CHECKLIST AKAMAI

Elenco OWASP con le 10 principali vulnerabilità per la sicurezza delle API

Le API sono diventate lo standard per la creazione e la connessione delle moderne applicazioni, specialmente con la crescente migrazione verso le architetture basate sui microservizi. Ecco perché è importante proteggere la vostra organizzazione dai rischi per la sicurezza delle API più comuni, come segnalato da OWASP (Open Worldwide Application Security Project). Esaminiamo insieme l'attuale elenco del 2023 per saperne di più sul vostro percorso di protezione delle API.

Protezione di Akamai dalle 10 principali vulnerabilità per la sicurezza delle API secondo OWASP

- ☑ **API1:2023 - Violazione dell'autorizzazione a livello di oggetto (BOLA):** le vulnerabilità BOLA si verificano quando l'autorizzazione di un client non è adeguatamente confermata per l'accesso a ID oggetto specifici.
- ☑ **API2:2023 - Violazione dell'autenticazione (BA):** le BA sono vulnerabilità di vasta portata che si verificano nel processo di autenticazione, esponendo il sistema ai criminali, che sfruttano questi punti deboli per compromettere la protezione delle API.
- ☑ **API3:2023 - Violazione dell'autorizzazione a livello della proprietà dell'oggetto (BOPLA):** la BOPLA è una falla nella sicurezza che si verifica quando un endpoint API espone inutilmente più proprietà di dati di quanto non sia necessario per svolgere la propria funzione, trascurando il principio del privilegio minimo.
- ☑ **API4:2023 - Utilizzo delle risorse illimitato:** si tratta di un tipo di vulnerabilità spesso definito esaurimento delle risorse API. Si verifica quando le API non limitano il numero di richieste inviate o il volume dei dati restituiti entro un certo periodo di tempo.
- ☑ **API5:2023 - Autorizzazione violata a livello di funzione (BFLA):** la violazione BFLA può verificarsi quando i modelli di controllo degli accessi per gli endpoint API non vengono implementati correttamente.
- ☑ **API6:2023 - Accesso illimitato a flussi aziendali sensibili:** questo rischio aumenta quando un'API espone operazioni di importanza critica, come la logica aziendale, senza un adeguato controllo sugli accessi.
- ☑ **API7:2023 - SSRF (Server-Side Request Forgery):** un SSRF permette a un criminale di indurre l'applicazione lato server a inviare richieste HTTPS a un dominio arbitrario da lui scelto.
- ☑ **API8:2023 - Errata configurazione della sicurezza:** si tratta di un'errata configurazione dei controlli di sicurezza, che può rendere un sistema vulnerabile agli attacchi.
- ☑ **API9:2023 - Gestione dell'inventario inadeguata:** rappresenta una sfida per tutte le organizzazioni che si occupano della gestione delle API. Le soluzioni per la sicurezza delle API possono proteggere le API note, ma le API sconosciute, comprese le API obsolete, legacy e/o non aggiornate, possono restare prive di patch e, quindi, vulnerabili agli attacchi.
- ☑ **API10:2023 - Utilizzo delle API non sicuro:** si tratta dei rischi associati all'utilizzo di API di terze parti, senza aver prima predisposto misure di sicurezza adeguate.

Desiderate saperne di più sulla differenza tra l'elenco OWASP delle 10 principali vulnerabilità per la sicurezza delle API del 2019 e quello del 2023? Date un'occhiata a questo blog.

Lavora con noi

Le organizzazioni e i loro fornitori dei servizi di sicurezza devono lavorare a stretto contatto, sincronizzando persone, processi e tecnologie, al fine di costituire una solida difesa contro i rischi per la sicurezza descritti nelle 10 principali vulnerabilità per la sicurezza delle API riportate nella Top 10 sulle vulnerabilità per la sicurezza delle API secondo OWASP.

Informazioni su Akamai

Akamai offre soluzioni per la sicurezza leader del settore, esperti della sicurezza altamente competenti e Akamai Connected Cloud, che raccoglie informazioni da milioni di attacchi alle applicazioni web, miliardi di richieste di bot e migliaia di miliardi di richieste API ogni giorno. Le soluzioni per la sicurezza delle applicazioni web e delle API di Akamai vi aiuteranno a proteggere la vostra organizzazione dalle forme più avanzate di attacchi alle applicazioni web, attacchi DDoS (Distributed Denial-of-Service) e attacchi basati sulle API.

 | Supporto | | Data di pubblicazione: 08/23