

A Practical Guide to Web Application Security

Introduction

Today, Web applications and sensitive corporate information are increasingly under attack by professional hackers. These antagonists recognize that network-layer attacks are yesterday's news, and they have moved to a new level of attacks—those targeting Web application vulnerabilities.

Making smart decisions about Web application security means being informed. Enterprises can ensure the safety and integrity of their Web applications by following these basic guidelines:

- Determine which Web applications are essential to business operations
- Get familiar with the most common—and most dangerous—Web application vulnerabilities
- Implement steps for protecting Web applications from attack and misuse
- Look for a comprehensive solution that addresses all of the key Web application security issues
- Assess the business benefits of Web application firewalls in detail
- Get an in-depth understanding of Web application firewall features and functionality

Table of Contents

2	Web Applications: The Bad with the Good
3	Web Application Security: The Business Benefits
	<ul style="list-style-type: none">• Preserve Brand and Revenue• Ensure Regulatory Compliance and Guard Against Identity Theft• Keep Management and Configuration Costs In Check
4	Protection in Depth
	<ul style="list-style-type: none">• Comprehensive inspection• Positive Security Model• Adaptive Learning• Multi-layer Cloaking
5	Protecting Web Applications from Attack and Misuse
	<ul style="list-style-type: none">• Prevent and Preempt
7	Not-So-Sweet 16
9	The Citrix Solution
10	Conclusion

Web Applications: The Bad with the Good

Web applications have reshaped business for the better by making e-commerce, online banking, and highly customized customer and partner portals possible. By moving business-critical applications and services like sales, support and purchasing to the Web, organizations have extended the boundaries of the enterprise—opening it up to enhance interaction with customers, suppliers, partners and employees. Web applications also speed and streamline internal processes. In short, they deliver the benefits businesses are always looking for, from higher employee productivity and lower support costs to increased customer satisfaction and greater revenue.

But there's a serious drawback to increased reliance on Web applications: they're inherently insecure and easily compromised. In fact, Symantec rates 73 percent of Web application vulnerabilities as easy to exploit.¹ Vulnerable Web applications not only put network systems and devices at much greater risk, they also offer a direct conduit to confidential customer data such as credit card numbers, account history and health records, as well as to sensitive corporate information.

- Symantec rates **73 percent** of Web application vulnerabilities as easy to exploit
- Gartner estimates that **75 percent** of all attacks are now aimed at Web applications
- The CSI/FBI Computer Crime Survey reported a **90-percent** surge in Web attacks in 2005

Network-layer defenses like traditional network firewalls and intrusion prevention systems (IPS) do little to protect Web applications, since simple IP packet inspection isn't effective at the application level. Not surprisingly, hackers are finding Web application weaknesses hard to resist; Gartner estimates that 75 percent of all attacks are now aimed at Web applications,² while the CSI/FBI Computer Crime Survey reported a 90-percent surge in Web attacks in 2005.³

How can an organization protect Web applications? By deploying security at the application layer. That's where Web application firewalls come in. These next-generation security appliances sit in front of Web application servers, where they terminate browser and Web services sessions and perform full bi-directional parsing of all application data. By examining the actual HTML session and understanding the context of client requests and application responses, Web application firewalls can enforce correct application behavior, block malicious activity, and help organizations ensure the safety of their sensitive information and systems. That yields a number of business benefits, from protecting brand equity and aiding regulatory compliance to meeting Service Level Agreements for Web applications to ensure their availability—and the revenue they generate.

¹ Reported in Symantec Internet Security Threat Report, January-June 2005, page 42.

² Reported in a Gartner note by Theresa Lanowitz, "Now Is the Time for Security at the Application Level," December 2005.

³ Reported in the CSI/FBI Computer Crime Survey, 2005.

Web Application Security: The Business Benefits

By safeguarding a company's critical Web applications, Web application firewalls deliver numerous business benefits.

PRESERVE BRAND AND REVENUE

When Web applications are left unprotected, brand image and customer satisfaction are put at risk. If hackers overwhelm servers with bogus requests and force the site out of service, customers and partners can't complete the transactions that sustain the business. When Web page content is modified without authorization or otherwise manipulated, customer trust erodes. And, most importantly, if customer information is compromised or stolen, the brand is surely irreparably damaged. And all of these things have been proven to do lasting damage to the brand.

