Trivy vs Snyk

Confronto tra due scanner di vulnerabilità per container

Giovanni Bellini
Matricola: 600035
ICT Risk Assessment
Corso di laurea magistrale in Informatica
Università degli Studi di Pisa

Febbraio 2024

Indice

Capitolo 1

Introduzione

In un'epoca in cui il software permea ogni aspetto della nostra vita quotidiana, la sicurezza informatica è diventata una pietra angolare nello sviluppo e nel deployment delle applicazioni. La continua espansione dell'utilizzo dei container e delle microservizi ha portato alla necessità di strumenti sofisticati capaci di identificare e mitigare le vulnerabilità in modo efficace ed efficiente. Questo report si propone di esplorare e confrontare due dei più rilevanti strumenti nel panorama della sicurezza informatica: Trivy e Snyk. Entrambi gli strumenti hanno guadagnato notorietà per la loro capacità di fornire analisi dettagliate e soluzioni alle vulnerabilità di sicurezza in applicazioni e container, ma presentano approcci, caratteristiche e punti di forza distinti.

1.1 Trivy

Trivy, sviluppato da Aqua Security, è un scanner di vulnerabilità semplice e completo, che si distingue per la sua facilità d'uso e la capacità di integrarsi senza soluzione di continuità in vari ambienti di sviluppo e pipeline CI/CD. La sua progettazione si concentra sulla velocità e sull'efficacia della scansione di immagini di container, repository Git, filesystem e configurazioni Infrastructure as Code (IaC), rendendolo uno strumento versatile per gli sviluppatori e i team di sicurezza.

1.2 Snyk

Snyk si posiziona come una soluzione SaaS di sicurezza per lo sviluppo software che enfatizza la collaborazione tra sviluppatori e professionisti della sicurezza. Offre una vasta gamma di funzionalità che vanno oltre la semplice scansione delle vulnerabilità, inclusa la gestione delle dipendenze, la correzione automatica e l'integrazione profonda con ambienti di sviluppo, sistemi di gestione del codice sorgente e pipeline di CI/CD. Snyk mira a dotare

i team di strumenti proattivi per affrontare le vulnerabilità all'interno del loro codice, delle dipendenze open source, dei container e delle configurazioni IaC.

Il confronto tra Trivy e Snyk richiede un'analisi approfondita delle loro capacità tecniche, facilità d'uso, integrazione con gli ambienti di sviluppo esistenti, e l'impatto sul flusso di lavoro di sviluppo e sicurezza. Questo report valuterà questi aspetti attraverso una metodologia dettagliata che include test empirici, interviste con gli utenti e l'analisi della documentazione ufficiale e delle recensioni della comunità. L'obiettivo è fornire una panoramica esauriente che aiuti gli sviluppatori, i team di sicurezza e le organizzazioni a prendere decisioni informate sulla scelta dello strumento più adatto alle loro esigenze specifiche nel contesto della sicurezza delle applicazioni e dei container.

Capitolo 2

Confronto

2.1 Il database

Il database di entrambi gli strumenti è un aspetto cruciale per la qualità e l'accuratezza delle analisi di vulnerabilità. Trivy e Snyk utilizzano database di vulnerabilità differenti, che influenzano la loro capacità di identificare e classificare le vulnerabilità. Trivy si basa su VulnDB, un database di vulnerabilità curato da Risk Based Security, che offre una copertura dettagliata e aggiornata delle vulnerabilità di sicurezza. Snyk, d'altro canto, utilizza un database di vulnerabilità proprietario, che combina dati provenienti da diverse fonti, inclusi i database NVD, NPM, RubyGems e altri. Questo approccio permette a Snyk di offrire una copertura più ampia e dettagliata delle vulnerabilità, ma può comportare un rischio di falsi positivi e falsi negativi, a causa della complessità e della varietà dei dati raccolti. Trivy, invece, offre una copertura più limitata, ma più accurata e affidabile, grazie alla cura e all'attenzione dedicata da Risk Based Security alla qualità dei dati e alla loro classificazione. In questa parte di testing, si è voluto valutare la capacità di Trivy e Snyk di identificare e classificare le vulnerabilità in base al database utilizzato. Per fare ciò, si è utilizzato un campione di immagini di container e repository Git, contenenti vulnerabilità note e ben documentate, e si è confrontato il risultato delle scansioni di Trivy e Snyk con le informazioni disponibili nei database VulnDB e Snyk. I risultati di questo test sono stati valutati in base alla precisione, alla completezza e alla tempestività delle informazioni fornite da Trivy e Snyk, e alla loro capacità di identificare e classificare le vulnerabilità in base al database utilizzato. L'aggiornamento dei database avviene per ogni tool in modo differente. Trivy, infatti, controlla la presenza di aggiornamenti del database ad ogni esecuzione, e scarica automaticamente la versione più recente. Snyk, invece, offre la possibilità di aggiornare manualmente il database, ma non è possibile controllare la presenza di aggiornamenti in modo automatico.

