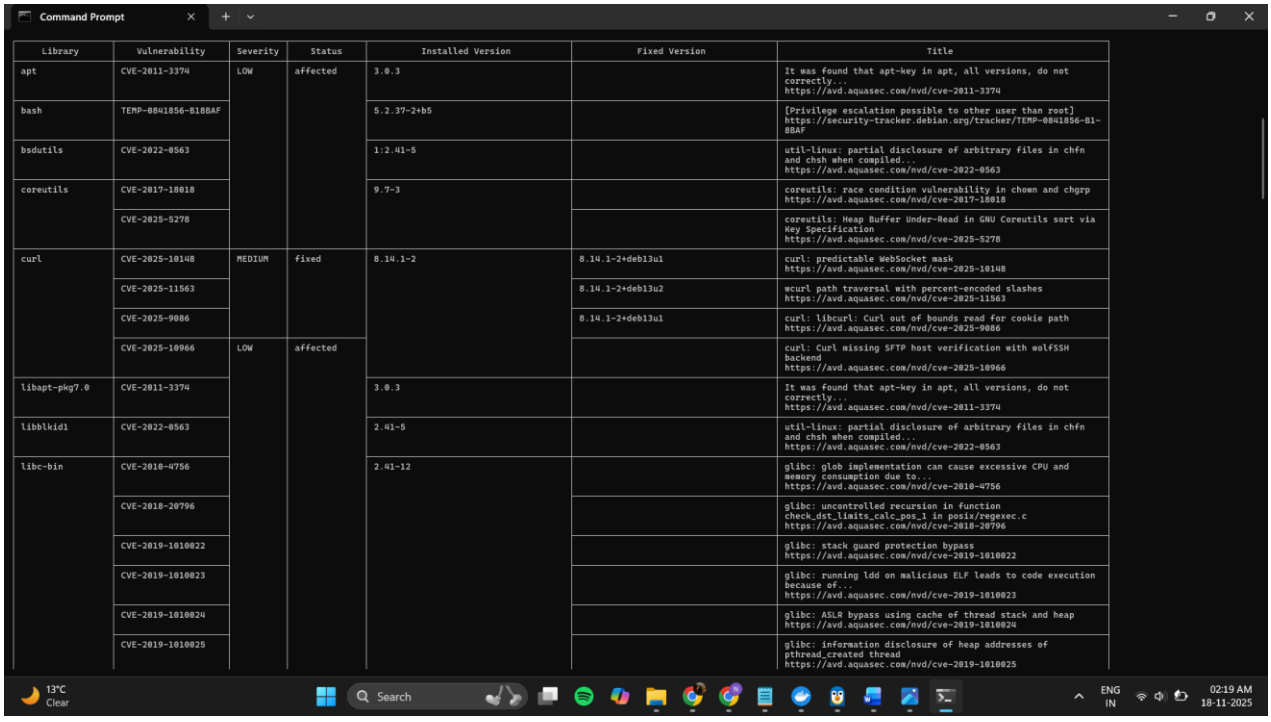
Trivy will:

- Fetch the latest vulnerability database
- Analyze all OS packages and libraries inside the image
- Display severity levels (LOW, MEDIUM, HIGH, CRITICAL)

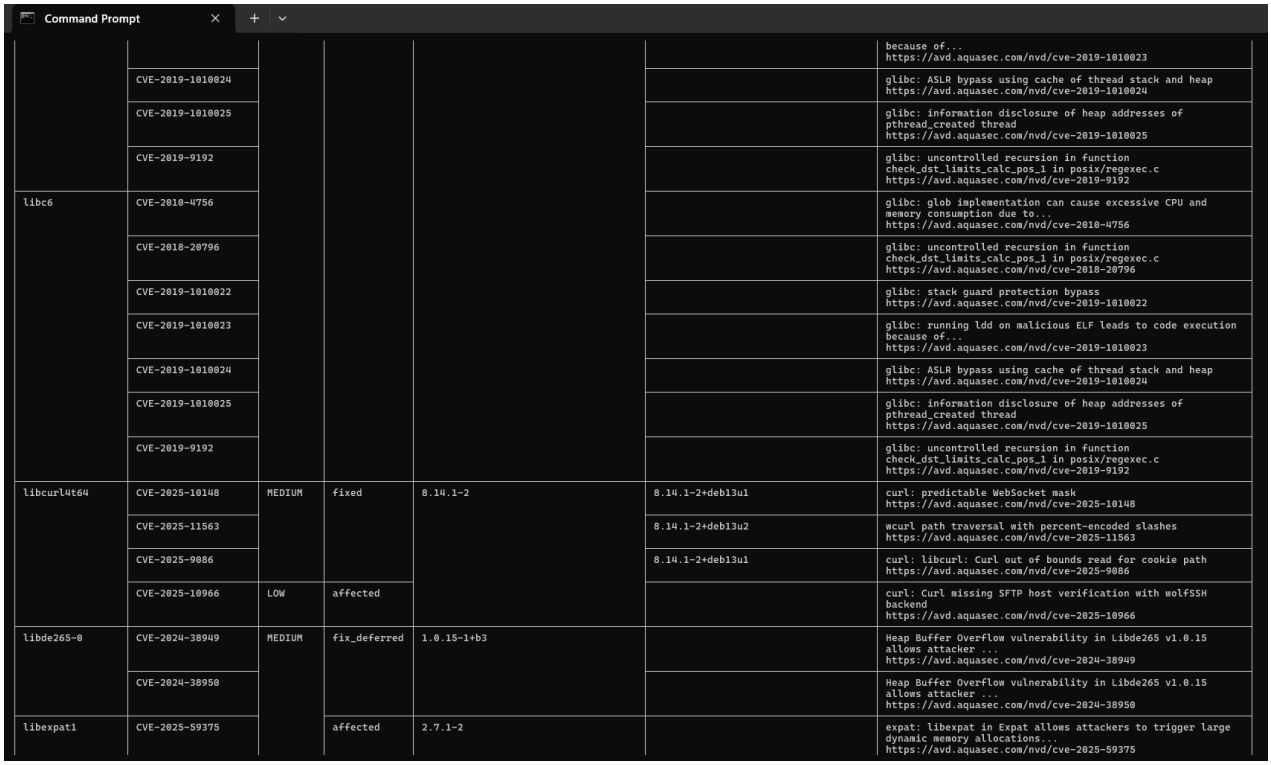
Output:



```
Command Prompt

C:\Users\namit>docker images
REPOSITORY      TAG       IMAGE ID       CREATED          SIZE
nginx-html-app  latest    752e523d02e9   38 minutes ago   225MB
nginx           latest    1beed3ca46ac   13 days ago      225MB
hello-world     latest    f7931603f70e   3 months ago     20.3kB

C:\Users\namit>trivy image nginx:latest
2025-11-18T02:00:04+05:30       INFO    [vulndb] Need to update DB
2025-11-18T02:00:04+05:30       INFO    [vulndb] Downloading vulnerability DB...
2025-11-18T02:00:04+05:30       INFO    [vulndb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-db:2"
75.20 MiB / 75.20 MiB [-------------------------------------------------------------------------------------------------------] 100.00% 3.52 MiB p/s 22s
2025-11-18T02:00:27+05:30       INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-11-18T02:00:27+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-18T02:00:27+05:30       INFO    [secret] Secret scanning is enabled
2025-11-18T02:00:27+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-18T02:00:27+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-18T02:00:32+05:30       INFO    [javadb] Downloading Java DB...
2025-11-18T02:00:32+05:30       INFO    [javadb] Downloading artifact...        repo="mirror.gcr.io/aquasec/trivy-java-db:1"
798.47 MiB / 798.47 MiB [-----------------------------------------------------------------------------------------------------] 100.00% 3.39 MiB p/s 3m56s
2025-11-18T02:04:29+05:30       INFO    [javadb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-java-db:1"
2025-11-18T02:04:29+05:30       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.
2025-11-18T02:04:29+05:30       INFO    Detected OS     family="debian" version="13.1"
2025-11-18T02:04:29+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-18T02:04:29+05:30       INFO    Number of language-specific files       num=0
2025-11-18T02:04:29+05:30       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:latest (debian 13.1) │ debian │       98        │    -    │
└──────────────────────────┴────────┴─────────────────┴─────────┘

Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


nginx:latest (debian 13.1)
==========================
Total: 98 (UNKNOWN: 0, LOW: 84, MEDIUM: 12, HIGH: 2, 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                    │
└─────────┴────────────────┴──────────┴────────┴───────────────────┴───────────────┴─────────────────────────────────────────────────────────────┘
```

