

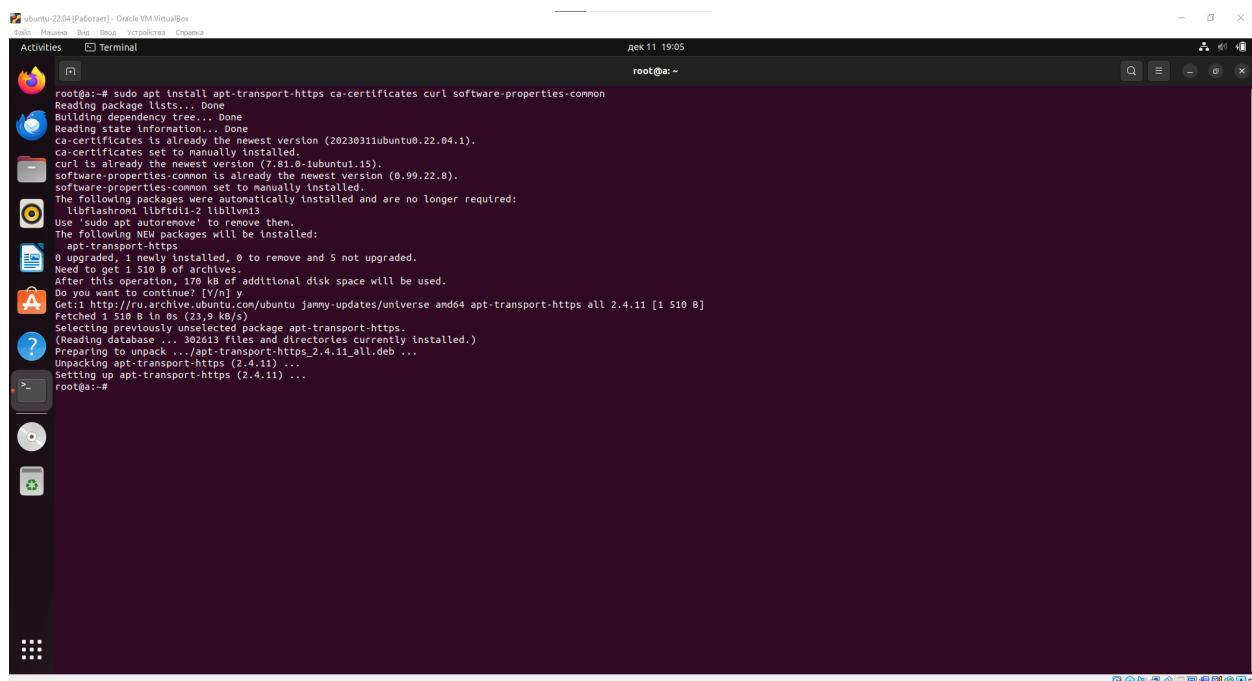
# INT-16

## Тестовое задание №2

## Развернем OWASP ZAP на виртуальной машине с Ubuntu

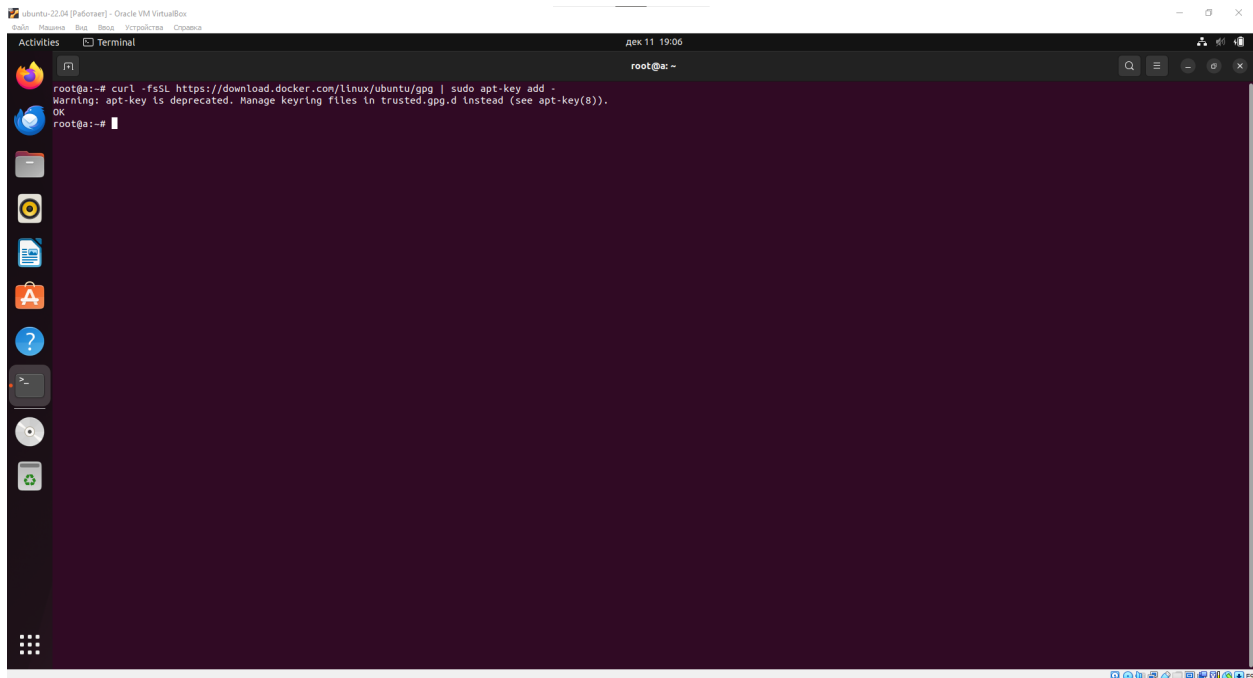
Сначала установим нужные пакеты для работы apt с ключами по HTTPS

```
sudo apt install apt-transport-https ca-certificates curl software-properties-common
```



