Akamai

백서

API 공격의 구조

BOLA 및 인벤토리 관리 악용 이해하기

서론

이제 대부분의 보안팀은 선제적 위협 탐색이 효과적인 기업 보안 프로그램의 필수 요소이며, 특히 API(Application Programming Interface)와 관련해서는 더욱 그러하다는 것을 알고 있습니다. API는 데이터, 기능, 워크플로우에 대한 직접적인 접속을 제공하는 경우가 많습니다. 애플리케이션을 보호하기 위해 기본 경계 보안 조치가 널리 사용되고 있지만, API 남용 및 기타 종류의 공격이 증가하고 있습니다. 실제로 최근 몇 년간 언론의 헤드라인을 장식한 가장 유명한 보안 인시던트 중 API와 관련된 것도 있었습니다. 이 백서는 BOLA(Broken Object Level Authorization)와 부적절한 인벤토리 관리 악용 같은 공격 프로필에 대한 이해도를 높이기 위해 다음과 같은 내용을 소개합니다.

- API의 기본 사항 검토
- API 보안이 점점 중요해지는 이유
- 몇 가지 유명한 API 보안 인시던트를 통해 API의 핵심 보안 영역 강조
- API 위협을 효과적으로 탐색하기 위해 필요한 기능 설명

API 및 엔드포인트 기본 사항

먼저 몇 가지 기본 용어를 살펴보겠습니다. API는 B2C(Business-To-Consumer) 기능, B2B(Business-To-Business) 협업 및 통합, 내부 개발 및 통합 기능 등 다양한 용도로 사용됩니다. 웹 브라우저에서 사용하는 것과 동일한 HTTP 프로토콜을 통해 통신하는 웹 API가 가장 일반적인 구축 모델입니다. 이러한 API가 제공하는 특정 기능을 서비스 또는 API 제품이라 부르기도 합니다.

API 보안에 대해 생각할 때 엔드포인트의 개념도 이해해야 합니다. 엔드포인트는 최종 사용자의 컴퓨팅 디바이스를 의미하기도 하지만, API의 맥락에서는 다른 의미를 갖습니다. API 엔드포인트는 API의 일부인 접속 가능한 단일 리소스와 이를 통해 수행할 수 있는 작업으로 생각할 수 있습니다.

> **다음은 간단한 사례입니다. 특정 회사의 주문 정보를 반환하는 API 엔드포인트는 다음과 같이 표현할 수 있습니다. GET /orders/{orderID}. 이 경우 GET은 특정 HTTP 방식이고, orders와 orderID는 API를 통해 요청되는 특정 리소스를 나타냅니다.**

