Akamai

WHITE PAPER

How Akamai Helps to Mitigate the OWASP API Security Top 10 Vulnerabilities

Introduction

Today's application programming interfaces (APIs) enable flexible, rapid, and economical integration between virtually any software, device, or data source. APIs serve a broad range of functionality and provide a foundation for innovation and digital transformation. Multi-cloud hybrid environments, mobile, and SaaS offerings are just some examples of the underlying importance of APIs. APIs have also become the de facto standard for building and connecting modern applications, especially with the increasing move to microservices-based architectures. Small, independent microservices are assembled into more complex applications using APIs. These APIs are important because they allow for interaction with the microservice itself. From simple internal flows between parts of a microservice application to major B2B transactions worth millions, it is important to properly secure APIs because they serve as the digital glue that connects different systems and partner ecosystems, enable digital and omnichannel customer experiences, and are vulnerable to virtually all the same risks related to classic web applications.

Our traditional understanding of APIs – e.g., machine-to-machine or third-party APIs – can and should be expanded to include mobile and web application services as a part of the microservices-based architecture. In other words, a web request within the microservices architecture is an API that serves as one in a series of calls to various microservices. Each of these calls can potentially open security holes and create privacy risks that can range from poor data validation, configuration errors, and flaws in implementation to the lack of integration between security components. This is important to note when addressing the vulnerabilities defined within the Open Web Application Security Project (OWASP) API Security Top 10.

In 2017, OWASP included underprotected APIs as part of its OWASP Top 10. Then in 2019, the project published the API Security Top 10 with a list of the most common types of API vulnerabilities. The goal of both the OWASP Top 10 and API Security Top 10 is to raise awareness about common security vulnerabilities that developers should consider, drive that awareness across an array of development practices, and help instill a culture of secure development practices. One should not treat these as simple checklists of attack vectors that can be blocked by one or any combination of web application and API protection (WAAP) solutions, API gateways, API management, and/or API specialist tools.

Mitigating API-related risks requires an understanding of not only the APIs themselves, but also the role that both security vendors and your organization have in securing them. Some risk areas can only be fully addressed by developers, but security vendors can help with specific areas. Addressing the API Security Top 10 requires an understanding of where and how (and how much) security providers can help augment your existing development practices.

> Our traditional understanding of APIs can and should be expanded to include mobile and web application services as a part of the microservices-based architecture.

The following describes the areas in which Akamai can help support your efforts with our edge security solutions, managed services, and intelligent edge platform.

API1:2019 Broken Object Level Authorization

OWASP Definition: APIs tend to expose endpoints that handle object identifiers, creating a wide attack surface-level access control issue. Object-level authorization checks should be considered in every function that accesses a data source using input from the user.

How Akamai Can Help

This vulnerability is present when a client's authorization is not properly validated to access the object IDs. Organizations can reduce this risk by not relying solely on object IDs passed in the request by a client or by using a non-guessable random ID for objects. The objective is to validate authorization for all accessed objects or mask the true ID of objects when appropriate, to further mitigate risk. This is because attackers may try to request resources directly and not through the expected application flow. Akamai can help in the following way:

- Akamai's web application and API protection (WAAP) solution – App & API Protector – can partially identify these requests through the Referer header validation.

API2:2019 Broken User Authentication

OWASP Definition: Authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other users' identities temporarily or permanently. Compromising a system's ability to identify the client/user compromises API security overall.

How Akamai Can Help

While organizations must fix their broken user authentication process to fully address this vulnerability, Akamai can help to detect and protect against many of the attack vectors that attempt to exploit it.

