Barracuda
Your journey, secured.

SOLUTION BRIEF

Barracuda Cloud Application Protection Protects Against the OWASP Top 10 Web Application Security Risks

Application-layer threats are evolving rapidly to evade traditional security measures — and the strategies and technologies being developed to combat them effectively are also growing more sophisticated. From advanced malicious bots that mimic human behavior, to multi-stage ransomware that exploits application vulnerabilities, to API and software-supply-chain attacks, to massive new vulnerabilities such as Log4J, there's a whole new world of threats out there.

OWASP — the premiere public-interest research organization documenting, analyzing, and ranking application and API threats — has taken notice of the dramatic changes to the application threat landscape. If you have anything to do with application security, you're already familiar with the OWASP Top 10 list of application threats. It's a handy summary of the most prominent and effective threat modalities, which can be tremendously helpful to IT security pros looking to prioritize efforts to improve app security infrastructures.

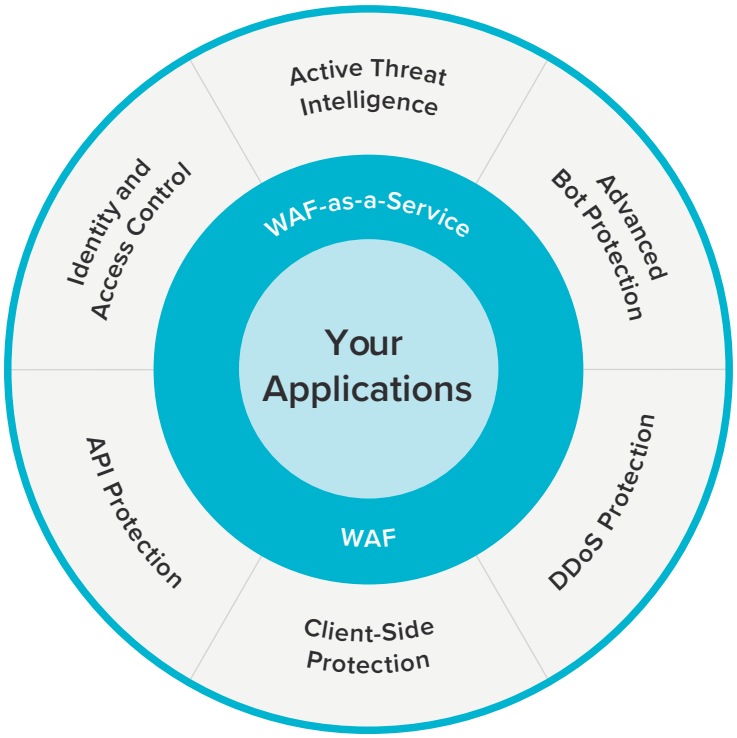
In 2021, OWASP released a comprehensive new list of the Top 10 Application Security Risks. This list has gone through a massive set of changes, and only 5 of the Top 10 from the previous list have been retained. In this evolution, the list is moving closer to being a standard that can be used to implement an Application Security program and serve better as a standard for creating the same.

Protecting against the OWASP Top 10 2021 with Barracuda Cloud Application Protection

Barracuda Cloud Application Protection offers comprehensive Web Application and API Protection for your web, API, and mobile applications. The table below lists the Top 10 Risks and the protective measures offered by Barracuda Cloud Application Protection.

