Akamai

WHITE PAPER

The OWASP Top 10

How Akamai Helps Protect Against Common Vulnerabilities

Introduction

The OWASP (Open Web Application Security Project) Top 10 list covers the most common vulnerabilities seen in web applications, raising awareness for organizations. Making the most of the OWASP Top 10 requires understanding where, how, and how much security vendors can help augment improvements to your own development practices. The following breakdown of the OWASP Top 10 vulnerabilities describes each of them and explains how Akamai can help support organizations with edge security solutions, managed services, and the world's largest intelligent edge platform.

Akamai Products

OWASP Top 10		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
Broken Access Control	A01			✓	✓	✓		✓		✓	
Cryptographic Failures	A02			✓		✓	✓				✓
Injection	A03			✓							
Insecure Design	A04			✓		✓					
Security Misconfiguration	A05		✓	✓	✓						
Vulnerable and Outdated Components	A06		✓	✓							✓
Identification and Authentication Failures	A07	✓		✓	✓	✓		✓		✓	
Software and Data Integrity Failures	A08		✓	✓			✓				✓
Security Logging and Monitoring Failures	A09		✓	✓		✓	✓		✓		
Server-Side Request Forgery	A10		✓	✓							

The OWASP Top 10 are categories of risks, not single risks. Akamai's solutions address these risk categories in multiple ways. Read the white paper to learn more.

A01: Broken Access Control

> "Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits."
>
> — Source: owasp.org

How Akamai helps

While organizations must fix their access control model to fully address the Broken Access Control vulnerability, Akamai's expertise in WAAP can help you to detect and protect against some of the attack vectors that attempt to exploit it:

- **Enterprise Application Access** enables a least-privilege access model for enterprise users, allowing only visibility and access for authorized applications by authenticated users — which supports a Zero Trust security model.
- **Akamai MFA** provides strong authentication services based on phish-resistant FIDO2 technology standards.
- **App & API Protector** — the Akamai WAAP solution — can help to block forceful browser attacks by checking the "referer" header and enforce authentication for APIs to strengthen access control with Akamai API Gateway.
- **Identity Cloud** provides granular access controls to end-user data, allowing for least-privilege access per internal user or system.
- **Bot Manager** prevents automated tooling attacks and login attacks.

