ENTREGABLE 1: Imágenes de 3 containers seguros

Debés generar y subir al registry tres imágenes reforzadas en seguridad correspondientes a:
Front End
API Layer
Database
Qué enviar:
URL de cada imagen en el registry, incluyendo nombre y versión (tag).
Estas imágenes deben poder ser descargadas para su revisión.

ENTREGABLE 2: Escaneo de vulnerabilidades

Realizar un análisis de seguridad de las imágenes para demostrar que están libres de vulnerabilidades críticas/altas.
Podés utilizar el scanner del propio registry o cualquier herramienta que prefieras.
Qué enviar:
Reporte del escaneo, en formato PDF o capturas claras.

ENTREGABLE 3: Docker Compose

Subir a un repo público de GitHub un archivo docker-compose.yml que permita orquestar las tres aplicaciones.
El repositorio debe incluir:
El docker-compose.yml
Un archivo README.md con instrucciones detalladas de uso, instalación y despliegue para que cualquier persona pueda levantar las aplicaciones.
Qué enviar:
URL del repositorio (público)

ENTREGABLE 4: Kubernetes Manifests

Crear los manifiestos necesarios para desplegar las tres aplicaciones en Kubernetes (Deployments, Services, ConfigMaps, Secrets, etc., según corresponda).
Esta entrega también debe estar en un repo público de GitHub, acompañado por un README.md con instrucciones claras de uso y despliegue.

Qué enviar:
URL del repositorio (público)
Resumen de lo que debés compartirnos:
URLs de las imágenes y sus versiones.
URL del repo con Docker Compose.
URL del repo con Kubernetes Manifests.
Reporte del escaneo de vulnerabilidades.

REPOSITORIO GITHUB:
https://github.com/AradiaEtreshka/hackademy-DockerK8s.git

ENTREGABLE 1:

Imágenes subidas al registry público:

- Front End: https://hub.docker.com/r/aradiaetreshka/frontend/tags
  - docker pull aradiaetreshka/frontend:v2
- API Layer: https://hub.docker.com/r/aradiaetreshka/backend/tags
  - docker pull aradiaetreshka/backend:v2
- Database: https://hub.docker.com/r/aradiaetreshka/database/tags
  - docker pull aradiaetreshka/database:v2

ENTREGABLE 2:
REPORTE DE ESCANEO DE VULNERABILIDADES

Se utilizó Aqua Security Trivy para auditar las imágenes antes del despliegue.

- Escaneo de vulnerabilidades Frontend

docker run --rm -v //var/run/docker.sock:/var/run/docker.sock aquasec/trivy image aradiaetreshka/frontend:v2

Report Summary

Target	Type	Vulnerabilities	Secrets
aradiaetreshka/frontend:v2 (alpine 3.22.2)	alpine	11	-

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

aradiaetreshka/frontend:v2 (alpine 3.22.2)

Total: 11 (UNKNOWN: 0, LOW: 3, MEDIUM: 5, HIGH: 3, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
busybox	CVE-2024-58251	MEDIUM	fixed	1.37.0-r19	1.37.0-r20	In netstat in BusyBox through 1.37.0, local users can launch of networ... https://avd.aquasec.com/nvd/cve-2024-58251
	CVE-2025-46394	LOW				In tar in BusyBox through 1.37.0, a TAR archive can have filenames... https://avd.aquasec.com/nvd/cve-2025-46394
busybox-binsh	CVE-2024-58251	MEDIUM				In netstat in BusyBox through 1.37.0, local users can launch of networ... https://avd.aquasec.com/nvd/cve-2024-58251
	CVE-2025-46394	LOW				In tar in BusyBox through 1.37.0, a TAR archive can have filenames... https://avd.aquasec.com/nvd/cve-2025-46394
libpng	CVE-2025-64720	HIGH		1.6.47-r0	1.6.51-r0	libpng: LIBPNG buffer overflow https://avd.aquasec.com/nvd/cve-2025-64720
	CVE-2025-65018					libpng: LIBPNG heap buffer overflow https://avd.aquasec.com/nvd/cve-2025-65018
	CVE-2025-66293				1.6.53-r0	libpng: LIBPNG out-of-bounds read in png_image_read_composite https://avd.aquasec.com/nvd/cve-2025-66293
	CVE-2025-64505	MEDIUM			1.6.51-r0	libpng: LIBPNG heap buffer overflow via malformed palette index https://avd.aquasec.com/nvd/cve-2025-64505
	CVE-2025-64506					libpng: LIBPNG heap buffer over-read https://avd.aquasec.com/nvd/cve-2025-64506
ssl_client	CVE-2024-58251			1.37.0-r19	1.37.0-r20	In netstat in BusyBox through 1.37.0, local users can launch of networ... https://avd.aquasec.com/nvd/cve-2024-58251
	CVE-2025-46394	LOW				In tar in BusyBox through 1.37.0, a TAR archive can have filenames... https://avd.aquasec.com/nvd/cve-2025-46394

Análisis Técnico: El escaneo reporta 0 Vulnerabilidades Críticas.

- Escaneo de vulnerabilidades Backend

docker run --rm -v //var/run/docker.sock:/var/run/docker.sock aquasec/trivy image aradiaetreshka/backend:v2

Report Summary

Target	Type	Vulnerabilities	Secrets
aradiaetreshka/backend:v2 (alpine 3.23.0)	alpine	0	-
home/aradia/backend-app	gobinary	0	-

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

Análisis Técnico: Resultado Clean (Total: 0).