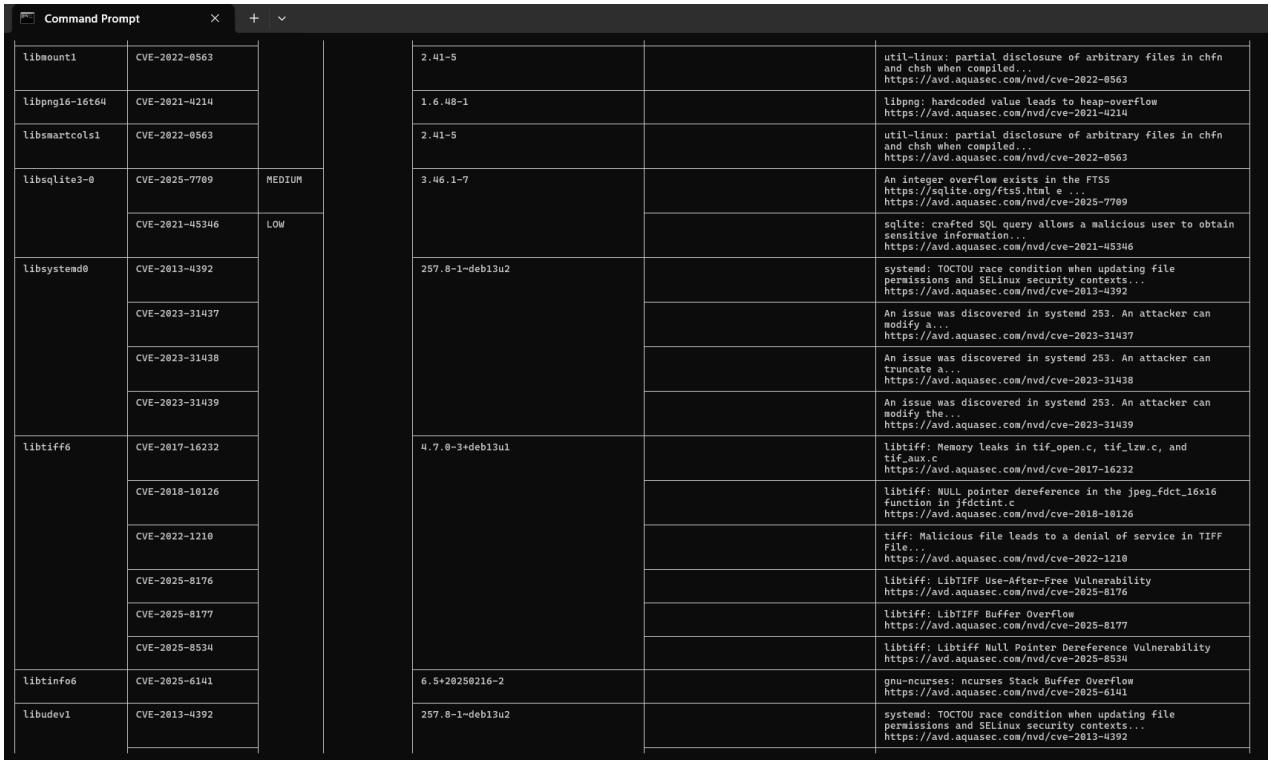


```
Command Prompt

┌─────────┬────────────────┬──────────┬────────┬───────────────────┬───────────────┬─────────────────────────────────────────────────────────────┐
│ 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-2025-10148 │ MEDIUM   │ fixed  │ 8.14.1-2          │ 8.14.1-2+deb13u1│curl: predictable WebSocket mask                           │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2025-10148                   │
│         ├────────────────┤          │        │                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2025-11563 │          │        │                   │ 8.14.1-2+deb13u2│wcurl path traversal with percent-encoded slashes           │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2025-11563                   │
│         ├────────────────┤          │        │                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2025-9086  │          │        │                   │ 8.14.1-2+deb13u1│curl: libcurl: Curl out of bounds read for cookie path     │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2025-9086                    │
│         ├────────────────┤          ├────────┤                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2025-10966 │ LOW      │affected│                   │               │curl: Curl missing SFTP host verification with wolfSSH       │
│         │                │          │        │                   │               │backend                                                      │
│         │                │          │        │                   │               │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...                                                 │
│         │                │          │        │                   │               │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...                                    │
│         │                │          │        │                   │               │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 ...                                │
│         │                │          │        │                   │               │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               │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2018-20796                   │
│         ├────────────────┤          │        │                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2019-1010022 │        │        │                   │               │glibc: stack guard protection bypass                         │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2019-1010022                 │
│         ├────────────────┤          │        │                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2019-1010023 │        │        │                   │               │glibc: running ldd on malicious ELF leads to code execution  │
│         │                │          │        │                   │               │because of...                                                │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2019-1010023                 │
│         ├────────────────┤          │        │                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2019-1010024 │        │        │                   │               │glibc: ASLR bypass using cache of thread stack and heap      │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2019-1010024                 │
│         ├────────────────┤          │        │                   ├───────────────┼─────────────────────────────────────────────────────────────┤
│         │ CVE-2019-1010025 │        │        │                   │               │glibc: information disclosure of heap addresses of           │
│         │                │          │        │                   │               │pthread_created thread                                       │
│         │                │          │        │                   │               │https://avd.aquasec.com/nvd/cve-2019-1010025                 │
└─────────┴────────────────┴──────────┴────────┴───────────────────┴───────────────┴─────────────────────────────────────────────────────────────┘
```

