Akamai

WHITE PAPER

Anatomia di un attacco alle API

Descrizione dello sfruttamento della gestione dell'inventario e delle vulnerabilità BOLA

Introduzione

La maggior parte dei team addetti alla sicurezza si è resa ormai conto che una ricerca proattiva delle minacce è un componente essenziale in un efficace programma di sicurezza aziendale, specialmente quando si tratta di API (Application Programming Interface). Le API spesso forniscono un accesso diretto a dati, funzionalità e workflow. Inoltre, mentre le misure basilari di sicurezza del perimetro di rete vengono perlopiù usate per proteggere le applicazioni, si assiste ad un aumento dell'abuso delle API e di altri tipi di attacchi. In realtà, alcuni dei problemi di sicurezza più significativi che hanno fatto notizia negli ultimi anni sono stati tutti correlati alle API. Per comprendere meglio i profili di questi attacchi, come lo sfruttamento di una gestione dell'inventario inadeguata e delle vulnerabilità BOLA (Broken Object Level Authorization), questo articolo si propone di:

- Esaminare i concetti di base delle API
- Scoprire perché la sicurezza delle API è un argomento sempre più importante
- Utilizzare alcuni problemi di sicurezza delle API di alto profilo per evidenziare le principali aree in questo contesto
- Illustrare le funzionalità necessarie per eseguire un'efficace ricerca delle minacce alle API

I concetti di base delle API e degli endpoint

Innanzitutto, iniziamo a rivedere alcuni termini di base. Le API vengono utilizzate per molti scopi, dalle funzionalità B2C (da azienda a consumatore), alla collaborazione e all'integrazione B2B (da azienda ad azienda) fino alle funzioni interne di sviluppo e integrazione. Le API web, che comunicano tramite lo stesso protocollo HTTP utilizzato dai browser web, sono il modello di implementazione più comune. Le specifiche funzionalità fornite da queste API vengono a volte definite "servizi o prodotti API".

Per quanto riguarda la sicurezza delle API, è inoltre importante chiarire il concetto di endpoint. Anche se questo termine viene spesso usato per indicare i dispositivi informatici degli utenti finali, può assumere un significato diverso nel contesto delle API. Possiamo considerare un endpoint API come una singola risorsa accessibile che fa parte di un'API, insieme all'operazione ad essa correlata.

> **Ecco un semplice esempio. Un endpoint API che restituisce le informazioni su un ordine per una specifica azienda potrebbe essere rappresentato nel modo seguente: GET /orders/{orderID}. In questo caso, GET è uno specifico metodo HTTP, mentre orders e orderID rappresentano la particolare risorsa richiesta tramite l'API.**

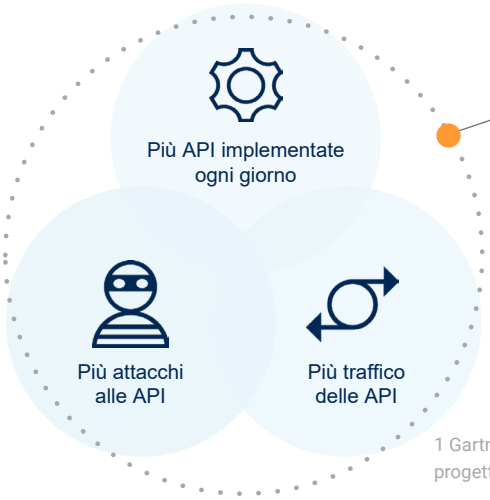
Perché le API rappresentano la nuova grande sfida in termini di sicurezza?

In passato, un criminale poteva prendere di mira un data center aziendale per accedere ai dati di un'organizzazione e per esfiltrarli da un server specifico. In alternativa, un criminale poteva tentare di esaminare il traffico di una rete aziendale per acquisire i dati sensibili. In questi casi, una ricerca proattiva delle minacce poteva incentrarsi su varie attività, come i test di penetrazione per eliminare i possibili punti di accesso per i criminali.

