Akamai

OWASP 상위 10대

Akamai가 일반적인 취약점을 보호하는 방법

서론

OWASP(Open Web Application Security Project) 상위 10대 목록은 웹 애플리케이션에서 가장 일반적인 취약점을 다루며 이에 대한 기업의 인식을 제고합니다. OWASP 상위 10대 리스크를 적극 활용하려면 보안 벤더사가 기업의 개발 사례를 어떻게 보완하고, 얼마나 보완하며, 어떤 부분을 보완할 수 있는지 파악해야 합니다. 아래 내용은 OWASP 상위 10대 취약점에 관해 자세히 설명하고 Akamai가 엣지 보안 솔루션, 관리형 서비스, 세계 최대 규모의 인텔리전트 엣지 플랫폼을 통해 기업을 지원하는 방법을 소개합니다.

Akamai 제품

OWASP 상위 10대 리스크		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Managed Security Services	Akamai MFA	Page Integrity Manager
잘못된 접속 제어	A01			✓	✓	✓		✓		✓	
암호화 실패	A02			✓		✓	✓				✓
인젝션	A03			✓							
안전하지 않은 설계	A04			✓		✓					
잘못된 보안 설정	A05		✓	✓	✓						
취약하고 오래된 구성요소	A06		✓	✓							✓
식별 및 인증 실패	A07	✓		✓	✓	✓		✓		✓	
소프트웨어 및 데이터 무결성 실패	A08		✓	✓			✓				✓
보안 로깅 및 모니터링 실패	A09		✓	✓		✓	✓		✓		
서버 측면 요청 위조	A10		✓	✓							

OWASP 상위 10대 항목은 한 가지 리스크가 아니라 리스크의 카테고리입니다. Akamai의 솔루션은 이러한 리스크 카테고리를 다양한 방식으로 해결합니다. 자세한 내용은 백서에서 확인하시기 바랍니다.

A01: 잘못된 접속 제어

> **"접속 제어는 사용자가 의도한 권한 이외의 작업을 수행할 수 없도록 정책을 적용합니다. 실패할 경우 일반적으로 무단 정보 공개, 수정 또는 모든 데이터의 파기 또는 사용자의 한계를 벗어난 업무 수행으로 이어집니다."**
>
> **- 출처: owasp.org**

Akamai의 지원 방법

기업이 손상된 접속 제어 취약점을 완전히 해결하려면 접속 제어 모델을 수정해야 합니다. 하지만 Akamai의 WAAP에 대한 전문 지식을 활용하면 이를 악용하려는 일부 공격 기법을 탐지하고 차단할 수 있습니다.

- **Enterprise Application Access**는 기업 사용자를 대상으로 최소 권한 접속 모델을 적용해 인증된 사용자가 권한이 있는 애플리케이션에만 접속하도록 허용함으로써 제로 트러스트 보안 모델을 지원합니다.
- **Akamai MFA**는 피싱 방지 FIDO2 기술 표준을 기반으로 강력한 인증 서비스를 제공합니다.
- **App & API Protector**는 Akamai WAAP 솔루션으로 Akamai API Gateway를 통해 'referer' 헤더를 확인하고 API에 대한 인증을 적용해 접속 제어를 강화함으로써 강력한 브라우저 공격을 차단합니다.
- **Identity Cloud**는 사용자 데이터에 대한 접속을 세분화함으로써 내부 사용자 또는 시스템별로 최소 권한 접속을 허용합니다.
- **Bot Manager**는 자동화된 툴 공격과 로그인 공격을 방지합니다.

