

Kritische Überlegungen zu API-Sicherheit und PCI DSS v4.0- Konformität

Einführung

Die Notwendigkeit, immer neue Vorschriften erfüllen zu müssen, kennen IT-Sicherheitsteams zur Genüge. Da hat man endlich die EU-Richtlinie zur Netz- und Informationssicherheit (NIS1) erfüllt und schon kommt NIS2. Angesichts der Tatsache, dass mehr als 130 Länder weltweit Datenschutzgesetze mit regelmäßigen Aktualisierungen erlassen haben¹, ist es nicht verwunderlich, dass nur 9 % der Führungskräfte² sehr zuversichtlich sind, alle Offenlegungsanforderungen erfüllen zu können.

Wenn Ihr Unternehmen die Version 4.0 des Payment Card Industry Data Security Standard (PCI DSS) einhalten muss, geht es Ihnen möglicherweise genauso. Seit 2018 muss jedes Unternehmen, das Kreditkarten wichtiger Anbieter akzeptiert und Karteninhaberdaten elektronisch verarbeitet, speichert oder überträgt, die Anforderungen gemäß PCI DSS-Version 3.2.1 erfüllen. Doch im März 2022 veröffentlichte der Payment Card Industry Data Security Council die Version 4.0 und gab Unternehmen zwei Jahre Zeit, die Einhaltung der neuen Regeln sicherzustellen. Bald darauf wurden auch schon Pläne für eine Reihe weiterer Aktualisierungen verkündet, die im März 2025 kommen sollen.

Diese Updates können eine Belastung für viel beschäftigte Sicherheitsteams darstellen, aber es steht einiges auf dem Spiel. Unter den zahlreichen Updates, die Unternehmen in PCI DSS v4.0 erfüllen müssen, gibt es auch welche, die mit API-Risiken und -Schwachstellen zusammenhängen. In diesem Whitepaper geben wir Einblicke in die Anforderungen von PCI DSS v4.0 in Bezug auf APIs, und wir zeigen, welchen Nutzen Akamai API Security in diesem Zusammenhang bietet.

1. Morrison Foerster, [Catch Up on Privacy Around the World on Data Privacy Day 2021!](#) 29. Januar 2021.

2. PwC, [CEE findings from the 2023 Global Digital Trust Insights Survey](#)



Was bleibt unverändert?

Die Anforderungen der ursprünglichen Version decken Sicherheitsgrundlagen ab, die heute genauso wichtig sind wie bei der Veröffentlichung des PCI DSS im Jahr 2006.

Zum Beispiel:

- Überwachung und Kontrolle des Zugriffs auf alle Verwaltungskonten in allen IT-Systemen, die Karteninhaberdaten verarbeiten oder speichern
- Zuweisung des Zugriffs auf System- und Karteninhaberdaten auf Need-to-know-Basis und Definieren der Zugriffsanforderungen nach Rolle

Was hat sich geändert?

Die Komplexität der Bedrohungslandschaft hat gegenüber 2006, als PCI DSS erstmals in Kraft trat, exponentiell zugenommen. Unternehmen müssen zwar immer noch berücksichtigen, dass Cyberkriminelle Bereiche wie privilegierte Konten und Nutzer mit übermäßigen Berechtigungen angreifen. Sie müssen aber auch ihre Compliance-Programme anpassen, um auf Angreifer reagieren zu können, die häufig Tausende von APIs in Zahlungstechnologien ins Visier nehmen. Diese Angreifer wissen, dass APIs leicht ausgenutzt werden können und eine effiziente Möglichkeit bieten, Karteninhaberdaten zu stehlen und die digitale Infrastruktur zu attackieren.

Die Ziele von PCI DSS v4.0 bestehen darin, den Sicherheitsanforderungen der Zahlungsbranche weiterhin gerecht zu werden, die Sicherheit als kontinuierlichen Prozess zu fördern, die Flexibilität für verschiedene Methoden zu erhöhen und die Validierungsmethoden zu verbessern. Diese Version verbessert den Schutz von Zahlungsdaten durch neue Kontrollen, um die Bedrohung durch komplexe Cyberangriffe wie API-Missbrauch abzuwehren.