In un mondo supportato dalle API, questa dinamica è diversa. Molte API sono per loro natura accessibili a chiunque dall'esterno con l'utilizzo di chiavi e credenziali, che spesso sono la loro unica linea di difesa, e i criminali stanno diventando sempre più abili nel violare queste componenti. Inoltre, alcuni dei tipi più pericolosi di abuso delle API possono provenire da utenti a cui è stato concesso l'accesso alle API, ma che scelgono di utilizzarle in modi non autorizzati.

Gli attacchi alle API nel mondo reale

Il traffico delle API rappresenta il 31% del traffico complessivo che viene protetto da Akamai. Questa crescita del traffico delle API ha un effetto a cascata, come, ad esempio, l'incremento nel numero di attacchi e abusi. Gartner prevede che le violazioni di dati e gli abusi delle API raddoppieranno nel 2024. Intanto, molti team addetti alla sicurezza faticano a tenere il passo con le strategie di protezione delle API. Mentre le API si moltiplicano sempre più, gli strumenti esistenti per la sicurezza delle applicazioni offrono una protezione delle API molto limitata.



Le soluzioni per la sicurezza delle applicazioni non sono concepite per le API

Entro il 2024, gli abusi di API e le relative violazioni di dati aumenteranno quasi del **doppio.**[1]

Il **31%** del traffico web è correlato alle API [2]

1 Gartner. Le prime 10 cose che i responsabili della progettazione di software devono sapere sulle API

2 I ricercatori delle minacce di Akamai hanno rilevato che il traffico delle API rappresenta il 31% del traffico complessivo che viene protetto da Akamai.

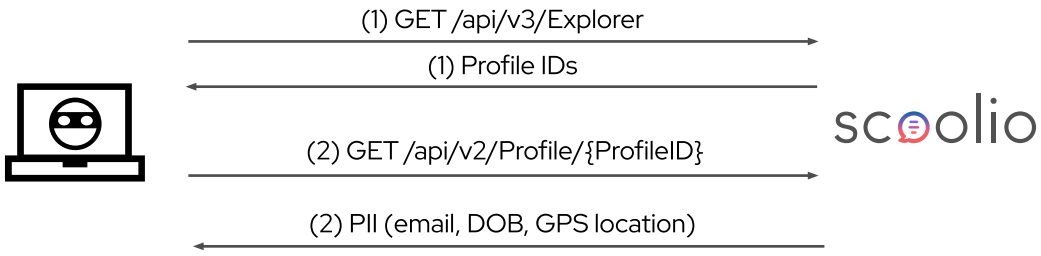
Per esaminare concretamente il problema, analizziamo un case study che illustra il reale impatto esercitato dagli attacchi alle API sulle aziende e sui loro clienti.

Case study

Attacchi per il controllo degli account | Scoolio

Un notevole esempio di questo tipo riguarda un problema che si è verificato nel 2021 e ha interessato Scoolio, un'app didattica tedesca, che raccoglie un gran numero di informazioni dagli studenti. Ad esempio, l'app conduce test sulla personalità, fornisce funzioni di chat e social network e gestisce varie attività, come il tutoraggio e la pianificazione degli studi. Queste funzioni contengono un patrimonio di PII. Lilith Wittmann, una ricercatrice che si occupa di sicurezza, ha scoperto una vulnerabilità BOLA nelle API dell'app didattica, che ha consentito di utilizzare due chiamate API per accedere alle PII e agli altri dati degli utenti in essa contenuti.

Ecco il suo funzionamento:



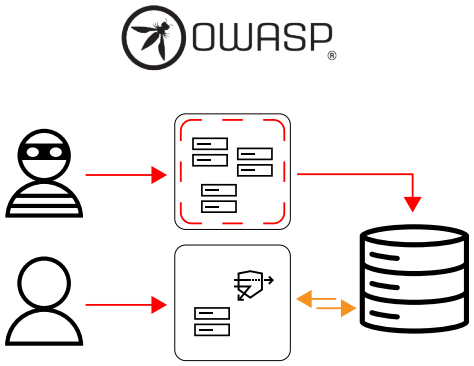
Passaggio 1
Invio di una chiamata API GET /api/v3/Explorer.
Questa chiamata ha restituito gli UUID, che sono stati definiti ProfileID in questa implementazione.