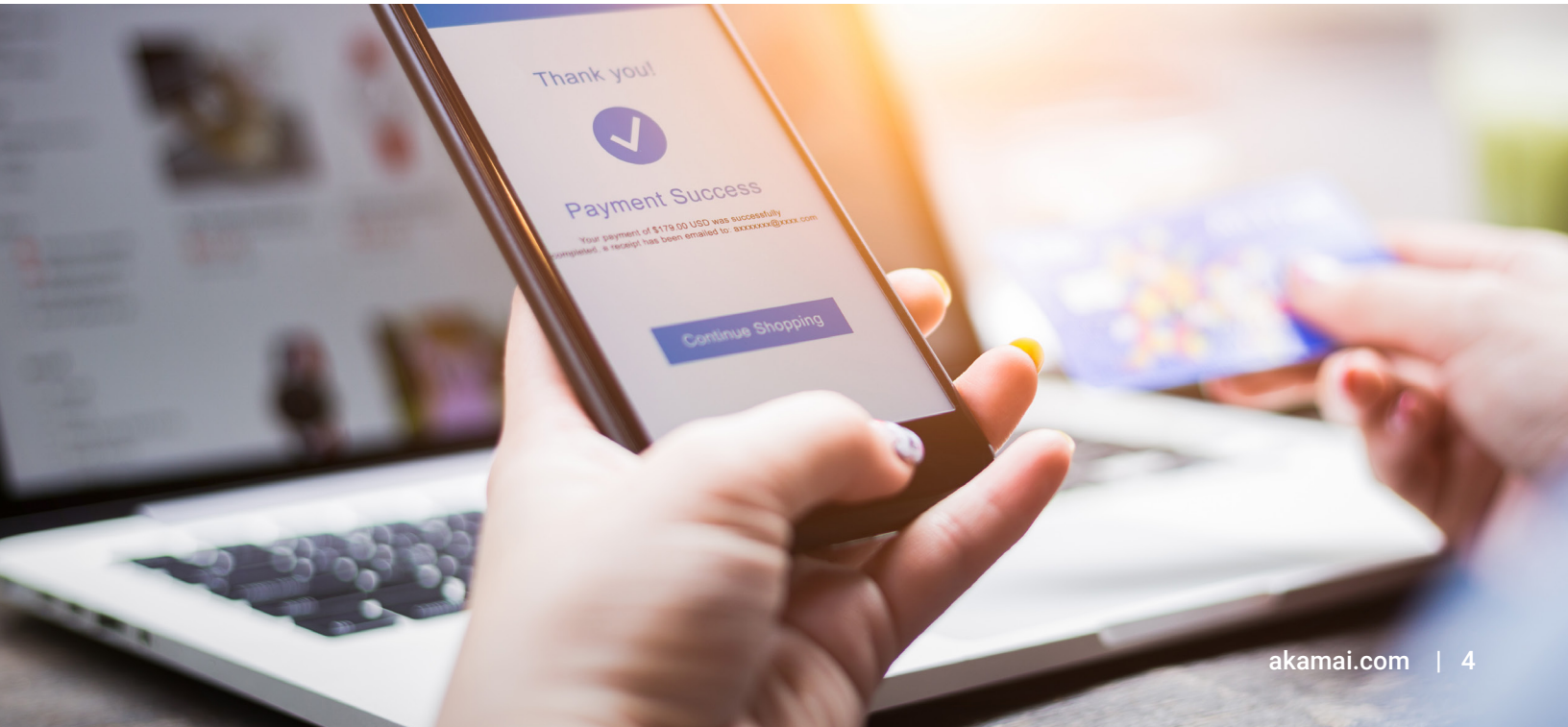
A02: Cryptographic Failures

> "The focus is on failures related to cryptography (or lack thereof). Which often lead to exposure of sensitive data. … For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws."
>
> — Source: owasp.org

How Akamai helps

Organizations cannot fully protect against cryptographic failures by using any one security solution. However, combining various solutions can help address some aspects of this vulnerability. For example, Akamai's:

- **App & API Protector** encrypts and protects sensitive data in transit with the latest versions of TLS and strong ciphers. It also helps to:
  - Maintain PCI compliance by serving exclusively from a secure CDN, which supports all branded TLS certificates and protects a customer's private keys.
  - Offer a CDN that is protected by operational and physical security — such as caged racks and motion detectors — that assure only authorized personnel can access the servers.
  - Locate and prevent sensitive data leaks with API PII learning.
- **Enterprise Application Access** can protect remote access by encrypting communication as well as by hiding confidential data from prying eyes on the network.
- **Enterprise Threat Protector** can help to prevent exposure of sensitive data.
- **Page Integrity Manager** can also detect PII data leaks through misuse of JavaScript code that could have resulted from cryptographic failures.