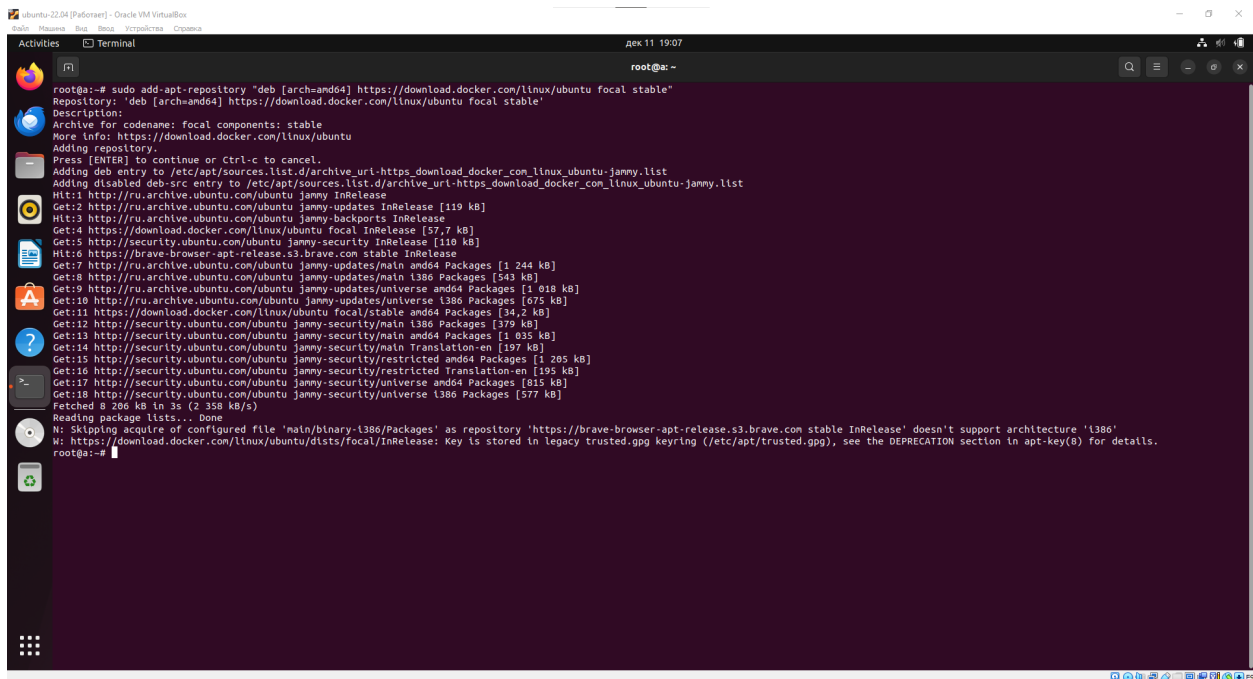
Далее загрузим ключ для репозитория Docker

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
```



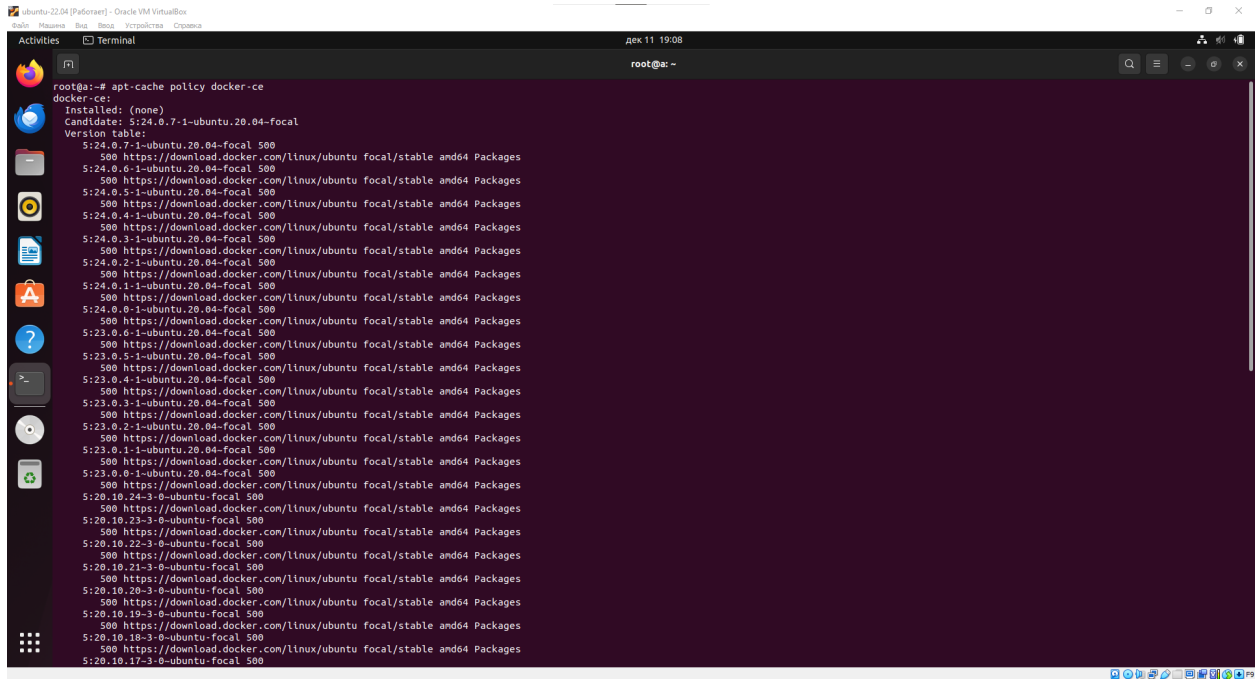
Теперь добавим репозиторий Docker в список репозиторийев apt

