```
PS C:\Users\dorda> trivy image dordavidisrael/hw3:web-service-1.0.0
2025-02-08T19:20:57+02:00       INFO    [vuln] Vulnerability scanning is enabled
2025-02-08T19:20:57+02:00       INFO    [secret] Secret scanning is enabled
2025-02-08T19:20:57+02:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-02-08T19:20:57+02:00       INFO    [secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-02-08T19:20:57+02:00       INFO    Detected OS     family="debian" version="12.9"
2025-02-08T19:20:57+02:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=105
2025-02-08T19:20:57+02:00       INFO    Number of language-specific files       num=1
2025-02-08T19:20:57+02:00       INFO    [python-pkg] Detecting vulnerabilities...
2025-02-08T19:20:57+02:00       WARN    Using severities from other vendors for some vulnerabilities. Read https://aquasecurity.github.io/trivy/v0.59/docs/scanner/vulnerability#severity-selection for details.

dordavidisrael/hw3:web-service-1.0.0 (debian 12.9)
==================================================
Total: 100 (UNKNOWN: 1, LOW: 70, MEDIUM: 23, HIGH: 5, CRITICAL: 1)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	affected	2.6.1		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			5.2.15-2+b7		[Privilege escalation possible to other user than root] https://security-tracker.debian.org/tracker/TEMP-0841856-B18BAF
bsdutils	CVE-2022-0563			1:2.38.1-5+deb12u3		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
coreutils	CVE-2016-2781		will_not_fix	9.1-1		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
	CVE-2017-18018		affected			coreutils: race condition vulnerability in chown and chgrp https://avd.aquasec.com/nvd/cve-2017-18018
gcc-12-base	CVE-2022-27943			12.2.0-14		binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943
	CVE-2023-4039					gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64 https://avd.aquasec.com/nvd/cve-2023-4039
gpgv	CVE-2022-3219			2.2.40-1.1		gnupg: denial of service issue (resource consumption) using compressed packets https://avd.aquasec.com/nvd/cve-2022-3219
libapt-pkg6.0	CVE-2011-3374			2.6.1		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			2.38.1-5+deb12u3		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libc-bin	CVE-2025-0395	MEDIUM		2.36-9+deb12u9		glibc: buffer overflow in the GNU C Library's assert() https://avd.aquasec.com/nvd/cve-2025-0395
	CVE-2010-4756	LOW				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-2025-0395	MEDIUM				glibc: buffer overflow in the GNU C Library's assert() https://avd.aquasec.com/nvd/cve-2025-0395
	CVE-2010-4756	LOW				glibc: glob implementation can cause excessive CPU and memory consumption due to... https://avd.aquasec.com/nvd/cve-2010-4756

```
PS C:\Users\dorda> trivy image dordavidisrael/hw3:worker-service-1.0.0
2025-02-08T19:21:05+02:00       INFO    [vuln] Vulnerability scanning is enabled
2025-02-08T19:21:05+02:00       INFO    [secret] Secret scanning is enabled
2025-02-08T19:21:05+02:00       INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-02-08T19:21:05+02:00       INFO    [secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-02-08T19:21:12+02:00       INFO    [python] Licenses acquired from one or more METADATA files may be subject to additional terms. Use `--debug` flag to see all affected packages.
2025-02-08T19:21:12+02:00       INFO    Detected OS     family="debian" version="12.9"
2025-02-08T19:21:12+02:00       INFO    [debian] Detecting vulnerabilities...   os_version="12" pkg_num=105
2025-02-08T19:21:12+02:00       INFO    Number of language-specific files       num=1
2025-02-08T19:21:12+02:00       INFO    [python-pkg] Detecting vulnerabilities...
2025-02-08T19:21:12+02:00       WARN    Using severities from other vendors for some vulnerabilities. Read https://aquasecurity.github.io/trivy/v0.59/docs/scanner/vulnerability#severity-selection fo

dordavidisrael/hw3:worker-service-1.0.0 (debian 12.9)
=====================================================
Total: 100 (UNKNOWN: 1, LOW: 70, MEDIUM: 23, HIGH: 5, CRITICAL: 1)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
apt	CVE-2011-3374	LOW	affected	2.6.1		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			5.2.15-2+b7		[Privilege escalation possible to other user than root] https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF
bsdutils	CVE-2022-0563			1:2.38.1-5+deb12u3		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
coreutils	CVE-2016-2781		will_not_fix	9.1-1		coreutils: Non-privileged session can escape to the parent session in chroot https://avd.aquasec.com/nvd/cve-2016-2781
	CVE-2017-18018		affected			coreutils: race condition vulnerability in chown and chgrp https://avd.aquasec.com/nvd/cve-2017-18018
gcc-12-base	CVE-2022-27943			12.2.0-14		binutils: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack exhaustion in demangle_const https://avd.aquasec.com/nvd/cve-2022-27943
	CVE-2023-4039					gcc: -fstack-protector fails to guard dynamic stack allocations on ARM64 https://avd.aquasec.com/nvd/cve-2023-4039
gpgv	CVE-2022-3219			2.2.40-1.1		gnupg: denial of service issue (resource consumption) using compressed packets https://avd.aquasec.com/nvd/cve-2022-3219
libapt-pkg6.0	CVE-2011-3374			2.6.1		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			2.38.1-5+deb12u3		util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
libc-bin	CVE-2025-0395	MEDIUM		2.36-9+deb12u9		glibc: buffer overflow in the GNU C Library's assert() https://avd.aquasec.com/nvd/cve-2025-0395
	CVE-2010-4756	LOW				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