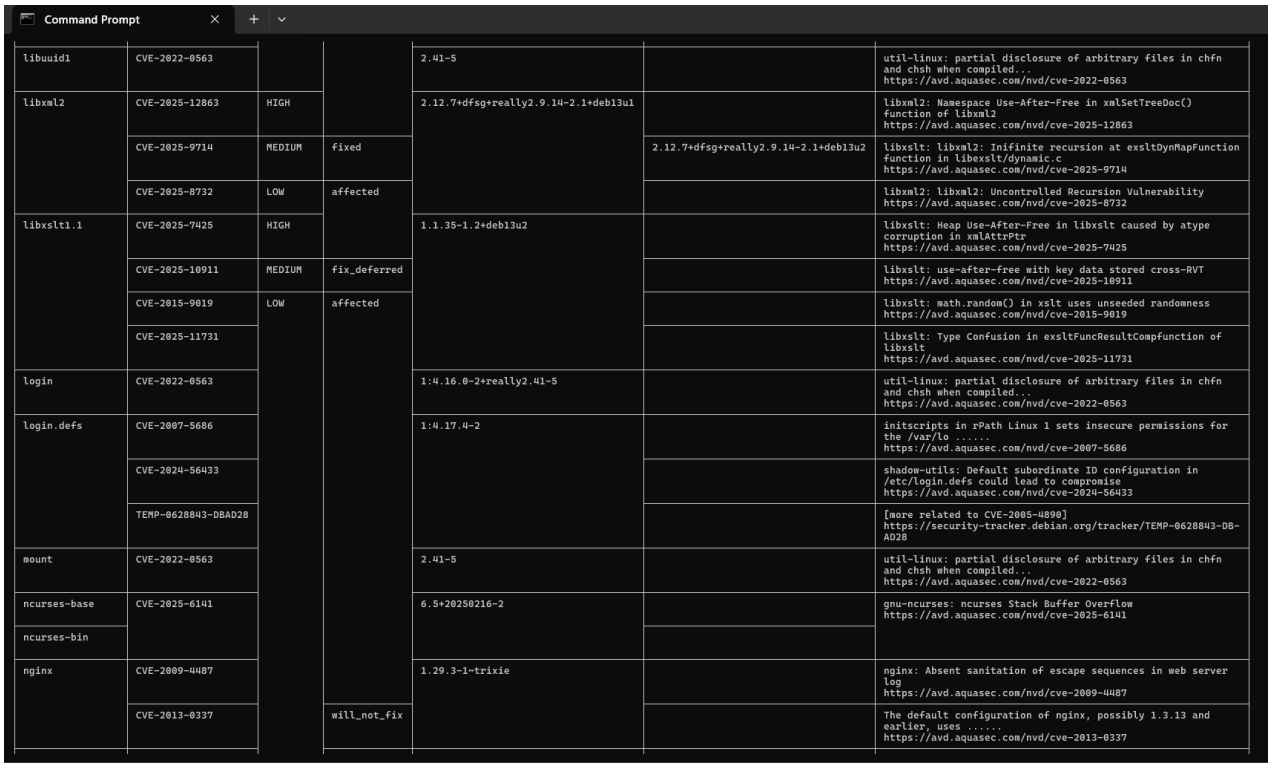


						because of... https://avd.aquasec.com/nvd/cve-2019-1010023
	CVE-2019-1010024					glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
	CVE-2019-1010025					glibc: information disclosure of heap addresses of pthread_created thread https://avd.aquasec.com/nvd/cve-2019-1010025
	CVE-2019-9192					glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2019-9192
libc6	CVE-2010-4756					glibc: glob implementation can cause excessive CPU and memory consumption due to... 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 https://avd.aquasec.com/nvd/cve-2018-20796
	CVE-2019-1010022					glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
	CVE-2019-1010023					glibc: running ldd on malicious ELF leads to code execution because of... https://avd.aquasec.com/nvd/cve-2019-1010023
	CVE-2019-1010024					glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
	CVE-2019-1010025					glibc: information disclosure of heap addresses of pthread_created thread 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 https://avd.aquasec.com/nvd/cve-2019-9192
libcurl4t64	CVE-2025-10148	MEDIUM	fixed	8.14.1-2	8.14.1-2+deb13u1	curl: predictable WebSocket mask https://avd.aquasec.com/nvd/cve-2025-10148
	CVE-2025-11563				8.14.1-2+deb13u2	wcurl path traversal with percent-encoded slashes https://avd.aquasec.com/nvd/cve-2025-11563
	CVE-2025-9086				8.14.1-2+deb13u1	curl: libcurl: Curl out of bounds read for cookie path https://avd.aquasec.com/nvd/cve-2025-9086
	CVE-2025-10966	LOW	affected			curl: Curl missing SFTP host verification with wolfSSH backend 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 ... https://avd.aquasec.com/nvd/cve-2024-38949
	CVE-2024-38950					Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... 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... 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... https://avd.aquasec.com/nvd/cve-2018-6829
	CVE-2024-2236					libgcrypt: vulnerable to Marvin Attack 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) https://avd.aquasec.com/nvd/cve-2011-3389
libgssapi-krb5-2	CVE-2018-5709			1.21.3-5		krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c 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. 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 https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c 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 https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c 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 https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c https://avd.aquasec.com/nvd/cve-2024-26461
liblastlog2-2	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libldap2	CVE-2015-3276			2.6.10+dfsg-1		openldap: incorrect multi-keyword mode cipherstring parsing https://avd.aquasec.com/nvd/cve-2015-3276
	CVE-2017-14159					openldap: Privilege escalation via PID file manipulation