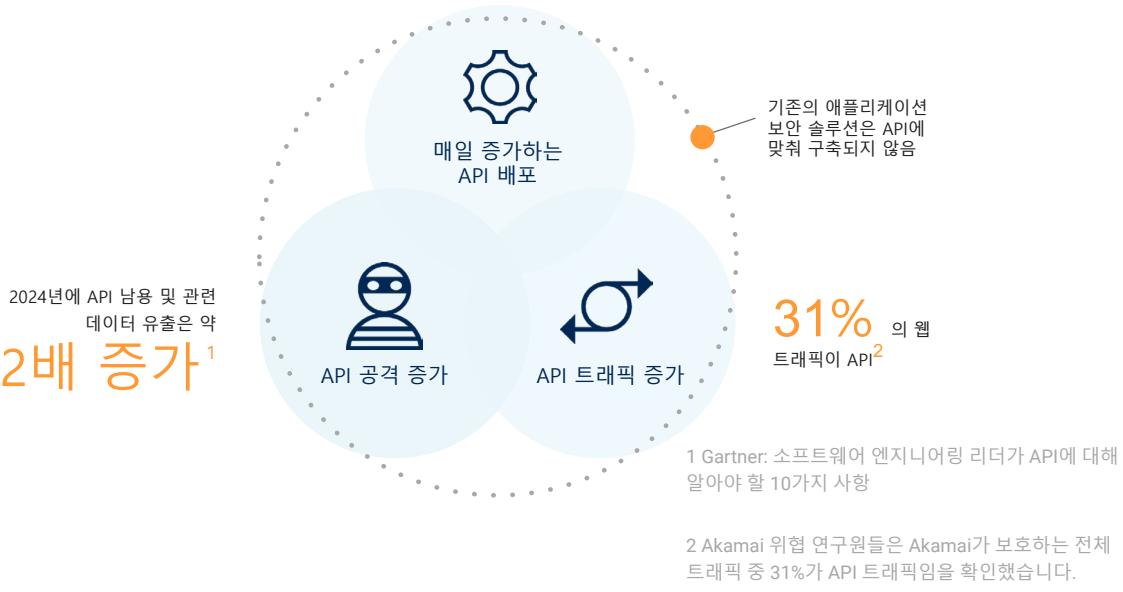
API가 차세대 보안 과제가 되는 이유

과거에는 공격자가 기업 데이터 센터에 침입해 특정 서버에서 기업의 데이터에 접속하고 유출하는 것을 목표로 삼았습니다. 또는 민감한 데이터를 캡처하기 위해 기업 네트워크 트래픽을 검사하려고 시도하기도 했습니다. 이러한 시나리오에서 선제적 위협 탐색은 공격자의 진입 지점을 차단하기 위한 침투 테스트 같은 활동을 중심으로 이루어질 수 있습니다.

API 사용 환경에서는 이러한 역학 관계가 달라집니다. 많은 API는 본질적으로 외부의 모든 사람이 접속할 수 있으며, 인증정보와 키가 유일한 방어선 역할을 하는 경우도 있습니다. 그리고 공격자는 이러한 요소를 감염시키는 데 점점 더 능숙해지고 있습니다. 또한, 가장 치명적인 API 남용 사례의 경우 API에 대한 접속 권한을 부여받았지만 승인되지 않은 방식으로 이를 사용하는 당사자로부터 발생할 수 있습니다.

실제 API 공격

Akamai가 보호하는 전체 트래픽의 31%는 API 트래픽입니다. 이러한 API 트래픽의 증가는 공격 및 악용 증가와 같은 다운스트림 효과로 이어집니다. Gartner는 2024년에 API 남용과 데이터 유출이 두 배 증가할 것으로 예상합니다. 많은 보안팀은 이를 따라잡기에 급급합니다. API는 계속 증가하는 반면, 기존 애플리케이션 보안 툴은 매우 제한적인 API 보안 기능을 제공합니다.



1 Gartner: 소프트웨어 엔지니어링 리더가 API에 대해 알아야 할 10가지 사항

2 Akamai 위협 연구원들은 Akamai가 보호하는 전체 트래픽 중 31%가 API 트래픽임을 확인했습니다.

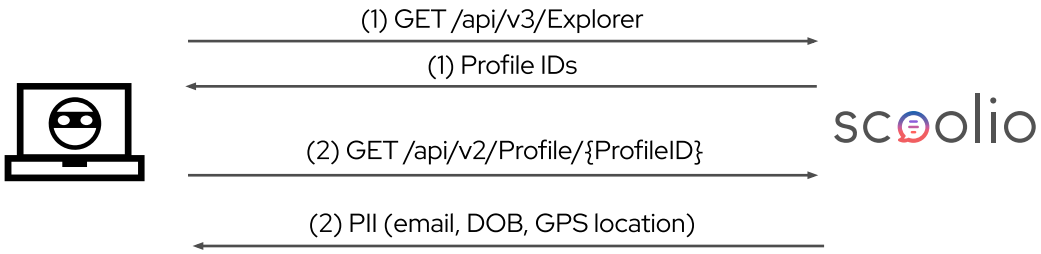
이 문제를 현실적으로 이해하기 위해 API 공격이 기업과 고객에게 미칠 수 있는 실제 영향을 보여주는 사례를 검토해 보겠습니다.

사례 연구

계정 탈취 | Scoolio

주목할 만한 사례로는 독일 교육 앱인 Scoolio에 영향을 준 2021년 인시던트가 있습니다. 이 앱은 학생 사용자로부터 광범위한 정보를 수집합니다. 예를 들어, 성격 테스트를 실시하고, 소셜 네트워킹 및 채팅 기능을 제공하고, 학습 계획 및 과외 같은 활동을 관리합니다. 이러한 기능을 통해 수많은 PII가 수집됩니다. 보안 연구원 릴리스 위트만(Lilith Wittmann)은 이 교육 앱의 API에서 두 번의 API 호출을 통해 교육 앱의 다른 사용자의 PII 및 기타 데이터에 접속할 수 있는 BOLA 취약점을 발견했습니다.

