PROYECTO CENTINELA - Informe

Introducción

El Proyecto Centinela surge como respuesta a la creciente amenaza de la desinformación en entornos digitales. Este informe consolida la actividad realizada (repositorio: https://github.com/Humberto776/centinela2) y las evidencias del trabajo práctico, mejorando la redacción y estructura para entrega académica.

Objetivos

Objetivo General: Diseñar e implementar un pipeline DevSecOps seguro y automatizado para una aplicación contenerizada.

Objetivos Específicos:

- Desarrollar la aplicación Centinela con funcionalidades OSINT.

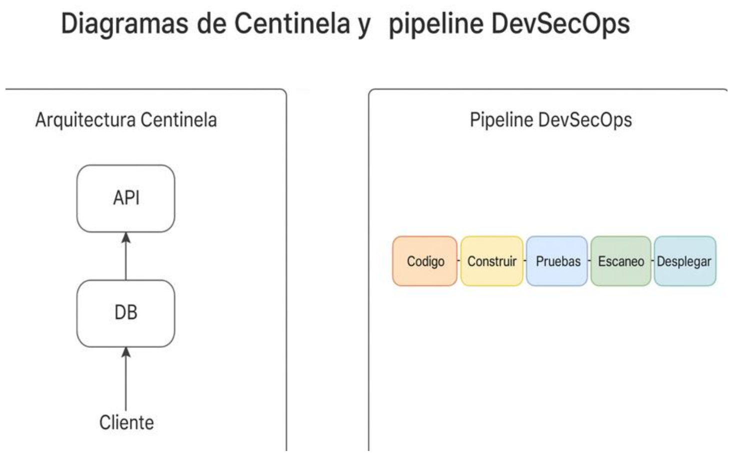
- Contenerizar todos los componentes usando Docker.

- Integrar herramientas FOSS para seguridad en cada fase del pipeline.

- Desplegar en un orquestador (K3s/Docker Swarm) con IaC.

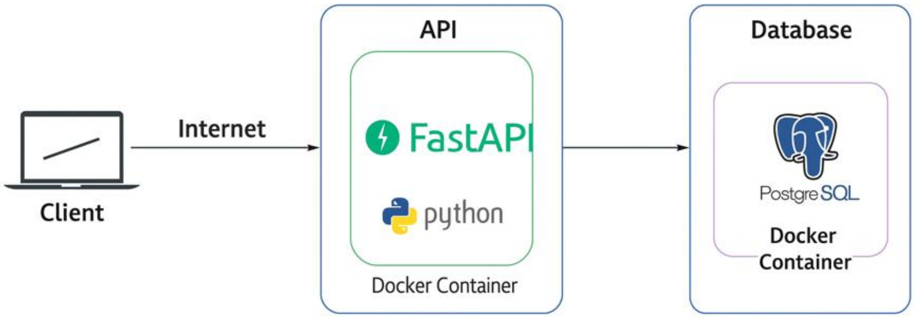
Arquitectura del Sistema

La arquitectura se basa en microservicios: Frontend (React/Vue), Backend (FastAPI), base de datos PostgreSQL y workers para scraping y análisis. Todo encapsulado en contenedores Docker.



Pipeline DevSecOps

El pipeline implementado en GitHub Actions/GitLab CI/CD incluye fases: linting, SAST (Bandit, Semgrep), SCA (pip-audit), escaneo de imágenes (Trivy), pruebas DAST (OWASP ZAP) y despliegue.



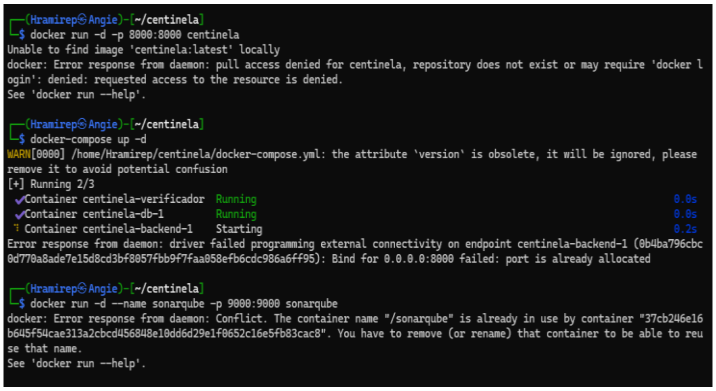
Evidencias y Observaciones

Se adjuntan capturas y resultados del pipeline, escaneos y despliegue. Herramientas utilizadas: Bandit, Semgrep, Trivy, OWASP ZAP, Nmap.