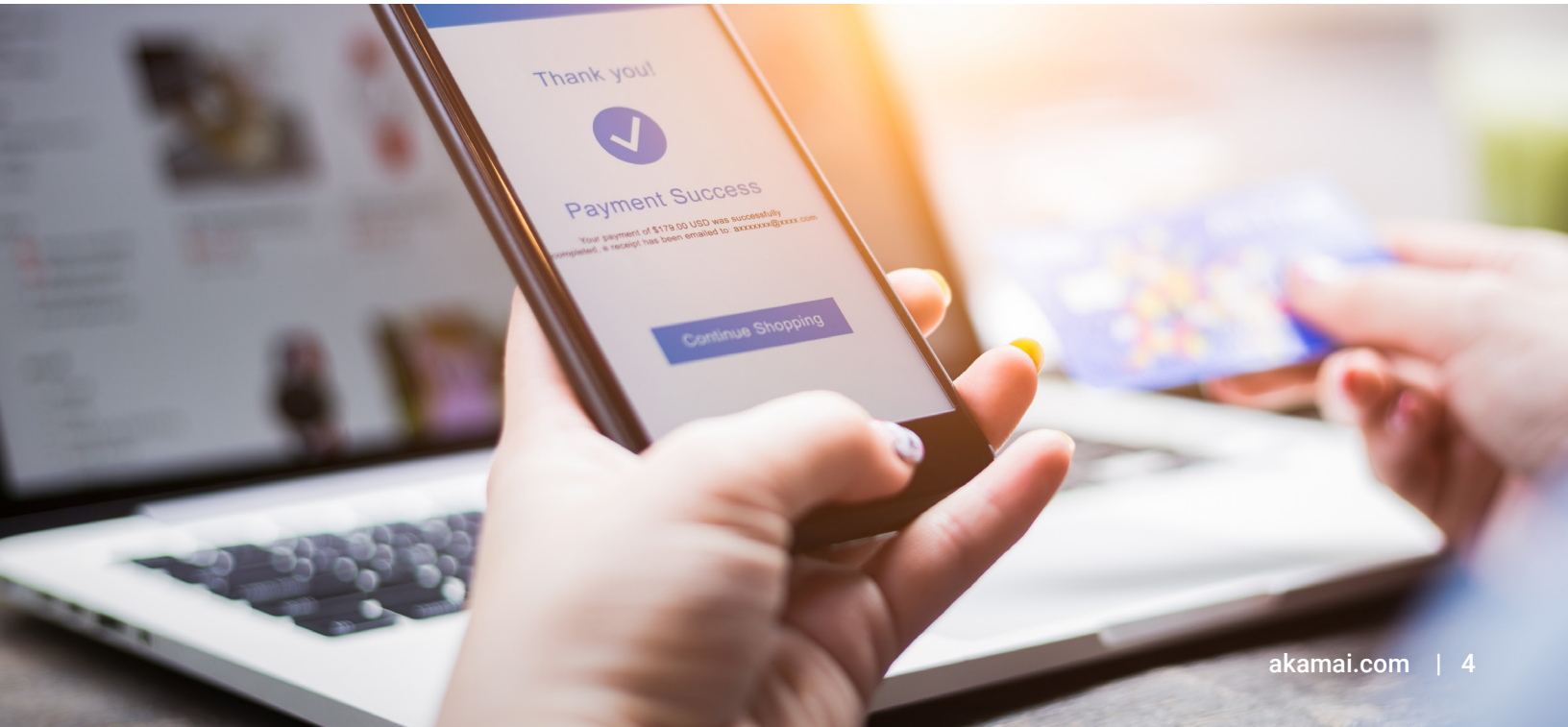
A02: 암호화 실패

> **"핵심은 암호화(또는 암호화 부족)와 관련된 실패입니다. 중요한 데이터가 유출될 수 있습니다. 예를 들면 암호, 신용카드 번호, 건강 기록, 개인 정보, 그리고 비즈니스 기밀은 특히 데이터가 개인 정보 보호법의 적용을 받는 경우 추가적인 보호가 필요합니다."**
>
> **- 출처: owasp.org**

Akamai의 지원 방법

기업은 단 하나의 솔루션만으로는 암호화 실패에서 완전히 안전할 수 없습니다. 하지만 여러 솔루션을 결합하면 암호화 실패의 일부 측면을 해결할 수 있습니다. 세부 내용은 다음과 같습니다.

- **App & API Protector**는 최신 버전의 TLS 및 강력한 암호화를 통해 전송 중인 중요 데이터를 암호화하고 보호합니다. 또한 다음과 같은 이점이 있습니다.
  - 모든 브랜드의 TLS 인증서를 지원하고 고객의 프라이빗 키를 보호하는 보안 CDN을 통해서만 서비스를 제공해 PCI 컴플라이언스를 준수합니다.
  - 권한 있는 직원만 서버에 접속할 수 있도록 하기 위해 케이지드 랙 및 모션 탐지기 같은 운영 및 물리적 보안으로 보호되는 CDN을 제공합니다.
  - API PII 학습을 통해 민감한 데이터 유출을 찾아 방지합니다.
- **Enterprise Application Access**는 통신을 암호화하고 기밀 데이터를 네트워크상의 해커로부터 숨기는 방식으로 원격 접속을 보호합니다.
- **Enterprise Threat Protector**는 중요한 데이터의 유출을 방지하는 데 도움이 됩니다.
- **Page Integrity Manager** 는 암호화 실패의 결과인 자바스크립트의 잘못된 사용으로 인해 발생하는 PII 데이터 유출을 탐지합니다.