작동 방식은 다음과 같습니다.



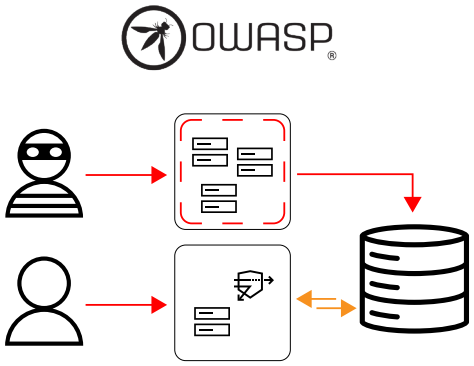
1단계
GET /api/v3/Explorer API 호출을 전송합니다.
이 호출은 이 구축에서는 ProfileID라고 하는 UUID를 반환했습니다.

2단계
GET /api/v2/Profile/{ProfileID} API 호출을 전송합니다.
이 요청은 이메일, 생년월일, GPS 위치 등 해당 사용자의 광범위한 PII를 반환합니다.

UUID 사용으로 얻는 가치

두 시나리오 모두 UUID 사용에 초점을 맞추고 있지만, 사실 UUID 사용은 매우 좋은 사례입니다. 예측 가능한 사용자 식별자 시퀀스 대신 무작위로 생성된 숫자를 사용하면 공격자가 사용자 정보에 일괄적으로 접속하기가 더 어려워집니다. 문제는 UUID 정보가 너무 무분별하게 노출되어 BOLA 취약점과 결합될 때 발생합니다.

부적절한 인벤토리 관리



이 API 취약점 악용의 또 다른 측면은 부적절한 인벤토리 관리를 이용했다는 점인데, 이는 OWASP API 상위 10대 목록에서 9번째에 해당합니다. 공격 순서를 자세히 살펴보면 첫 번째 단계는 API 버전 3에 적용되고 두 번째 단계는 버전 2에 대해 수행되었음을 알 수 있습니다. 버전 3에서는 PII에 대한 접속을 보다 엄격하게 관리할 수 있도록 개선되었습니다. 하지만 이런 개선사항은 더 취약한 버전 2에 여전히 누구나 접속할 수 있다는 사실에 의해 약화되었습니다. 결국 버전 2와 버전 3 모두 BOLA 취약점의 영향을 받았습니다. 하지만 버전 2가 불필요했기 때문에 취약점의 영향이 더욱 심각해졌습니다.

오늘날 기업은 API를 보호하기 위해 어떤 조치를 취하고 있나요?

많은 기업이 다음 세 가지 요소에 중점을 두고 API 보안에 접근합니다.

1. 중앙 집중식 권한 부여 - 먼저, 모든 API 접속 포트에 중앙 집중식 권한 부여 엔진을 구축하면 개발 과정에서 실수로 인해 권한 부여 메커니즘에 결함이 생기는 것을 방지해 API 취약점 리스크를 줄일 수 있습니다.

2. API 테스트 - 두 번째로 중요한 관행은 API 테스트입니다. 정적 코드 분석과 동적 테스트를 모두 사용해 모든 취약점, 특히 잘못된 권한에 대해 테스트하면 개발 프로세스 초기에 문제를 발견할 수 있습니다.

3. 런타임 보호 - 세 번째 핵심 요소는 프로덕션 환경을 위한 런타임 보안 기능입니다. 아무리 선제적인 팀이라도 배포 전에 모든 취약점을 파악할 수는 없습니다. 따라서 프로덕션 데이터에 대한 사용자 접속을 검사하고 알려진 취약점 카테고리의 악용을 최대한 방지하는 것이 중요합니다.

