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

With the Internet continually evolving to enable organizations to establish a global presence, conduct transactions and deliver real-time communications, it creates the need to ensure a heightened level of Web security. 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 and cost to recover customer confidence.

Gartner Group estimates 75 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: Web site defacements, phishing scams, unauthorized access to data, theft of personal information, denial of service attacks, bot infection or a combination of malicious behavior.

Most applications are vulnerable to such attacks, because application developers may not consistently employ secure coding practices. For most corporations, the company Web site is the main Web application and can fall victim to unsecured Web servers or minor code flaws from repeated updates. With 70 to 90 percent of Web applications acting as carriers of application vulnerabilities, it's important to evaluate products that can protect against current and new forms of Web-based attacks.

The Barracuda Web Application Firewall provide award-winning protection against hackers leveraging protocol or application vulnerabilities.

Comprehensive Protection Against Top 10 Application Vulnerabilities

To improve application security, the Open Web Application Security Project (OWASP) compiled a list of the 10 worst Web threats. In Jan. 2005, the payment card industry leveraged OWASP's list as a basis for the Payment Card Industry Data Security Standard (PCI DSS) to ensure the secure storage and transfer of cardholder data. OWASP updated its list of top 10 vulnerabilities in 2007 to the reflect changes in hacker activity.

The Barracuda Web Application Firewall provides complete protection for Web applications and are designed to enforce policies for both internal and external data security standards, such as the Payment Card Industry Data Security Standard (PCI DSS). At the same time, the Barracuda Web Application Firewall features a number of additional traffic management capabilities designed to improve the performance, scalability and manageability of today's most demanding data center infrastructures.

Vulnerability	Description	Barracuda Web Application Firewall Solution
Cross Site Scripting (XSS)	Injects malicious code from a trusted source as a script to access cookies or session tokens, attack a local network, or gain access to sensitive information stored by a browser or spoof content to confuse the user	Terminates connections to validate user input and inspects incoming requests before forwarding them to back end servers.
Injection Flaws	Relays unauthorized create, read, update or delete commands through a Web application to access data on another system, such as the operating system, database or an external program	Inspects each request from the clients to the back end systems for valid code inputs and blocks any malevolent commands.
Malicious File Execution	Leverages any Web application that accepts user inputted information to open, read, modify or execute files on the server to cause a total server compromise	Blocks operating system (OS) command injections attempting to access or request the server to act inappropriately.
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	Creates a Web site structure using granular URL and form-level settings to treat any anomalous access request as invalid or potential for exposure.

RELEASE 1
DECEMBER 2007

Recent Web Security Incidents

- Credit card and personal information stolen from TJMaxx
- Alicia Keys' MySpace page infecting visitors with malware
- Al Gore's Web site hacked to host links to online pharmaceuticals

"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 you can
- Infected browsers can scan, infect, spread

Source: OWASP, 11/2007

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.

http://www.PCISecurityStandards org
Barracuda Networks PCI DSS White Paper

Vulnerability	Description	Barracuda Web Application Firewall Solution
Cross site Request Forgery (CSRF)	Hijacks a browser from a logged-in victim to send a pre-determined request to vulnerable Web applications without the victim's knowledge	Injects randomized tokens into online forms to authenticate data streams, eliminating the ability to submit malicious requests and cause harmful activity.
Information leakage and Improper Error Handling	Exploits error messages to gather information about the OS and server versions, directories, patch levels, internal addresses to launch targeted attacks on the server with known platform vulnerabilities	Cloaks details of the Web application infrastructure and blocks a server's error messages from being sent out to the client. Filters and intercepts outbound traffic to prevent the transmission of sensitive information, and blocks or masks attempts to access credit card numbers, social security numbers, client records or any other specified data type.
Broken Authentication and Session Management	Hijacks a session using cookies, form fields or other authentication tokens by leveraging the inability to protect credentials and tokens throughout their lifecycle	Fully terminates and proxies every connection to insulate each unique user session from exposure and can stamp or encrypt the session cookies, thus making them tamper proof. Also has the ability to ensure that all hidden or read-only form fields are not changed by the user.
Insecure Cryptographic Storage	Abuses the difficulty application developers face in encrypting credit card numbers, account records, user credentials or proprietary information for storage	Filters and intercepts outbound traffic to prevent the transmission of sensitive information. Blocks attempts to access credit card numbers, social security numbers, client records or any other specified data type.
Insecure Communications	Failure by applications to encrypt network traffic containing sensitive communications	Transforms a plain HTTP Web site into a HTTPS site without changing any code to ensure secure transmission of data. Engages SSL to transmit data on the front end on behalf of an application, while sending plain text requests and responses to the back end servers.
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 granular URL and form-level settings to create the Web site structure that validates incoming and outgoing session content. The Web site structure can be used to restrict users from guessing and accessing resources deemed restricted from the public, such as Web pages under development.

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. built its reputation as the worldwide leader in content security appliances by offering easy to use and affordable products that protect organizations from email, Web and IM threats. Barracuda Networks has leveraged its success in the security market to offer networking products that improve application delivery and network access as well as world-class solutions for message archiving, backup and data protection. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar, are amongst the 70,000 organizations protecting their networks with Barracuda Networks' solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user license fees. Barracuda Networks is privately held with its headquarters in Campbell, Calif. Barracuda Networks has offices in 10 international locations and distributors in more than 80 countries worldwide. For more information, please visit http://www.barracudanetworks.com.

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