libmount1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libpng16-16t64	CVE-2021-4214			1.6.48-1		libpng: hardcoded value leads to heap-overflow https://avd.aquasec.com/nvd/cve-2021-4214
libsmartcols1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libsqlite3-0	CVE-2025-7709	MEDIUM		3.46.1-7		An integer overflow exists in the FTS5 https://sqlite.org/fts5.html e ... https://avd.aquasec.com/nvd/cve-2025-7709
	CVE-2021-45346	LOW				sqlite: crafted SQL query allows a malicious user to obtain sensitive information... https://avd.aquasec.com/nvd/cve-2021-45346
libsystemd0	CVE-2013-4392			257.8-1~deb13u2		systemd: TOCTOU race condition when updating file permissions and SELinux security contexts... https://avd.aquasec.com/nvd/cve-2013-4392
	CVE-2023-31437					An issue was discovered in systemd 253. An attacker can modify a... https://avd.aquasec.com/nvd/cve-2023-31437
	CVE-2023-31438					An issue was discovered in systemd 253. An attacker can truncate a... https://avd.aquasec.com/nvd/cve-2023-31438
	CVE-2023-31439					An issue was discovered in systemd 253. An attacker can modify the... https://avd.aquasec.com/nvd/cve-2023-31439
libtiff6	CVE-2017-16232			4.7.0-3+deb13u1		libtiff: Memory leaks in tif_open.c, tif_lzw.c, and tif_aux.c https://avd.aquasec.com/nvd/cve-2017-16232
	CVE-2018-10126					libtiff: NULL pointer dereference in the jpeg_fdct_16x16 function in jfdctint.c https://avd.aquasec.com/nvd/cve-2018-10126
	CVE-2022-1210					tiff: Malicious file leads to a denial of service in TIFF File... https://avd.aquasec.com/nvd/cve-2022-1210
	CVE-2025-8176					libtiff: LibTIFF Use-After-Free Vulnerability https://avd.aquasec.com/nvd/cve-2025-8176
	CVE-2025-8177					libtiff: LibTIFF Buffer Overflow https://avd.aquasec.com/nvd/cve-2025-8177
	CVE-2025-8534					libtiff: Libtiff Null Pointer Dereference Vulnerability https://avd.aquasec.com/nvd/cve-2025-8534
libtinfo6	CVE-2025-6141			6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow https://avd.aquasec.com/nvd/cve-2025-6141
libudev1	CVE-2013-4392			257.8-1~deb13u2		systemd: TOCTOU race condition when updating file permissions and SELinux security contexts... https://avd.aquasec.com/nvd/cve-2013-4392



libuuid1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libxml2	CVE-2025-12863	HIGH		2.12.7+dfsg+really2.9.14-2.1+deb13u1		libxml2: Namespace Use-After-Free in xmlSetTreeDoc() function of libxml2 https://avd.aquasec.com/nvd/cve-2025-12863
	CVE-2025-9714	MEDIUM	fixed		2.12.7+dfsg+really2.9.14-2.1+deb13u2	libxslt: libxml2: Inifinite recursion at exsltDynMapFunction function in libexslt/dynamic.c https://avd.aquasec.com/nvd/cve-2025-9714
	CVE-2025-8732	LOW	affected			libxml2: libxml2: Uncontrolled Recursion Vulnerability https://avd.aquasec.com/nvd/cve-2025-8732
libxslt1.1	CVE-2025-7425	HIGH		1.1.35-1.2+deb13u2		libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xwlAttrPtr https://avd.aquasec.com/nvd/cve-2025-7425
	CVE-2025-10911	MEDIUM	fix_deferred			libxslt: use-after-free with key data stored cross-RVT https://avd.aquasec.com/nvd/cve-2025-10911
	CVE-2015-9019	LOW	affected			libxslt: math.random() in xslt uses unseeded randomness https://avd.aquasec.com/nvd/cve-2015-9019
	CVE-2025-11731					libxslt: Type Confusion in exsltFuncResultCompfunction of libxslt https://avd.aquasec.com/nvd/cve-2025-11731
login	CVE-2022-0563			1:4.16.0-2+really2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
login.defs	CVE-2007-5686			1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo https://avd.aquasec.com/nvd/cve-2007-5686
	CVE-2024-56433					shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise https://avd.aquasec.com/nvd/cve-2024-56433
	TEMP-0628843-DBAD28					[more related to CVE-2005-4890] https://security-tracker.debian.org/tracker/TEMP-0628843-DB-AD28
mount	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
ncurses-base	CVE-2025-6141			6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow https://avd.aquasec.com/nvd/cve-2025-6141
ncurses-bin						
nginx	CVE-2009-4487			1.29.3-1~trixie		nginx: Absent sanitation of escape sequences in web server log https://avd.aquasec.com/nvd/cve-2009-4487
	CVE-2013-0337		will_not_fix			The default configuration of nginx, possibly 1.3.13 and earlier, uses https://avd.aquasec.com/nvd/cve-2013-0337

ncurses-bin						
nginx	CVE-2009-4487			1.29.3-1~trixie		nginx: Absent sanitation of escape sequences in web server log https://avd.aquasec.com/nvd/cve-2009-4487
	CVE-2013-0337		will_not_fix			The default configuration of nginx, possibly 1.3.13 and earlier, uses https://avd.aquasec.com/nvd/cve-2013-0337
passwd	CVE-2007-5686		affected	1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo https://avd.aquasec.com/nvd/cve-2007-5686
	CVE-2024-56433					shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise https://avd.aquasec.com/nvd/cve-2024-56433
	TEMP-0628843-DBAD28					[more related to CVE-2005-4890] https://security-tracker.debian.org/tracker/TEMP-0628843-DB-AD28
perl-base	CVE-2011-4116			5.40.1-6		perl: File::Temp insecure temporary file handling https://avd.aquasec.com/nvd/cve-2011-4116
sysvinit-utils	TEMP-0517018-A83CE6			3.14-4		[sysvinit: no-root option in expert installer exposes locally exploitable security flaw] https://security-tracker.debian.org/tracker/TEMP-0517018-A8-3CE6
tar	CVE-2005-2541			1.35+dfsg-3.1		tar: does not properly warn the user when extracting setuid or setgid... https://avd.aquasec.com/nvd/cve-2005-2541
	TEMP-0290435-0B57B5					[tar's rmt command may have undesired side effects] https://security-tracker.debian.org/tracker/TEMP-0290435-0B-57B5
util-linux	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563

```
C:\Users\namit>
```

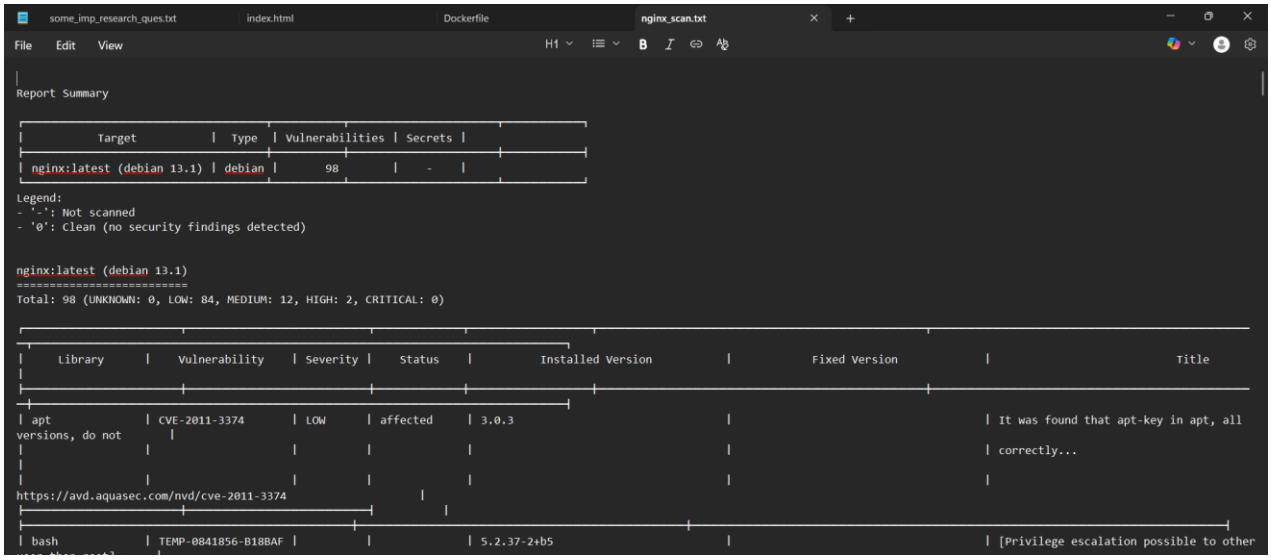
Step 5: Save Report to a File

You can export the results in different formats.