```
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"
```



Проверим, что установка Docker будет происходить не из репозитория Ubuntu

```
apt-cache policy docker-ce
```



```
root@a:~# apt-cache policy docker-ce
docker-ce:
  Installed: (none)
  Candidate: 5:24.0.7-1-ubuntu.20.04-focal
  Version table:
   5:24.0.7-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.6-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.5-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.4-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.3-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.2-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.1-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:24.0.0-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.6-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.5-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.4-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.3-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.2-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.1-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:23.0.0-1-ubuntu.20.04-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.24-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.23-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.22-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.21-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.20-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.19-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.18-3-0-ubuntu-focal 500
     500 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages
   5:20.10.17-3-0-ubuntu-focal 500
```

Теперь можно сделать обновление с последующей установкой Docker

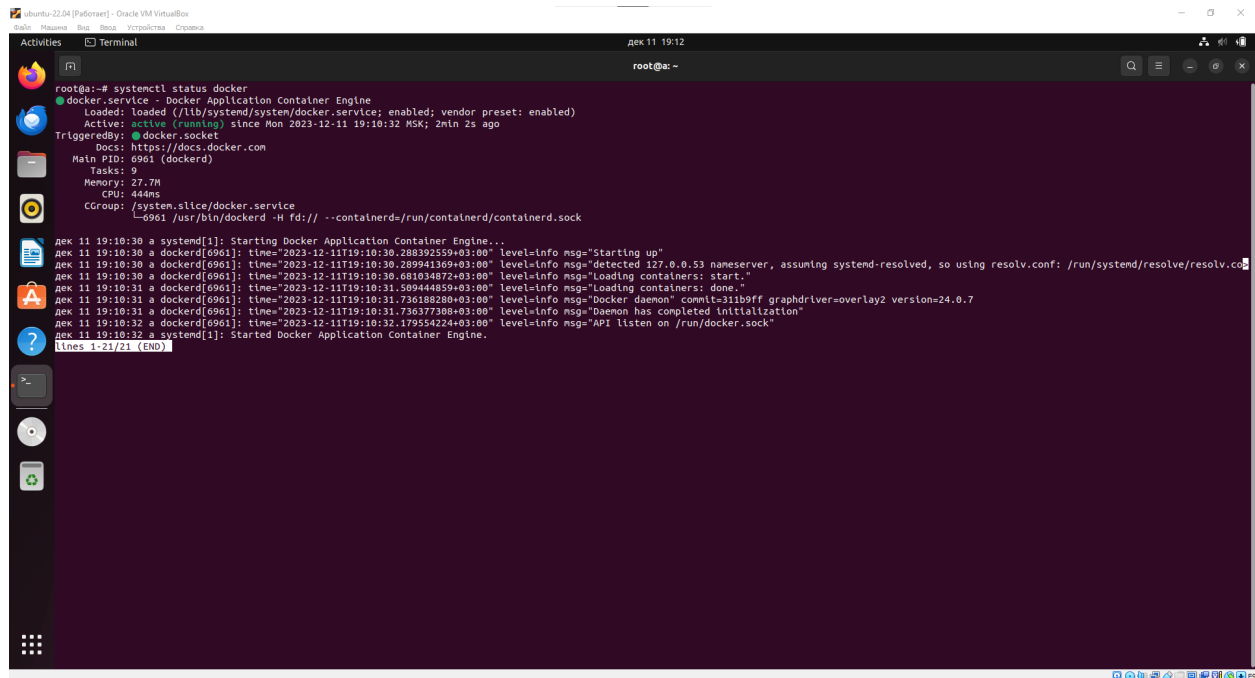
```
sudo apt update
sudo apt install docker-ce
```

```
root@:~# sudo apt update
Hit:1 http://ru.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://ru.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://ru.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 https://download.docker.com/linux/ubuntu focal InRelease
Hit:6 https://brave-browser-apt-release.s3.brave.com stable InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
10 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://download.docker.com/linux/ubuntu/dists/focal/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
E: Skipping acquire of configured file 'main/binary-t386/packages' as repository 'https://brave-browser-apt-release.s3.brave.com stable InRelease' doesn't support architecture 't386'
root@:~#
```