PCI DSS v4.0 – Allgemeiner Überblick

| | |
|---|--|
| Aufbau und Wartung sicherer Netzwerke und Systeme | Installation und Verwaltung von Netzwerksicherheitskontrollen |
| | Anwendung sicherer Konfigurationen auf alle Systemkomponenten |
| Schutz von Kontodaten | Schutz gespeicherter Kontodaten |
| | Schutz von Karteninhaberdaten mit starker Kryptographie während der Übertragung über offene, öffentliche Netzwerke |
| Einsatz eines Programms für Sicherheitsmanagement | Schutz aller Systeme und Netzwerke vor schädlicher Software |
| | Entwicklung und Pflege sicherer Systeme und Software |
| Implementierung wirkungsvoller Maßnahmen zur Zugriffskontrolle | Beschränkung des Zugriffs auf Systemkomponenten und Karteninhaberdaten je nach Geschäftsinformationsbedarf |
| | Nutzeridentifizierung und Authentifizierung des Zugriffs auf Systemkomponenten |
| | Beschränkung des physischen Zugriffs auf Karteninhaberdaten |
| Regelmäßiges Überwachen und Testen der Netzwerke | Protokollierung und Prüfung aller Zugriffe auf Karteninhaberdaten |
| | Regelmäßige Sicherheitstests für Systeme und Netzwerke |
| Durchsetzen von Informationssicherheitsrichtlinien | Unterstützung der Informationssicherheit mit Unternehmensrichtlinien und -programmen |

PCI-DSS-Anforderungen für APIs

Anforderung 6: Entwicklung und Pflege sicherer Systeme und Software

PCI DSS v4.0-Anforderung 6 bezieht sich speziell auf APIs. Dieses Whitepaper behandelt zwar die einzelnen Unterabschnitte von Anforderung 6, Akamai API Security ist jedoch für viele Fälle relevant, die sich aus den PCI-DSS-Anforderungen insgesamt ergeben.

Anforderung 6 bezieht sich auf die folgenden Aspekte:

- Maßgeschneiderte und kundenspezifische Software muss sicher entwickelt werden
- Sicherheitslücken müssen identifiziert und behoben werden
- Öffentlich zugängliche Webanwendungen müssen vor Angriffen geschützt werden
- Änderungen an allen Systemkomponenten müssen sicher verwaltet werden



Anforderung 6.2.2

Diese Anforderung behandelt Schulungen für Softwareentwickler, die an maßgeschneiderter und nutzerdefinierter Software arbeiten. Diese Entwickler müssen mindestens einmal alle zwölf Monate in Bezug auf Sicherheitsaspekte, die für ihre Tätigkeit relevant sind, geschult werden. Das schließt sicheres Softwaredesign und sichere Codierungstechniken mit ein. Diese Schulung vermittelt, wie Sicherheitstesttools zur Erkennung von Software-Schwachstellen verwendet werden.

API Security kann mit Schulungen der Akamai University und Workshops zum Thema API-Sicherheit zur Erfüllung dieser Anforderung beitragen.

Akamai University

Präsenzs Schulungen zur Plattform sind über die Akamai University verfügbar und stehen allen Kunden von API Security zur Verfügung.

Workshops zu API Security

API Security führt Online- und Präsenz-Workshops zu den Funktionen der Plattform und des Active-Testing-Moduls durch und trägt gleichzeitig dazu bei, dass Kunden APIs entwickeln, die die Sicherheit vom Code bis zur Produktion gewährleisten.



 **Workshop zur API-Sicherheit**

Dieser Workshop richtet sich an technische Fachkräfte und Führungskräfte, die sich für ein Verständnis von APIs (Application Programming Interfaces) und deren Risiken interessieren. Sie erhalten praktische Einblicke in die Techniken, die Angreifer verwenden, um anfällige APIs auszunutzen, was auch APIs mit unbeabsichtigtem Daten- und Internetzugriff einschließt.