Save as a text file:

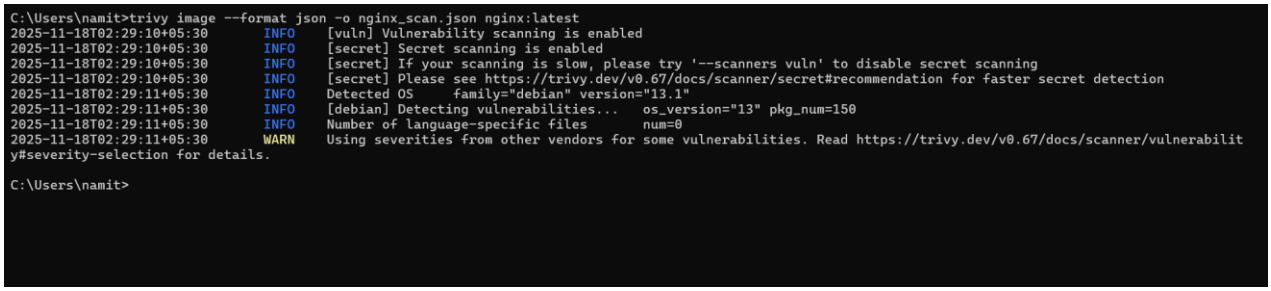
```
trivy image nginx:latest > nginx_scan.txt
```

```
trivy image nginx:latest > nginx_scan.txt
2025-11-18T02:24:13+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-18T02:24:13+05:30       INFO    [secret] Secret scanning is enabled
2025-11-18T02:24:13+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-18T02:24:13+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-18T02:24:13+05:30       INFO    Detected OS     family="debian" version="13.1"
2025-11-18T02:24:13+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-18T02:24:13+05:30       INFO    Number of language-specific files       num=0
2025-11-18T02:24:13+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.

C:\Users\namit>
```



Save as a JSON report:

```
trivy image --format json -o nginx_scan.json nginx:latest
```



Step 6: Scan a Local Image

If you've built your own Docker image:

```
docker build -t myapp:1.0 .

trivy image myapp:1.0
```

```
C:\Users\namit\nginx-html-app>docker build -t myapp:1.0 .
[+] Building 0.6s (7/7) FINISHED                                                                    docker:desktop-linux
 => [internal] load build definition from Dockerfile                                                                0.0s
 => => transferring dockerfile: 110B                                                                                0.0s
 => [internal] load metadata for docker.io/library/nginx:latest                                                     0.1s
 => [internal] load .dockerignore                                                                                   0.0s
 => => transferring context: 2B                                                                                     0.0s
 => [internal] load build context                                                                                   0.0s
 => => transferring context: 32B                                                                                    0.0s
 => [1/2] FROM docker.io/library/nginx:latest@sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad  0.1s
 => => resolve docker.io/library/nginx:latest@sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad  0.1s
 => CACHED [2/2] COPY index.html /usr/share/nginx/html/                                                             0.0s
 => exporting to image                                                                                              0.2s
 => => exporting layers                                                                                             0.0s
 => => exporting manifest sha256:f64da5b877984cd860b721fdd225a62e665d6fb72d1bf4811be2b75e264e068e                   0.0s
 => => exporting config sha256:14a1ab9baf8ebb8e17707a455e463ba9826cef5c05f5776e3fa5d7d966470c87                     0.0s
 => => exporting attestation manifest sha256:cf11c739fc36c9c0b5c96856eac2894d035fae72ce619224db611ea08478add4       0.1s
 => => exporting manifest list sha256:c7ec4358cff6e1770746f1bfe6bcc0c8dca7985fb44069aacca27e22b3043bb4              0.0s
 => => naming to docker.io/library/myapp:1.0                                                                        0.0s
 => => unpacking to docker.io/library/myapp:1.0                                                                     0.0s

C:\Users\namit\nginx-html-app>
```

```
C:\Users\namit\nginx-html-app>trivy image myapp:1.0
2025-11-18T02:33:07+05:30       INFO    [vuln] Vulnerability scanning is enabled
2025-11-18T02:33:07+05:30       INFO    [secret] Secret scanning is enabled
2025-11-18T02:33:07+05:30       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-11-18T02:33:07+05:30       INFO    [secret] Please see https://trivy.dev/v0.67/docs/scanner/secret#recommendation for faster secret detection
2025-11-18T02:33:10+05:30       INFO    Detected OS     family="debian" version="13.1"
2025-11-18T02:33:10+05:30       INFO    [debian] Detecting vulnerabilities...   os_version="13" pkg_num=150
2025-11-18T02:33:10+05:30       INFO    Number of language-specific files       num=0
2025-11-18T02:33:10+05:30       WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.67/docs/scanner/vulnerability#severity-selection for details.

Report Summary
```