```
root@:~# sudo apt install docker-ce
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashromd libfdt1-2 liblvm13
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  containerd.io docker-buildx-plugin docker-ce-cli docker-ce-rootless-extras docker-compose-plugin git git-man l1berror-perl libslirp0 pigz slirp4netns
Suggested packages:
  aufs-tools cgroup-lite git-daemon-run | git-daemon-sysvinit git-doc git-email git-gui gitk gitweb git-cvs git-mediawiki git-svn
The following NEW packages will be installed:
  containerd.io docker-buildx-plugin docker-ce-cli docker-ce-rootless-extras docker-compose-plugin git git-man l1berror-perl libslirp0 pigz slirp4netns
0 upgraded, 12 newly installed, 0 to remove and 10 not upgraded.
Need to get 119 MB of archives.
After this operation, 432 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu jammy/universe amd64 pigz amd64 2.6-1 [63,6 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 l1berror-perl all 0.17029-1 [26,5 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git-man all 1:2.34.1-1ubuntu1.10 [954 kB]
Get:4 http://ru.archive.ubuntu.com/ubuntu jammy-updates/main amd64 git amd64 1:2.34.1-1ubuntu1.10 [3 166 kB]
Get:5 https://download.docker.com/linux/ubuntu focal/stable amd64 containerd.io amd64 1.6.26-1 [29,5 MB]
Get:6 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 libslirp0 amd64 4.6.1-1build1 [61,5 kB]
Get:7 https://download.docker.com/linux/ubuntu focal/stable amd64 slirp4netns amd64 1.0.1-2 [28,2 kB]
Get:8 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-buildx-plugin amd64 0.11.2-1-ubuntu.20.04-focal [28,2 MB]
Get:9 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce-cli amd64 5:24.0.7-1-ubuntu.20.04-focal [13,3 MB]
Get:10 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce amd64 5:24.0.7-1-ubuntu.20.04-focal [22,6 MB]
Get:11 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-ce-rootless-extras amd64 5:24.0.7-1-ubuntu.20.04-focal [9 037 kB]
Get:12 https://download.docker.com/linux/ubuntu focal/stable amd64 docker-compose-plugin amd64 2.21.0-1-ubuntu.20.04-focal [11,9 MB]
Fetched 119 MB in 20s (6 029 kB/s)
Selecting previously unselected package pigz.
(Reading database ... 302617 files and directories currently installed.)
Preparing to unpack .../00-pigz_2.6-1_amd64.deb ...
Unpacking pigz (2.6-1) ...
Selecting previously unselected package containerd.io.
Preparing to unpack .../01-containerd.io_1.6.26-1_amd64.deb ...
Unpacking containerd.io (1.6.26-1) ...
Selecting previously unselected package docker-buildx-plugin.
Preparing to unpack .../02-docker-buildx-plugin_0.11.2-1-ubuntu.20.04-focal_amd64.deb ...
Unpacking docker-buildx-plugin (0.11.2-1-ubuntu.20.04-focal) ...
Selecting previously unselected package docker-ce-cli.
Preparing to unpack .../03-docker-ce-cli_5:24.0.7-1-ubuntu.20.04-focal_amd64.deb ...
Unpacking docker-ce-cli (5:24.0.7-1-ubuntu.20.04-focal) ...
Selecting previously unselected package docker-ce.
Preparing to unpack .../04-docker-ce_5:24.0.7-1-ubuntu.20.04-focal_amd64.deb ...
Unpacking docker-ce (5:24.0.7-1-ubuntu.20.04-focal) ...
Selecting previously unselected package docker-ce-rootless-extras.
Preparing to unpack .../05-docker-ce-rootless-extras_5:24.0.7-1-ubuntu.20.04-focal_amd64.deb ...
Unpacking docker-ce-rootless-extras (5:24.0.7-1-ubuntu.20.04-focal) ...
Selecting previously unselected package docker-compose-plugin.
Preparing to unpack .../06-docker-compose-plugin_2.21.0-1-ubuntu.20.04-focal_amd64.deb ...
Unpacking docker-compose-plugin (2.21.0-1-ubuntu.20.04-focal) ...
```

## Проверим статус Docker

```
sudo systemctl status docker
```



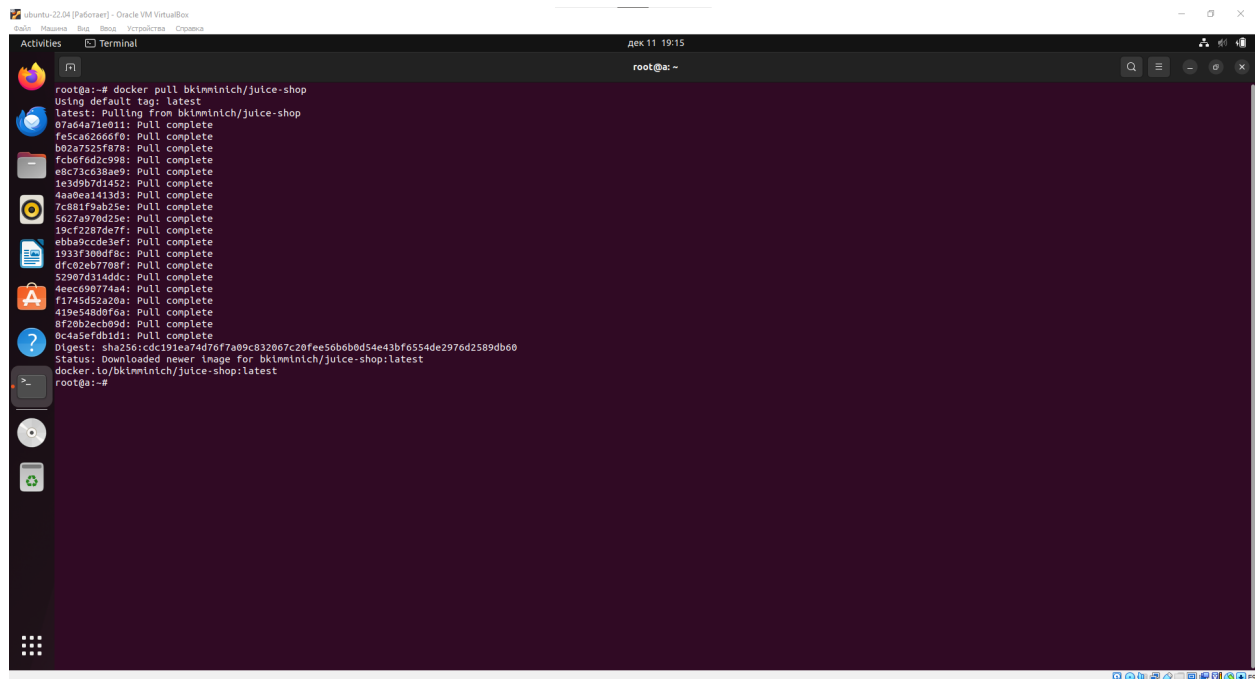
The terminal window shows the command `systemctl status docker` being executed. The output displays the Docker service status as 'active (running)' and provides details about its configuration and logs. The logs show the Docker daemon starting up, including messages about the daemon's version (24.0.7) and the API listening on `/run/docker.sock`.