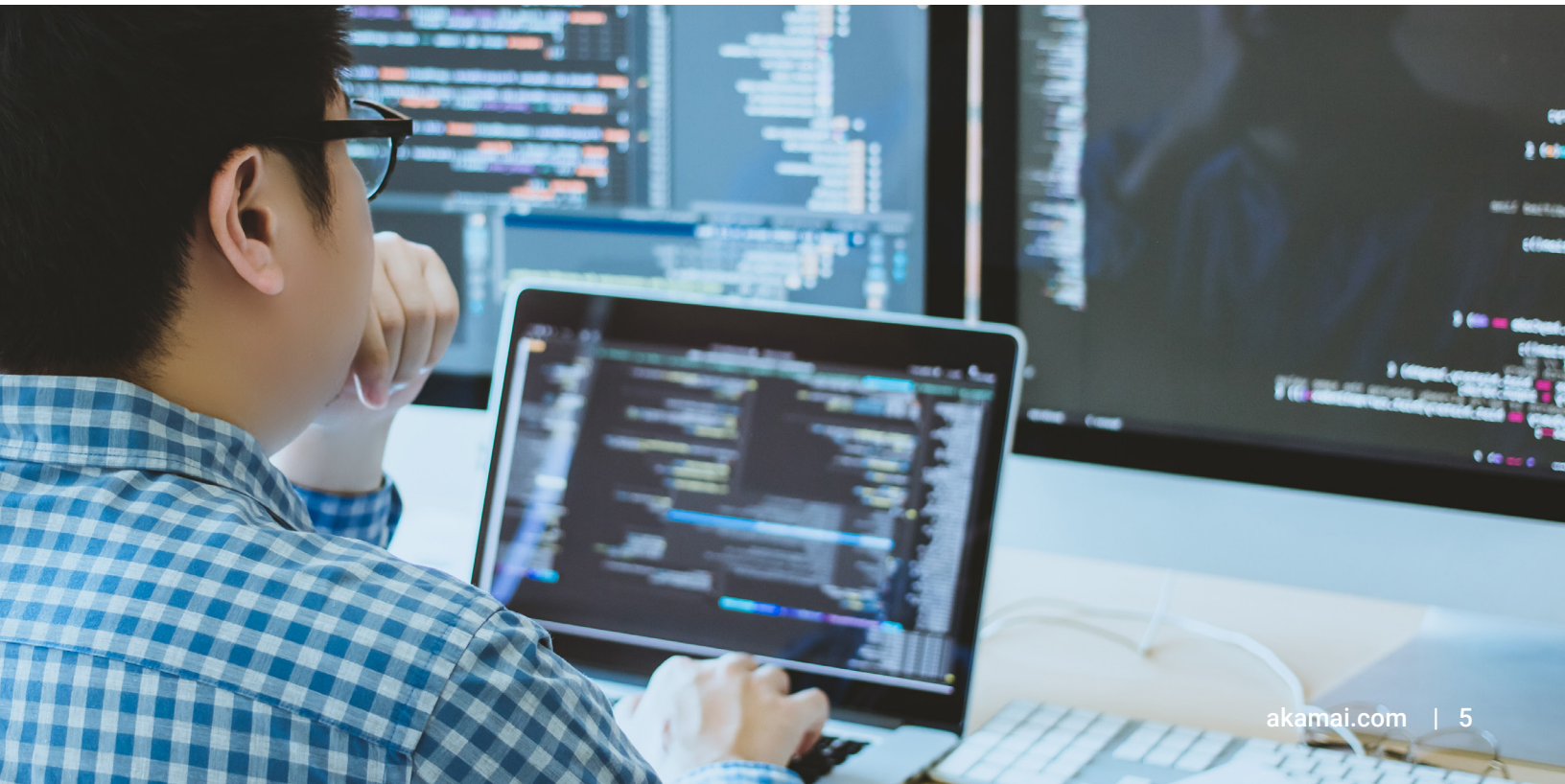
A03: 인젝션

> **SQL, NoSQL, OS, LDAP 인젝션 등과 같은 인젝션 취약점은 신뢰할 수 없는 데이터가 명령어 또는 쿼리의 일부로 전송될 때 발생합니다. 공격자의 악성 데이터는 프로그램(interpreter)을 속여 의도하지 않은 명령어를 실행하거나 적절한 권한 없이 데이터에 접근하도록 만들 수 있습니다.**
>
> **- 출처: Akamai**

Akamai의 지원 방법

WAAP를 사용하면 웹 애플리케이션과 API 인젝션 결함으로 인한 리스크를 차단할 수 있습니다. 그러나 기업은 이와 동시에 개발 주기를 기반으로 발견되지 않은 취약점을 모두 해결할 수 있도록 항상 웹 애플리케이션에 패치를 적용해야 합니다.