Außerdem erhalten Sie einen Überblick über den tatsächlichen API-Traffic und erfahren, wie er in Akamai API Security – mithilfe von Funktionen wie APL-Posture-Management und Laufzeitschutz – überwacht und analysiert wird.

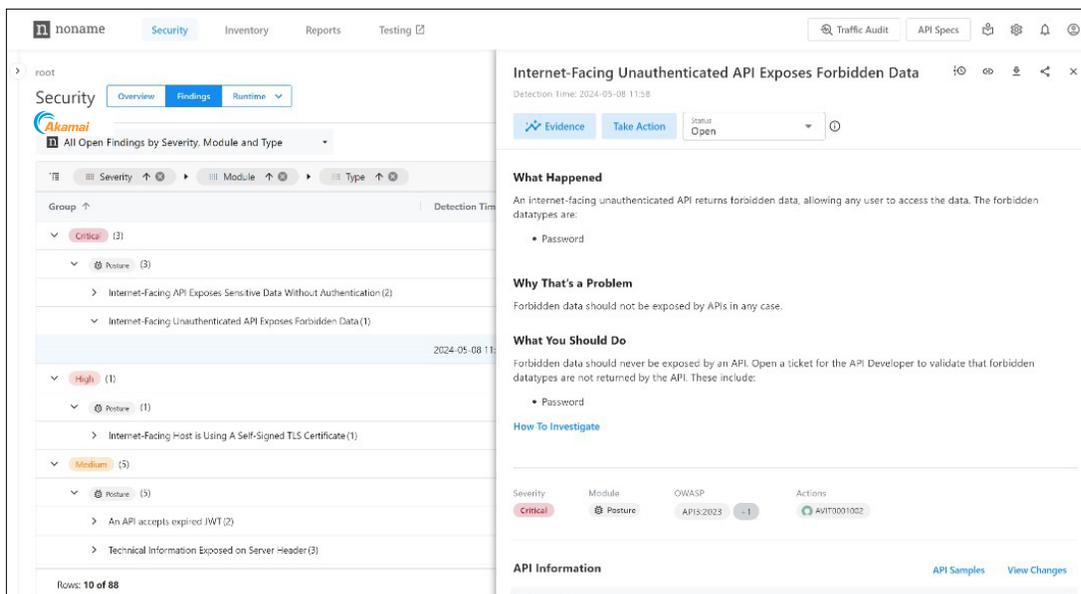
 **Etwa 4 Stunden**

Anforderung 6.2.3

Die Anforderung umfasst Überprüfungsroutrinen für maßgeschneiderten Anwendungscode (das heißt für den Code, der von einem Drittanbieter entwickelt wurden und bei dem es sich nicht um gängige Standardanwendungen handelt). So ist sichergestellt, dass keine Schwachstellen in die Produktion gelangen. Konkret auf APIs bezogen, werden Unternehmen aufgefordert zu bestätigen, dass die betreffende Software die Funktionen externer Komponenten wie Bibliotheken, Frameworks und APIs sicher verwendet.

API Security erfüllt diese Anforderung auf unterschiedliche Weise:

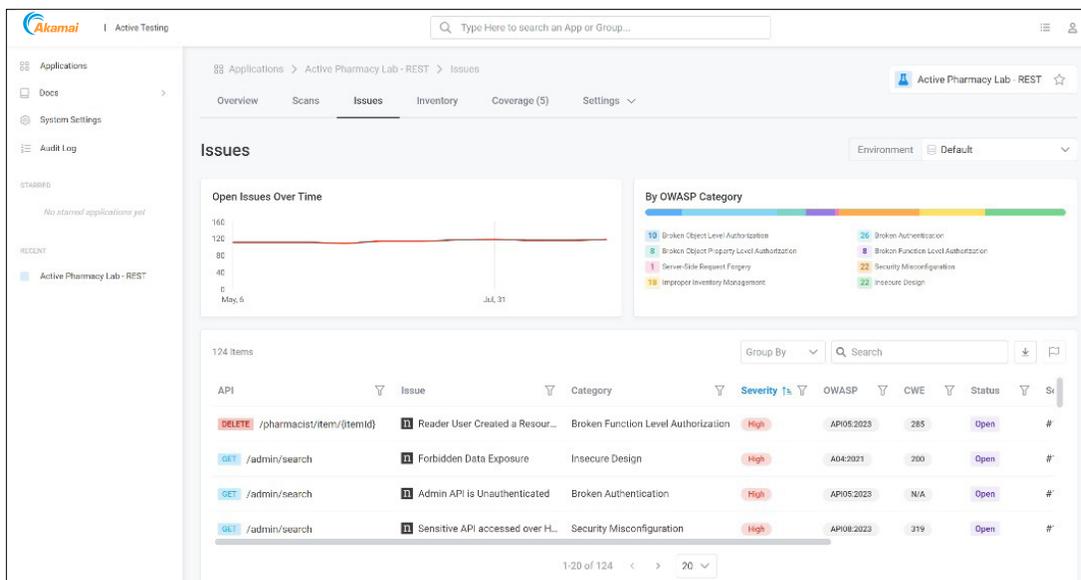
- API Security kann bestätigen, welche API-basierten Komponenten verwendet werden und wie ihr Sicherheitsstatus ist. Unternehmen haben so die Möglichkeit, Fehlkonfigurationen zu erkennen, die Sicherheitslücken zur Folge haben könnten. Ein Beispiel wäre hier die Verwendung schwacher Verschlüsselungscodes.
- API Security kann auch überprüfen, ob APIs normal verwendet werden und sich wie erwartet verhalten. Anschließend kann die IT-Abteilung Kontrollen implementieren, um Cyberkriminelle daran zu hindern, Ihre Systeme zu missbrauchen – zum Beispiel wenn ein Angreifer das Verhalten der Anwendung testet, um Logikschwachstellen zu erkennen.
- Darüber hinaus kann API Security erkennen, welche Frameworks von Drittanbietern Funktionen für Ihre APIs bereitstellen, sodass Sicherheitsteams diese dann mit Listen veralteter und anfälliger Frameworks abgleichen können.
- API Security bietet außerdem eine vollständige Bestandsaufnahme all Ihrer APIs, einschließlich der verschiedenen Versionen, sodass Sie Einblicke in potenzielle nicht dokumentierte Funktionen und Backdoors erhalten, um die Sie sich kümmern müssen.



The screenshot displays the Akamai API Security console interface. On the left, a navigation pane shows 'Security' with sub-sections for 'Overview', 'Findings', and 'Runtime'. Below this, a list of findings is shown, filtered by severity. The selected finding is 'Internet-Facing Unauthenticated API Exposes Forbidden Data', which is categorized as 'Critical' and detected on '2024-05-08 11:58'. The main panel on the right provides detailed information about this finding, including a 'What Happened' section explaining that an unauthenticated API returns forbidden data (like passwords), a 'Why That's a Problem' section stating that forbidden data should not be exposed, and a 'What You Should Do' section advising to validate that forbidden datatypes are not returned. The 'API Information' section at the bottom shows the finding's severity (Critical), module (Posture), OWASP category (API:2023), and actions (AVIT001002).

Auch Active Testing ist in mehrfacher Hinsicht für Anforderung 6.2.3 relevant:

- Active Testing kann die Sicherheit Ihres API-Codes prüfen und mit dazu beitragen, dass keine API-bezogenen Schwachstellen in die Produktion gelangen.
- Active Testing unterstützt auch die Implementierung von Best Practices für die sichere Codierung von APIs, mit denen Sie einen programmatischen Ansatz zur kontinuierlichen sicheren Bereitstellung von Code verfolgen können.
- Active Testing umfasst die automatisierte Codeprüfung, kann aber auch manuell verwendet werden, um gegebenenfalls erforderliche manuelle Codeprüfungen zu berücksichtigen.