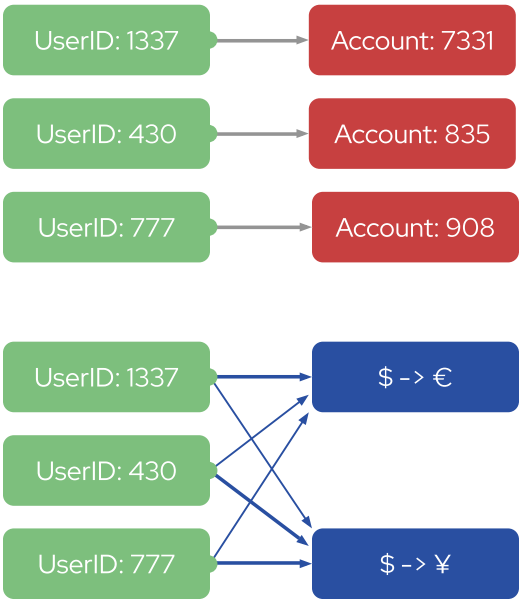
이 세 가지 관행은 API 보안 전략의 훌륭한 토대를 제공합니다. 하지만 완벽하거나 포괄적이지 않다는 점도 기억해야 합니다. 예를 들어, 중앙 집중식 권한을 부여하는 기업이라도 개발자가 항상 모범 사례를 준수할 것이라 보장할 수 없습니다. 마지막으로, 기존의 애플리케이션 보호 툴은 알려진 공격 패턴을 탐지하는 데는 능숙하지만 BOLA와 같은 미묘한 위협을 탐지하는 데는 취약한 경우가 많습니다.

이러한 토대 위에 고급 BOLA 탐지 기술을 어떻게 구축할 수 있을까요?

BOLA 및 기타 미묘한 API 취약점을 탐지하고 방어하기 위한 핵심 중 하나는 API 활동과 관련된 주체 간의 관계를 모델링하는 것입니다. 여기에는 리소스 뿐만 아니라 리소스에 접속하려는 사용자 등 행위자도 포함됩니다. API와 상호작용하는 행위자 주체와 비즈니스 프로세스 주체 간의 이러한 연결을 매핑할 수 있다면, 동일한 API 이벤트를 분석할 때 합법적인 활동과 불법적인 활동을 구분할 수 있습니다.

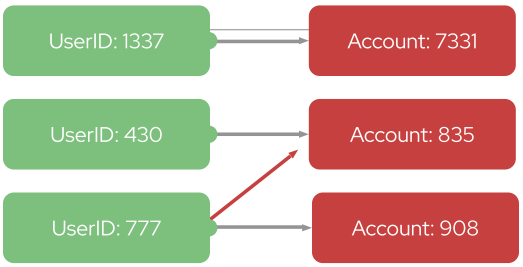
관계 매핑

다음과 같은 기본적인 사례를 통해 관계 매핑을 제대로 이해할 수 있습니다. 은행 애플리케이션은 두 가지 작업을 지원합니다. 한 가지 작업은 계정 잔액, 최근 트랜잭션 등의 정보를 포함한 계정 데이터를 읽는 것입니다. 두 번째 작업은 환율을 보는 것입니다. 이 예에서 사용자와 리소스 간의 관계는 매우 다릅니다. 계정 정보에 대한 접속은 한 명의 사용자로 제한되어야 합니다. 반대로 환율 기능은 일반적으로 모든 사용자가 사용할 수 있어야 합니다.



이것은 매우 기본적인 사례이지만, 주체 간의 관계 매핑에 대한 보다 정교한 모델을 구축하면 보다 실질적으로 BOLA를 차단 및 탐지할 수 있습니다.

여기서는 사용자가 자신이 소유하지 않은 계정에 접속하려고 시도하는 경우를 살펴봅니다. 특정 API 호출은 동일할 수 있지만 주체 매핑이 제공하는 추가 맥락을 통해 해당 호출이 허용되어서는 안 된다는 것을 명확히 알 수 있습니다.



실제 고급 BOLA 공격 탐지

이제 이 개념을 사례 연구 취약점과 같이 더 복잡한 사례에 적용해 보겠습니다. 아래는 시나리오와 관련된 주체의 일부입니다.