- **App & API Protector**는 인젝션 공격을 광범위하게 차단하는 기능을 즉각 제공하는 적응형 보안 엔진(ASE)을 갖춘 업계 최고의 WAAP 솔루션입니다. ASE 페널티 박스는 최근에 WAAP를 사용해 인젝션 공격을 시도한 클라이언트에서 들어오는 모든 트래픽을 일시적으로 차단할 수 있습니다.
- 맞춤형 룰이 포함된 가상 패치는 애플리케이션에 패치를 적용할 때까지 새로 등장하는 인젝션 취약점이나 애플리케이션 변경에 따른 새로운 취약점을 신속히 해결하도록 지원합니다. 보안팀은 Akamai의 API 기능을 활용해 가상 패치를 자동화하고 DevSecOps 프로세스에 통합할 수 있습니다.
- **Client Reputation**은 인젝션 기반 공격을 탐지하고 차단하는 데 도움이 되며, 웹 공격자 카테고리에 속하는 악성 클라이언트의 리스크 점수를 제공합니다.



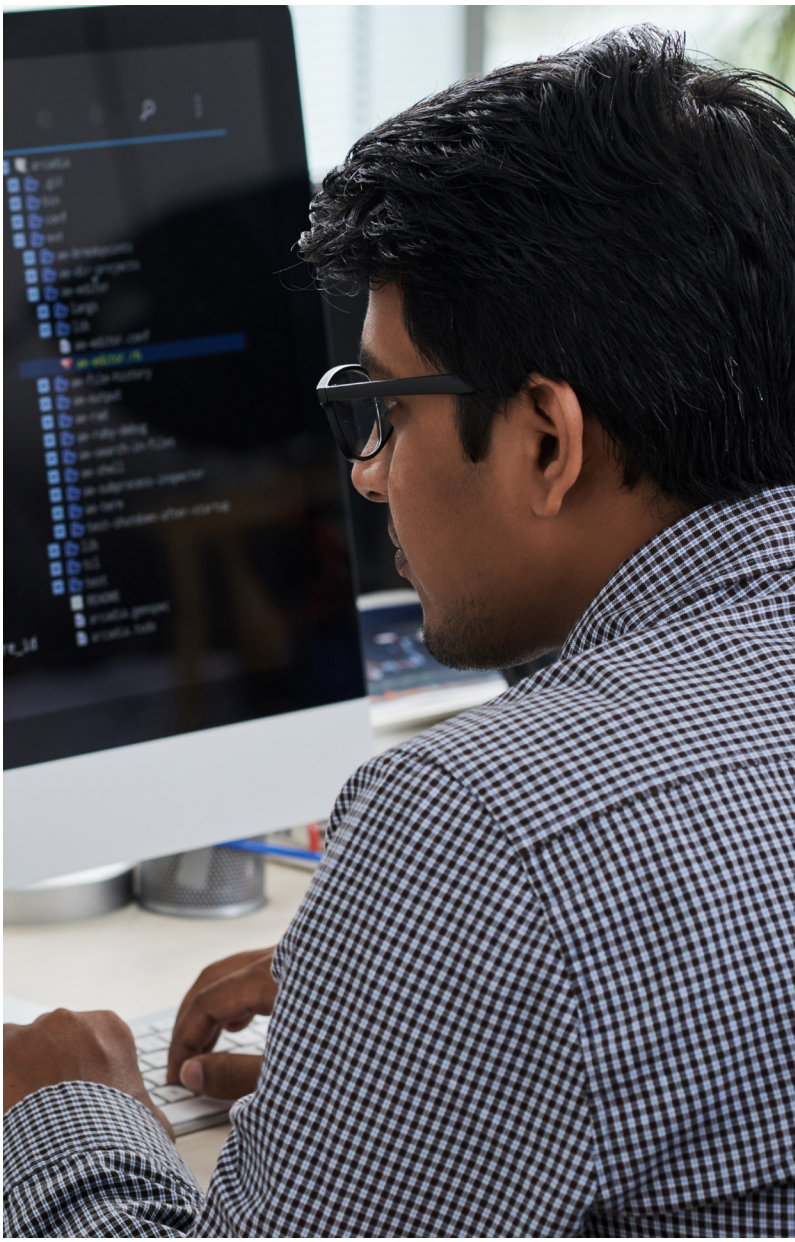
A04: 안전하지 않은 설계

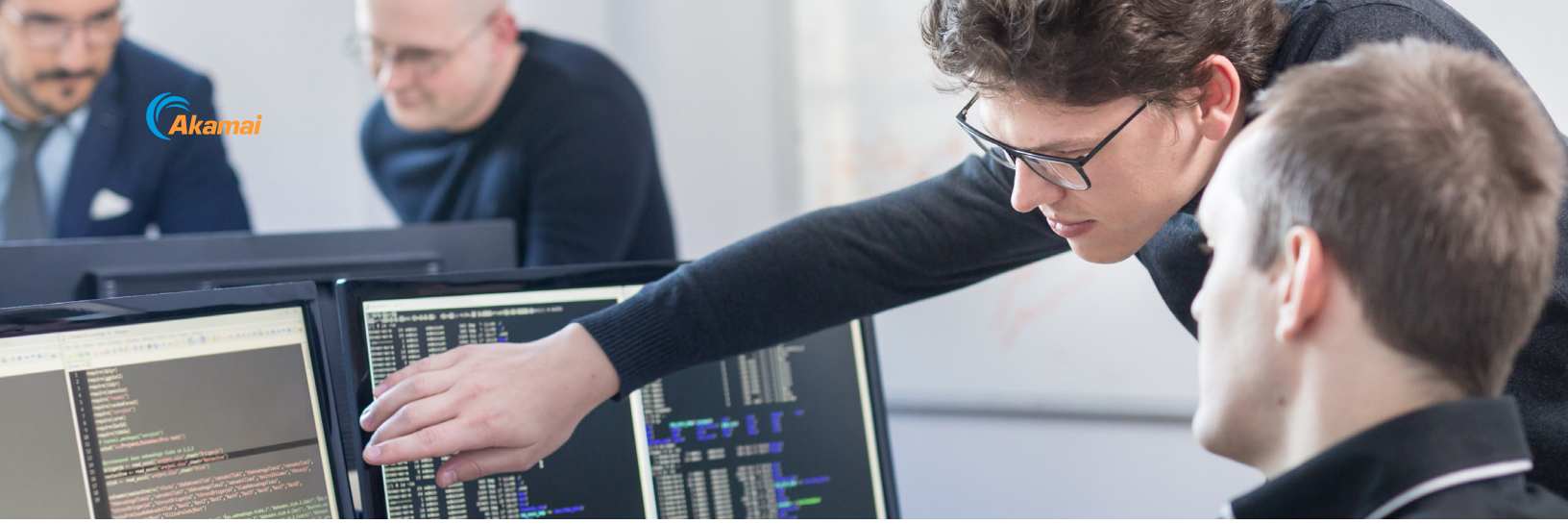
> **"안전하지 않은 설계는 다양한 약점을 나타내는 광범위한 카테고리로서 '누락 또는 비효율적인 제어 설계'로 표현됩니다. 안전하지 않은 설계와 안전하지 않은 구현에는 차이가 있습니다. 설계가 안전하더라도 구현에 결함이 있으면 악용될 수 있는 취약점으로 이어질 수 있습니다. 안전하지 않은 설계는 완벽한 구현으로 해결할 수 없고 특정 공격을 방어하기 위해 필요한 보안 제어가 만들어지지 않았습니다."**
>