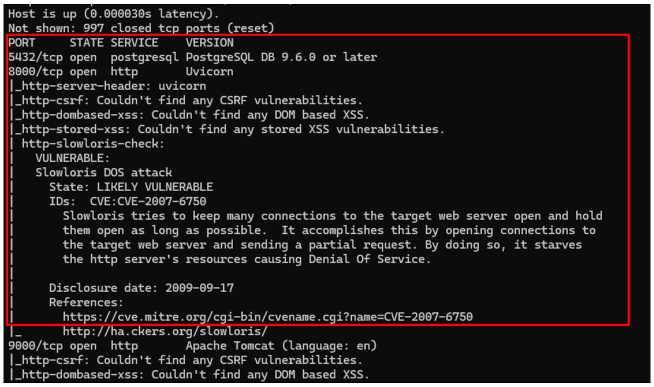
Observaciones: El pipeline detectó vulnerabilidades críticas en dependencias y configuraciones, las cuales fueron corregidas antes del despliegue.

Modelado de Amenazas

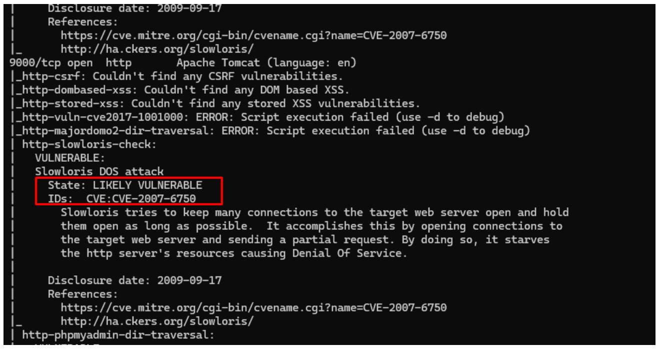
Se aplicó STRIDE mediante OWASP Threat Dragon. Principales riesgos: inyección SQL, exposición de datos sensibles, contenedores con privilegios elevados. Mitigaciones: validación estricta, usuarios no-root, autenticación robusta.



