WHITE PAPER

How Akamai Augments Your Security Practice to Mitigate the OWASP Top 10 Risks

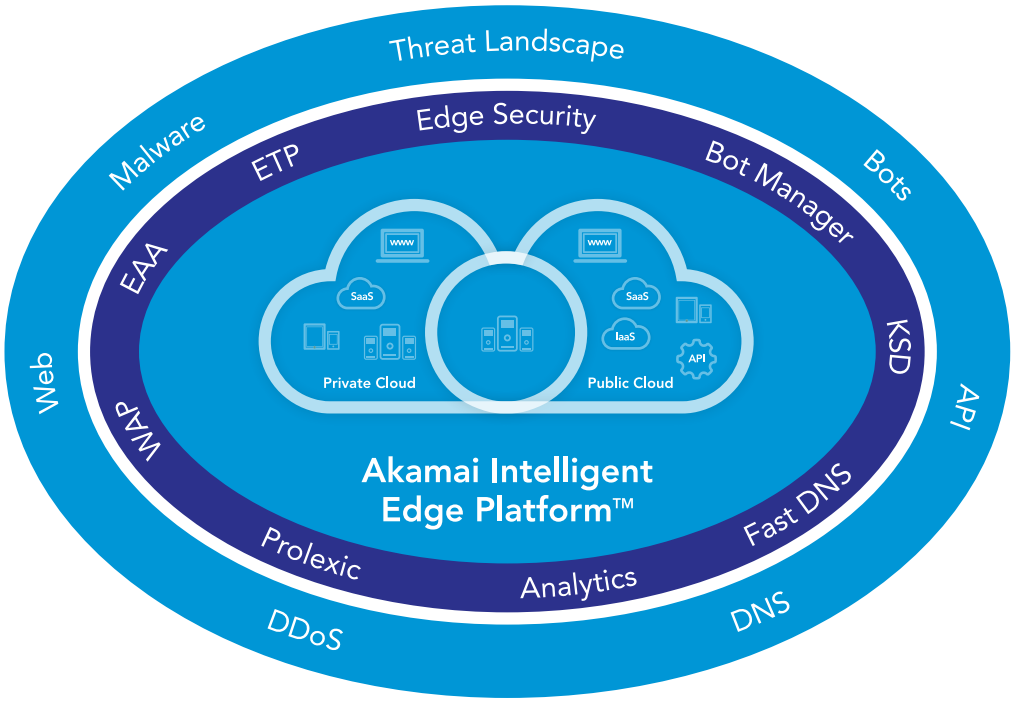
Akamai

Introduction

The OWASP Top 10 provides a list of the most common types of vulnerabilities often seen in web applications. To call out a common misperception often perpetuated by security vendors, the OWASP Top 10 does not provide a checklist of attack vectors that can be simply blocked by a web application firewall (WAF). Instead, its objective is to raise awareness about common security vulnerabilities that application developers should consider, drive that awareness across an array of development practices, and help instill a culture of secure development.

Addressing the OWASP Top 10 requires understanding the role that both security vendors and your own organization have in securing your web applications. Some risk areas can only be addressed by application developers themselves. Many security vendors may be able to help in some areas, but often cannot provide complete or the best coverage possible against a vulnerability. Better solutions provide a combination of people, processes, and technologies to mitigate risks associated with the Top 10.

Making the most of the OWASP Top 10 requires understanding where and how — and how much — security vendors can help augment improvements to your own development practices. The following describes the role that Akamai can have in supporting your efforts with our edge security solutions,[1] managed services,[2] and secure intelligent edge platform.[3]



A1: Injection

Impact: Severe	**Prevalence:** Common	**Exploitability:** Easy

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.

How Akamai Can Help

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

- Akamai WAF[4] provides extensive protection against injection attacks with existing, out-of-the-box-rules.
- 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. Virtual patching can also be automated and integrated into DevSecOps processes, leveraging Akamai's OPEN API capabilities.
- Client Reputation[5] provides a risk score for highly active malicious clients in the Web Attackers category to help identify and block injection-based attacks.
- Injection-based attacks can also be further analyzed by the WAF with a Penalty Box Alert Mode

A2: Broken Authentication

Impact: Severe	**Prevalence:** Common	**Exploitability:** Easy

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.

How Akamai Can Help

While organizations must fix their broken 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 WAF provides a rate-control capability, which can handle brute-force attacks.
- Bot management solutions[6] can detect and manage the automation used in credential stuffing attacks.
- HTTP cookies can be encrypted on the Akamai platform[7] to prevent cookie tampering and modification, which can strengthen the authentication process.
- Enterprise Application Access (EAA)[8] can proxy access to applications through a "least-privilege access model," reducing the attack surface of the application and enhancing access with two-factor authentication (2FA) and multi-factor authentication (MFA) capabilities.

A3: Sensitive Data Exposure

Impact: Severe	**Prevalence:** Widespread	**Exploitability:** Average

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

How Akamai Can Help

Sensitive Data Exposure covers many aspects of how data is transmitted, stored, and shared — including unintentionally exposing data from an unprotected web page — and cannot be fully protected by any single security solution alone. However, various solutions can help address some aspects of this vulnerability. For example:

- Akamai encrypts and protects sensitive data in transit and helps to maintain PCI compliance by serving exclusively from a secure CDN with caged racks, supporting all branded SSL certificates, and protecting a customer's private keys.
- Enterprise Application Access can protect remote access by encrypting communication and hiding confidential data from prying eyes on the network.
- Enterprise Application Access can also integrate with data loss prevention (DLP) solutions using ICAP to further protect sensitive data from exposure.
- Enterprise Threat Protector (ETP)[9] can help with sensitive data exposure.