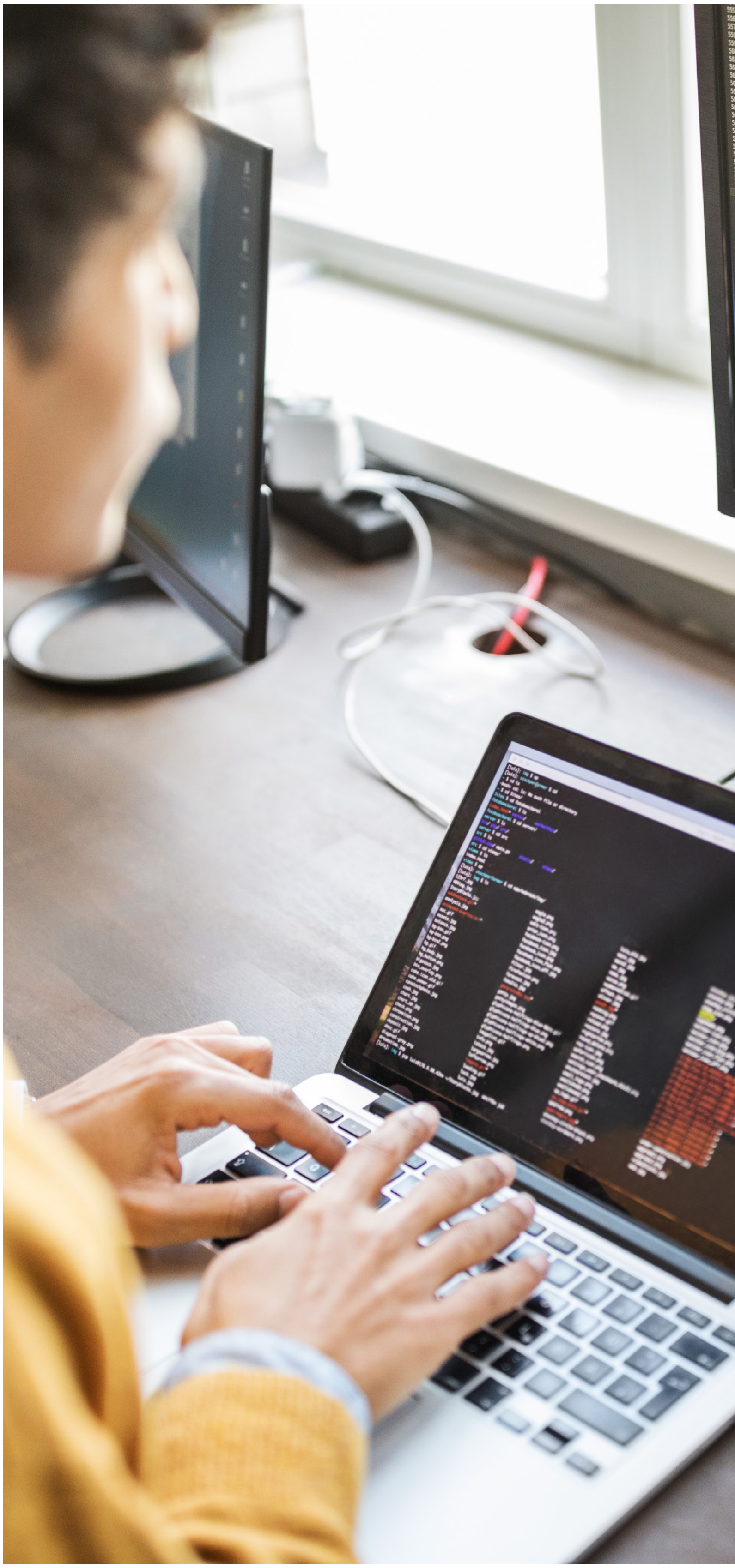
- Akamai's API gateway capabilities support JSON Web Token (JWT) validation for authentication on individual resources – with keys that check claims inside tokens and compute RSA digital signatures – to ensure tokens were not tampered with.
- Akamai's bot management solution can detect and manage the automation used in credential stuffing and brute-force authentication attacks.

While organizations must fix their broken user authentication process to fully address this vulnerability, Akamai can help to detect and protect against many of the attack vectors that attempt to exploit it.

API3:2019 Excessive Data Exposure

OWASP Definition: Looking forward to generic implementations, developers tend to expose all object properties without considering their individual sensitivity, relying on clients to perform data filtering before displaying it to the user.

Without control over a client's state, servers perform more filtering, which can be abused to gain access to sensitive data.



How Akamai Can Help

APIs should only return data that is relevant and required for its intended purpose. When excessive data is exposed – e.g., software technology, versions, etc. – it allows attackers to mine for vulnerabilities and sensitive data. While organizations reduce the unnecessary exposure of object properties and review them for sensitivity, various Akamai solutions can help address some aspects of this vulnerability.

- App & API Protector with Advanced Security Management includes positive API security that defines acceptable JSON and XML object formats to filter out those that may inadvertently expose excessive data.
- App & API Protector allows custom response actions so customers can define and serve HTML, XML, JSON-based, or other types of responses to mislead attackers looking for sensitive data.

API4:2019 Lack of Resources and Rate Limiting

OWASP Definition: Quite often, APIs do not impose any restrictions on the size or number of resources that can be requested by the client/user. Not only can this impact the API server performance, leading to a denial of service (DoS), but it also leaves the door open to authentication flaws such as brute force.

How Akamai Can Help

APIs often do not limit the number of requests they serve within a given time, nor limit the amount of data returned. This can lead to attackers performing DoS attacks that make the system unavailable to legitimate users. Akamai solutions provide rate limiting and protection from low-and-slow attacks to throttle and control API requests.

- App & API Protector with Advanced Security Management provides rate controls that allow customers to define thresholds for requests on a per-API basis. It limits clients when they exceed those thresholds. Throttling capabilities can apply to the entire API, selected resources, and/or HTTP verbs for a given resource.