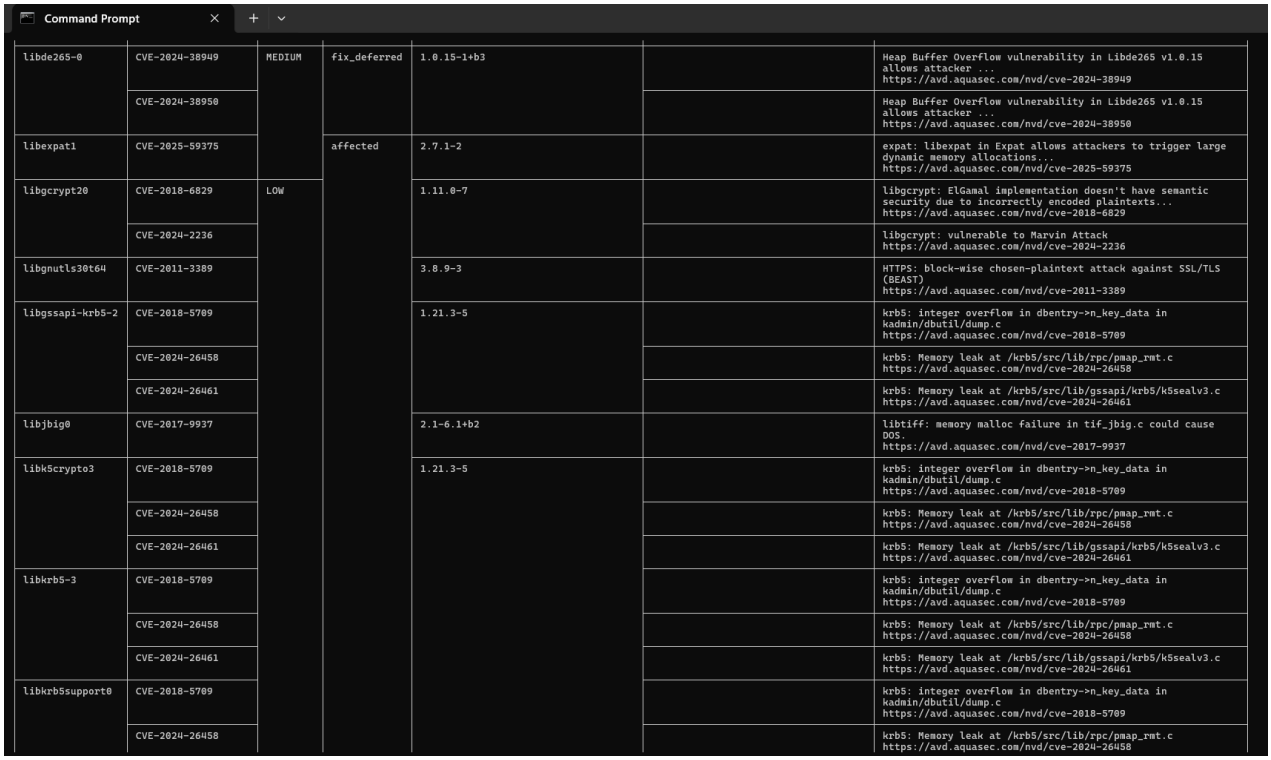
Target	Type	Vulnerabilities	Secrets
myapp:1.0 (debian 13.1)	debian	98	-

```
Legend:
- '-': Not scanned
- '0': Clean (no security findings detected)


myapp:1.0 (debian 13.1)
=======================
Total: 98 (UNKNOWN: 0, LOW: 84, MEDIUM: 12, HIGH: 2, CRITICAL: 0)
```

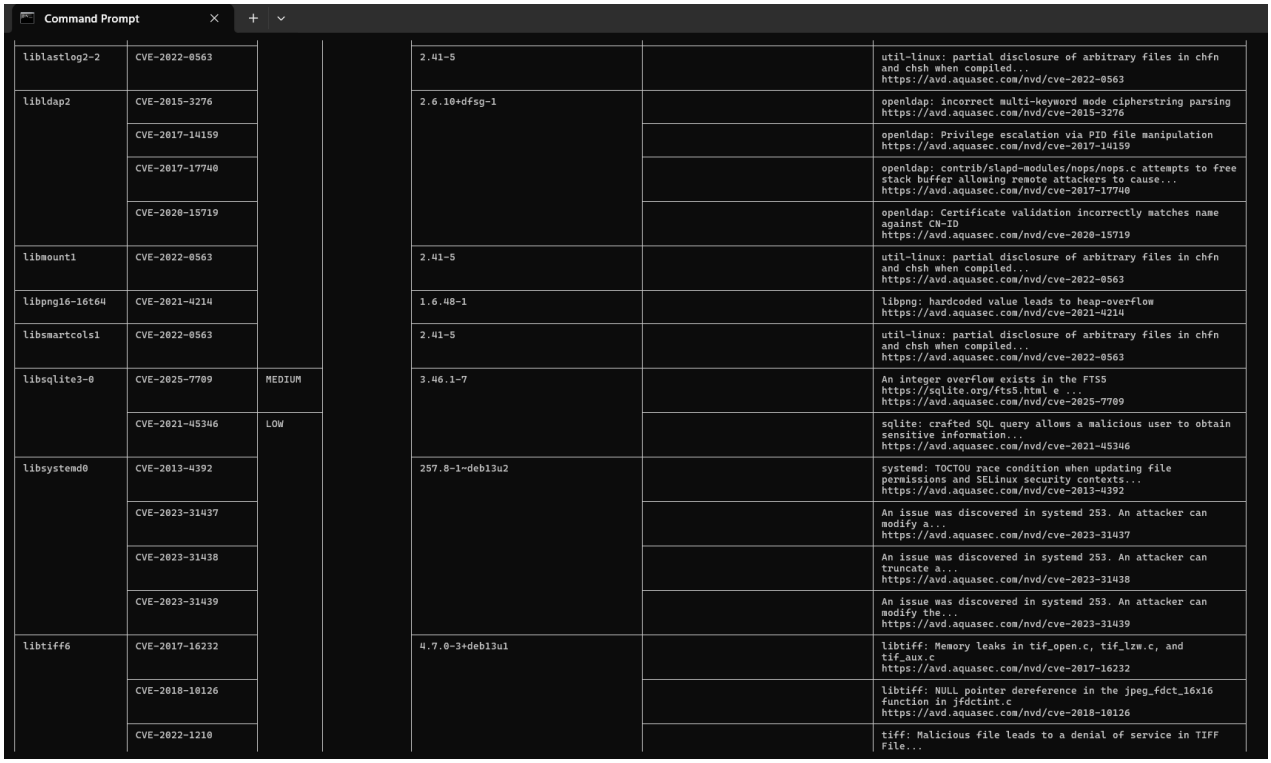
Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	affected	3.0.3		It was found that apt-key in apt, all versions, do not correctly... https://avd.aquasec.com/nvd/cve-2011-3374
bash	TEMP-0841856-B18BAF			5.2.37-2+b5		[Privilege escalation possible to other 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-2025-10148	MEDIUM	fixed	8.14.1-2	8.14.1-2+deb13u1	curl: predictable WebSocket mask https://avd.aquasec.com/nvd/cve-2025-10148
	CVE-2025-11563				8.14.1-2+deb13u2	wcurl path traversal with percent-encoded slashes https://avd.aquasec.com/nvd/cve-2025-11563
	CVE-2025-9086				8.14.1-2+deb13u1	curl: libcurl: Curl out of bounds read for cookie path https://avd.aquasec.com/nvd/cve-2025-9086
	CVE-2025-10966	LOW	affected			curl: Curl missing SFTP host verification with wolfSSH backend 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