Passaggio 2
Invio di una chiamata API GET /api/v2/Profile/{ProfileID}.
Questa richiesta ha restituito le PII complete per l'utente in questione, tra cui indirizzo e-mail, data di nascita, posizione GPS e molto altro.

Il valore dell'utilizzo degli UUID

Anche se entrambi i casi si sono focalizzati sull'utilizzo degli UUID, si tratta, in realtà, di un'ottima pratica. L'utilizzo di numeri generati casualmente invece di una sequenza prevedibile di ID utente rende più difficile per i criminali accedere alle informazioni di utenti in massa. Il problema nasce nel momento in cui le informazioni degli UUID vengono esposte in modo troppo permissivo insieme alle vulnerabilità BOLA.

Gestione dell'inventario inadeguata



Un altro aspetto di questa vulnerabilità delle API riguarda lo sfruttamento di una gestione dell'inventario inadeguata, che si trova al punto 9 dell'elenco OWASP con i 10 principali rischi alla sicurezza delle API. Se guardiamo attentamente alla sequenza dell'attacco, notiamo che il primo passaggio viene applicato alla versione 3 dell'API, mentre il secondo passaggio viene applicato alla versione 2. I miglioramenti apportati alla versione 3 hanno fornito un accesso molto più controllato alle PII. Tuttavia, questi miglioramenti sono stati pregiudicati dal fatto che la versione 2 più vulnerabile è rimasta accessibile a tutti. In conclusione, sia la versione 2 che la versione 3 sono state interessate dalla vulnerabilità BOLA. Tuttavia, l'inutile presenza della versione 2 ha reso l'impatto della vulnerabilità più serio.

Quali operazioni devono effettuare le organizzazioni per proteggere le loro API?

L'approccio alla sicurezza delle API adottato da molte organizzazioni si focalizza sui seguenti tre elementi fondamentali:

1. Autorizzazione centralizzata: innanzitutto, l'implementazione di un motore dedicato a questa funzionalità per tutte le porte di accesso alle API ne riduce il rischio di vulnerabilità, eliminando eventuali errori di sviluppo che determinano meccanismi di autorizzazione errati.

2. Esecuzione di test delle API: si tratta della seconda pratica importante. L'esecuzione di test su tutte le vulnerabilità, soprattutto la violazione dell'autorizzazione, utilizzando l'analisi statica del codice e test dinamici, fa emergere i problemi tempestivamente nel processo di sviluppo.

3. Protezione del runtime: il terzo elemento fondamentale è rappresentato dalle protezioni del runtime nell'ambiente di produzione. Anche i team maggiormente proattivi non riescono ad individuare ogni vulnerabilità in anticipo in fase di implementazione, pertanto è essenziale esaminare l'accesso degli utenti ai dati di produzione e prevenire il più possibile lo sfruttamento delle vulnerabilità di categorie note.

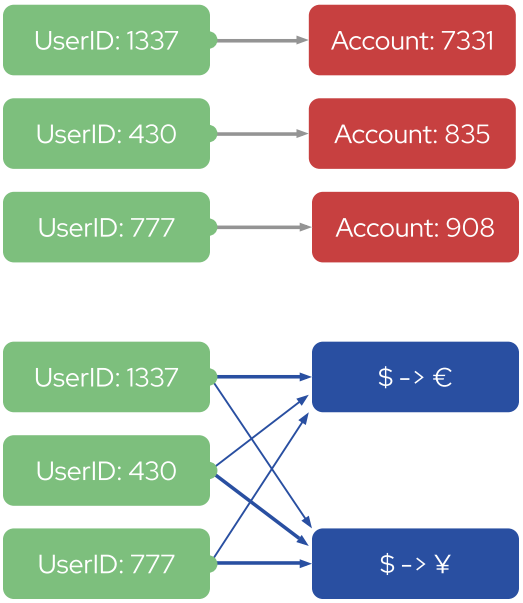
Anche se queste tre pratiche forniscono un'eccellente base in una strategia di sicurezza delle API, è importante ricordare che non sono perfette né complete. Ad esempio, persino le organizzazioni con un'autorizzazione centralizzata non possono garantire che gli sviluppatori seguano sempre le best practice più appropriate. Infine, gli strumenti di protezione delle applicazioni esistenti sono spesso in grado di rilevare gli schemi di attacco noti, ma non di individuare le minacce più sofisticate, come le vulnerabilità BOLA.