> **- 출처: owasp.org**

Akamai의 지원 방법

기업은 첫 번째 설계 단계부터 보안을 통합해야 합니다. 만약 보안 기능을 통합하기 힘들다면 개발팀은 상당한 어려움을 겪을 수 있습니다. Akamai 제품을 사용하면 기업은 취약한 설계 보안으로 인해 앱과 API가 손상되는 것을 방지할 수 있습니다.

- **App & API Protector**는 WAAP 솔루션과 ASE로 구성되어 있고 프로덕션 단계에서 발생할 수 있는 일부 설계 취약점을 탐지하고 수정할 수 있습니다. 또한 자동화를 활용해 사람의 분석이 필요한 작업은 사람이 처리하지만, 일상적인 작업의 부하를 분산하고 간소화합니다. 이런 자동화 기능에는 자동 업데이트, 셀프 튜닝, API 검색, 간소화된 프로그래밍 기능, 사용자 경험이 포함됩니다.
- **Enterprise Application Access**는 권한 있는 사용자만 애플리케이션에 접속할 수 있도록 합니다. 이 최소 권한 접근 방식은 VPN과 같은 네트워크 접속 솔루션에서 쉽게 발생할 수 있는 다른 애플리케이션으로의 측면 이동을 방지합니다.





A05: 잘못된 보안 설정

> **"이전 버전 이후 이 리스크 카테고리에서 특정 형태의 잘못된 설정이 있는지 애플리케이션의 90%를 테스트한 결과, 평균 발생률은 4%였고, 20만 8천여 건의 CWE(Common Weakness Enumeration)가 나타났습니다. 반복적이고 조율된 애플리케이션 보안 설정 프로세스가 없으면 시스템 리스크가 높아집니다."**
>
> **- 출처: owasp.org**

