AKAMAI 체크리스트

OWASP 상위 10대 API 보안

특히 마이크로서비스 기반 아키텍처로 전환하는 경우가 증가하면서 API는 최신 애플리케이션을 구축하고 연결하는 표준으로 자리 잡았습니다. 따라서 OWASP(Open Worldwide Application Security Project)에서 식별한 가장 일반적인 API 보안 리스크로부터 기업을 보호하는 것이 중요합니다. 현재 2023년 목록을 검토하고 API 보안을 위한 여정에서 더 많은 정보를 확보하세요.

Akamai의 OWASP API 10대 커버리지

- **API1:2023 — 손상된 오브젝트 수준의 권한 확인:** 특정 오브젝트 ID에 접속하기 위해 클라이언트의 권한이 제대로 검증되지 않은 경우 BOLA 취약점이 발생할 수 있습니다.
- **API2:2023 — 취약한 인증:** BA는 인증 프로세스의 광범위한 취약점을 의미하며, 이러한 취약점을 악용해 API 오브젝트 보안을 손상시킬 수 있는 공격자에게 시스템을 노출시킵니다.
- **API3:2023 — 손상된 오브젝트 프로퍼티 수준의 권한 확인:** BOPLA는 API 엔드포인트가 최소 권한 원칙을 무시하고 해당 기능에 필요한 것보다 많은 데이터 속성을 불필요하게 노출하는 보안 결함입니다.
- **API4:2023 — 무제한 리소스 사용** 이는 API 리소스 고갈이라고도 하는 취약점의 한 종류로, API가 주어진 시간 내에 제공하는 요청 수나 데이터 양에 제한을 두지 않는 취약점입니다.
- **API5:2023 — 손상된 기능 수준의 권한 확인:** API 엔드포인트에 대한 접속 제어 모델이 잘못 구축된 경우 BFLA가 발생할 수 있습니다.
- **API6:2023 — 민감한 비즈니스 플로우에 대한 무제한 접속:** 이러한 리스크는 API가 충분한 접속 제어 없이 비즈니스 로직 같은 중요한 작업을 노출할 때 발생합니다.
- **API7:2023 — 서버 측 요청 위조:** SSRF를 사용하면 공격자는 서버 측 애플리케이션이 공격자가 선택한 임의의 도메인에 HTTPS 요청을 하도록 유도할 수 있습니다.
- **API8:2023 — 잘못된 보안 설정:** 이 리스크는 보안 제어를 부적절하게 설정해 시스템을 공격에 취약하게 만드는 것을 말합니다.
- **API9:2023 — 부적절한 인벤토리 관리:** 이 리스크는 API를 관리하는 모든 기업이 직면한 과제입니다. API 보안 솔루션은 알려진 API를 보호할 수 있지만 중단된 API, 레거시 API, 오래된 API 등 알 수 없는 API에는 패치가 적용되지 않아 공격에 취약할 수 있습니다.
- **API10:2023 — 안전하지 않은 API 사용:** 이 리스크는 적절한 보안 조치를 취하지 않고 써드파티 API를 사용할 때 발생할 수 있는 리스크를 의미합니다.

2019년과 2023년 OWASP 상위 10대 API 보안 리스크 목록의 차이점에 대해 자세히 알고 싶으신가요? **이 블로그 게시물을 확인하세요**.

Akamai와 협력

기업과 기업의 보안 벤더사가 OWASP 상위 10대 API 보안 리스크에 설명된 보안 리스크에 대비해 강력한 방어 체계를 구축하려면 인력, 프로세스, 기술을 조율하며 서로 긴밀하게 협력해야 합니다.

Akamai 소개

Akamai는 업계 최고의 보안 솔루션과 경험이 풍부한 전문가, 수백만 건의 웹 애플리케이션 공격, 수십억 건의 봇 요청, 매일 수조 건의 API 요청으로부터 인사이트를 확보하는 Akamai Connected Cloud를 제공합니다. Akamai의 웹 애플리케이션 및 API 보안 솔루션은 가장 발전된 형태의 웹 애플리케이션, DDoS(Distributed Denial-of-Service), API 기반 공격으로부터 기업을 보호합니다.

 | 지원 | | 2023년 08월 발행