

Barracuda Networks OWASP Protection – Top 10

Today's companies need to increase efforts to protect against a crippling Web site hack or data breach as Web applications and Web site attacks are increasing in frequency. Being compromised can damage an organization's reputation and result in a loss of customers and impact their bottom line. Forrester estimates that over 67 percent of Internet vulnerabilities happen at the application layer. Web security breaches can occur during a simple Web site 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), Web site defacements, theft of personal information, Denial of Service attacks, bot infection or a combination of malicious behavior.

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 2010 list:

Vulnerability	Description	Barracuda Web Application Firewall Solution
Injection Flaws	Occurs when untrusted data is sent to a Web application. Injection flaws are prevalent, particularly in legacy code, and are often found in SQL queries, LDAP queries, XPath queries, OS commands, and program arguments.	Inspects each client request for valid code inputs and blocks any malevolent content.
Cross Site Scripting (XSS)	Injects malicious code from a trusted source to execute scripts in the victim's browser which can hijack user sessions, deface Web sites, or redirect the user to malicious sites.	Inspects all traffic to remove malicious script content before forwarding them to back end servers.
Broken Authentication and Session Management	Hijacks a session using cookies, form fields or other authentication tokens by leveraging the inability to secure credentials throughout client sessions.	Monitors and proxies every unique user session to prevent hijacking. Digitally signs or encrypts the session cookies, making them tamper proof. Ensures session form fields and authentication tokens are read-only.
Insecure Direct Object Reference	Exposes a reference to an internal object such as a file, directory, database record, URL or form that can be manipulated to gain unauthorized access or reduce system performance.	Adaptively profiles Web traffic to build a positive security profile that can be used as a whitelist of valid client actions. Anything deviating from the security profile is treated as an anomaly and blocked.
Cross site Request Forgery (CSRF)	Hijacks a browser from a logged in victim to send forged requests without the victim's knowledge.	Injects randomized tokens into online forms and URLs to authenticate data streams, eliminating the ability to submit unauthorized or malicious requests.
Security Misconfiguration	Exploits application stack vulnerabilities such as unpatched software, misconfigured servers, zero-day threats and undeleted default accounts.	Filters application error or status responses to prevent attackers from profiling software vulnerabilities. Applies strong authentication and authorization policies to secure access control. Proxies traffic to prevent direct access to backend servers.
Insecure Cryptographic Storage	Exploits applications that fail to store sensitive information such as credit card numbers, social security numbers or user credentials as encrypted fields.	Filters and intercepts outbound traffic to prevent the transmission of sensitive information.

RELEASE 2 JULY 2010

Recent Web Security Incidents

- US Treasury Web site hacked using XSS to serve malware
- Heartland Payment Systems loses 100M credit card accounts
- Wyndham Hotels hacked three times in one year
- 32M Rockyou accounts stolen using SQL Injection

"Why WebApp Security Matters"

- Cross site scripting and cross site request forgery have evolved
 - Any Web site visited can infect a browser
 - Infected browsers can do anything
 - Infected browsers can scan, infect, spread
- Source: OWASP

OWASP

A worldwide free and open community focused on improving the security of application software. OWASP strives to make application security "visible" for people and organizations to make informed decisions about application security risks. The top 10 list originated from a collective of top security experts from around the world.

Payment Card Industry Data Security Standard (PCI DSS)

Targeted at merchants, processors and point-of-sale providers handling and storing sensitive account information, PCI DSS is comprised of 12 requirements to address proper use of firewalls, message encryption, access controls, networking monitoring and the implementation of an information security policy.

Vulnerability	Description	Barracuda Web Application Firewall Solution
Failure to Restrict URL Access	Guesses or tampers with an HTTP request to gain access to a Web site's resources, also known as 'forceful browsing'.	Provides a granular URL and form-level rules engine that restricts access to unauthorized resources. Seamless integration with credentialing systems provides strong access control.
Insufficient Transport Layer Protection	Failure by applications to encrypt network traffic containing sensitive communications.	Provides Instant SSL functionality that transforms an HTTP Web site into an encrypted HTTPS site without having to change any code. Modifies all outbound URL references to use HTTPS instead of HTTP.
Unvalidated Redirects and Forwards	Redirection parameters used by applications are not validated or are exposed. Allows attackers to hijack redirects and send users anywhere.	Inspects and validates all form and URL parameters to block unauthorized redirects.

The Barracuda Web Application Firewall is the complete and powerful security solution for Web applications and Web sites. 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 Web site. 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 over 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.

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

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premise-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.



Barracuda Networks
 3175 S. Winchester Boulevard
 Campbell, CA 95008
 United States
 +1 408.342.5400
www.barracuda.com
info@barracuda.com