But with an application firewall in place, companies can be confident of optimal Web application availability without performance degradation. Application firewalls also maintain the integrity of Web content, since they can block transmission of defaced or otherwise altered pages. Together, these capabilities protect the good name of the business.

ENSURE REGULATORY COMPLIANCE AND GUARD AGAINST IDENTITY THEFT

HIPAA. Sarbanes-Oxley. Gramm-Leach-Bliley. There's no shortage of federal, state and industry-specific regulations, but the challenge for businesses comes down to one thing: demonstrate compliance. Failure to do so can mean severe financial penalties as well as possible prison sentences for company personnel.

Noncompliance is a real possibility when vulnerable Web applications leave confidential personal and financial data exposed. Even if a Web application doesn't directly store information subject to compliance, it often provides a pipeline to the systems on which that information resides.

Web application firewalls protect Web applications, services and back-end databases by blocking malicious attacks. They can also block unauthorized outbound transmission of confidential customer data—like credit card and social security numbers—in application responses. Further, they even transform digits to obscure items that are transmitted back to customers, offering further assurance that sensitive information isn't revealed, and providing an extra layer of defense that complements the application code.

It is essential for an organization to be able to prove compliance with any number of regulations through detailed logging, reporting and alerting. A solid pillar of defense against identity theft, fraud and loss of sensitive corporate information is needed to prove this level of compliance and ensure application availability to legitimate users.

KEEP MANAGEMENT AND CONFIGURATION COSTS IN CHECK

As the importance of Web applications has increased, so has their number—and the administrative load they impose. Further, many companies have deployed Web applications on an ad hoc or as-needed basis in response to immediate business requirements. That's made for a complex and sometimes fragile Web application environment comprising numerous discrete, single-function devices like proxy servers, caching solutions and SSL accelerators.

But a single Web application firewall can perform numerous functions in addition to protecting XML and HTML applications—from SSL acceleration and layer-7 proxying to Web I/O acceleration and business object protection. Deploying application firewalls can reduce load on back-end servers, reducing the number of servers required for a Web application.

Further, Web application firewalls make patch management easier. First, they keep companies from having to wait for vendors or in-house developers to deliver patches, since they provide protection for the application upon deployment. Second, they reduce the chaos that comes from having to respond immediately to CERT advisories and other warnings; instead of undertaking urgent, reactive steps, companies can maintain application security while a patch is developed, tested and deployed. Both help in considerably reducing administrative and operational expense, and ease the tense moments spent waiting for critical patches to be delivered.

Protection in Depth

The key to keeping Web applications safe from attack is close examination of all of their numerous moving parts. This is exactly where network firewalls and intrusion prevention systems (IPSs) come up short. Network firewalls, for example, are designed and deployed to provide basic access control by inspecting IP packets. They don't understand application languages like HTML and XML—and they don't understand HTTP sessions. Consequently, they can't validate user inputs to an HTML application, or detect maliciously modified parameters in a URL request. And this leaves the application vulnerable to a range of serious exploits.

An IPS, meanwhile, can detect and block attacks within the network. But like network firewalls, IPSs have little or no understanding of application languages—which means they can't stop session-based application-layer attacks or detect the injection of malicious code. On top of that, an IPS is known for generating false positives, so that aside from leaving Web applications unprotected, it can also risk wasting valuable IT resources and frustrate application users. Because application firewalls understand the language Web applications speak, they generate far fewer false positives.

THREE MOST COMMON WEB APPLICATION EXPLOITS

- **Cross-site scripting (XSS)**
- **Buffer overflow**
- **SQL injection**

There's another important issue to keep in mind: a lot of today's Web application traffic is encrypted for security using the SSL (Secure Sockets Layer) standard. But neither network firewalls nor most intrusion prevention systems can decrypt SSL traffic for inspection. Consequently, they're powerless to stop, or even detect, encrypted exploits from entering the network and striking directly at Web applications.

In short, network firewalls and intrusion prevention systems by themselves do not offer sufficient protection for Web applications. But by deploying a comprehensive application firewall solution, companies can address all application vulnerabilities. In evaluating application firewall options, organizations should look for the following features:

COMPREHENSIVE INSPECTION

The application firewall should include inspection technology capable of reconstructing all bi-directional communications for each user session to ensure correct application behavior and the validity of user and machine inputs. The solution

should include these main functions: bi-directional analysis of all application traffic; complete header and payload inspection; full application parsing; semantic extraction of relevant application objects; and traffic sessionization—or, the ability to remember on a per-session basis everything the Web server sends to each client and verify the responses from the clients.