A4: XML External Entities (XXE)

Impact: Severe	**Prevalence:** Common	**Exploitability:** Average

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial-of-service attacks.

How Akamai Can Help

- Akamai WAF includes rules that can detect and stop XXE attacks before the XML parser processes the dangerous external entity.
- Akamai WAF includes API protection capabilities with API request constraints that can be used to validate XML and JSON against predefined formats to block XXE attacks.

A5: Broken Access Control

Impact: Severe	**Prevalence:** Common	**Exploitability:** Average

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data — accessing other users' accounts, viewing sensitive files, modifying other users' data, changing access rights, etc.

How Akamai Can Help

While organizations must fix their access control model to fully address this vulnerability, Akamai can help 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.
- API Gateway[10] can enforce authentication for APIs to strengthen access control.
- Akamai WAF can help to block forceful browser attacks by referrer checking.
- HTTP cookies can be encrypted on the Akamai platform, which strengthens access control.

A6: Security Misconfiguration

Impact: Moderate	**Prevalence:** Widespread	**Exploitability:** Easy

Security misconfiguration is the most commonly seen issue. This is often a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, or verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

How Akamai Can Help

By definition, Security Misconfiguration (a.) covers multiple aspects of application security and (b.) requires organizations to properly configure security controls. While not a substitute for proper configuration, Akamai can help to protect against data leakage:

- Akamai WAF includes an outbound anomaly attack group to catch information leakage like error codes, as well as source code resulting from security misconfiguration out of the box.
- Virtual patching with custom rules can help to quickly address detected data leakage until the application can be patched.
- Brute-force attacks using default credentials can be protected with rate controls.
- Weak security configuration on Content Security Policy headers can be strengthened on the Akamai platform.

A7: Cross-Site Scripting (XSS)

Impact: Moderate	**Prevalence:** Widespread	**Exploitability:** Easy

XSS flaws occur whenever an application (a.) includes untrusted data in a new web page without proper validation or escaping, or (b.) updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites.

How Akamai Can Help

Organizations can use a WAF security solution to protect web applications against XSS flaws. However, organizations should always patch web applications to address any discovered vulnerabilities based on their development lifecycle.

- Akamai WAF products have existing XSS WAF rules to identify and stop XSS attacks out of the box.
- Virtual patching with custom rules can help quickly address emerging XSS 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 Attackers category to help block XSS-based attacks.
- Akamai Platform can set security response policy headers on the fly to protect against XSS attacks.

A8: Insecure Deserialization

Impact: Severe	**Prevalence:** Common	**Exploitability:** Difficult

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

How Akamai Can Help

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

- Akamai WAF rules detect deserialization attacks.
- Virtual patching with custom rules can help to quickly address new deserialization flaws until the application can be patched.
- Akamai WAF includes API protection capabilities with a positive security model that defines acceptable XML and JSON object formats to filter out maliciously crafted XML and JSON.

A9: Using Components with Known Vulnerabilities

Impact: Moderate	**Prevalence:** Widespread	**Exploitability:** Average

Components such as libraries, frameworks, and other software modules run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

How Akamai Can Help

While popular and widely used to reduce development times and costs, third-party components are a very common entry point for vulnerabilities into even your most proprietary applications. There are several risks. Organizations often lose track — and security teams are often completely unaware — of what third-party components are in use within their applications. In addition, organizations have no control over how quickly or when newly discovered vulnerabilities are addressed by the third-party entity. As a result, patching applications directly in a timely manner can be difficult or impossible, necessitating the use of a security solution such as a WAF:

- Akamai WAF includes multiple rules designed to address known vulnerabilities — whether specifically in your applications or third-party components.
- Virtual patching with custom rules can help to quickly address emerging vulnerabilities or new vulnerabilities exposed from application changes, until the application can be patched.
- Akamai WAF provides API protection capabilities to protect APIs for third-party components from attacks exploiting known vulnerabilities.
- Client Reputation provides a risk score for malicious clients in the Web Scanning category to help protect against exploitation of new vulnerabilities.

A10: Insufficient Logging and Monitoring

Impact: Moderate	**Prevalence:** Widespread	**Exploitability:** Average

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems; maintain persistence; pivot to more systems; and tamper, extract, or destroy data. Most breach studies show that the time to detect a breach is usually more than 200 days, and that such breaches are typically detected by external parties rather than internal processes or monitoring.

How Akamai Can Help

Insufficient Logging and Monitoring does not describe a vulnerability per se, but 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 Akamai's Luna Control Center[11] graphical user interface.

- Akamai integrates with organizations' existing SIEM infrastructure to correlate Akamai-detected events with those from other security vendors.
- Akamai managed security services provide 24/7 analysis and response capabilities.
- Akamai WAF includes a Penalty Box capability that allows for increased logging of suspicious sessions for further in-depth analysis.
- Akamai 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.
- Akamai Enterprise Threat Protector enables full visibility into all external DNS requests from an enterprise — both malicious and benign.

Conclusion

The best defense against OWASP Top 10 vulnerabilities can be achieved when organizations and their security vendor work together to align their people, processes, and technologies. Akamai provides industry-leading technology and highly experienced people to align with your processes. To learn more about Akamai's edge security portfolio, please take a look at the detailed information on 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.

Sources

1. Edge Security
2. Services & Support
3. Akamai Intelligent Edge Platform™
4. Kona Site Defender (KSD) and Web Application Protector (WAP)
5. Client Reputation
6. Bot Manager
7. Secure CDN
8. Enterprise Application Access
9. Enterprise Threat Protector
10. API Gateway
11. Luna Control Center