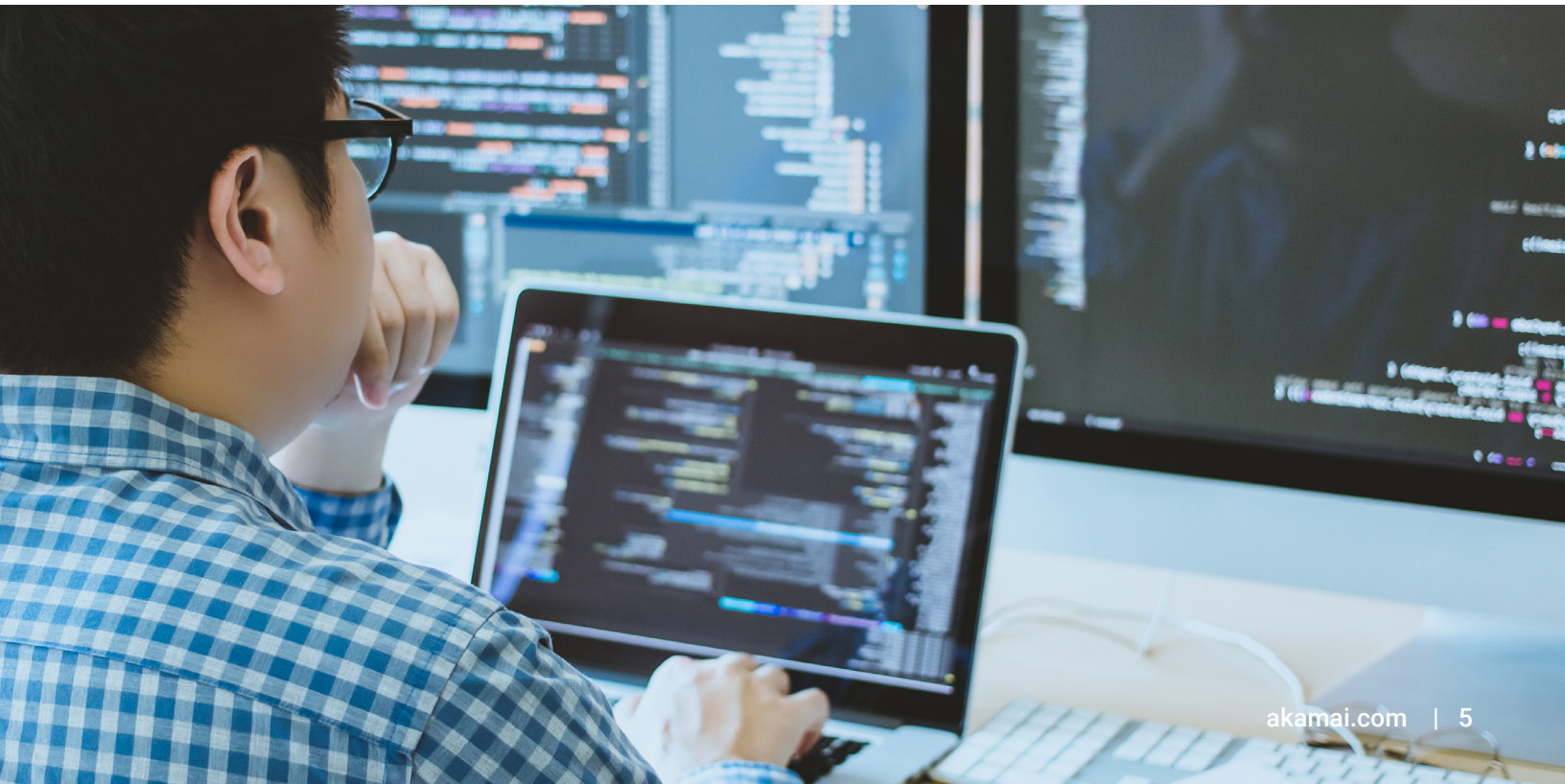
A03: Injection

> "Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization."
>
> — Source: Akamai

How Akamai helps

You can use WAAP to mitigate the risk from web application and API injection flaws. However, organizations should always patch web applications to address any discovered vulnerabilities based on their respective development lifecycles.

- **App & API Protector** offers an industry-leading WAAP solution with an adaptive security engine (ASE), which provides extensive protection against injection attacks using existing, out-of-the-box-rules. The ASE penalty box can temporarily block all traffic coming from clients that have recently attempted an injection attack using WAAP.
- Virtual patching with custom rules can help quickly address emerging injection vulnerabilities or new vulnerabilities exposed from application changes until the application can be patched. Security organizations can also automate virtual patching and integrate it into DevSecOps processes by leveraging Akamai's API capabilities.
- **Client Reputation** can help identify and block injection-based attacks and provides a risk score for highly active malicious clients in the web attackers category.