The screenshot displays the Akamai Active Testing dashboard for an application named "Active Pharmacy Lab - REST". The interface includes a navigation sidebar on the left with options like Applications, Docs, System Settings, and Audit Log. The main content area shows the "Issues" tab, which contains a line graph titled "Open Issues Over Time" and a "By OWASP Category" bar chart. Below these charts is a table listing 124 items, with the following visible rows:

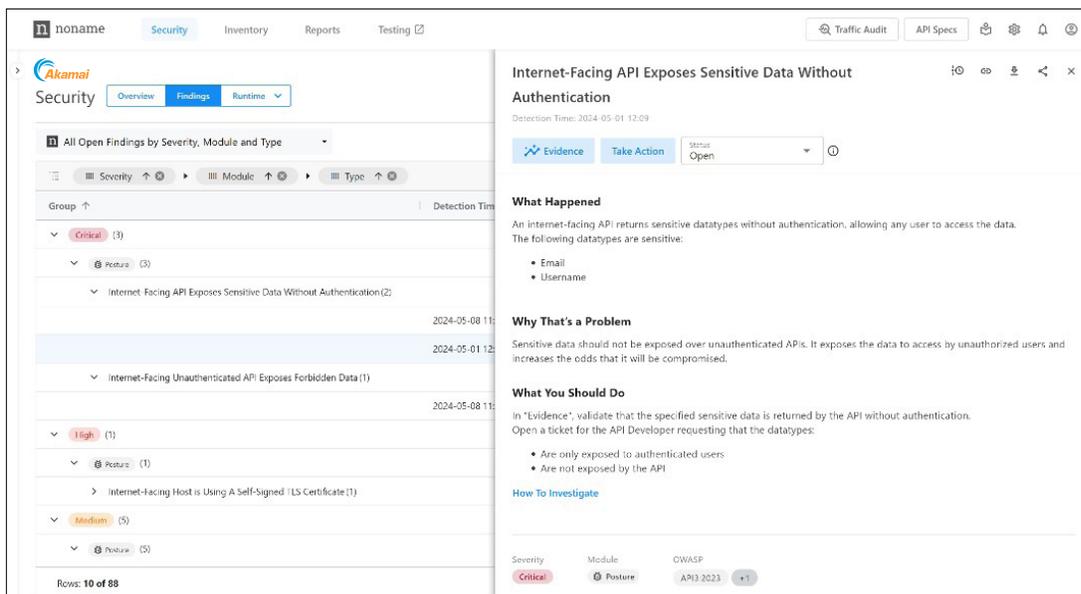
| API | Issue | Category | Severity | OWASP | CWE | Status | St |
|----------------------------------|----------------------------------|-------------------------------------|----------|------------|-----|--------|----|
| DELETE /pharmacist/item/{itemId} | Reader User Created a Resour... | Broken Function Level Authorization | High | API05:2023 | 285 | Open | # |
| GET /admin/search | Forbidden Data Exposure | Insecure Design | High | A04:2021 | 200 | Open | # |
| GET /admin/search | Admin API is Unauthenticated | Broken Authentication | High | API05:2023 | N/A | Open | # |
| GET /admin/search | Sensitive API accessed over H... | Security Misconfiguration | High | API08:2023 | 319 | Open | # |

Anforderung 6.2.4

Diese Anforderung umfasst die Verwendung von Software-Engineering-Techniken oder anderen Methoden, mit denen sich verbreitete Softwareangriffe und verwandte Sicherheitsrisiken verhindern oder abwehren lassen. Die in dieser Anforderung genannten Bedrohungen reichen von relativ einfachen Injection-Angriffen bis hin zu ausgefeilteren, bei der API-Geschäftslogik ansetzenden Angriffen.