- App & API Protector protects API back-end infrastructure from resource exhaustion launched via low-and-slow DoS attacks (e.g., Slow POST).

- App & API Protector with Advanced Security Management can restrict the size, type, and depth of requests; for example, request constraints can be used to validate JSON and XML against predefined formats to prevent resource exhaustion.

API5:2019 Broken Function Level Authorization

OWASP Definition: Complex access control policies with different hierarchies, groups, and roles, and an unclear separation between administrative and regular functions, tend to lead to authorization flaws. By exploiting these issues, attackers gain access to other users' resources and/or administrative functions.

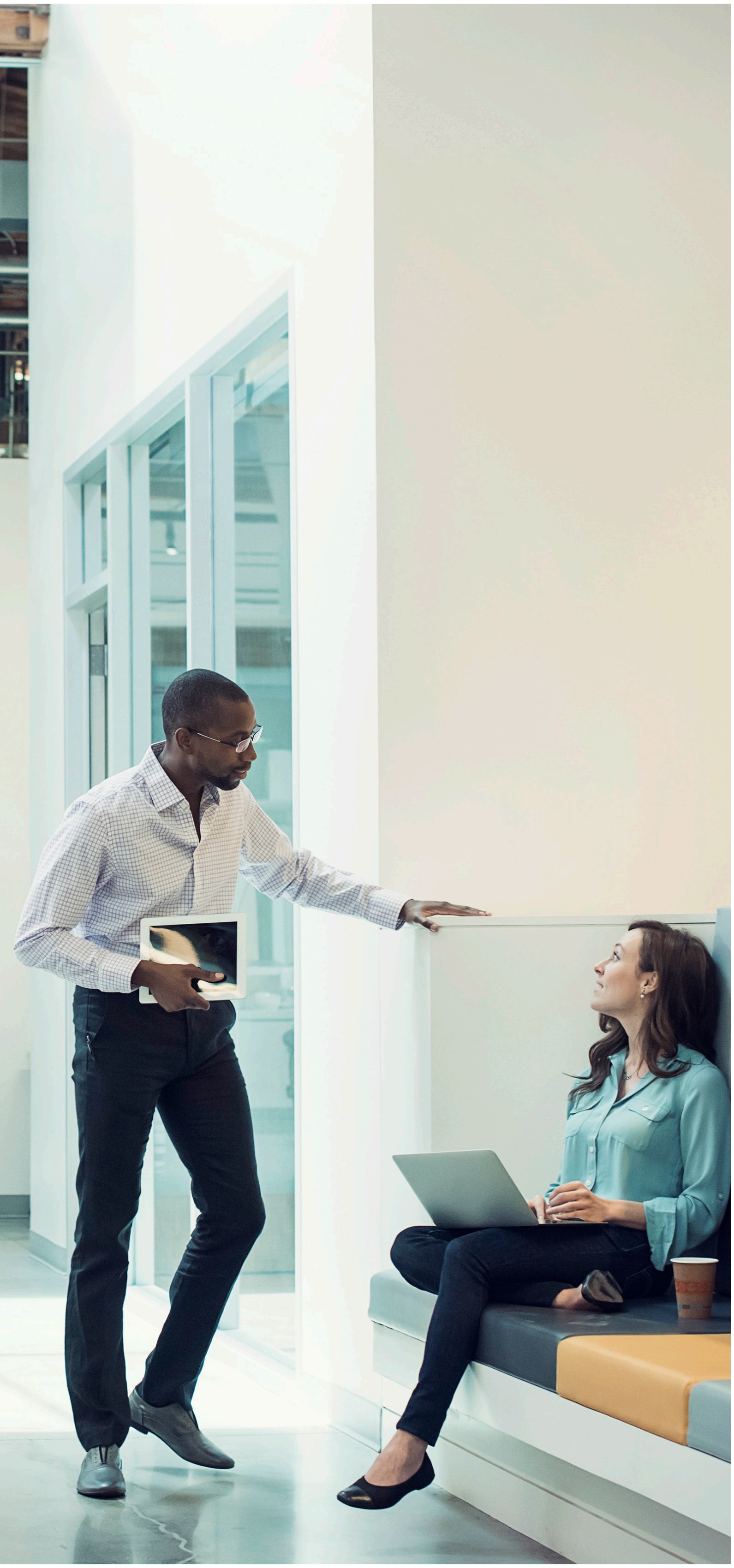
How Akamai Can Help

While organizations must work to fix their access control models to fully address this vulnerability, Akamai can help detect and protect against some of the attack vectors that attempt to exploit broken function level authorization.