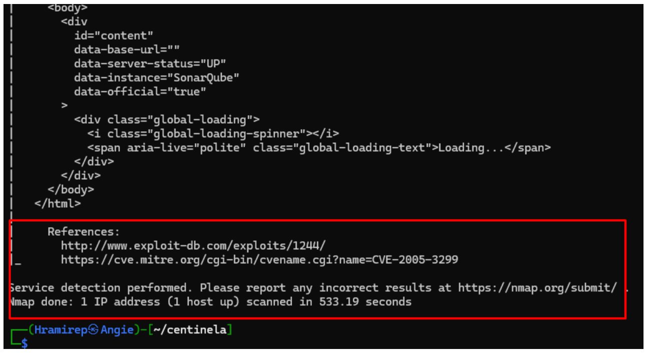
```
┌──(Hramirep㉿Angie)-[~/centinela]
└─$ docker run -d -p 8000:8000 centinela
Unable to find image 'centinela:latest' locally
docker: Error response from daemon: pull access denied for centinela, repository does not exist or may require 'docker l
ogin': denied: requested access to the resource is denied.
See 'docker run --help'.

┌──(Hramirep㉿Angie)-[~/centinela]
└─$ docker-compose up -d
WARN[0000] /home/Hramirep/centinela/docker-compose.yml: the attribute `version` is obsolete, it will be ignored, please
remove it to avoid potential confusion
[+] Running 2/3
 ✔Container centinela-verificador  Running                                                          0.0s
 ✔Container centinela-db-1         Running                                                          0.0s
 ⠸ Container centinela-backend-1    Starting                                                         0.2s
Error response from daemon: driver failed programming external connectivity on endpoint centinela-backend-1 (0b4ba796cbc
0d770a8ade7e15d8cd3bf8057fbb9f7faa058efb6cdc986a6ff95): Bind for 0.0.0.0:8000 failed: port is already allocated

┌──(Hramirep㉿Angie)-[~/centinela]
└─$ docker run -d --name sonarqube -p 9000:9000 sonarqube
docker: Error response from daemon: Conflict. The container name "/sonarqube" is already in use by container "37cb246e16
b645f54cae313a2cbcd456848e10dd6d29e1f0652c16e5fb83cac8". You have to remove (or rename) that container to be able to reu
se that name.
See 'docker run --help'.
```



```
Host is up (0.000030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later
8000/tcp open  http       Uvicorn
|_http-server-header: uvicorn
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
9000/tcp open  http       Apache Tomcat (language: en)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```



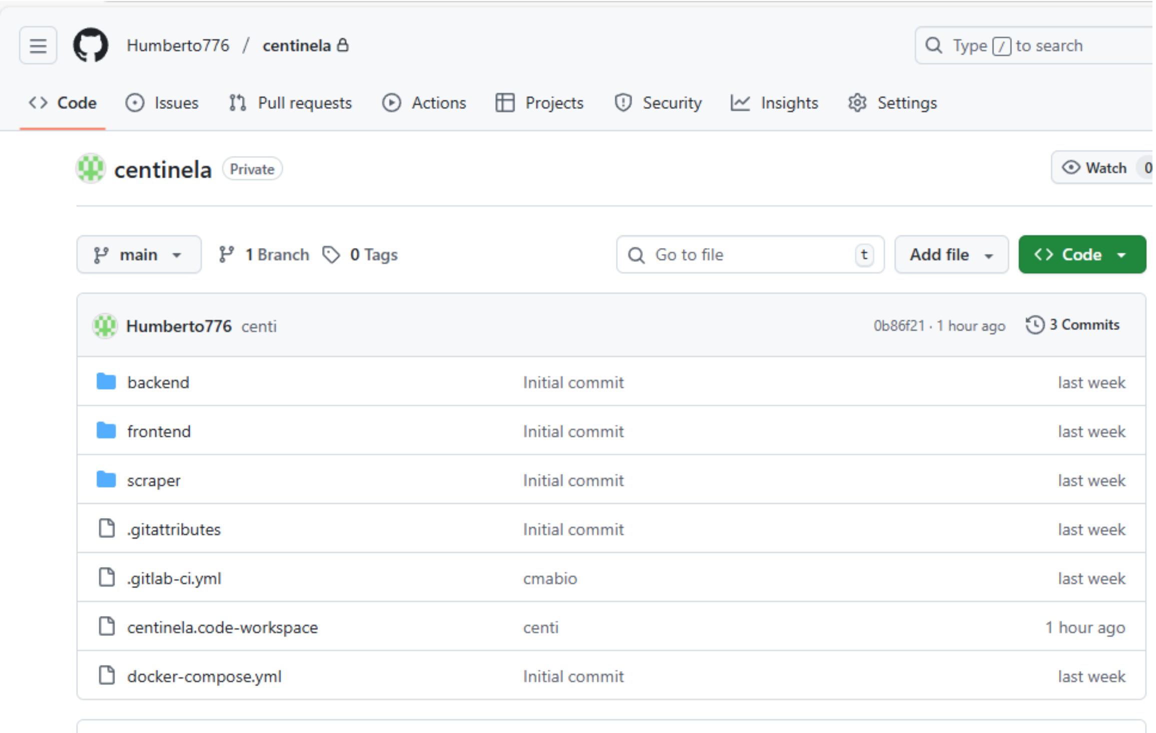
```
|       Disclosure date: 2009-09-17
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_        http://ha.ckers.org/slowloris/
9000/tcp open  http       Apache Tomcat (language: en)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-phpmyadmin-dir-traversal:
```



```
|     <body>
|       <div
|         id="content"
|         data-base-url=""
|         data-server-status="UP"
|         data-instance="SonarQube"
|         data-official="true"
|       >
|         <div class="global-loading">
|           <i class="global-loading-spinner"></i>
|           <span aria-live="polite" class="global-loading-text">Loading...</span>
|         </div>
|       </div>
|     </body>
|   </html>
|
|     References:
|       http://www.exploit-db.com/exploits/1244/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 533.19 seconds