API Security erfüllt diese Anforderung auf unterschiedliche Weise:

- Das Laufzeitsicherheitsmodul in der API-Security-Lösung von Akamai kann potenziell schädliche Aktivitäten erkennen, die auf die Ausnutzung der Geschäftslogik der API und ihrer unbeaufsichtigten ML-Komponente abzielen. Das Laufzeitsicherheitsmodul erkennt autonom Abweichungen vom typischen API-Verhalten und gibt bei potenziellen Angriffen Warnungen aus.
- API Security kann auch Abwehrstrategien für Injection-Angriffe ermitteln und vorschlagen, um die zugrunde liegenden Schwachstellen zu beheben.



The screenshot displays the Akamai API Security interface. On the left, a list of findings is shown, categorized by severity: Critical (3), High (1), and Medium (5). The selected finding is 'Internet-Facing API Exposes Sensitive Data Without Authentication' (Critical), detected on 2024-05-01 12:09. The right-hand pane provides details for this finding, including a 'What Happened' section explaining that sensitive data (Email and Username) is exposed without authentication. It also includes a 'Why That's a Problem' section stating that this exposes data to unauthorized users and a 'What You Should Do' section advising to validate sensitive data is returned only to authenticated users. A 'How To Investigate' section is also present. At the bottom, a table shows the finding's metadata: Severity: Critical, Module: Posture, and CWASP: API3.2023 (+1).

- API Security korreliert alle relevanten Aktivitäten und Aktionen und kann so die für den Angriff verantwortlichen Akteure identifizieren. Auf diese Weise können Sie den Angriff blockieren und die erforderlichen Kontrollen und Abhilfemaßnahmen implementieren, um die Ursache des Angriffs zu beheben.

The screenshot shows the Akamai API Security interface. On the left, there's a sidebar with 'Security' selected and a list of attackers, including 'JWT: test@test.com' with a 'Medium' risk score. The main area is titled 'Attacker Information' and shows a 'Confidence' of 31%, 'Attacker Risk' of 'Medium', and 'Country' as 'United States'. Below this is a table of incidents:

| Last Activity | Incident | Severity | Triggered On | Actions |
|------------------|---|----------|---|----------|
| 2024-08-11 06:48 | Scraping Attack on Authenticated API Succeeded | Medium | /api/v2/account/<guid>/details GET tal-lab.nonamesec.com | Evidence |
| 2024-08-11 02:47 | API With Broken Object Level Autho Succeeded | Low | /api/v2/account/<guid>/details GET tal-lab.nonamesec.com | Evidence |
| 2024-08-11 06:46 | API With Broken Object Level Autho Succeeded | Low | /api/v2/account/<guid>/details GET tal-lab.nonamesec.com | Evidence |
| 2024-08-01 00:01 | API With Broken Object Level Autho Succeeded | Low | /api/v2/account/<guid>/details GET tal-lab.nonamesec.com | Evidence |
| 2024-08-01 06:01 | Scraping Attack on Authenticated API Succeeded | Medium | /api/v2/account/<guid>/details GET sce-lab.nonamesec.com | Evidence |
| 2024-08-01 06:01 | API With Broken Object Level Autho Succeeded | Low | /api/v2/account/<guid>/details GET sce-lab.nonamesec.com | Evidence |

- In ähnlicher Weise werden auch Injection-Angriffe erkannt. API Security bietet auch hier Anleitungen zur Problembekämpfung.

Auch Active Testing berücksichtigt Anforderung 6.2.4 in mehrfacher Hinsicht:

- Active Testing kann die Sicherheit Ihres API-Codes prüfen und dazu beitragen, dass keine API-bezogenen Schwachstellen und Fehlkonfigurationen in der Geschäftslogik in die Produktion gelangen. Fehler in der Geschäftslogik lassen sich durch Nutzung von Inline-APIs und Komponenten für die Anwendungssicherheit wie Web Application Firewalls und API-Gateways nur sehr schwer erkennen. Diese Tools arbeiten ohne Berücksichtigung des Kontexts von API-Transaktionen und sind nicht in der Lage, schädliche oder ungewöhnliche Aktivitäten einzelnen Angreifern zuzuordnen.