- Akamai Enterprise Application Access enables a least-privilege access model for enterprise users, allowing only visibility and access to authorized applications by authenticated users. This helps create separation between administrative and regular user functions and mitigates the risk of authorization flaws with a Zero Trust security model.

- App & API Protector can be used to automatically discover sensitive API endpoints (e.g., administrative panels) that may be inadvertently exposed to the public.

Akamai solutions provide rate limiting and protection from low-and-slow attacks to throttle and control API requests.



API6:2019 Mass Assignment

OWASP Definition: Binding client-provided data (e.g., JSON) to data models, without proper properties filtering based on an allowlist, usually leads to a mass assignment. Either guessing objects' properties, exploring other API endpoints, reading the documentation, or providing additional object properties in request payloads allows attackers to modify object properties they are not supposed to.

How Akamai Can Help

Modern API frameworks encourage developers to automatically bind client input into code variables and internal objects. While legitimate users should be allowed to update some data fields, they should not be able to change user-level permissions and/or other administrative functions. API endpoints are considered vulnerable if they automatically convert the client input into internal object properties without taking into account its level of exposure and sensitivities. Akamai can help mitigate this risk.

- App & API Protector with Advanced Security Management includes positive API security that defines acceptable JSON and XML object formats to filter out those that are maliciously crafted.

API7:2019 Security Misconfiguration

OWASP Definition: Security misconfiguration is commonly a result of unsecured default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, unnecessary HTTP methods, permissive cross-origin resource sharing (CORS), and verbose error messages containing sensitive information.

How Akamai Can Help

By definition, security misconfiguration covers multiple aspects of the application and API security and requires organizations to properly configure security controls. While not a substitute for proper configuration, Akamai can help protect against data leakage, fix misconfigured headers, restrict unnecessary methods, and more.

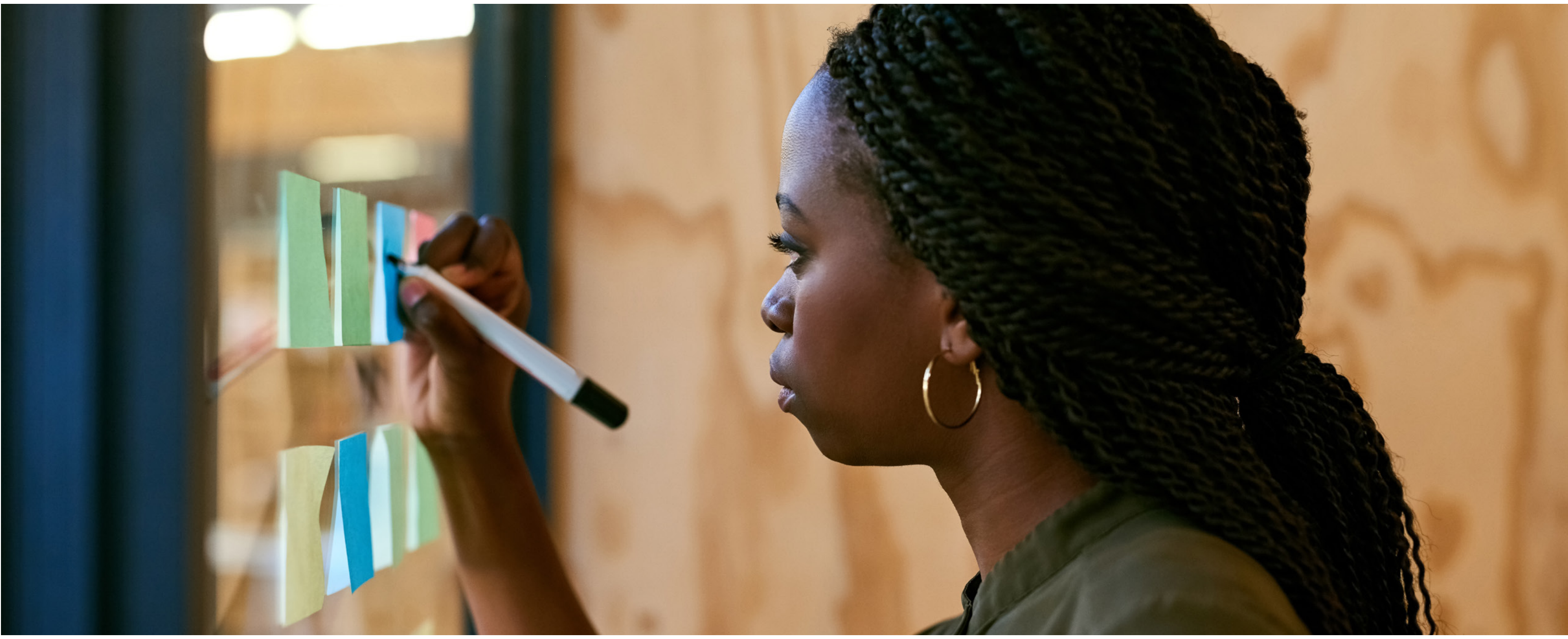
- App & API Protector with Advanced Security Management can be used to inspect the HTTP response from web applications to detect sensitive data leaving a web application, such as SQL error codes/messages, directory, and filename leakages.