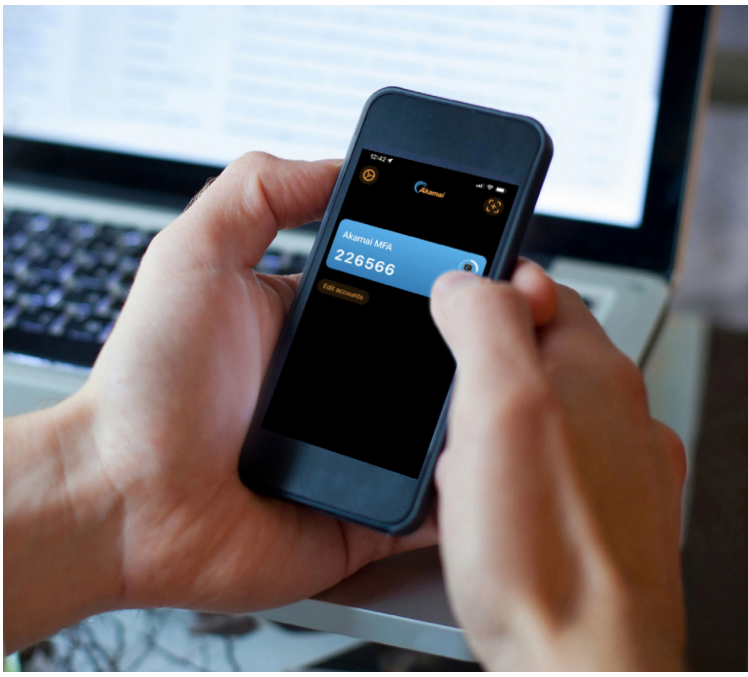
Akamai의 지원 방법

잘못된 보안 설정은 애플리케이션 보안의 여러 측면을 포함합니다. 또한 기업에서는 보안 제어를 적절히 설정해야 합니다. Akamai 제품은 이를 다음과 같은 방식으로 지원합니다.

- **App & API Protector**는 올바른 설정을 대체할 수는 없지만 다음과 같은 방법으로 도움을 줄 수 있습니다.
  1. 잘못된 보안 설정으로 노출되는 소스 코드와 오류 메시지 등의 정보 유출을 파악할 수 있는 아웃바운드 비정상 공격 그룹이 포함되어 있습니다.
  2. XML 분석기(parser)가 위험한 외부 개체를 처리하기 전에 XXE 공격을 탐지해 차단하는 룰을 구축합니다.
  3. 개발자가 프로덕션 서버에 남긴 알려진 중요한 파일에 대한 접속을 탐지할 수 있는 룰을 구축합니다.
- **Akamai Guardicore Segmentation**은 애플리케이션과 인터넷 간의 무단 또는 계획되지 않은 통신에 대한 가시성과 세분화된 제어를 제공함으로써, 잘못된 설정으로 인한 데이터 유출을 방어합니다.
- 맞춤형 룰이 포함된 가상 패치는 애플리케이션에 패치를 적용할 때까지 탐지된 데이터 유출을 신속하게 해결하도록 지원합니다.
- **App & API Protector**와 **Bot Manager**를 사용하면 기본 인증정보를 사용한 무차별 대입 공격을 전송률 제어 기능으로 보호할 수 있습니다.
- 콘텐츠 보안 정책과 기타 보안 관련 HTTP 헤더의 취약한 보안 설정은 Akamai 플랫폼에서 강화할 수 있습니다.
- **App & API Protector**의 자동 API 검색 기능을 사용하면 엔드포인트, 정의, 리소스 및 트래픽 특성 등 API를 지속적으로 자동 검색하고 프로파일링할 수 있습니다.

A06: 취약하고 오래된 구성요소

> "라이브러리, 프레임워크, 기타 소프트웨어 모듈 같은 구성요소는 애플리케이션과 동일한 권한으로 실행됩니다. 또한 스크립트는 애플리케이션 데이터에 대한 완전한 접속과 함께 신뢰할 수 있는 애플리케이션 리소스 역할을 합니다. 취약한 구성요소가 악용되면 심각한 데이터 손실 또는 서버 장악으로 이어질 수 있습니다."
>
> - 출처: Akamai



Akamai의 지원 방법

보안팀은 애플리케이션 내에 어떤 써드파티 구성요소가 있는지 전혀 파악하지 못하고 놓치는 경우가 종종 발생합니다. 또한 새로 발견된 취약점을 써드파티가 얼마나 빨리 해결할 수 있는지 관리할 수 없습니다. 이러한 가시성의 부족과 불확실성 문제를 해결하려면 WAAP 등의 보안 솔루션 뿐만 아니라 다음과 같은 스크립트 보안이 필요합니다.

- **App & API Protector**는 애플리케이션이나 써드파티 구성요소 등 알려진 취약점을 해결하도록 설계된 다양한 룰을 갖고 있습니다. 또한 API에 통합된 써드파티 구성요소가 악용되더라도 API를 보호하는 보안 기능을 제공합니다.
- **Akamai Guardicore Segmentation** 인사이트 모듈을 사용하면 네트워크상에서 취약한 모든 자산을 쿼리할 수 있습니다. 또한, 세분화된 적용을 통해 패치가 적용될 때까지 영향을 받는 모든 자산을 링펜싱할 수 있습니다.
- 맞춤형 룰이 포함된 가상 패치는 애플리케이션에 패치를 적용할 때까지 새로 등장하는 취약점이나 애플리케이션 변경에 따른 새로운 취약점을 신속히 해결하도록 지원합니다.
- **Client Reputation**은 웹 스캐닝 카테고리에서 악성 클라이언트에 리스크 점수를 지정해 새로운 취약점 악용을 차단하도록 지원합니다.
- **Page Integrity Manager**는 실제 사용자 세션에서 스크립트 실행 동작을 지속적으로 분석해 의심스럽거나 명백한 악성 행동을 파악합니다. 지속적으로 업데이트되는 CVE(Common Vulnerabilities and Exposures) 데이터베이스를 사용해 퍼스트파티·써드파티 스크립트에서 알려진 취약점이 있는 URL로 데이터가 유출되는 것을 차단합니다.