The screenshot shows the Akamai Active Testing interface. The main view is for an issue titled 'Reader User Created a Resource' with a 'High' severity and 'Open' status. The issue details include:

- Category:** Broken Function Level Authorization
- Description:** The API endpoint failed to properly check the user's permissions and identity, allowing a user with 'reader' permissions to create/update a resource. This is a serious security issue known as Broken Function Level Authorization (BFLA), and it can enable attackers to bypass authorization checks and access unauthorized functionalities.
- Remediation:** We recommend implementing a proper authorization mechanism that includes object-level authorization checks for every API endpoint. This mechanism should verify the identity and permissions of the requesting user before allowing any actions on the resource. Additionally, consider implementing access control lists (ACLs) or role-based access control (RBAC) to provide finer-grained control over the API resources.

On the right side, there are sections for 'Security Frameworks' and 'Compliance Violations'.

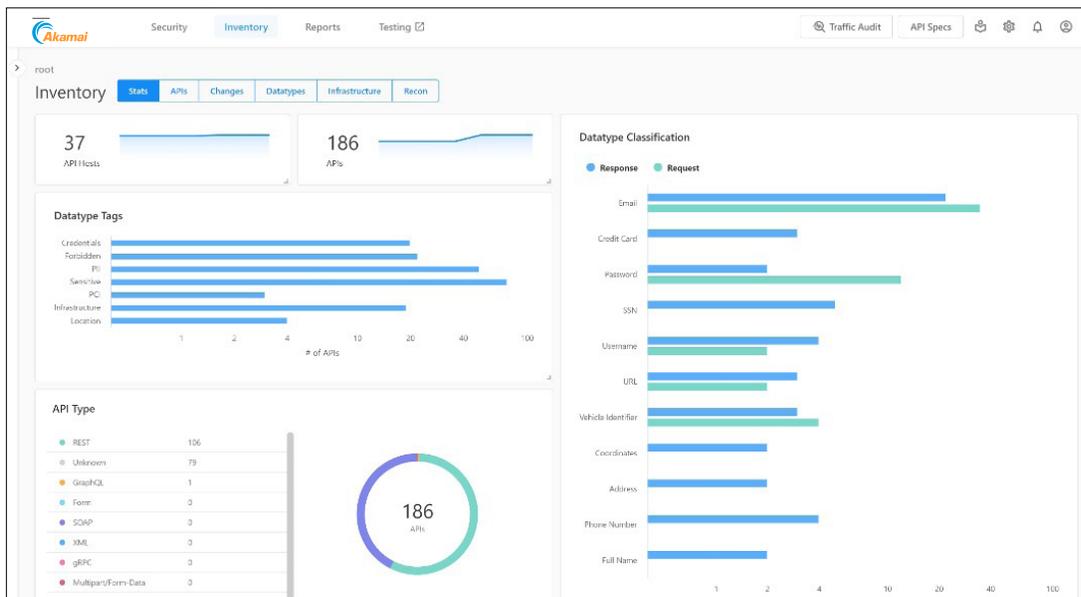
- Active Testing kann auch API-Komponenten sicher wiederverwenden, um die Entwicklung unter Einhaltung der höchsten Sicherheitsstandards zu beschleunigen.

Anforderung 6.3.2

Um Schwachstellen- und Patch-Management ordnungsgemäß durchzuführen, müssen Unternehmen jetzt alle ihre maßgeschneiderten Software-Lösungen identifizieren und auflisten, einschließlich der von ihnen integrierten Software von Drittanbietern.