- App & API Protector provides custom rules that can be used to detect the presence of personally identifiable information, such as Social Security numbers, and be used to virtually patch APIs.

- Granular control of CORS policies with full CORS functionality can be set and enforced at the edge with API gateway capabilities.

- App & API Protector provides the option for custom response actions at the edge where customers can define and serve HTML, XML, JSON-based, or other types of responses to mislead attackers looking for sensitive data in error messages.

- App & API Protector can add and remove HTTP headers to patch misconfigurations and enforce security best practices.



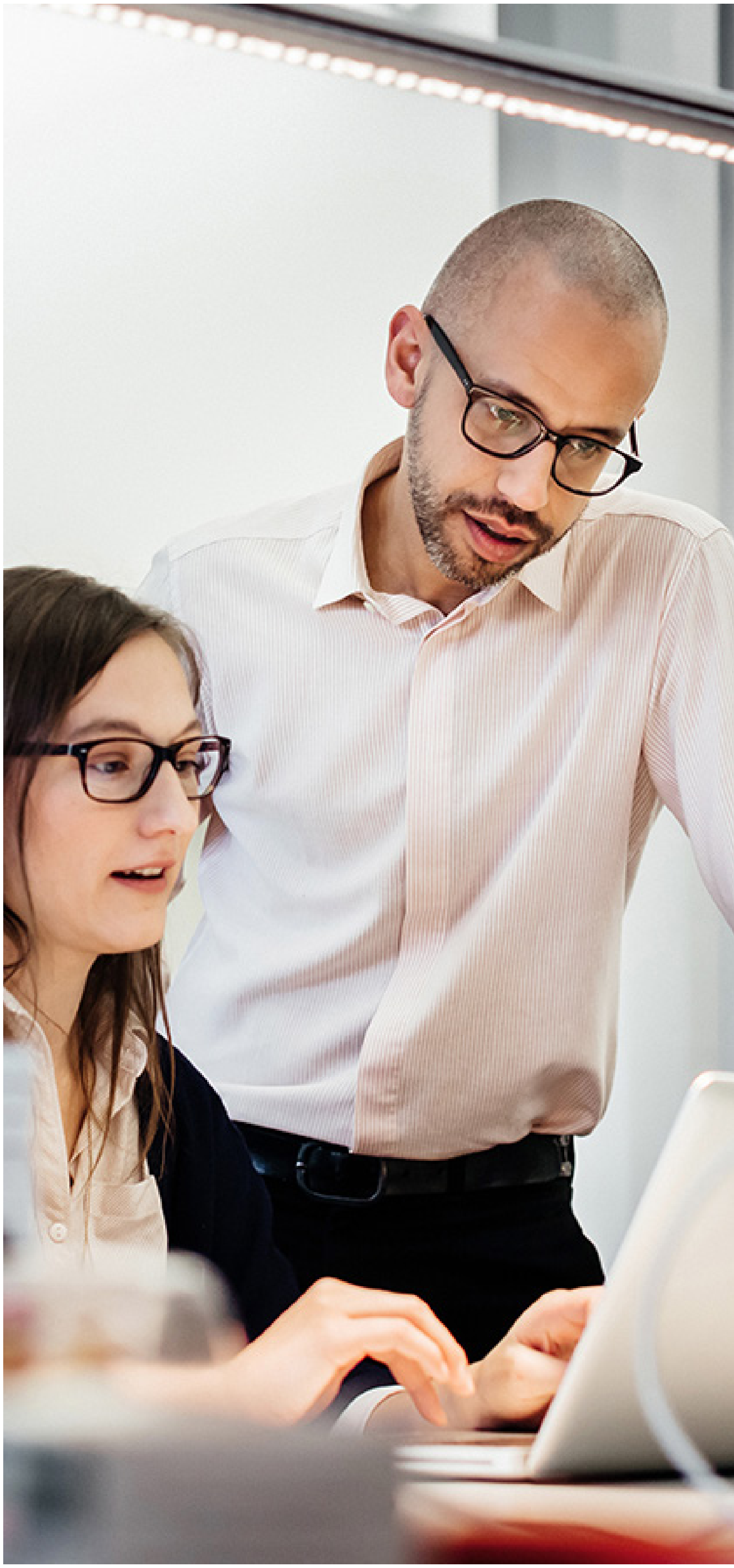
API8:2019 Injection

OWASP Definition: Injection flaws, such as SQL, NoSQL, command injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's malicious data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

How Akamai Can Help

Organizations can use a WAAP solution to protect web applications and APIs against injection flaws. However, organizations should always patch web applications and APIs to address any discovered vulnerabilities based on their development lifecycle.