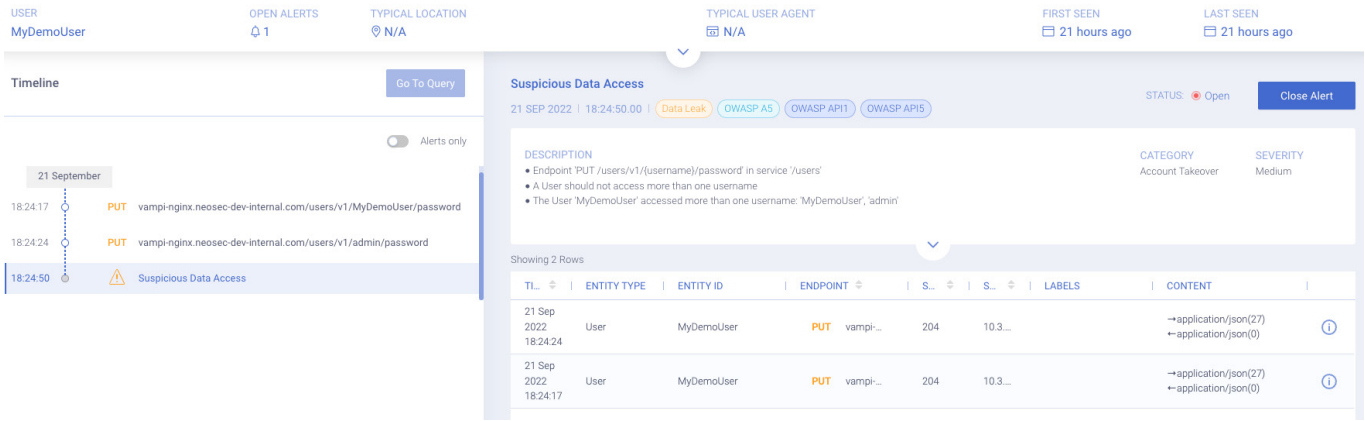
scoolio

GET/api/v3/Profile/ {ProfileID}

헤더:

- 권한: <MyAccessToken>

행위자 주체는 녹색으로 강조 표시되어 있고 요청된 리소스(프로필 ID)는 빨간색으로 강조 표시되어 있습니다. 이러한 관계를 이해한 후에는 적절한 경우 행위자의 접속을 단일 리소스로 제한하는 등의 일반적인 로직을 적용하기 위한 단계를 수행할 수 있습니다. 관계는 이보다 더 복잡할 수 있고 일대다 차원을 포함할 수 있기 때문에 이 작업은 결코 간단하지 않습니다. 하지만 머신 러닝과 행동 애널리틱스 같은 기술을 사용하면 가능합니다. 예를 들어, 고객 중 한 곳의 BOLA 취약점을 성공적으로 탐지한 결과는 다음과 같습니다.



이 사례는 실험실 환경에서 BOLA 취약점을 시뮬레이션했습니다. 주체 매핑과 행동 애널리틱스를 통해 Akamai 플랫폼은 BOLA를 탐지하고 많은 정보가 담긴 알림을 생성했습니다. 보안 분석가나 위협 탐색가가 이 알림을 확인하면 MyDemoUser가 비밀번호를 변경하기 위해 자신의 사용자 프로필에 접속(제재된 행동)한 것을 알 수 있습니다. 그러나 그 직후 타임라인에서 관리자 비밀번호를 변경하기 위해 또 다른 API 호출을 한 것을 볼 수 있습니다. 이는 행위자와 리소스 간의 관계를 고려할 때 명백히 승인되지 않은 행위이기 때문에 알림이 생성되었습니다.

API 보안 이니셔티브의 시작점

API 보안은 대부분의 기업에서 지속적으로 진행 중인 작업입니다. 따라서 어디서부터 시작해야 할지 알기 어려울 수 있습니다. 위의 3가지 기본 원칙은 좋은 출발점을 제시하지만 구축 시 다음 3가지 권장 사항을 준수하면 접근 방식의 효과를 크게 높일 수 있습니다.

1. 항상 최신 API 인벤토리 확보
2. 비프로덕션 및 프로덕션 API 환경 모니터링
3. 주체 간의 관계 강화

모르는 API는 보호할 수 없습니다. 따라서 효과적인 API 보안은 최신 API 인벤토리 및 보안 체계 평가에서 시작됩니다. 마찬가지로, API 보안 모니터링 기능을 개발할 때 제품 및 비프로덕션 API 구축 모두로 확장해야 합니다. 그리고 가장 중요한 것은 API 모니터링 및 적용이 단순히 작업을 넘어 API 활동과 관련된 주체 간의 관계를 고려해야 한다는 것입니다. 이를 통해 취약점과 보안 격차를 찾아내고 의도된 API 사용 모델 컴플라이언스를 적용할 수 있습니다. API의 행동을 이해하면 API 남용을 간파할 수 있습니다.

API 공격과 이를 방어하는 방법에 대해 자세히 알고 싶으신가요? OWASP API 상위 10대 취약점 분석 결과를 확인해 보세요.

Akamai

Akamai는 구축 및 전송되는 장소에 상관 없이 만들어지는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 직원, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 X(기존의 Twitter) LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다.