A07: 식별 및 인증 실패

> "인증 및 세션 관리와 관련된 애플리케이션 기능은 종종 잘못 구현되기 때문에 공격자가 암호, 키 또는 세션 토큰을 탈취하거나 기타 구현 취약점을 악용해 임시 또는 영구적으로 다른 사용자의 신원 정보를 사용할 수 있습니다."
>
> - 출처: Akamai

Akamai의 지원 방법

취약점을 완전히 해결하려면 근본적인 허점을 수정해야 합니다. 하지만 그렇게 하지 않더라도 아래에 나열된 Akamai 솔루션을 사용하면 식별 및 인증 실패를 악용하려는 많은 공격 기법을 탐지하고 보호하는 데 도움이 됩니다.

- **Bot Manager**는 인증정보 크리덴셜 스터핑 공격에 사용되는 자동화된 공격을 탐지하고 방어합니다.
- **Account Protector**는 사용자 계정에 대한 무단 접속을 시도하는 계정 탈취 시도를 방어합니다.
- **Enterprise Application Access**는 '최소 권한 접속 모델'을 통해 애플리케이션에 프록시로 접속할 수 있기 때문에 공격표면을 줄이고 접속을 강화합니다.
- **Akamai MFA**는 피싱 방지 FIDO2 기술을 사용해 강력한 인증을 제공합니다.
- **App & API Protector**는 무차별 대입 공격을 처리할 수 있는 전송률 제어 기능을 제공합니다.
- **Identity Cloud**는 2단계 인증 및 리스크 기반 인증 기능을 통해 사용자 인증정보와 프로필 정보를 안전하게 관리합니다.

A08: 소프트웨어 및 데이터 무결성 실패

> "소프트웨어와 데이터 무결성 실패는 무결성 위반으로부터 보호하지 못하는 코드 및 인프라와 관련이 있습니다. 예를 들어 애플리케이션이 신뢰할 수 없는 출처, 리포지토리와 콘텐츠 전송 네트워크(CDN)의 플러그인, 라이브러리 또는 모듈에 의존하는 경우가 있습니다. 보안이 취약한 CI 및 CD 파이프라인은 무단 접속, 악성 코드 또는 시스템 감염을 일으킬 수 있습니다."
>
> - 출처: owasp.org

Akamai의 지원 방법

기업은 WAAP를 사용해 소프트웨어 및 데이터 무결성 실패로부터 웹 애플리케이션과 API를 보호할 수 있습니다. 이와 동시에 개발 주기를 기반으로 발견되지 않은 취약점을 모두 해결할 수 있도록 항상 웹 애플리케이션에 패치를 적용해야 합니다.

- **App & API Protector**
  - 역직렬화 공격을 강력하게 차단합니다.
  - 최신 TLS 버전 및 강력한 암호화를 구현해 데이터 무결성 문제를 일으킬 수 있는 중간자 공격을 방지합니다.
  - Edge DNS와 함께 DNSSEC를 구현해 DNS 레코드의 데이터 오리진 인증 및 데이터 무결성 보호를 보장합니다. 이렇게 하면 DNS 레코드를 변조해 사용자를 신뢰할 수 없는 소스로 유도하는 것을 방지할 수 있습니다.
- **Akamai Guardicore Segmentation** 인사이트 모듈을 사용하면 손상된 업데이트를 수신한 네트워크의 모든 자산을 쿼리할 수 있습니다. 또한 세밀한 적용을 통해 수정이 생성될 때까지 영향을 받는 자산을 링펜싱할 수 있습니다.
- **Enterprise Threat Protector**는 애플리케이션 관리자 및 고급 사용자를 위험한 환경이나 신뢰할 수 없는 소스로 유인할 수 있는 피싱 공격을 탐지합니다.
- 맞춤형 룰이 포함된 가상 패치는 애플리케이션에 패치를 적용할 때까지 새로운 역직렬화 취약점을 신속히 해결하도록 지원합니다.
- **Page Integrity Manager**는 써드파티 스크립트를 탐지하고 변경 사항을 모니터링한 다음 감염된 스크립트에 대해 조치를 취합니다.