- App & API Protector protects against injection attacks (e.g., SQLi, XSS, CMDi, RFI, and LFI) and automatically inspects JSON and XML requests.
- Virtual patching with custom rules can address new or emerging injection vulnerabilities exposed from changing applications and APIs. Virtual patching can also be automated and integrated into CI/CD workflows, leveraging Akamai's AppSec configuration APIs.
- App & API Protector protects APIs from abusive clients by immediately and persistently blocking active attack sessions. Any client whose request is in violation will be placed in a "penalty box" and have their requests denied for 10-minute increments.



API9:2019 Improper Assets Management

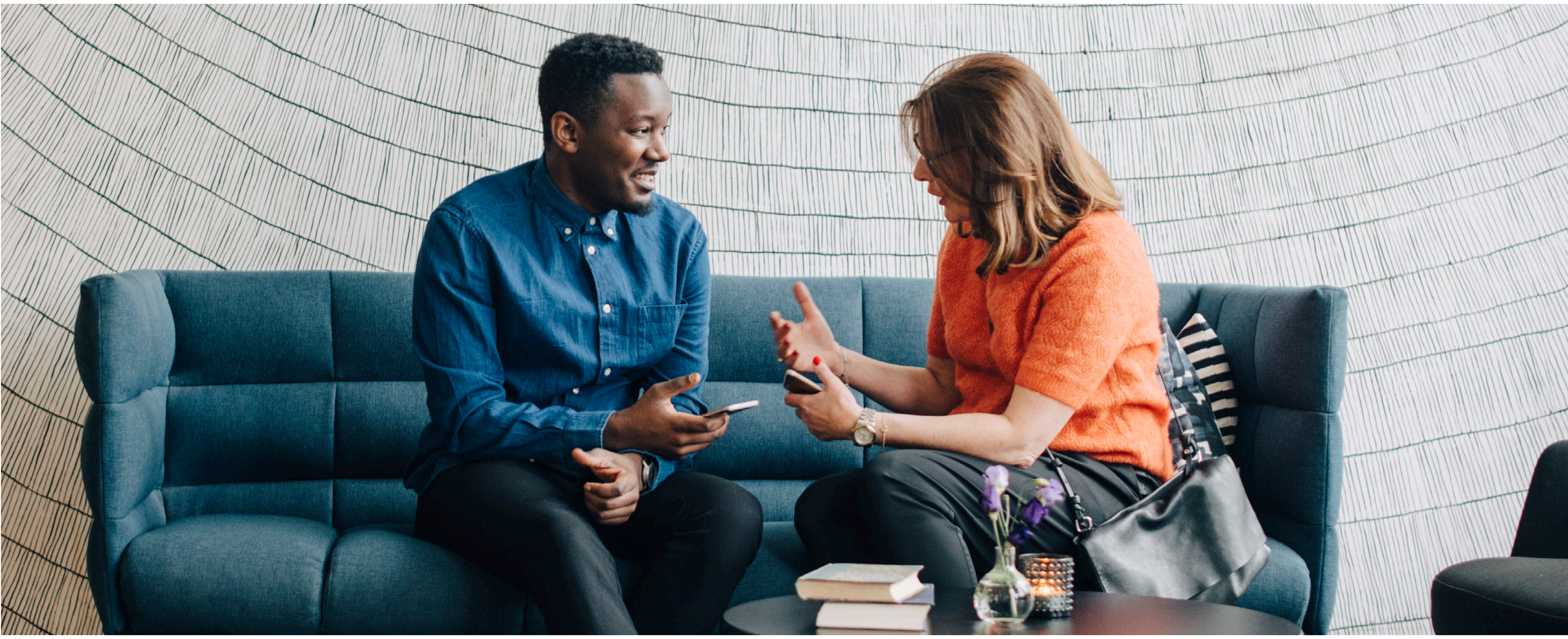
OWASP Definition: APIs tend to expose more endpoints than traditional web applications, making proper and updated documentation highly important. Proper hosts and deployed API versions inventory also play an important role to mitigate issues such as deprecated API versions and exposed debug endpoints.

How Akamai Can Help

API security solutions can protect known APIs, but unknown APIs – including deprecated, legacy, and/or outdated APIs – may be left unpatched and vulnerable to attack. Attackers can potentially gain access to sensitive data or even the server through unknown APIs that are connected to the same database. Akamai can discover and profile APIs to mitigate this risk.