```
root@:~# systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2023-12-11 19:10:32 MSK; 2min 2s ago
     TriggeredBy: ● docker.socket
     Docs: https://docs.docker.com
   Main PID: 6961 (dockerd)
      Tasks: 9
     Memory: 27.7M
        CPU: 444ms
     CGroup: /system.slice/docker.service
             └─6961 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

дек 11 19:10:30 a systemd[1]: Starting Docker Application Container Engine...
дек 11 19:10:30 a dockerd[6961]: ttime="2023-12-11T19:10:30.288392559+03:00" level=info msg="Starting up"
дек 11 19:10:30 a dockerd[6961]: ttime="2023-12-11T19:10:30.289941369+03:00" level=info msg="detected 127.0.0.53 nameserver, assuming systemd-resolved, so using resolv.conf: /run/systemd/resolv.conf"
дек 11 19:10:30 a dockerd[6961]: ttime="2023-12-11T19:10:30.681034872+03:00" level=info msg="Loading containers: start."
дек 11 19:10:31 a dockerd[6961]: ttime="2023-12-11T19:10:31.509444859+03:00" level=info msg="Loading containers: done."
дек 11 19:10:31 a dockerd[6961]: ttime="2023-12-11T19:10:31.736188280+03:00" level=info msg="Docker daemon" commit=311b9ff graphdriver=overlay2 version=24.0.7
дек 11 19:10:31 a dockerd[6961]: ttime="2023-12-11T19:10:31.736377388+03:00" level=info msg="Daemon has completed initialization"
дек 11 19:10:32 a dockerd[6961]: ttime="2023-12-11T19:10:32.179554224+03:00" level=info msg="API listen on /run/docker.sock"
дек 11 19:10:32 a systemd[1]: Started Docker Application Container Engine.
lines 1-21/21 (END)
```

Установим web-приложение для сервера