In che modo è possibile utilizzare questa base con tecniche di rilevamento delle vulnerabilità BOLA più avanzate?

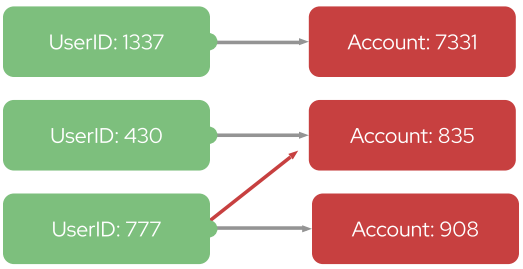
Una delle chiavi per il rilevamento e la mitigazione delle vulnerabilità BOLA e di altre vulnerabilità delle API più sofisticate consiste nel modellare la relazione esistente tra le entità coinvolte nelle attività delle API, tra cui persone, come gli utenti, che tentano di accedere alle risorse, oltre alle risorse stesse. Associando questi collegamenti tra le entità coinvolte e i processi aziendali che interagiscono con un'API, è possibile differenziare le attività legittime da quelle non legittime durante l'analisi di eventi delle API altrimenti identici.

Illustrazione dell'associazione delle relazioni

Per comprendere meglio l'associazione delle relazioni, consideriamo questo esempio di base. Un'applicazione di banking supporta due operazioni: una consiste nel leggere i dati dei conti bancari, incluse informazioni come l'estratto conto, le transazioni recenti, ecc.; l'altra consiste nel visualizzare i tassi di cambio della valuta. La relazione tra utenti e risorse in questi esempi è molto diversa. L'accesso alle informazioni dei conti deve essere limitata a un solo utente, invece la funzione di visualizzazione dei tassi di cambio deve essere resa generalmente disponibile per tutti gli utenti.



Anche se si tratta di un esempio molto semplice, costruire un modello più sofisticato di associazioni delle relazioni esistenti tra le entità lo rende molto più pratico per prevenire o rilevare le vulnerabilità BOLA.



Qui viene illustrato il tentativo da parte di un utente di accedere ad un conto di cui non è proprietario. La specifica chiamata API può essere identica, ma il nuovo contesto fornito dall'associazione delle entità fa capire che non dovrebbe essere consentita.

L'avanzato rilevamento degli attacchi BOLA in pratica

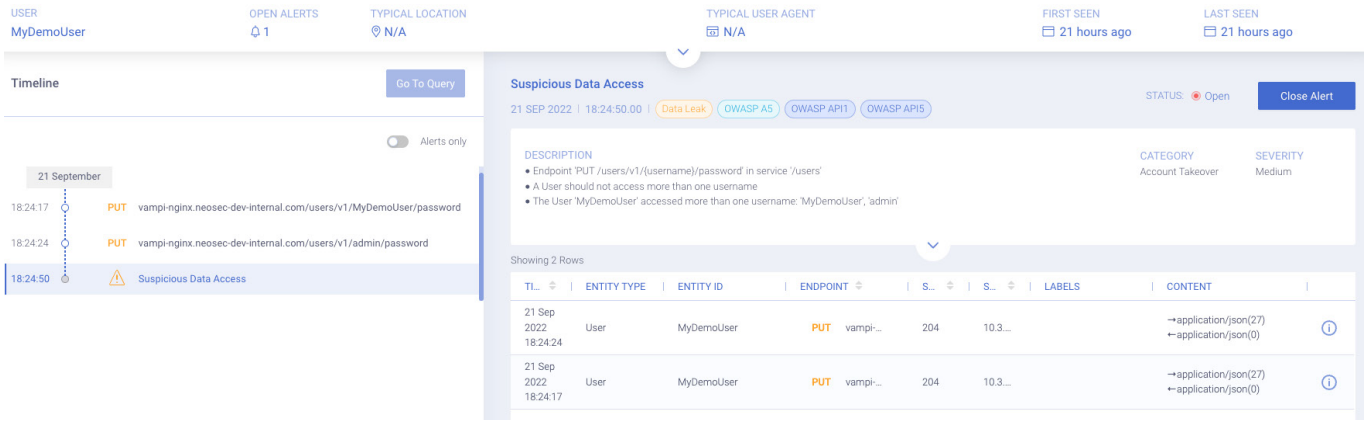
Ora, applichiamo questo concetto ad esempi più complessi, come le vulnerabilità del case study. Di seguito, vengono riportati gli snippet delle entità coinvolte in questo scenario:

scoolio

GET/api/v3/Profile/ {ProfileID}

Intestazioni:
- Autorizzazione: <MyAccessToken>

L'entità coinvolta è evidenziata in verde, mentre la risorsa richiesta (ID profilo) è evidenziata in rosso. Una volta comprese queste relazioni, è possibile eseguire alcune operazioni per applicare la logica generale, come la limitazione dell'accesso da parte di un'entità ad una singola risorsa, se necessario. Si tratta di un processo tutt'altro che banale poiché le relazioni possono essere più complesse rispetto a questo esempio e includere dimensioni multidirezionali. Tuttavia, tecniche come l'apprendimento automatico e l'analisi del comportamento lo rendono possibile. Ad esempio, un rilevamento riuscito di una vulnerabilità BOLA per uno dei nostri clienti potrebbe risultare simile a quanto segue:



In questo esempio, una vulnerabilità BOLA è stata simulata in un laboratorio. Tramite l'associazione delle entità e l'analisi del comportamento, la nostra piattaforma ha rilevato la vulnerabilità BOLA e ha generato un avviso informativo. Un analista della sicurezza o un ricercatore delle minacce che visualizza l'avviso vedrà che MyDemoUser è entrato nel proprio profilo utente per cambiare la password, un'operazione autorizzata. Tuttavia, subito dopo questa operazione, possiamo notare che l'utente ha eseguito un'altra chiamata API per cambiare la password dell'amministratore. Poiché, in tal caso, si tratta ovviamente di un'operazione non autorizzata in base alla relazione tra l'utente e la risorsa, è stato generato il relativo avviso.

Da dove iniziare con le iniziative di sicurezza delle API

La sicurezza delle API richiede un impegno continuo per la maggior parte delle organizzazioni e può risultare difficile sapere da dove iniziare. Anche se i tre pilastri fondamentali riportati sopra forniscono un utile punto di partenza, l'efficacia dell'approccio adottato viene notevolmente migliorata se si seguono questi tre consigli in fase di implementazione:

1. Garantire un inventario delle API sempre aggiornato
2. Monitorare gli ambienti delle API di produzione e non
3. Rafforzare le relazioni tra le entità

Non potete proteggere le API se non le conoscete. Un'efficace protezione delle API inizia con un inventario delle API aggiornato e una valutazione del loro sistema di sicurezza. Analogamente, durante lo sviluppo delle funzionalità di monitoraggio della sicurezza delle API, è importante estenderle alle implementazioni delle API di produzione e non. Ancora più importante, il monitoraggio e l'applicazione delle API deve estendersi oltre le semplici operazioni e considerare le relazioni esistenti tra le entità coinvolte nelle attività delle API. In tal modo, è possibile individuare le vulnerabilità e le falle nella sicurezza, applicando, al contempo, la conformità con i modelli di utilizzo delle API previsti. Comprendere il comportamento delle API consente di individuare eventuali abusi.

Siete interessati a saperne di più sugli attacchi alle API e su come potete proteggervi? Date un'occhiata al nostro elenco OWASP con i 10 principali rischi alla sicurezza delle API.