- App & API Protector automatically discovers unknown APIs – including their endpoints, resources, characteristics, and definitions – to enable security teams to stay on top of changing definitions and discover deprecated and/or legacy APIs.
- App & API Protector offers custom rules that can be used to virtually patch and address vulnerabilities that are exposed from changing API definitions.
- API gateway capabilities can help version APIs appropriately manage their lifecycles.

> API security solutions can protect known APIs, but unknown APIs – including deprecated, legacy, and/or outdated APIs – may be left unpatched and vulnerable to attack.



API10:2019 Insufficient Logging and Monitoring

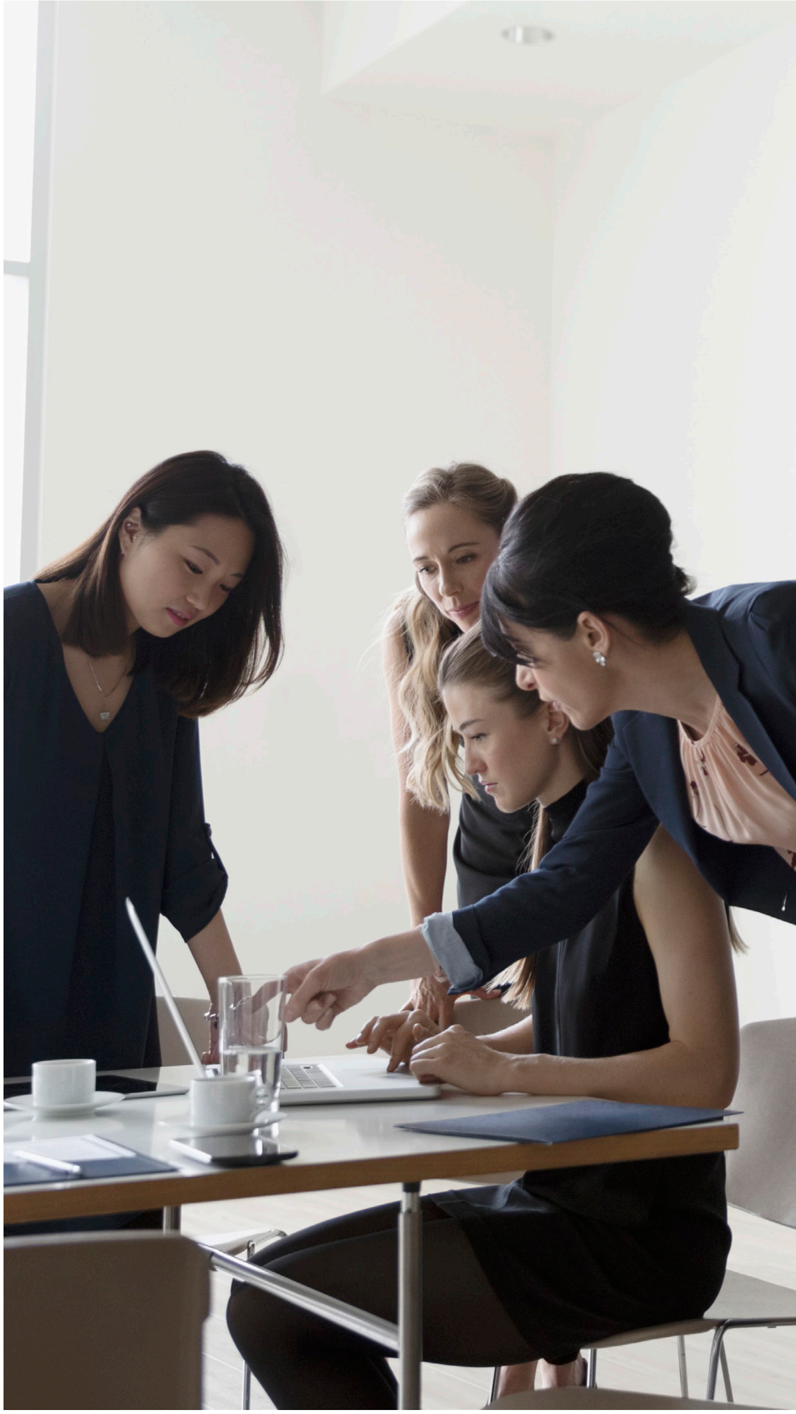
OWASP Definition: Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allow attackers to further attack systems, maintain persistence, pivot to more systems to tamper with, or extract or destroy data. Most breach studies demonstrate the time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