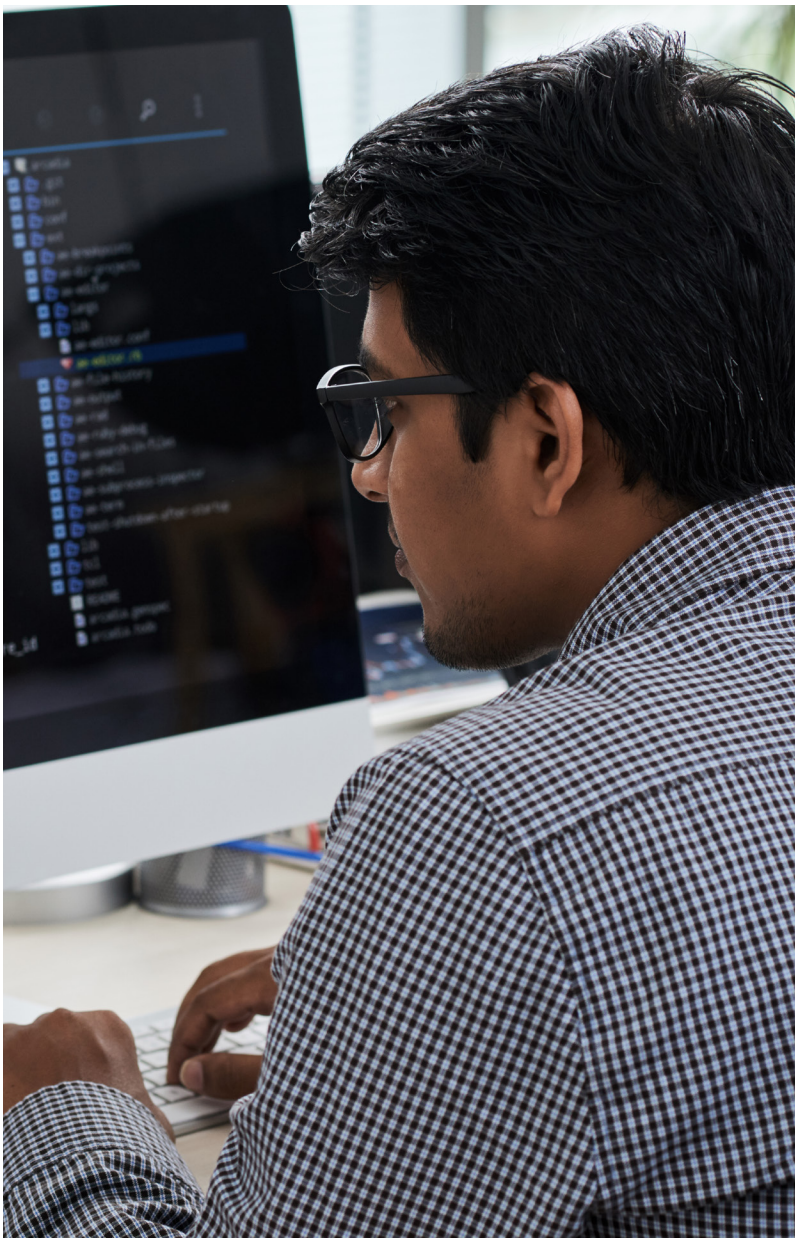
A04: Insecure Design

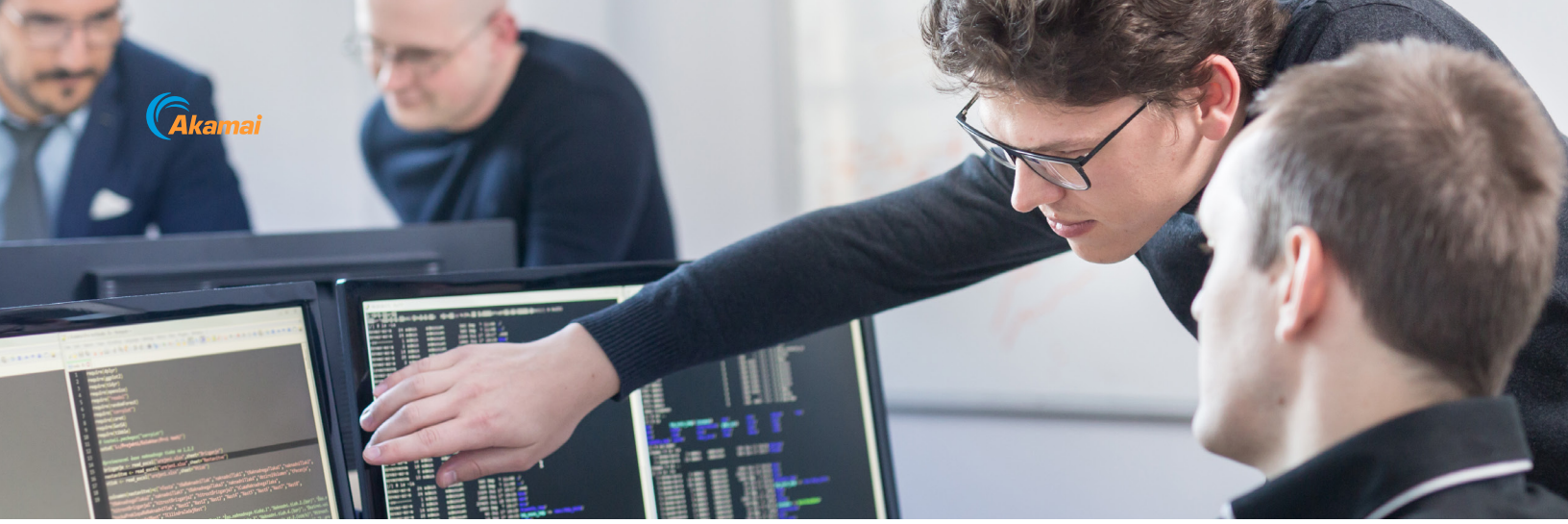
> "Insecure design is a broad category representing different weaknesses, expressed as 'missing or ineffective control design.' There is a difference between insecure design and insecure implementation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks."
>
> — Source: owasp.org

How Akamai helps

Organizations should integrate security from the very first design stages. However, development teams may struggle to achieve that if security is hard to incorporate. Akamai products help organizations shift left faster to prevent design insecurities from compromising their apps and APIs.

- **App & API Protector** — which comprises our WAAP solution and ASE — may also detect and remedy some design flaws that make it to production. It also leverages automation to offload and simplify routine tasks — leaving those that require human analysis to humans. This automation includes automatic updates, self-tuning, API discovery, simplified programmability, and user experience.
- **Enterprise Application Access** ensures only authorized users can access applications. This least-privilege approach prevents lateral movement to other applications, which can happen easily with network access solutions such as VPNs.





A05: Security Misconfiguration

> "[Since] the previous edition, 90% of applications were tested for some form of misconfiguration, with an average incidence rate of 4%, and over 208k occurrences of a Common Weakness Enumeration (CWE) in this risk category. Without a concerted, repeatable application security configuration process, systems are at a higher risk."
>
> — Source: owasp.org