A09: 보안 로깅 및 모니터링 실패

"로깅, 탐지, 모니터링 및 활성 응답이 불충분하면 언제든지 발생합니다.

- 로그인, 로그인 실패, 고부가-가치 트랜젝션 등 감사 가능-한 이벤트는 기록되지 않습-니다.
- 경고 및 오류로 인해 로그 메시지가 생성되지 않거나 부적절하거나 불분명한 로그 메시지가 생성됩니다.
- 애플리케이션 및 API 로그는 의심스러운 활동을 모니터링하지 않습니다.
- 로그는 로컬에만 저장됩니다.
- 적절한 경고 임계값과 응답 에스컬레이션 프로세스가 마련되어 있지 않거나 유효-하지 않습니다.
- 동적 애플리케이션 보안 테스트(DAST) 툴을 사용한 모의 해킹 및 스캔은 알림을 트리거하지 않습니다.

애플리케이션은 실시간 또는 거의 실시간으로 진행 중인 공격을 탐지, 에스컬레이션 또는 알릴 수 없습니다."

- 출처: owasp.org

Akamai의 지원 방법

보안 로깅 및 모니터링 실패는 기업의 취약점 해결 능력과 이를 악용하려는 시도 간의 격차를 드러냅니다. Akamai는 다음을 비롯한 여러 기능을 통해 모든 공격에 대한 탁월한 가시성을 제공합니다.

- Akamai는 Akamai Control Center 그래픽 사용자 인터페이스 내에서 대시보드와 리포팅 툴을 제공합니다.
- Akamai의 애플리케이션 보안 제품은 기업의 기존 SIEM 인프라에 통합되어 Akamai에서 탐지한 이벤트를 다른 보안 벤더사의 이벤트와 통합합니다.
- **Managed Security Service**는 24시간 연중무휴 분석과 대응 기능을 제공합니다.
- **App & API Protector**에는 추가 심층 분석을 위해 악의적이거나 의심스러운 활동을 보여준 IP의 로깅을 늘릴 수 있는 페널티 박스 기능이 포함되어 있습니다.
- **Enterprise Application Access**는 모든 엔터프라이즈 애플리케이션에 대한 접속을 인증 및 제어하는 통합 ID 관리 솔루션을 제공합니다. 이 솔루션은 ID 인지 프록시 기능과 결합되어 모든 GET 및 POST 동작은 물론 사용자 동작에 대한 세부적인 가시성을 확보하도록 지원합니다.
- **Enterprise Threat Protector**는 모든 외부 DNS 요청(악성 및 정상 모두)에 대한 완벽한 가시성을 제공합니다.
- **Akamai Guardicore Segmentation**은 네트워크 내 통신 흐름에 대한 심층적인 가시성을 제공하기 때문에 무단 또는 예기치 않은 통신이 발생할 경우 알림이 트리거될 수 있으며 보안 정책을 개별 프로세스 또는 서비스 수준까지 적용해 통신을 제한할 수 있습니다. 추가적인 침해 탐지 모듈을 사용하면 잠재적인 위협을 신속하게 탐지하고 해결할 수 있습니다.

A10: 서버 측면 요청 위조

> **"SSRF 취약점은 웹 애플리케이션이 사용자가 제공한 URL의 유효성을 검사하지 않고 원격 리소스를 가져올 때마다 발생합니다. 공격자는 방화벽, VPN 또는 다른 유형의 네트워크 접속 제어 목록(ACL)으로 보호되는 경우에도 애플리케이션에서 조작된 요청을 예기치 않은 대상으로 전송하도록 강제할 수 있습니다."**
>
> **- 출처: owasp.org**

Akamai의 지원 방법

Akamai WAAP에는 URL 인젝션을 찾을 수 있는 룰이 포함되어 있습니다. 이 기능은 공격자가 서버를 다른 곳으로 유도해 보안 분석가에게 유효한 요청처럼 보이도록 요청을 제출하는 것을 방지할 수 있습니다.

- **App & API Protector** 룰은 이러한 악용 요청이 취약한 서버에 도달하는 것을 원천적으로 차단합니다.
- **Akamai Guardicore Segmentation**은 서버 수준에서 예기치 않은 아웃바운드 트래픽을 모니터링하고 차단합니다.

결론

OWASP 상위 10대 취약점에 대한 최적의 방어 체계를 구축하려면, 기업과 보안 벤더사가 협력해 최대한 신속하게 취약점을 공개하고 이를 방어하는 솔루션을 구현해야 합니다. Akamai의 엣지 보안 포트폴리오에 대해 자세히 알아보기 Akamai와의 파트너십을 통해 완벽한 비즈니스 보안 체계를 구축하는 방법에 대해 알아보고 이에 관한 논의를 진행하고 싶으신 경우 Akamai 영업 담당자에게 연락하시기 바랍니다.