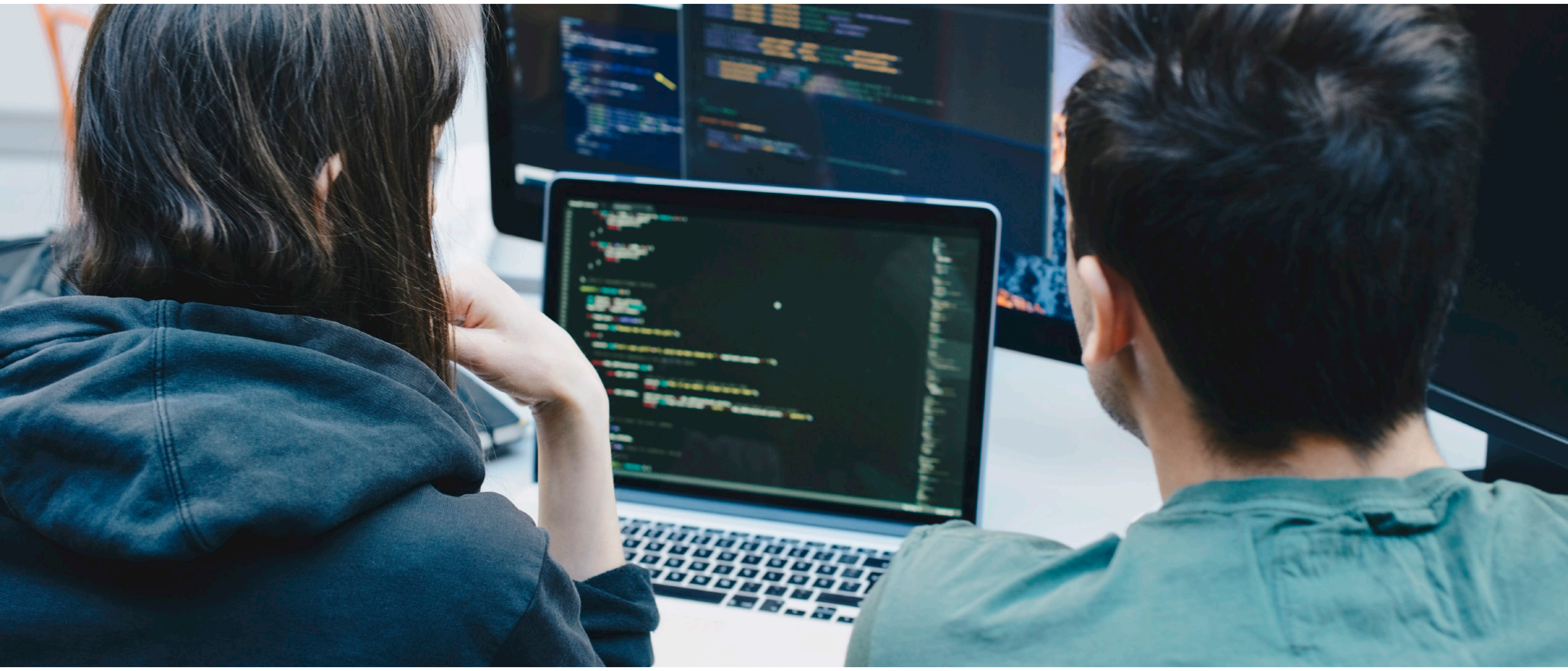
How Akamai Can Help

Insufficient logging and monitoring do not describe a vulnerability per se, but rather a gap in an organization's ability to address vulnerabilities and the attackers' attempt to exploit them. Akamai provides multiple capabilities to provide organizations with greater visibility into attacks.

- Akamai provides detailed attack telemetry and analysis of security events with our web security analytics dashboard and reporting to monitor and evaluate security events at the API level.
- App & API Protector integrates with both on-premises and cloud-based security information and event management solutions (SIEMs; e.g., Splunk, QRadar, and ArcSight) with full data logs to help correlate Akamai-detected events with other security solutions.
- App & API Protector can dynamically increase audit logging for suspicious clients. This trap-and-trace configuration can be implemented with the security alert to place suspicious clients on a "watch list." Doing so initiates a full audit logging for the client.
- Akamai managed security service provides 24/7 monitoring, security management, and threat mitigation.

Akamai provides detailed attack telemetry and analysis of security events with our web security analytics dashboard.





Conclusion

Organizations and their security vendors must work closely together, aligning across people, processes, and technologies to institute a solid defense against the security risks outlined in the OWASP API Security Top 10. Akamai provides industry-leading security solutions, highly experienced experts, and an intelligent edge platform that gleans insight from millions of web application attacks, billions of bot requests, and as many as trillions of API requests every single day. Akamai's web application and API security solutions will help secure your organization against the most-advanced forms of web application, DDoS, and API-based attacks.

To learn more about Akamai's edge security portfolio, please take a look at our website; if you would like to discuss and explore in more detail how we can partner to build the best protection for your business, please reach out to your Akamai sales representative today.