Le immagini Docker sottoposte a scansione sono state selezionate in base alla loro

popolarità e alla loro rilevanza nel panorama delle applicazioni e dei servizi cloud. In particolare, si è scelto di testare le seguenti immagini:

- **nginx:latest**: una delle immagini di container più popolari e utilizzate, che offre un server web leggero e performante basato su Nginx.
- **mongo:latest**: una delle immagini di container più popolari e utilizzate, che offre un database NoSQL flessibile e scalabile basato su MongoDB.
- **wordpress:latest**: una delle immagini di container più popolari e utilizzate, che offre una piattaforma di blogging e CMS basata su WordPress.
- **alpine:latest**: una delle immagini di container più leggere e minimali, basata su Alpine Linux, che offre un ambiente di esecuzione ideale per applicazioni e servizi cloud.
- **centos:latest**: una delle immagini di container più stabili e affidabili, basata su CentOS, che offre un ambiente di esecuzione robusto e ben supportato per applicazioni e servizi cloud.

I risultati rilevati da entrambi i tool sono riportati nella tabella seguente:

2.2 Utilizzo in pipeline CI/CD

2.3 Differenze di funzionalità

Durante il testing, sono state rilevate le seguenti funzionalità uniche per ciascuno strumento:

2.3.1 Trivy: scansione di cluster Kubernetes

Trivy offre la possibilità di eseguire la scansione di un intero cluster Kubernetes, identificando e classificando le vulnerabilità presenti nei pod, nei deployment e nei servizi. Questa funzionalità è particolarmente utile per i team di sicurezza e per gli amministratori di sistema, che possono utilizzare Trivy per identificare e mitigare le vulnerabilità in modo proattivo, prima che possano essere sfruttate da attaccanti. Durante il testing, si è verificato che Trivy è in grado di eseguire la scansione di un cluster Kubernetes in modo rapido ed efficiente, fornendo un report dettagliato delle vulnerabilità rilevate e delle azioni consigliate per mitigarle.

2.3.2 Trivy: Scansione delle Configurazioni Infrastructure as Code (IaC)

Trivy offre la possibilità di eseguire la scansione delle configurazioni Infrastructure as Code (IaC), identificando e classificando le vulnerabilità presenti nei file di configurazione di Terraform, CloudFormation e altri strumenti di automazione dell'infrastruttura. Questa funzionalità è particolarmente utile per i team di sviluppo e per gli amministratori di sistema, che possono utilizzare Trivy per identificare e mitigare le vulnerabilità nelle configurazioni IaC, prima che possano essere sfruttate da attaccanti. Durante il testing, si è verificato che Trivy è in grado di eseguire la scansione delle configurazioni IaC in modo rapido ed efficiente, fornendo un report dettagliato delle vulnerabilità rilevate e delle azioni consigliate per mitigarle.

2.3.3 Trivy:

2.3.4 Snyk: Monitoraggio Continuo

Snyk offre un monitoraggio continuo delle applicazioni e delle dipendenze, inviando notifiche in tempo reale in caso di nuove vulnerabilità che influenzano il codice già in uso. Questo assicura che i team possano reagire rapidamente a nuove minacce. Durante il testing, è stato possibile osservare il funzionamento di questa funzione, avendo ricevuto e-mail contenenti nuove vulnerabilità pubblicate solamente giorni prima, come riportato in figura 2.1.

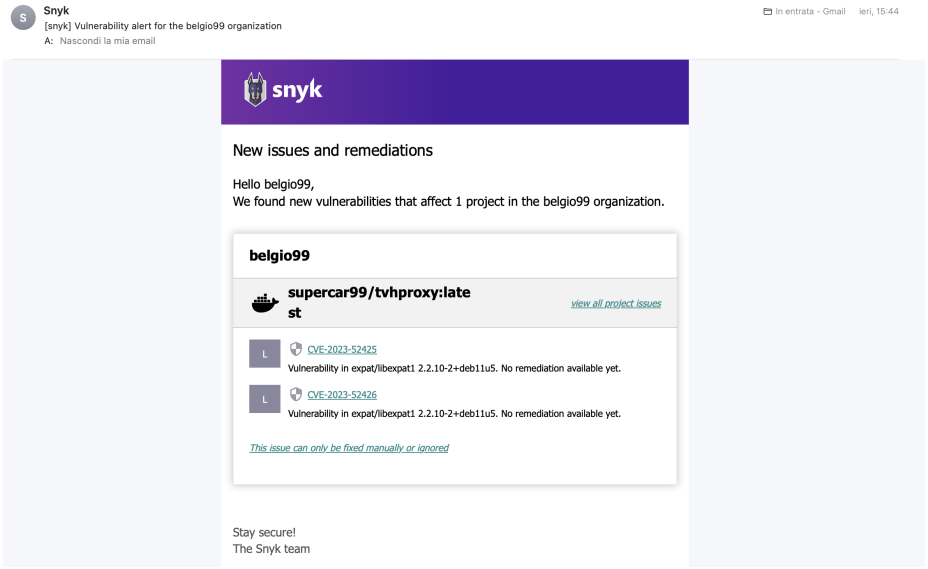

Figura 2.1: E-mail ricevuta da Snyk contenente notifica di rilevazione di nuove vulnerabilità

Dopo la ricezione della e-mail, è stata subito eseguita una scansione con Trivy, che ha confermato la presenza delle vulnerabilità segnalate da Snyk. Questo conferma che entrambi i database utilizzati da Trivy e Snyk sono aggiornati tempestivamente.