API Security erfüllt diese Anforderung auf verschiedene Weisen:

- API Security kann eine vollständige und umfassende Bestandsaufnahme aller APIs erstellen, einschließlich der Frameworks von Drittanbietern, die die Sicherheitslage Ihrer APIs beeinflussen können.
- API Security kann auch Veränderungen an der Funktionalität Ihrer APIs überwachen und identifizieren. Darüber hinaus kann die Lösung Ihren tatsächlichen API-Traffic mit API-Spezifikationen vergleichen und Abweichungen identifizieren, die sich auf die API-Funktionalität auswirken können.
- API Security kann die Art der Daten überwachen, die über Ihre APIs ausgetauscht werden, und Richtlinien erstellen, um speziell mit Blick auf die PCI DSS-Compliance Probleme beim Datenaustausch zu beheben.



- Mit API Security können Sie nach bestimmten Mustern suchen, etwa nach den für PCI DSS relevanten Datentypen (z. B. der 16-stelligen Kreditkartennummer), und Datenrichtlinien anwenden, um entsprechend zu reagieren.



noname Security **Inventory** Reports Testing

root

Inventory **Stats** **APIs** Changes Datatypes Infrastructure Recon

Akamai Reset View Save Filter As Search APIs

| Host | Path | Method | API Risk | Auth | Internet Facing | API Environment | Findings |
|------------------------------|-----------------------------------|--------|----------|---------------------------------|-----------------|-----------------|----------|
| demo-us1s-vampi.nonamesec.co | /users/v1 | GET | 6.7 | Not Detected | HTTP | Production | None |
| demo-us1s-vampi.nonamesec.co | /users/v1/debug | GET | 6.7 | Not Enforced | HTTPS | Production | ⊗ |
| demo-us1s-vampi.nonamesec.co | /users/v1/%20OR%20%20=% | GET | 6.3 | Not Detected | HTTPS | Production | ⊗ |
| demo-us1s-crapi.nonamesec.co | /identity/api/v2/vehicle/vehicles | GET | 6.2 | header: authorization: sub: JWT | HTTPS | Production | None |
| 3.86.114.171.8868 | /identity/api/v2/vehicle/vehicles | GET | 6.1 | header: authorization: sub: JWT | HTTP | Undefined | None |
| wawindows-ego723cu57yak.az | / | GET | 5.5 | Not Detected | HTTP & HTTPS | Undefined | None |
| wapythonwithstartup-ego722cu | / | GET | 5.3 | Not Detected | HTTP & HTTPS | Undefined | None |
| wanode-ego723cu57yak.azure | / | GET | 5.5 | Not Detected | HTTP & HTTPS | Undefined | None |

- API Security ermöglicht Ihnen auch die Implementierung komplexer Prüfungen und Warnungen. So können beispielsweise bestimmte Daten in APIs mit bestimmten Eigenschaften zugelassen sein (z. B. intern ausgerichtet oder über bestimmte Methoden authentifiziert), in anderen dagegen unzulässig sein.

Fazit

APIs sind in modernen Anwendungsumgebungen zur Standardmethode für Konnektivität und Datenaustausch geworden. Vor diesem Hintergrund ist der Schutz von APIs sowohl aufseiten der Vorproduktion (Shift-Left) als auch der Postproduktion entscheidend, damit der Betrieb gesichert bleibt. API Security erfüllt die neuen Anforderungen von PCI DSS v4.0 und darüber hinaus durch Anwendung einer intuitiven und einfach zu implementierenden Lösung.

API Security deckt die wesentlichen Funktionen ab, die Sie benötigen, um eine API-Sicherheitsstrategie für API-Erkennung, API-Posture-Management, API-Laufzeitschutz und API-Sicherheitstests zu implementieren.

Erfahren Sie, wie Sie sich **vor den OWASP API Security Top 10** schützen können.

Erfahren Sie, wie wir Sie unterstützen können, und vereinbaren Sie eine individuelle **Demo zu Akamai API Security**.



Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. Gemeinsam mit Ihnen können wir auf diese Weise Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf [X](#) und [LinkedIn](#).
Veröffentlicht: 09/24.