```
docker pull bkimminich/juice-shop
```

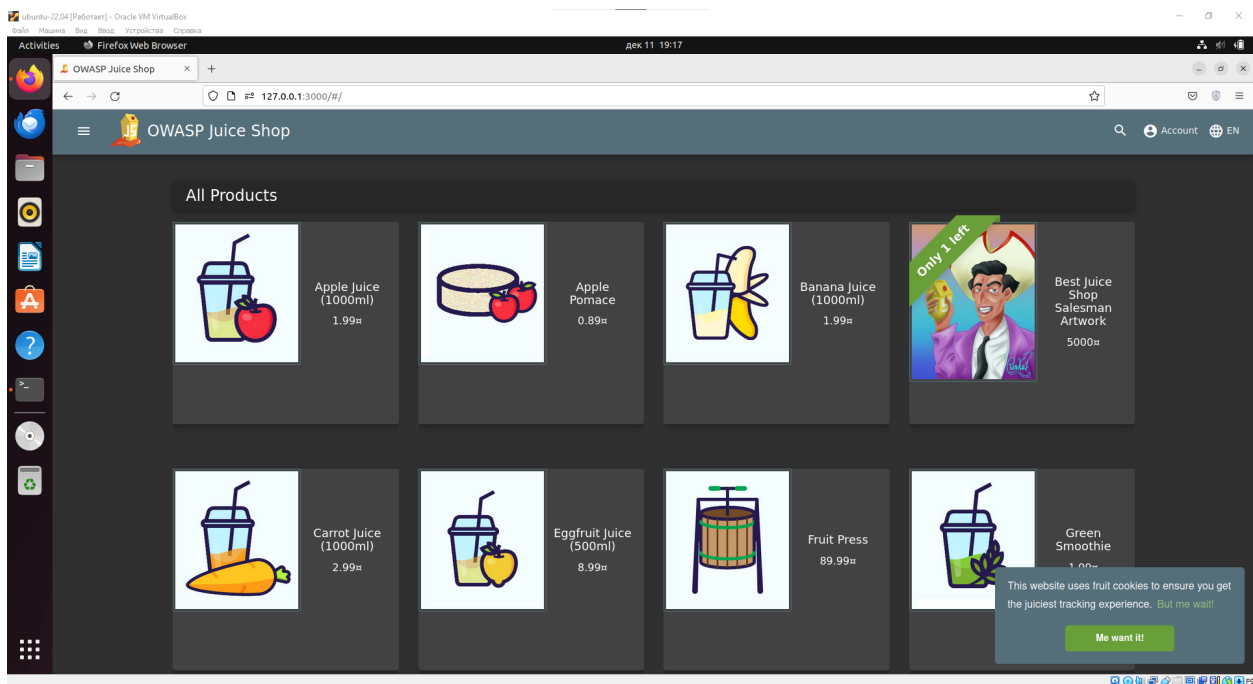
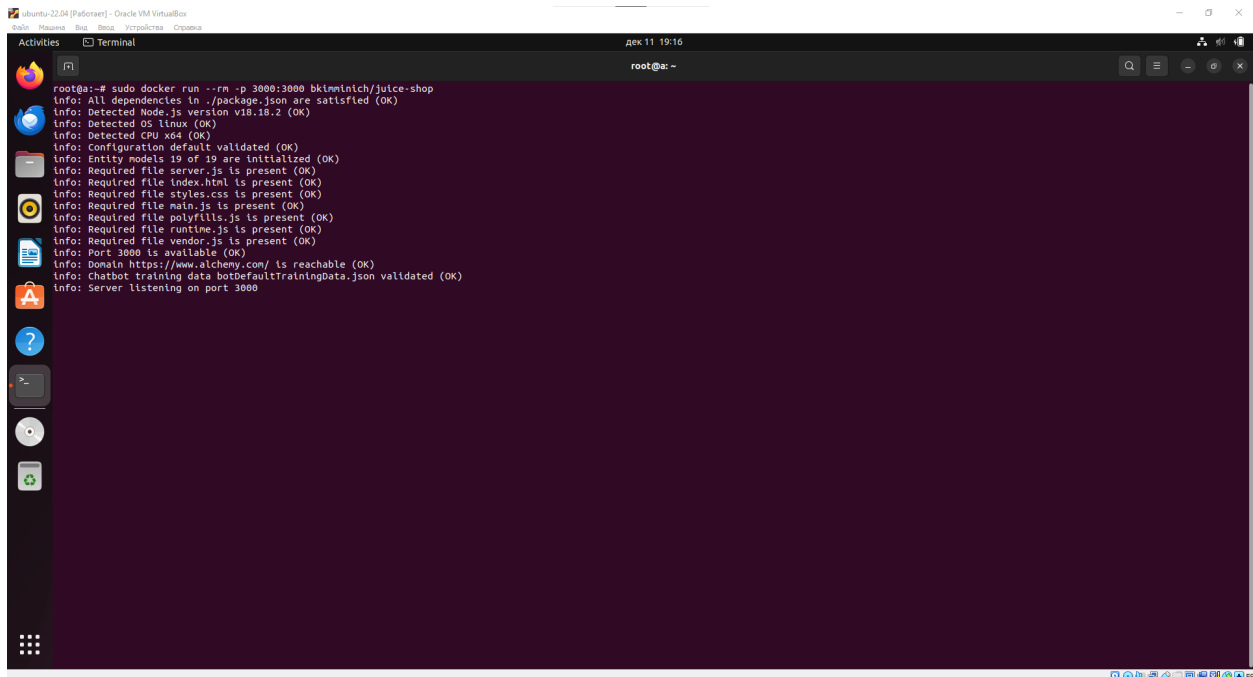


The terminal window shows the command `docker pull bkimminich/juice-shop` being executed. The output displays the progress of pulling the latest image from the Docker Hub repository. The pull is successful, and the image is now available locally.

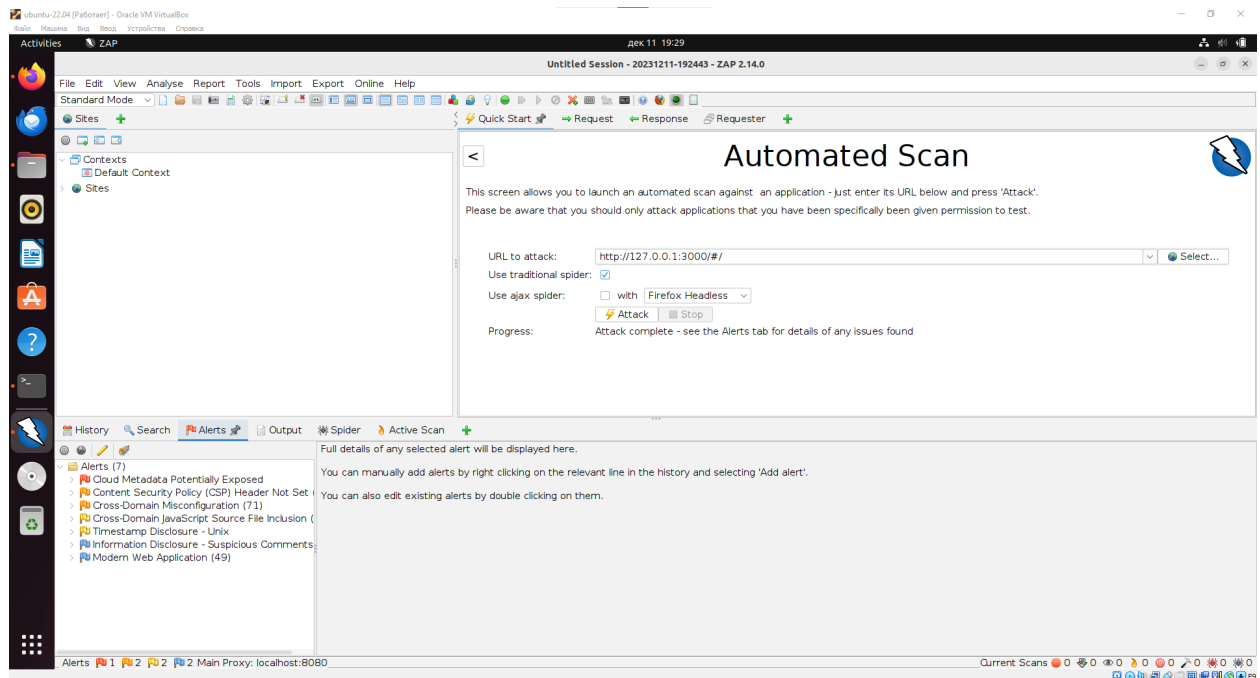
```
root@:~# docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
07a64a71e011: Pull complete
f5c5a62666f0: Pull complete
b02a7525f878: Pull complete
fcb0f6d2c99b: Pull complete
e8c73c638ae9: Pull complete
1e3d9b7d1452: Pull complete
4aa0eas413d9: Pull complete
fcb0f6d2c99b: Pull complete
5627a970d25e: Pull complete
