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Vulnerable and Outdated Components	A06		✓	✓							✓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.