To use *trivy* - run command :

```
docker run --rm -v ~/.trivy:/root/.cache/ aquasec/trivy:0.40.0 image ghcr.io/mlflow/mlflow:v2.3.0 --severity HIGH,CRITICAL
```

Result :

```
C:\Taras\education\data-engineering>docker run --rm -v ~/.trivy:/root/.cache/ aquasec/trivy:0.40.0 image ghcr.io/mlflow/mlflow:v2.3.0 --severity HIGH,CRITICAL
2023-05-02T14:10:02.427Z        INFO    Vulnerability scanning is enabled
2023-05-02T14:10:02.427Z        INFO    Secret scanning is enabled
2023-05-02T14:10:02.427Z        INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2023-05-02T14:10:02.427Z        INFO    Please see also https://aquasecurity.github.io/trivy/v0.40/docs/secret/scanning/#recommendation for faster secret detection
2023-05-02T14:10:03.957Z        INFO    Detected OS: debian
2023-05-02T14:10:03.957Z        INFO    Detecting Debian vulnerabilities...
2023-05-02T14:10:03.988Z        INFO    Number of language-specific files: 1
2023-05-02T14:10:03.988Z        INFO    Detecting python-pkg vulnerabilities...
2023-05-02T14:10:04.024Z        INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.

ghcr.io/mlflow/mlflow:v2.3.0 (debian 11.6)
==========================================
Total: 20 (HIGH: 19, CRITICAL: 1)
```

Library	Vulnerability	Severity	Installed Version	Fixed Version	Title
bash	CVE-2022-3715	HIGH	5.1-2+deb11u1		a heap-buffer-overflow in valid_parameter_transform https://avd.aquasec.com/nvd/cve-2022-3715
e2fsprogs	CVE-2022-1304		1.46.2-2		e2fsprogs: out-of-bounds read/write via crafted filesystem https://avd.aquasec.com/nvd/cve-2022-1304
libcom-err2					
libdb5.3	CVE-2019-8457	CRITICAL	5.3.28+dfsg1-0.8		sqlite: heap out-of-bound read in function rtreenode() https://avd.aquasec.com/nvd/cve-2019-8457
libext2fs2	CVE-2022-1304	HIGH	1.46.2-2		e2fsprogs: out-of-bounds read/write via crafted filesystem https://avd.aquasec.com/nvd/cve-2022-1304
libgcrypt20	CVE-2021-33560		1.8.7-6		libgcrypt: mishandles ElGamal encryption because it lacks exponent blinding to address a... https://avd.aquasec.com/nvd/cve-2021-33560
libncursesw6	CVE-2022-29458		6.2+20201114-2	6.2+20201114-2+deb11u1	ncurses: segfaulting OOB read https://avd.aquasec.com/nvd/cve-2022-29458
	CVE-2023-29491				Local users can trigger security-relevant memory corruption via malformed data https://avd.aquasec.com/nvd/cve-2023-29491
libss2	CVE-2022-1304		1.46.2-2		e2fsprogs: out-of-bounds read/write via crafted filesystem https://avd.aquasec.com/nvd/cve-2022-1304
libssl1.1	CVE-2023-0464		1.1.1n-0+deb11u4		Denial of service by excessive resource usage in verifying X509 policy constraints... https://avd.aquasec.com/nvd/cve-2023-0464
libtinfo6	CVE-2022-29458		6.2+20201114-2	6.2+20201114-2+deb11u1	ncurses: segfaulting OOB read https://avd.aquasec.com/nvd/cve-2022-29458
	CVE-2023-29491				Local users can trigger security-relevant memory corruption via malformed data https://avd.aquasec.com/nvd/cve-2023-29491

To use *grype* - run command(on Ubuntu) :

```
curl -sSfL https://raw.githubusercontent.com/anchore/grype/main/install.sh | sh -s -- -b .


grype ghcr.io/mlflow/mlflow:v2.3.0
```

Result:

```
tarassito@DESKTOP-I9VMMOT:~/education$ grype ghcr.io/mlflow/mlflow:v2.3.0
 ✔ Vulnerability DB        [no update available]
 ✔ Parsed image
 ✔ Cataloged packages      [164 packages]
 ✔ Scanning image...       [112 vulnerabilities]
   ├── 3 critical, 26 high, 15 medium, 8 low, 59 negligible (1 unknown)
   └── 12 fixed

NAME              INSTALLED           FIXED-IN            TYPE    VULNERABILITY        SEVERITY
Flask             2.2.3               2.3.2               python  GHSA-m2qf-hxjv-5gpq  High
apt               2.2.4                                   deb     CVE-2011-3374        Negligible
bash              5.1-2+deb11u1       (won't fix)         deb     CVE-2022-3715        High
bsdutils          1:2.36.1-8+deb11u1                      deb     CVE-2022-0563        Negligible
certifi           2022.12.7           2022.12.07          python  GHSA-43fp-rhv2-5gv8  Medium
coreutils         8.32-4+b1                               deb     CVE-2017-18018       Negligible
coreutils         8.32-4+b1           (won't fix)         deb     CVE-2016-2781        Low
docker            6.0.1                                   python  CVE-2018-10892       Medium
docker            6.0.1                                   python  CVE-2019-13139       High
docker            6.0.1                                   python  CVE-2019-13509       High
docker            6.0.1                                   python  CVE-2019-16884       High
docker            6.0.1                                   python  CVE-2019-5736        High
```

I didn’t find how to filter SEVERITY in *grype*. But we can see more CVE in *grype* - 3 Critical , 26 High vs 1 Critical and 19 HIgh in *trivy*.