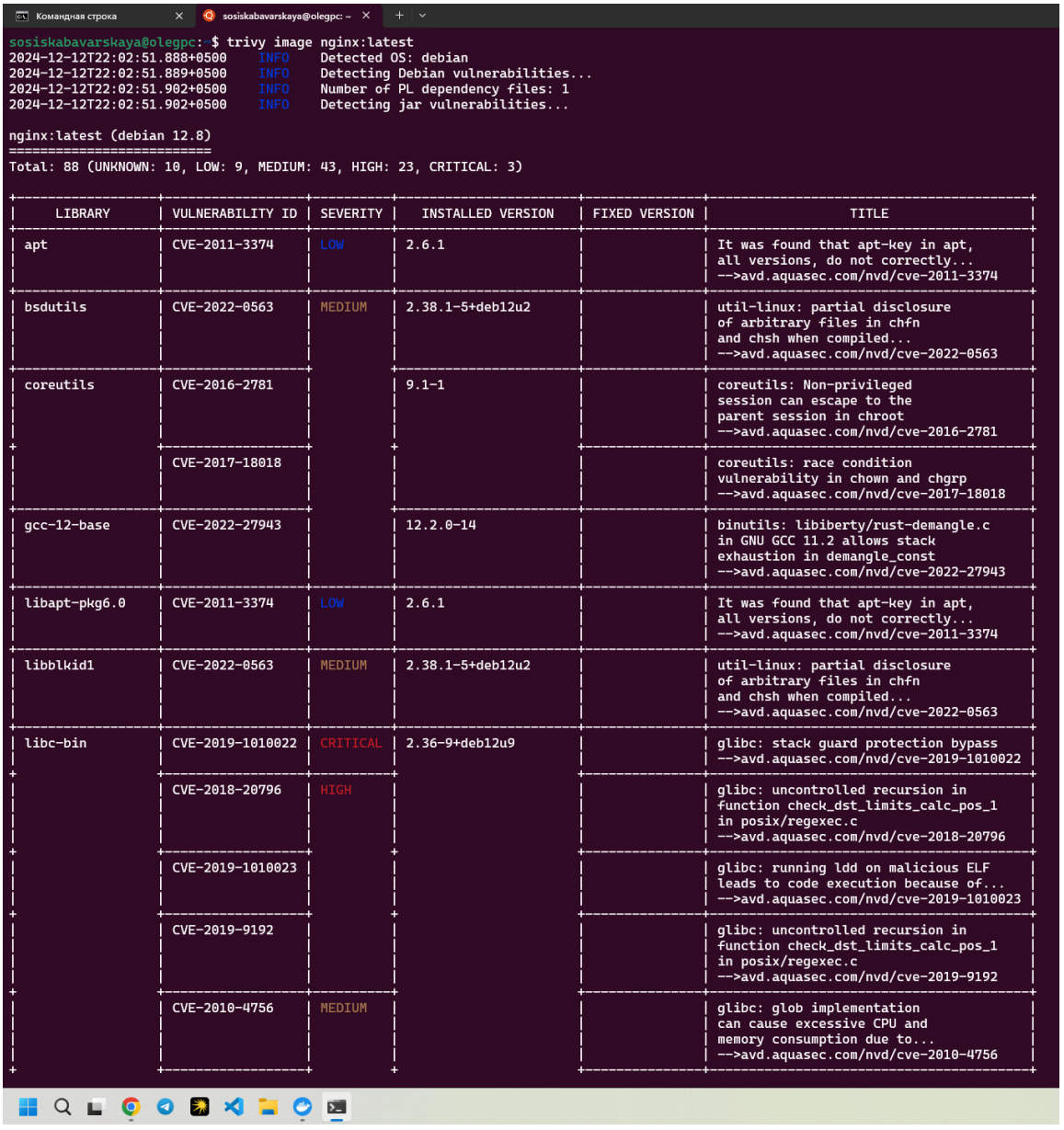
ДЗ6

1. Установите Trivy и просканируйте образ nginx:latest



```
Командная строка  sosiskabavarskaya@olegpc: ~

sosiskabavarskaya@olegpc:~$ trivy image nginx:latest
2024-12-12T22:02:51.888+0500    INFO    Detected OS: debian
2024-12-12T22:02:51.889+0500    INFO    Detecting Debian vulnerabilities...
2024-12-12T22:02:51.902+0500    INFO    Number of PL dependency files: 1
2024-12-12T22:02:51.902+0500    INFO    Detecting jar vulnerabilities...

nginx:latest (debian 12.8)
==========================
Total: 88 (UNKNOWN: 10, LOW: 9, MEDIUM: 43, HIGH: 23, CRITICAL: 3)

+----------------+------------------+----------+-------------------+---------------+---------------------------------------+
|    LIBRARY     | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |                 TITLE                 |
+----------------+------------------+----------+-------------------+---------------+---------------------------------------+
| apt            | CVE-2011-3374    | LOW      | 2.6.1             |               | It was found that apt-key in apt,     |
|                |                  |          |                   |               | all versions, do not correctly...     |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2011-3374  |
+----------------+------------------+----------+-------------------+---------------+---------------------------------------+
| bsdutils       | CVE-2022-0563    | MEDIUM   | 2.38.1-5+deb12u2  |               | util-linux: partial disclosure        |
|                |                  |          |                   |               | of arbitrary files in chfn            |
|                |                  |          |                   |               | and chsh when compiled...             |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563  |
+----------------+------------------+----------+-------------------+---------------+---------------------------------------+
| coreutils      | CVE-2016-2781    |          | 9.1-1             |               | coreutils: Non-privileged             |
|                |                  |          |                   |               | session can escape to the             |
|                |                  |          |                   |               | parent session in chroot              |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2016-2781  |
+                +------------------+          +                   +               +---------------------------------------+
|                | CVE-2017-18018   |          |                   |               | coreutils: race condition             |
|                |                  |          |                   |               | vulnerability in chown and chgrp      |
|                |                  |          |                   |               | -->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          |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-27943 |
+----------------+------------------+----------+-------------------+               +---------------------------------------+
| libapt-pkg6.0  | CVE-2011-3374    | LOW      | 2.6.1             |               | It was found that apt-key in apt,     |
|                |                  |          |                   |               | all versions, do not correctly...     |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2011-3374  |
+----------------+------------------+----------+-------------------+               +---------------------------------------+
| libblkid1      | CVE-2022-0563    | MEDIUM   | 2.38.1-5+deb12u2  |               | util-linux: partial disclosure        |
|                |                  |          |                   |               | of arbitrary files in chfn            |
|                |                  |          |                   |               | and chsh when compiled...             |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2022-0563  |
+----------------+------------------+----------+-------------------+               +---------------------------------------+
| libc-bin       | CVE-2019-1010022 | CRITICAL | 2.36-9+deb12u9    |               | glibc: stack guard protection bypass  |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010022 |
+                +------------------+----------+                   +               +---------------------------------------+
|                | CVE-2018-20796   | HIGH     |                   |               | glibc: uncontrolled recursion in      |