Command Prompt

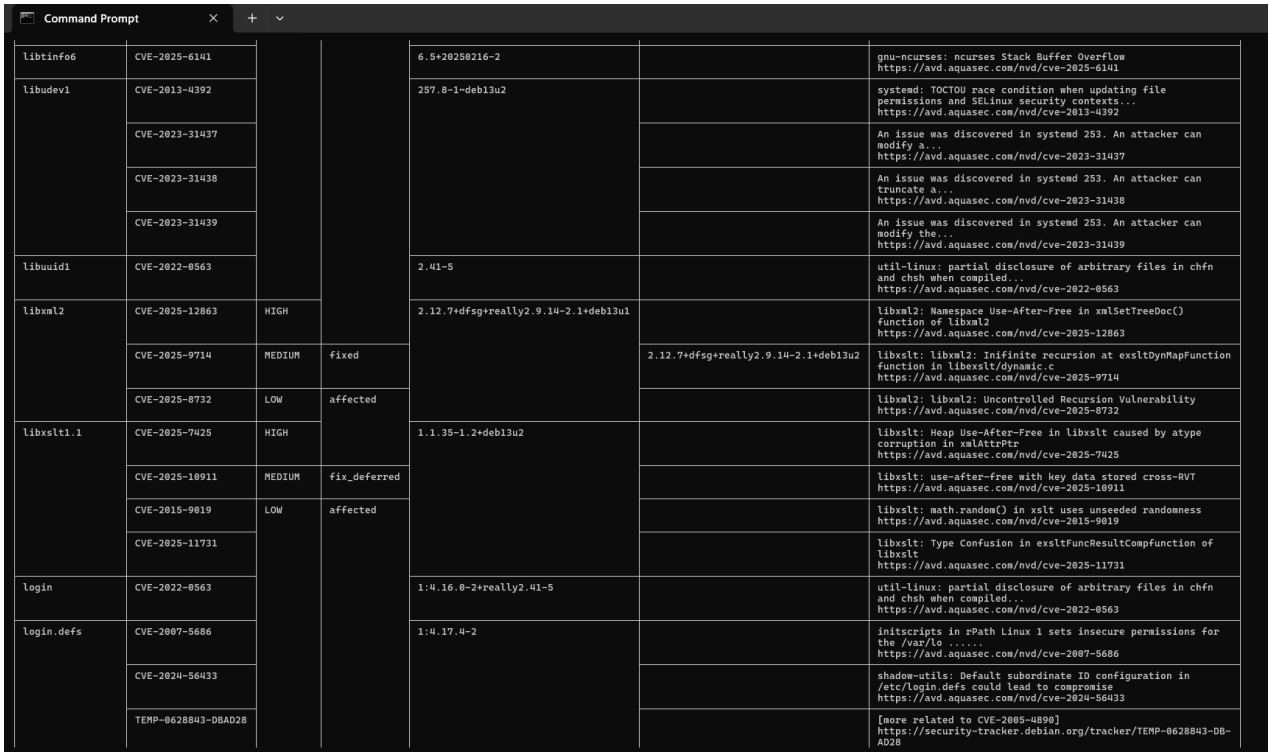
libc-bin	CVE-2010-4756			2.41-12		glibc: glob implementation can cause excessive CPU and memory consumption due to... https://avd.aquasec.com/nvd/cve-2010-4756
	CVE-2018-20796					glibc: uncontrolled recursion in function check_dst_limits_calc_pos_1 in posix/regexec.c https://avd.aquasec.com/nvd/cve-2018-20796
	CVE-2019-1010022					glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
	CVE-2019-1010023					glibc: running ldd on malicious ELF leads to code execution because of... https://avd.aquasec.com/nvd/cve-2019-1010023
	CVE-2019-1010024					glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
	CVE-2019-1010025					glibc: information disclosure of heap addresses of pthread_created thread 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 https://avd.aquasec.com/nvd/cve-2019-9192
libc6	CVE-2010-4756					glibc: glob implementation can cause excessive CPU and memory consumption due to... 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 https://avd.aquasec.com/nvd/cve-2018-20796
	CVE-2019-1010022					glibc: stack guard protection bypass https://avd.aquasec.com/nvd/cve-2019-1010022
	CVE-2019-1010023					glibc: running ldd on malicious ELF leads to code execution because of... https://avd.aquasec.com/nvd/cve-2019-1010023
	CVE-2019-1010024					glibc: ASLR bypass using cache of thread stack and heap https://avd.aquasec.com/nvd/cve-2019-1010024
	CVE-2019-1010025					glibc: information disclosure of heap addresses of pthread_created thread 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 https://avd.aquasec.com/nvd/cve-2019-9192
libcurl4t64	CVE-2025-10148	MEDIUM	fixed	8.14.1-2	8.14.1-2+deb13u1	curl: predictable WebSocket mask https://avd.aquasec.com/nvd/cve-2025-10148
	CVE-2025-11563				8.14.1-2+deb13u2	wcurl path traversal with percent-encoded slashes https://avd.aquasec.com/nvd/cve-2025-11563
	CVE-2025-9086				8.14.1-2+deb13u1	curl: libcurl: Curl out of bounds read for cookie path https://avd.aquasec.com/nvd/cve-2025-9086
	CVE-2025-10966	LOW	affected			curl: Curl missing SFTP host verification with wolfSSH backend



libde265-0	CVE-2024-38949	MEDIUM	fix_deferred	1.0.15-1+b3		Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... https://avd.aquasec.com/nvd/cve-2024-38949
	CVE-2024-38950					Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attacker ... 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... 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... https://avd.aquasec.com/nvd/cve-2018-6829
	CVE-2024-2236					libgcrypt: vulnerable to Marvin Attack 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) https://avd.aquasec.com/nvd/cve-2011-3389
libgssapi-krb5-2	CVE-2018-5709			1.21.3-5		krb5: integer overflow in dbentry->n_key_data in kadmin/dbutil/dump.c https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c 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. 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 https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c 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 https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458
	CVE-2024-26461					krb5: Memory leak at /krb5/src/lib/gssapi/krb5/k5sealv3.c 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 https://avd.aquasec.com/nvd/cve-2018-5709
	CVE-2024-26458					krb5: Memory leak at /krb5/src/lib/rpc/pmap_rmt.c https://avd.aquasec.com/nvd/cve-2024-26458