19cf2287de7f: Pull complete
ebba9ecdc3ef: Pull complete
1933f300df8c: Pull complete
dfc02eb7708f: Pull complete
52907d314ddc: Pull complete
4eac690774a4: Pull complete
f1745d52a20a: Pull complete
419e548d0f6a: Pull complete
bf20b2ecb09d: Pull complete
dc4a5efdbd1d: Pull complete
Digest: sha256:cdc191e674d707fa09c832067c20fee56b0bd54e43bf0554de2976d2589db00
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
root@:~#
```

Теперь запустим приложение

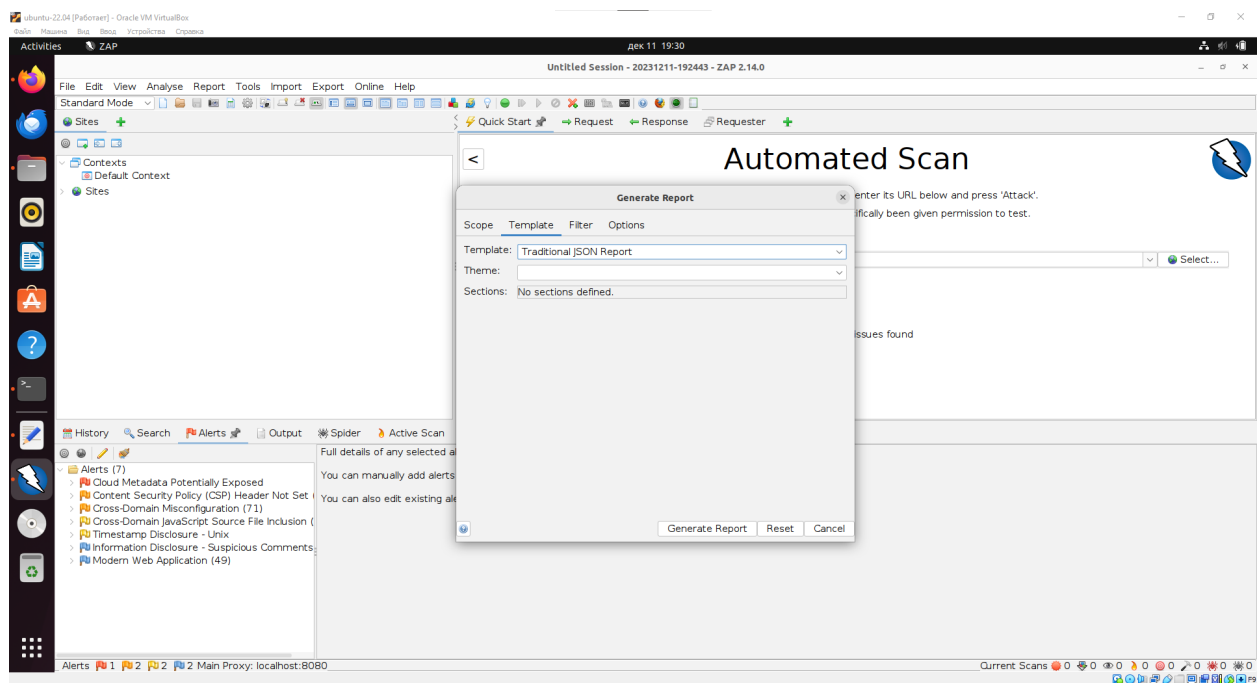
```
sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
```

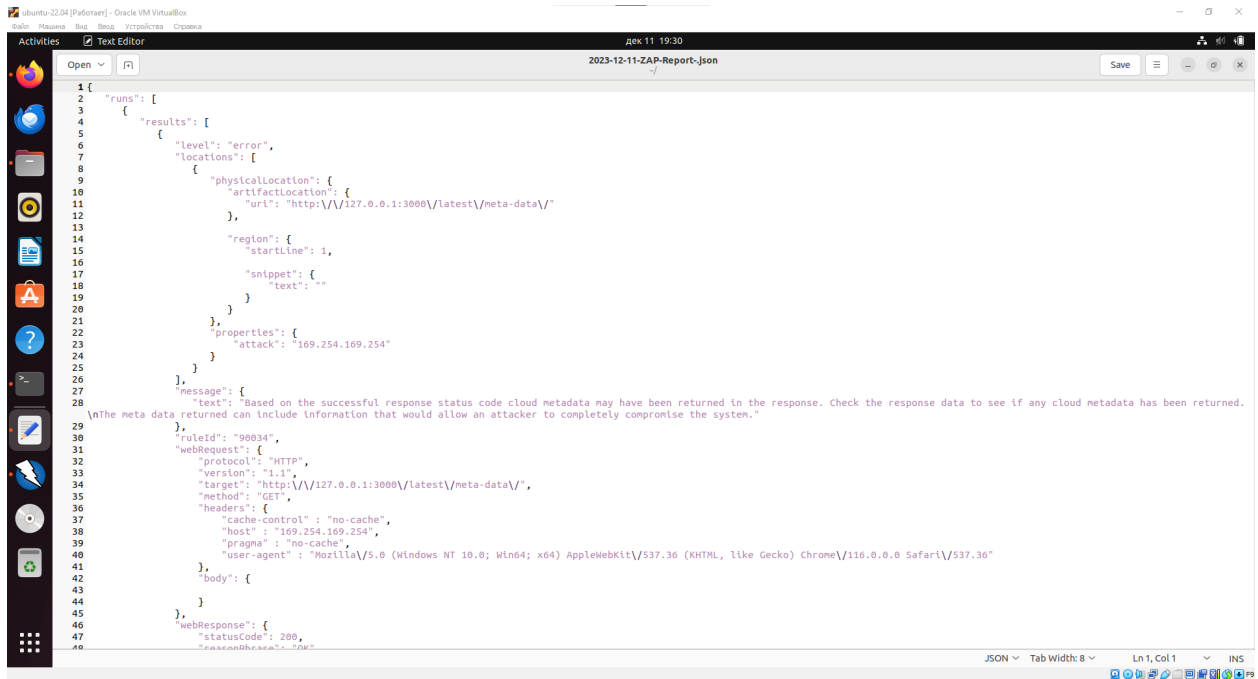


После установки ZAP откроем его и проведем тестирование сайта



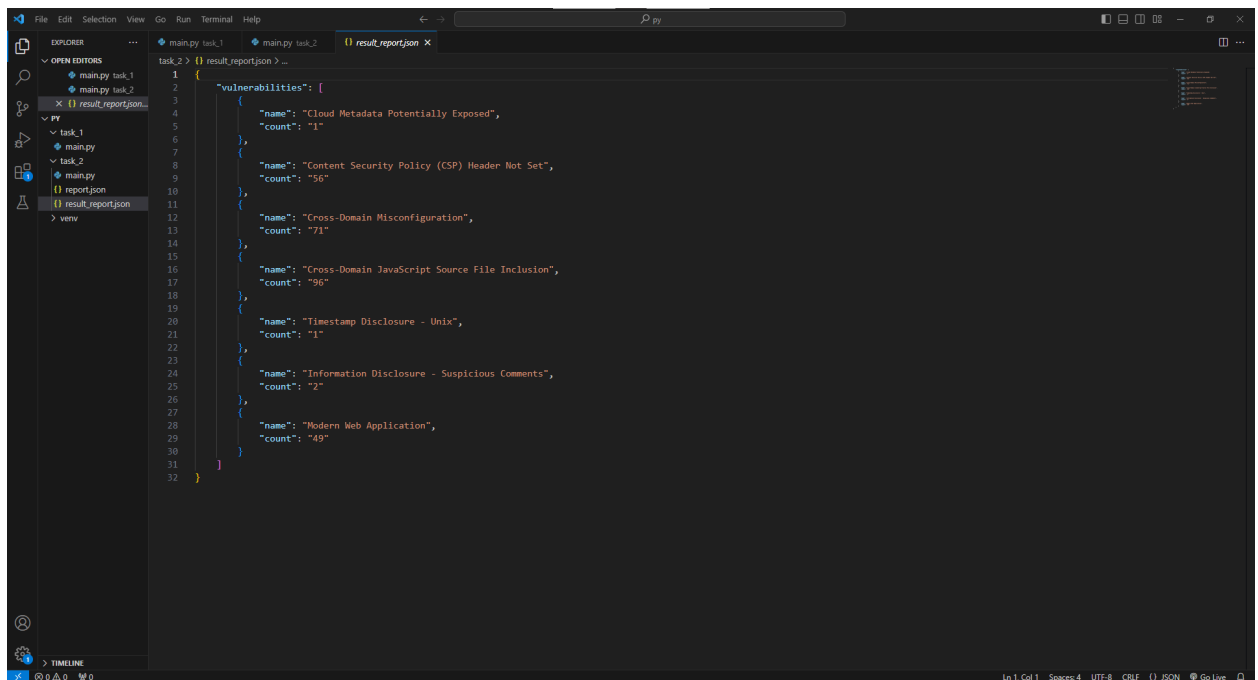
Выгрузим отчет в формате JSON