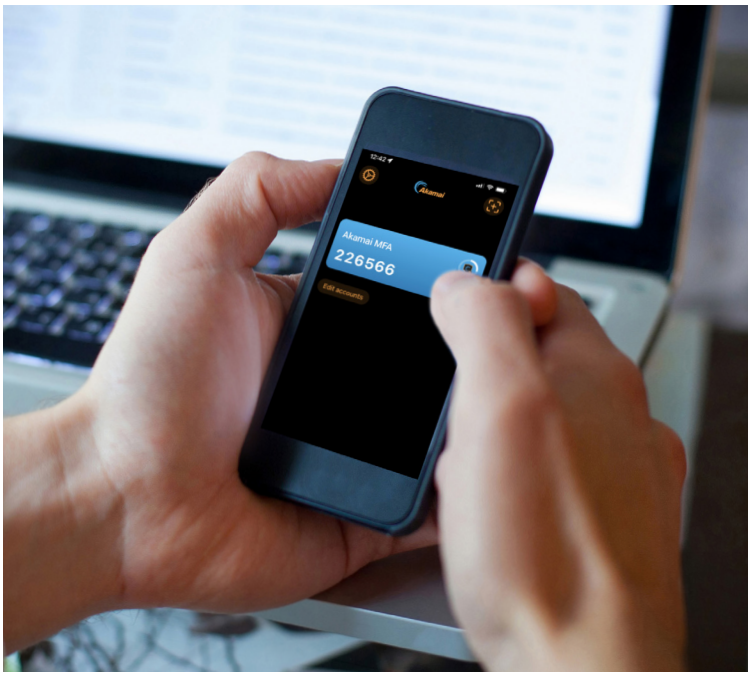
How Akamai helps

By definition, Security Misconfiguration covers multiple aspects of application security. It also requires organizations to properly configure security controls. Akamai's products help in the following ways:

- While not a substitute for proper configuration, **App & API Protector** can help by:
  1. Using outbound anomaly attack groups to catch information leakage like error codes, as well as source code resulting from security misconfigurations that exist out of the box.
  2. Implementing rules that can detect and stop XXE attacks before the XML parser processes the dangerous external entity.
  3. Implementing rules that can detect access to known sensitive files left by developers on the production servers.
- **Akamai Guardicore Segmentation** helps to protect against data leakage due to misconfigurations by providing visibility and granular control over any unauthorized or unplanned communications between your applications and the internet.
- Virtual patching with custom rules can help to quickly address detected data leakage until your team can patch the application.
- With **App & API Protector** and **Bot Manager**, brute-force attacks using default credentials can be protected with rate controls.
- Weak security configuration of Content Security Policy and other security-relevant HTTP headers can be strengthened on the Akamai platform.
- With automatic API Discovery in **App & API Protector**, you can automatically and continuously discover and profile your APIs, including endpoints, definitions, and resource and traffic characteristics.

A06: Vulnerable and Outdated Components

> "Components such as libraries, frameworks, and other software modules run with the same privileges as the application. Additionally, scripts act as trusted application resources with full access to application data. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover."
>
> — Source: Akamai



How Akamai helps

Organizations often lose track — and security teams are often completely unaware — of what third-party components exist within their applications. In addition, organizations have no control over how quickly, if ever, the third party will address newly discovered vulnerabilities. Mitigating this lack of visibility and certainty necessitates the use of a security solution such as WAAP and script protection such as the following:

- **App & API Protector** includes multiple rules designed to address known vulnerabilities — whether specifically in your applications or in third-party components. It also provides API protection capabilities, which protect APIs even when third-party components incorporated in the API open it to abuse.
- The **Akamai Guardicore Segmentation** insight module allows you to query for any assets in your network that may be vulnerable. The included granular enforcement further allows you to ringfence any affected assets until a patch has been applied.
- Virtual patching with custom rules helps to quickly address emerging vulnerabilities or new vulnerabilities exposed from application changes until the application can be patched.
- **Client Reputation** provides a risk score for malicious clients in the web scanning category to help protect against exploitation of new vulnerabilities.
- **Page Integrity Manager** constantly analyzes the behavior of script execution, in real user sessions, to identify suspicious or outright malicious behavior. It also blocks data exfiltration from first- and third-party scripts to URLs with known vulnerabilities using a constantly updated Common Vulnerabilities and Exposures (CVE) database.

A07: Identification and Authentication Failures

> "Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently."
>
> — Source: Akamai

How Akamai helps

Organizations must fix their lapses to fully address this vulnerability. Nonetheless, the Akamai solutions listed below can help detect and protect against many of the attack vectors that attempt to exploit identification and authentication failures:

- **Bot Manager** can detect and mitigate automated attacks such as those used in credential stuffing attacks.
- **Account Protector** mitigates account takeover attempts where imposters try to gain unauthorized access to user accounts.
- **Enterprise Application Access** can proxy access to applications through a "least-privilege access model," reducing the attack surface of the application and enhancing access.
- **Akamai MFA** provides strong authentication using phish-resistant FIDO2 technology.
- **App & API Protector** provides a rate-control capability, which can handle brute-force attacks.
- **Identity Cloud** provides secure management of end-user credentials and profile information protected by two-factor authentication and risk-based authentication capabilities.