- Escaneo de vulnerabilidades database

docker run --rm -v //var/run/docker.sock:/var/run/docker.sock aquasec/trivy image aradiaetreshka/database:v2

Report Summary

Target	Type	Vulnerabilities	Secrets
aradiaetreshka/database:v2 (oracle 9.7)	oracle	1	-
usr/lib/mysqlsh/lib/python3.13/site-packages/antlr4_python3_runtime-4.13.2.dist--info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/bcrypt-4.3.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/certifi-2025.8.3.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/cffi-2.0.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/charset_normalizer-3.4.3.dist-info-/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/circuitbreaker-2.1.3.dist-info/MET-ADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/cryptography-44.0.3.dist-info/META-DATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/idna-3.10.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/invoke-2.2.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/oci-2.160.1.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/paramiko-4.0.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/pip-24.2.dist-info/METADATA	python-pkg	1	-
usr/lib/mysqlsh/lib/python3.13/site-packages/proxmoxer-2.2.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/pycparser-2.23.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/pynacl-1.5.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/pyopenssl-24.3.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/python_dateutil-2.9.0.post0.dist-i-nfo/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/pytz-2025.2.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/pyyaml-6.0.2.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/requests-2.32.5.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/six-1.17.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/svg_py-1.6.0.dist-info/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/typing_extensions-4.12.2.dist-info-/METADATA	python-pkg	0	-
usr/lib/mysqlsh/lib/python3.13/site-packages/urllib3-2.5.0.dist-info/METADATA	python-pkg	2	-
usr/local/bin/gosu	gobinary	12	-

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

aradiaetreshka/database:v2 (oracle 9.7)
==========
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
systemd-libs	CVE-2025-4598	MEDIUM	fixed	252-55.0.3.el9_7.2	252-55.0.3.el9_7.7	systemd-coredump: race condition that allows a local attacker to crash a SUID... https://avd.aquasec.com/nvd/cve-2025-4598

Python (python-pkg)
==========
Total: 3 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 2, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
pip (METADATA)	CVE-2025-8869	MEDIUM	fixed	24.2	25.3	pip: pip missing checks on symbolic link extraction https://avd.aquasec.com/nvd/cve-2025-8869
urllib3 (METADATA)	CVE-2025-66418	HIGH		2.5.0	2.6.0	urllib3 is a user-friendly HTTP client library for Python. Starting in https://avd.aquasec.com/nvd/cve-2025-66418
	CVE-2025-66471					urllib3 is a user-friendly HTTP client library for Python. Starting in https://avd.aquasec.com/nvd/cve-2025-66471

usr/local/bin/gosu (gobinary)
==========
Total: 12 (UNKNOWN: 0, LOW: 0, MEDIUM: 8, HIGH: 4, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
stdlib	CVE-2025-58183	HIGH	fixed	v1.24.6	1.24.8, 1.25.2	golang: archive/tar: Unbounded allocation when parsing GNU sparse map https://avd.aquasec.com/nvd/cve-2025-58183
	CVE-2025-58186					Despite HTTP headers having a default limit of 1MB, the number of... https://avd.aquasec.com/nvd/cve-2025-58186
	CVE-2025-58187				1.24.9, 1.25.3	Due to the design of the name constraint checking algorithm, the proce... https://avd.aquasec.com/nvd/cve-2025-58187
	CVE-2025-61729				1.24.11, 1.25.5	Within HostnameError.Error(), when constructing an error string, there ... https://avd.aquasec.com/nvd/cve-2025-61729
	CVE-2025-47912	MEDIUM			1.24.8, 1.25.2	net/url: Insufficient validation of bracketed IPv6 hostnames in net/url https://avd.aquasec.com/nvd/cve-2025-47912
	CVE-2025-58185					encoding/asn1: Parsing DER payload can cause memory exhaustion in encoding/asn1 https://avd.aquasec.com/nvd/cve-2025-58185
	CVE-2025-58188					crypto/x509: golang: Panic when validating certificates with DSA public keys in crypto/x509... https://avd.aquasec.com/nvd/cve-2025-58188
	CVE-2025-58189					crypto/tls: go crypto/tls ALPN negotiation error contains attacker controlled information https://avd.aquasec.com/nvd/cve-2025-58189
	CVE-2025-61723					encoding/pem: Quadratic complexity when parsing some invalid inputs in encoding/pem https://avd.aquasec.com/nvd/cve-2025-61723
	CVE-2025-61724					net/textproto: Excessive CPU consumption in Reader.ReadResponse in net/textproto https://avd.aquasec.com/nvd/cve-2025-61724
	CVE-2025-61725					net/mail: Excessive CPU consumption in ParseAddress in net/mail https://avd.aquasec.com/nvd/cve-2025-61725
	CVE-2025-61727				1.24.11, 1.25.5	An excluded subdomain constraint in a certificate chain does not restr https://avd.aquasec.com/nvd/cve-2025-61727

Análisis Técnico: Se valida la ausencia de vulnerabilidades Críticas. Las vulnerabilidades de nivel Medio/Alto detectadas corresponden a la utilidad gosu y librerías auxiliares del sistema operativo base (Oracle Linux).

ENTREGABLE 3 y 4 se encuentran los archivos de manifiestos y compose en el repositorio:
https://github.com/AradiaEtreshka/hackademy-DockerK8s.git