```
1 {
2   "runs": [
3     {
4       "results": [
5         {
6           "level": "error",
7           "locations": [
8             {
9               "physicalLocation": {
10                "artifactLocation": {
11                  "url": "http://127.0.0.1:3000/latest/meta-data/"
12                },
13                "region": {
14                  "startLine": 1,
15                  "snippet": {
16                    "text": ""
17                  }
18                }
19              },
20              "properties": {
21                "attack": "169.254.169.254"
22              }
23            },
24            "message": {
25              "text": "Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system."
26            },
27            "ruleId": "90034",
28            "webRequest": {
29              "protocol": "HTTP",
30              "version": "1.1",
31              "target": "http://127.0.0.1:3000/latest/meta-data/",
32              "method": "GET",
33              "headers": {
34                "cache-control": "no-cache",
35                "host": "169.254.169.254",
36                "pragma": "no-cache",
37                "user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36"
38              },
39              "body": {
40                "text": ""
41              }
42            },
43            "webResponse": {
44              "statusCode": 200,
45              "contentType": "text/plain"
46            }
47          ]
48        }
49      ]
50    }
51  ]
52 }
```

Пропустим отчет через скрипт и получим



```
1 task2 > {} result_report.json > ...
2 {
3   "vulnerabilities": [
4     {
5       "name": "Cloud Metadata Potentially Exposed",
6       "count": "1"
7     },
8     {
9       "name": "Content Security Policy (CSP) Header Not Set",
10      "count": "56"
11    },
12    {
13      "name": "Cross-Domain Misconfiguration",
14      "count": "71"
15    },
16    {
17      "name": "Cross-Domain JavaScript Source File Inclusion",
18      "count": "96"
19    },
20    {
21      "name": "Timestamp Disclosure - Unix",
22      "count": "1"
23    },
24    {
25      "name": "Information Disclosure - Suspicious Comments",
26      "count": "2"
27    },
28    {
29      "name": "Modern Web Application",
30      "count": "49"
31    }
32  ]
33 }
```