

#1 Code Security

#1 Code Security

코드는 클라우드 기반이든 아니든 응용 프로그램의 가장 내부적인 부분 또는 레이어 중 하나입니다. 또한 조직에게 가장 큰 보안 통제를 제공하는 주요 공격 표면 중 하나입니다. 개발자 또는 보안 팀은 노출된 각 서비스, API 엔드포인트 및 기타 부분, 그리고 API 엔드포인트를 통해 엄격한 액세스 관리 및 위협 모니터링을 통해 보안 문제를 최소화할 수 있습니다. 모든 통신에 대해 내부 또는 외부 모두를 위한 TLS 암호화가 코드 보안의 추가적인 레이어를 보장하기 위한 표준이 되어야 합니다.

코드 품질과 보안은 무엇인가요?

코드 품질과 보안은 두 가지 매우 다른 but 연결된 코드 개발 프로세스 측면입니다. 코드 품질은 개발자들에게 중요한 고려 사항이며, 코드 보안은 테스트 부서의 고민거리입니다. 현재 점점 내장된 시장에서 코드를 클라우드 배포하기 전에 코드에서 잠재적인 보안 위험을 확인하고 보안 사고의 범위를 확인하는 것은 모든 응용 프로그램 개발자의 책임입니다.

코드 취약점이란 무엇인가요?

코드 취약점은 코드에서의 결함 또는 오류로, 보안 위험을 초래하고 위험 요소가 코드를 어떤 엔드포인트에든 연결하고 모든 데이터를 추출하거나, 더 나쁜 경우에는 코드를 변조하고 기타 작업을 수행할 수 있는 기회를 제공합니다. 또한 코드 취약점은 사용자 및 개발자를 다양한 종류의 보안 위협으로 취약하게 만듭니다.

보안 코드 분석은 무엇인가요?

보안 코드 분석은 논리 오류, 구현, 스타일 가이드 등을 확인하여 기존의 보안 취약점을 식별하기 위한 수동 또는 자동화된 검사 프로세스입니다. 오늘날은 정적 애플리케이션 보안 테스트 (SAST)와 같은 도구를 사용하여 보안 코드 검토를 수행할 수 있으며, 이러한 도구는 개발자들이 효과적으로 보안 업무를 수행하는 데 도움을 주는뿐만 아니라 GitHub, GitLab, Eclipse, IntelliJ 등과 호환되어 개발자들이 선호하는 환경에서 작업할 수 있습니다.

코드에 보안을 어떻게 제공할 수 있나요?

SAST와 유사하게 코드 보안을 제공하는 두 가지 더 선호되는 방법은 Dynamic Application Security Testing (DAST)와 Interactive Application Security Testing (IAST)입니다. 코드에 보안을 제공하기 위한 몇 가지 권장 방법은 통신의 포트 범위를 제한하고 응용 프로그램의 타사 라이브러리를 자동으로 스캔하며 동적 프로빙 공격을 시작하는 것입니다.

🔄Revision #1

★Created 2023-09-02 12:06:42 UTC by Admin

✎Updated 2023-09-02 12:09:51 UTC by Admin