|                |                  |          |                   |               | function check_dst_limits_calc_pos_1  |
|                |                  |          |                   |               | in posix/regexec.c                    |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2018-20796 |
+                +------------------+          +                   +               +---------------------------------------+
|                | CVE-2019-1010023 |          |                   |               | glibc: running ldd on malicious ELF   |
|                |                  |          |                   |               | leads to code execution because of... |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-1010023 |
+                +------------------+          +                   +               +---------------------------------------+
|                | CVE-2019-9192    |          |                   |               | glibc: uncontrolled recursion in      |
|                |                  |          |                   |               | function check_dst_limits_calc_pos_1  |
|                |                  |          |                   |               | in posix/regexec.c                    |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2019-9192  |
+                +------------------+----------+                   +               +---------------------------------------+
|                | CVE-2010-4756    | MEDIUM   |                   |               | glibc: glob implementation            |
|                |                  |          |                   |               | can cause excessive CPU and           |
|                |                  |          |                   |               | memory consumption due to...          |
|                |                  |          |                   |               | -->avd.aquasec.com/nvd/cve-2010-4756  |
+                +------------------+----------+                   +               +---------------------------------------+
```

2. Список критических уязвимостей:

   a. CVE-2019-1010022 - уязвимость связана с библиотекой GNU Libc и предоставляет возможность для переполнения буфера, это может позволить обойти защиту стека и выполнить произвольный код.

   b. CVE-2017-9117 - уязвимость либы libtiff, связана с ошибкой внутренней функции, может привести к переполнению буфера при

обработке tiff файлов и далее возможно выполнение произвольного кода.

3.

```
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl get pods
NAME                                READY   STATUS    RESTARTS   AGE
nginx-deployment-54b9c68f67-2tn4z   1/1     Running   0          28s
nginx-deployment-54b9c68f67-jf548   1/1     Running   0          28s
nginx-deployment-54b9c68f67-mrr8x   1/1     Running   0          28s
sosiskabavarskaya@olegpc:~/repos/kubernates_example$ kubectl exec -it nginx-deployment-54b9c68f67-2tn4z -- /bin/bash
root@nginx-deployment-54b9c68f67-2tn4z:/# curl http://google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
root@nginx-deployment-54b9c68f67-2tn4z:/#
```

```
sosiskabavarskaya@olegpc: $ sudo falco
[sudo] password for sosiskabavarskaya:
Thu Dec 12 22:56:32 2024: Falco version: 0.39.2 (x86_64)
Thu Dec 12 22:56:32 2024: Falco initialized with configuration files:
Thu Dec 12 22:56:32 2024:    /etc/falco/falco.yaml | schema validation: ok
Thu Dec 12 22:56:32 2024: System info: Linux version 5.15.167.4-microsoft-standard-WSL2 (root@f9c826d3017f) (gcc (GCC) 11.2.0, GNU ld (GNU Binutils) 2.37) #1 SMP Tue Nov 5 00:21:55 UTC 2024
Thu Dec 12 22:56:32 2024: Loading rules from:
Thu Dec 12 22:56:32 2024:    /etc/falco/falco_rules.yaml | schema validation: ok
Thu Dec 12 22:56:32 2024:    /etc/falco/falco_rules.local.yaml | schema validation: none
Thu Dec 12 22:56:32 2024: The chosen syscall buffer dimension is: 8388608 bytes (8 MBs)
Thu Dec 12 22:56:32 2024: Starting health webserver with threadiness 8, listening on 0.0.0.0:8765
Thu Dec 12 22:56:32 2024: Loaded event sources: syscall
Thu Dec 12 22:56:32 2024: Enabled event sources: syscall
Thu Dec 12 22:56:32 2024: Opening 'syscall' source with modern BPF probe.
Thu Dec 12 22:56:32 2024: One ring buffer every '2' CPUs.
22:56:37.329836100: Notice A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/usr/bin/bash parent=runc command=bash terminal=34816 exe_flags=EXE_WRITABLE|EXE_LOWER_LAYER container_id=489c25e94bbb container_name=<NA>)
```