A08: Software and Data Integrity Failures

> "Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise."
>
> — Source: owasp.org

How Akamai helps

Organizations can use WAAP to protect web applications and APIs against software and data integrity failures. However, organizations should always patch web applications to address any discovered vulnerabilities based on their development lifecycle.

- **App & API Protector**
  - Provides strong protection against deserialization attacks.
  - Prevents machine-in-the-middle attacks that can result in data integrity issues through implementation of latest TLS versions and strong ciphers.
  - Ensures data origin authentication and data integrity protection of the DNS records by implementing DNSSEC with Edge DNS. This prevents tampering of DNS records that can direct the users to untrusted sources.
- The insight module in **Akamai Guardicore Segmentation** allows you to query for any assets in your network that have received the corrupted update. The included granular enforcement further allows you to ringfence these affected assets until a fix has been created.
- **Enterprise Threat Protector** detects phishing attacks, which can lure admins and super-users of the applications to hostile environments or untrusted sources.
- Virtual patching with custom rules can help to quickly address new deserialization flaws until the application can be patched.
- **Page Integrity Manager** detects third-party scripts, monitors them for changes, and then takes action on scripts that have been compromised.

A09: Security Logging and Monitoring Failures

"Insufficient logging, detection, monitoring, and active response occurs any time:

- Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.
- Logs of applications and APIs are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response escalation processes are not in place or effective.
- Penetration testing and scans by dynamic application security testing (DAST) tools do not trigger alerts.

The application cannot detect, escalate, or alert for active attacks in real-time or near real-time."

— Source: owasp.org

How Akamai helps

Security logging and monitoring failures present a gap in an organization's ability to address vulnerabilities and attempts to exploit them. Akamai provides multiple capabilities to provide organizations with greater visibility into attacks, including:

- Akamai provides dashboards and reporting tools within the Akamai Control Center graphical user interface.
- Akamai's application security products integrate with an organization's existing SIEM infrastructure to correlate Akamai-detected events with those from other security vendors.
- **Managed Security Service** provides 24/7 analysis and response capabilities.
- **App & API Protector** includes a penalty box capability that allows for increased logging of IPs that showed malicious or suspicious activities for further in-depth analysis.
- **Enterprise Application Access** provides an integrated identity management solution to authenticate and control access to all enterprise applications. When combined with its Identity-Aware Proxy capability, organizations can get fine-grained visibility into user actions, up to and including visibility into every GET/POST action.
- **Enterprise Threat Protector** enables full visibility into all external DNS requests from an enterprise — both malicious and benign.
- **Akamai Guardicore Segmentation** provides deep visibility into communication flows within your network, so alerts can be triggered when unauthorized or unexpected communication occurs, and security policies can be enforced down to the individual process or service level to restrict this communication. With the added breach detection module, potential threats can be quickly detected and remediated.

A10: Server-Side Request Forgery

> "SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL)."
>
> — Source: owasp.org

How Akamai helps

Akamai WAAP includes rules that can look for injection of URLs. This capability can prevent attackers from inducing the server to go somewhere else and submit a request — i.e., to make it look like a valid request to your security analysts.

- **App & API Protector** rules help prevent those exploit requests from reaching the vulnerable server in the first place.
- **Akamai Guardicore Segmentation** can monitor and block unexpected outbound traffic at the server level.

Conclusion

Mounting the best defense against OWASP Top 10 vulnerabilities requires organizations and their security vendors working together to surface vulnerabilities as soon as possible and implementing solutions to mitigate them. Learn more about Akamai's edge security portfolio. If you would like to discuss and explore how we can partner to build the best protection for your business, please reach out to your Akamai sales representative.