TOP 10 RISK	DESCRIPTION	BARRACUDA WEB APPLICATION FIREWALL SOLUTION
A01: Broken Access Control	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, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.	Intelligently profiles web traffic to build a positive security profile that can be used as a whitelist of valid application resources and usage; traffic anomalous to this profile is denied. Web-based Allow Deny Rules (ADRs) allow for granular specification of precise application domains that are accessible with and without authentication. Provides a granular URL and form-level rules engine that restricts access to unauthorized resources. Seamless integration with multiple credentialing systems, e.g., LDAP, RADIUS, SiteMinder, RSA SecurID, SAML, AD FS, etc., provides strong single and multifactor access control.
A02: Cryptographic Failures	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.	Intercepts and filters server responses to prevent data leakage of sensitive information like SSN and credit card numbers. Custom patterns can also be defined and blocked or masked from being leaked. Sensitive information can be masked inside logs. Implements strong cryptography in SSL offloading and instant SSL features to secure data in transit. Instant SSL easily transforms HTTP-only applications to use an HTTPS front-end, which is offloaded to the Barracuda Web Application Firewall. Enables usage of the most secure TLS protocols, with cipher- suite selection, Perfect Forward Secrecy (PFS), and HSTS.
A03: Injection	Injection flaws, such as SQL, 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.	Employs a mix of positive and negative security for filtering all web-based inputs inside URL, forms, cookies, and headers to prevent known and unknown (zero-day) attacks. Blocks any inputs that can be executed unintentionally inside interpreters. Detects obfuscated malicious payloads meant to evade detection. Deep inspects entire client requests – URL, query and form parameters, cookies, headers, etc., to detect script injection. Prior to inspection, it de-obfuscates (normalizes) all malicious payloads for common encoding schemes and applies other protocol and limit-based checks.
A04: Insecure Design	Broad category representing different weaknesses, expressed as "missing or ineffective control design".	Provides comprehensive API for all the configuration elements, which can be used to implement a secure development life cycle (SDLC) policy. For inherent flaws in the backend application, virtual patching can be done to suitably handle implementation risks.
A05: Security Misconfiguration	Exploits application stack vulnerabilities such as unpatched software, zero-day threats, and undeleted default accounts. Also exploits misconfigured HTTP headers and verbose error messages that contain sensitive information.	Filters application error or status responses to prevent attackers from profiling software vulnerabilities or identifying sensitive application-related information. Employs a mix of positive and negative security for filtering all web-based inputs to prevent known and unknown (zero-day) attacks. Applies strong authentication and authorization policies to secure access control. Proxies traffic to prevent direct access to backend servers. XML firewall protects against XML attacks including XXE attacks. All untrusted user inputs are validated, and any malicious data is identified and blocked. Protects the entire API attack surface, including dynamically generated URLs and URLs that use resource names as directories. Allows for virtual patching to easily close any open vulnerabilities. Protects the XML parser against any types of attacks and enables SSL/TLS and AAA offload to completely secure the API surface.

TOP 10 RISK	DESCRIPTION	BARRACUDA WEB APPLICATION FIREWALL SOLUTION
A06: Vulnerable and Outdated Components I	Occurs when attackers can take control of and exploit vulnerable libraries, frameworks, and other modules running with full privileges.	Implements a hardened operating system and networking stack that proxies and shields vulnerable system stacks and components. Achieves security through obscurity by cloaking or masking responses that expose information about libraries, frameworks, and other modules. Virtual patching capability, with integration with over 25 well known vulnerability scanners, ensures that any identified vulnerabilities are automatically patched on the Barracuda WAF. Barracuda WAF provides support for implementing a Content Security Policy and Sub Resource Integrity to safeguard users of the application and to ensure that external files/library references are monitored for changes
A07: Identification and Authentication Failures	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.	Enforces session security and integrity in web applications by encrypting session tokens. Prevents MITM, MITB, and cookie replay attacks. Protects against tampering of hidden variables. Integrates with hardened browsers to prevent client-side session hijacking by keyloggers, framegrabbers, and other client-side malware.
A08: Software and Data Integrity Failures	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.	XML and JSON firewalls ensure that all XML, JSON and SOAP requests are inspected and validated. Also inspects all incoming requests for deserialization attack patterns and block any matching requests. Enforce size checks on all incoming traffic and block attacks against the parsers.
A09: Security Logging and Monitoring Failures	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 time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.	Provides extensive logging and reporting for all HTTP/HTTPS requests with ready integration with multiple SIEM vendors. Detailed log entries provide visibility into each part of the incoming request. This enables a centralized auditing and regulatory compliance framework for any protected application. Powerful reporting and notification modules provide a large number of pre-canned reports and threshold-based notifications to immediately identify security issues.
A10: Server-Side request forgery (SSRF)	Occurs whenever the 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 security controls such as firewalls, VPN or any type of network access control list.	Sanitizes all user input to ensure that client supplied data is not malicious. ACLs can be created to block HTTP redirections. Additional checks can be implemented for parameters and headers of a request to implement a strict control on input values..



Barracuda Cloud Application Protection is an integrated platform that brings a comprehensive set of interoperable capabilities together to ensure complete application security. Combine full WAF functionality with a complete set of advanced security services and solutions that protect your applications against today's multiplying threats. Whether your applications are deployed on-premises, in the cloud, or hybrid, Barracuda Cloud Application Protection makes it easy to keep them secure and available. Barracuda Cloud Application Protection protects your applications against OWASP Top 10 Web and API risks, Zero-Day Threats, DDoS, bots and client-side attacks while remaining easy to setup and maintain. Barracuda Cloud Application Protection is available as hardware, virtual, public cloud instances, containers and SaaS to protect your applications wherever they reside.

Barracuda®
Your journey, secured.