Barracuda

Solution Brief

Barracuda Web Application Firewall Protects Against the Top 10 Biggest Web Site Threats

Today's companies need to increase efforts to protect against a crippling website hack or data breach as web applications and website attacks are increasing in frequency. Being compromised can damage an organization's reputation and result in loss of customers and impact its bottom line. Forrester estimates that more than 67 percent of Internet vulnerabilities happen at the application layer. Web security breaches can occur during a simple website visit through a browser infection or from malicious code added into a form field with instructions to transmit sensitive data or reveal network configurations. Typical web-based attacks can include: SQL Injections, Cross-Site Scripting (XSS), website defacements, theft of personal information, Denial of Service (DoS) attacks, bot infection, or a combination of malicious behaviors.

Applications are vulnerable to such attacks due to the difficulty of consistently applying secure coding practices in a fast moving, ever changing environment. In addition, vulnerabilities in the underlying server or software infrastructure that are used to host web applications introduce additional vectors for attackers to exploit. With the majority of attacks targeting web applications today, it is important to evaluate products that can protect against current and new forms of web-based attacks.

Comprehensive Protection Against Top 10 Application Vulnerabilities

In the interest of improving application security, the Open Web Application Security Project (OWASP) periodically compiles a list of the Top 10 web threats. This list is used as a basis for regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS) to ensure the secure storage and transfer of sensitive data on the web. The Barracuda Web Application Firewall provides complete protection against all of the OWASP Top 10 vulnerabilities, including the recently updated (November 2017) list:

Vulnerability	Description	Barracuda Web Application Firewall Solution
Injection Flaws	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.
Broken Authentication	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.

Vulnerability	Description	Barracuda Web Application Firewall Solution
Sensitive Data Exposure	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.
XML External Entities (XXE)	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.	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.
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.
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.
Cross-Site Scripting (XSS)	Injects malicious code from a trusted source to execute scripts in the victim's browser that can hijack user sessions, deface websites, or redirect the user to malicious sites.	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.
Insecure Deserialization	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.
Using Components with Known Vulnerabilities	Occurs when attackers are able to 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.
Insufficient Logging and Monitoring	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.

The Barracuda Web Application Firewall is the complete and powerful security solution for web applications and websites. The Barracuda Web Application Firewall provides award-winning protection against hackers leveraging protocol or application vulnerabilities to instigate identity theft, denial of service, data theft, or defacement of your website. It has data-center ready functionalities such as load balancing, SSL offloading, high availability clustering, and third party reporting integrations that make the Barracuda Web Application Firewall the most powerful and easy-to-use solution.

With more than a decade of experience in securing web applications, the Barracuda Web Application Firewall is the proven solution used by many of the largest organizations in the world to secure their valuable assets against web threats.

To learn more about the Barracuda Web Application Firewall, please visit http://www.barracuda.com/waf or call Barracuda Networks for a free 30-day evaluation at 1-408-342-5400 or 1-888-268-4772. For more information on our other security and productivity solutions, please visit http://www.barracuda.com/products.

About Barracuda Networks, Inc.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit http://www.barracuda.com.