liblastlog2-2	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libldap2	CVE-2015-3276			2.6.10+dfsg-1		openldap: incorrect multi-keyword mode cipherstring parsing https://avd.aquasec.com/nvd/cve-2015-3276
	CVE-2017-14159					openldap: Privilege escalation via PID file manipulation https://avd.aquasec.com/nvd/cve-2017-14159
	CVE-2017-17740					openldap: contrib/slapd-modules/nops/nops.c attempts to free stack buffer allowing remote attackers to cause... https://avd.aquasec.com/nvd/cve-2017-17740
	CVE-2020-15719					openldap: Certificate validation incorrectly matches name against CN-ID https://avd.aquasec.com/nvd/cve-2020-15719
libmount1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libpng16-16t64	CVE-2021-4214			1.6.48-1		libpng: hardcoded value leads to heap-overflow https://avd.aquasec.com/nvd/cve-2021-4214
libsmartcols1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libsqlite3-0	CVE-2025-7709	MEDIUM		3.46.1-7		An integer overflow exists in the FTS5 https://sqlite.org/fts5.html e ... https://avd.aquasec.com/nvd/cve-2025-7709
	CVE-2021-45346	LOW				sqlite: crafted SQL query allows a malicious user to obtain sensitive information... https://avd.aquasec.com/nvd/cve-2021-45346
libsystemd0	CVE-2013-4392			257.8-1~deb13u2		systemd: TOCTOU race condition when updating file permissions and SELinux security contexts... https://avd.aquasec.com/nvd/cve-2013-4392
	CVE-2023-31437					An issue was discovered in systemd 253. An attacker can modify a... https://avd.aquasec.com/nvd/cve-2023-31437
	CVE-2023-31438					An issue was discovered in systemd 253. An attacker can truncate a... https://avd.aquasec.com/nvd/cve-2023-31438
	CVE-2023-31439					An issue was discovered in systemd 253. An attacker can modify the... https://avd.aquasec.com/nvd/cve-2023-31439
libtiff6	CVE-2017-16232			4.7.0-3+deb13u1		libtiff: Memory leaks in tif_open.c, tif_lzw.c, and tif_aux.c https://avd.aquasec.com/nvd/cve-2017-16232
	CVE-2018-10126					libtiff: NULL pointer dereference in the jpeg_fdct_16x16 function in jfdctint.c https://avd.aquasec.com/nvd/cve-2018-10126
	CVE-2022-1210					tiff: Malicious file leads to a denial of service in TIFF File...



libtinfo6	CVE-2025-6141			6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow https://avd.aquasec.com/nvd/cve-2025-6141
libudev1	CVE-2013-4392			257.8-1~deb13u2		systemd: TOCTOU race condition when updating file permissions and SELinux security contexts... https://avd.aquasec.com/nvd/cve-2013-4392
	CVE-2023-31437					An issue was discovered in systemd 253. An attacker can modify a... https://avd.aquasec.com/nvd/cve-2023-31437
	CVE-2023-31438					An issue was discovered in systemd 253. An attacker can truncate a... https://avd.aquasec.com/nvd/cve-2023-31438
	CVE-2023-31439					An issue was discovered in systemd 253. An attacker can modify the... https://avd.aquasec.com/nvd/cve-2023-31439
libuuid1	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libxml2	CVE-2025-12863	HIGH		2.12.7+dfsg+really2.9.14-2.1+deb13u1		libxml2: Namespace Use-After-Free in xmlSetTreeDoc() function of libxml2 https://avd.aquasec.com/nvd/cve-2025-12863
	CVE-2025-9714	MEDIUM	fixed		2.12.7+dfsg+really2.9.14-2.1+deb13u2	libxslt: libxml2: Inifinite recursion at exsltDynMapFunction function in libexslt/dynamic.c https://avd.aquasec.com/nvd/cve-2025-9714
	CVE-2025-8732	LOW	affected			libxml2: libxml2: Uncontrolled Recursion Vulnerability https://avd.aquasec.com/nvd/cve-2025-8732
libxslt1.1	CVE-2025-7425	HIGH		1.1.35-1.2+deb13u2		libxslt: Heap Use-After-Free in libxslt caused by atype corruption in xmlAttrPtr https://avd.aquasec.com/nvd/cve-2025-7425
	CVE-2025-10911	MEDIUM	fix_deferred			libxslt: use-after-free with key data stored cross-RVT https://avd.aquasec.com/nvd/cve-2025-10911
	CVE-2015-9019	LOW	affected			libxslt: math.random() in xslt uses unseeded randomness https://avd.aquasec.com/nvd/cve-2015-9019
	CVE-2025-11731					libxslt: Type Confusion in exsltFuncResultCompfunction of libxslt https://avd.aquasec.com/nvd/cve-2025-11731
login	CVE-2022-0563			1:4.16.0-2+really2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
login.defs	CVE-2007-5686			1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo https://avd.aquasec.com/nvd/cve-2007-5686
	CVE-2024-56433					shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise https://avd.aquasec.com/nvd/cve-2024-56433
	TEMP-0628843-DBAD28					[more related to CVE-2005-4890] https://security-tracker.debian.org/tracker/TEMP-0628843-DB-AD28

						AD28
mount	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
ncurses-base	CVE-2025-6141			6.5+20250216-2		gnu-ncurses: ncurses Stack Buffer Overflow https://avd.aquasec.com/nvd/cve-2025-6141
ncurses-bin						
nginx	CVE-2009-4487			1.29.3-1~trixie		nginx: Absent sanitation of escape sequences in web server log https://avd.aquasec.com/nvd/cve-2009-4487
	CVE-2013-0337		will_not_fix			The default configuration of nginx, possibly 1.3.13 and earlier, uses https://avd.aquasec.com/nvd/cve-2013-0337
passwd	CVE-2007-5686		affected	1:4.17.4-2		initscripts in rPath Linux 1 sets insecure permissions for the /var/lo https://avd.aquasec.com/nvd/cve-2007-5686
	CVE-2024-56433					shadow-utils: Default subordinate ID configuration in /etc/login.defs could lead to compromise https://avd.aquasec.com/nvd/cve-2024-56433
	TEMP-0628843-DBAD28					[more related to CVE-2005-4890] https://security-tracker.debian.org/tracker/TEMP-0628843-DB-AD28
perl-base	CVE-2011-4116			5.40.1-6		perl: File::Temp insecure temporary file handling https://avd.aquasec.com/nvd/cve-2011-4116
sysvinit-utils	TEMP-0517018-A83CE6			3.14-4		[sysvinit: no-root option in expert installer exposes locally exploitable security flaw] https://security-tracker.debian.org/tracker/TEMP-0517018-A8-3CE6
tar	CVE-2005-2541			1.35+dfsg-3.1		tar: does not properly warn the user when extracting setuid or setgid... https://avd.aquasec.com/nvd/cve-2005-2541
	TEMP-0290435-0B57B5					[tar's rmt command may have undesired side effects] https://security-tracker.debian.org/tracker/TEMP-0290435-0B-57B5
util-linux	CVE-2022-0563			2.41-5		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563

C:\Users\namit\nginx-html-app>

Step 7: Update Vulnerability Database

Keep Trivy's database up-to-date:

```
trivy image --download-db-only
```

```
C:\Users\namit\nginx-html-app>trivy image --download-db-only

C:\Users\namit\nginx-html-app>
```

Step 8: Clean Up

Remove images (optional):

```
docker rmi nginx:latest
```

```
C:\Users\namit\nginx-html-app>docker rmi nginx:latest
Untagged: nginx:latest
Deleted: sha256:1beed3ca46acebe9d3fb62e9067f03d05d5bfa97a00f30938a0a3580563272ad

C:\Users\namit\nginx-html-app>
```