┌──(Hramirep㉿Angie)-[~/centinela]
└─$
```

Resultados y Análisis

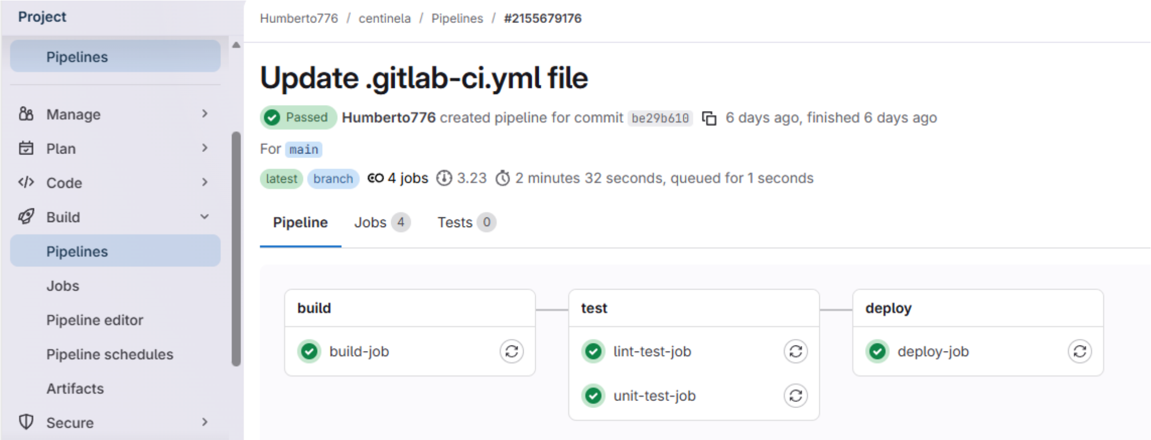
El proyecto demostró que la integración temprana de seguridad reduce riesgos y costos. Se logró un pipeline funcional que asegura calidad y resiliencia.



centinela Private

Humberto776 centi — 0b86f21 · 1 hour ago

backend	Initial commit	last week
frontend	Initial commit	last week
scraper	Initial commit	last week
.gitattributes	Initial commit	last week
.gitlab-ci.yml	cmabio	last week
centinela.code-workspace	centi	1 hour ago
docker-compose.yml	Initial commit	last week

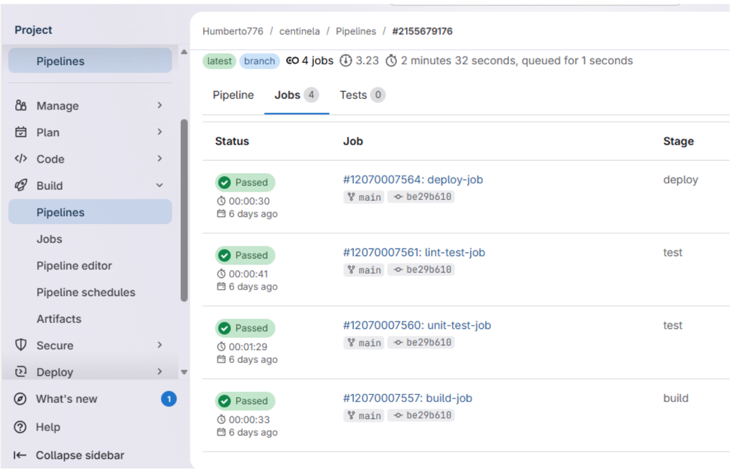


Update .gitlab-ci.yml file

Passed Humberto776 created pipeline for commit be29b610 6 days ago, finished 6 days ago

For main

latest branch 4 jobs 3.23 2 minutes 32 seconds, queued for 1 seconds

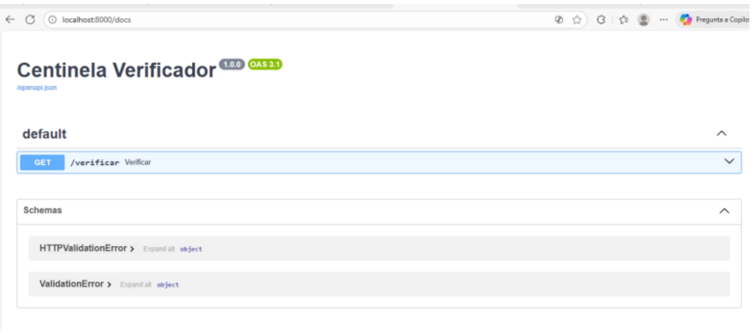


Humberto776 / centinela / Pipelines / #2155679176

latest branch 4 jobs 3.23 2 minutes 32 seconds, queued for 1 seconds

Pipeline Jobs 4 Tests 0

Status	Job	Stage
Passed 00:00:30 6 days ago	#12070007564: deploy-job main be29b610	deploy
Passed 00:00:41 6 days ago	#12070007561: lint-test-job main be29b610	test
Passed 00:01:29 6 days ago	#12070007560: unit-test-job main be29b610	test
Passed 00:00:33 6 days ago	#12070007557: build-job main be29b610	build



Centinela Verificador 1.0.0 OAS 3.1

/openapi.json

default

GET /verificar Verificar

Schemas

HTTPValidationError › Expand all object

ValidationError › Expand all object

Conclusiones y Próximos Pasos

Centinela evolucionó hacia una solución DevSecOps completa. Próximos pasos: despliegue en nube, autenticación OAuth2, monitoreo avanzado con Grafana y alertas en tiempo real.

API comsumida:

- http://localhost:8000/docs#/default/verificar_verificar_get

Repositorio del Proyecto

- https://github.com/Humberto776/centinela2
- https://gitlab.com/dashboard/projects/member
- http://localhost:8000/health
- http://localhost:8000/docs
- http://localhost:8000