POSITIVE SECURITY MODEL

The positive security model is based on HTTP industry standards and best coding practices for HTML and Java. Basically, it allows an application firewall to recognize good application behavior without the need for attack signatures or pattern-matching techniques. Application behavior deviating from the positive security model is treated as potentially malicious and is blocked.

The benefit of the positive security model is that it is the only proven method for delivering zero-day protection—in other words, it secures companies against unpublished exploits. Further, it ensures Request for Comment compliance and enforces security in real time.

ADAPTIVE LEARNING

Application firewalls use adaptive learning to exceed out-of-the-box protection against Web-based threats. Adaptive learning allows security policies to be tailored for any application, including those using client-side JavaScript. Adaptive learning can automatically learn the behavior of an application and generate human-readable policy recommendations. A security manager can then selectively apply recommendations to strengthen the security policy and enable permissible application behavior.

MULTI-LAYER CLOAKING

Multi-layer cloaking takes away a hacker's ability to conduct reconnaissance on a targeted Web site. It hides sensitive information about an application environment—such as application server, database technology, server operating system, or internal domain naming—making it much more difficult for an attacker to devise an effective strategy for exploiting known vulnerabilities, or finding new ones. When sensitive information at multiple communication layers is cloaked, hackers are robbed of the chance to track down valuable intelligence about the application infrastructure, thus greatly reducing the risk of attack.

Protecting Web Applications from Attack and Misuse

PREVENT AND PREEMPT

That sums up a key element in a comprehensive approach to Web application security. Enterprises that want to ensure the integrity of their Web applications should follow this strategic checklist for safeguarding them from attack and misuse:

- ☑ **Protect both application infrastructure and application users**

Many companies define application security requirements too narrowly, addressing only the application program and data. But they should address Web application security in terms of infrastructure and users as well. While some exploits target the application (buffer overflows), others target a device like the back-end database (SQL injection), or the trust relationship with the user (cross-site scripting, or XSS). A comprehensive approach to Web application security addresses all of these elements.

✓ **Defeat zero-day attacks**

Attacks that exploit vulnerabilities in custom application code, or in packaged code for which the vendor has not yet released a patch, are known as zero-day attacks. Signature- and correlation-based solutions cannot offer protection from such attacks. The only viable defense against zero-day attacks is one employing a positive security model that understands and enforces correct application behavior, thus enabling a device to allow legal traffic while blocking illegal traffic in real time.

✓ **Implement key cloaking capabilities**

Taking away a hacker's ability to survey Web application details is critical in ensuring security. Companies should be sure to implement these capabilities:

- Remove unnecessary response headers
- Rewrite application URLs to hide internal structures
- Remove HTML comments that leak information
- Obfuscate cookie names, values and URLs, and sign and validate hidden form fields to prevent tampering

WEB APPLICATION SECURITY: KEY COMPONENTS

- **Protect application infrastructure and end users, in addition to the applications themselves**
- **Guard against zero-day exploits**
- **Prevent sensitive corporate or customer data from slipping through**
- **Eliminate the false positives that can block benign application traffic**

✓ **Prevent leakage of sensitive corporate or customer data**

Inspecting only inbound traffic is an incomplete way of securing Web application traffic; enterprises also have to keep a close eye on what's heading out. Keeping data confidential means taking the following steps:

- Inspect the entire data stream, not just HTTP headers, for restricted traffic
- Ensure precision when matching data objects like credit card numbers; they should be tested for validity before real-time action is taken
- Provide an option to transform matching data objects; for example, rather than blocking an entire credit card number, leave the last four digits visible for verification

✓ **Don't block benign traffic**

In the drive to safeguard Web applications, companies have to be careful about false positives and blocking traffic that poses no threat. The mitigation or complete elimination of false positives requires each of the following:

- True application-layer inspection
- Full communications context
- A semantic understanding of all application data

✔ **Deploy consistent security for all applications**

Companies typically have multiple Web applications that are vulnerable to common exploits, such as SQL injection attacks. In such cases, global security settings can be used to apply security policy consistently across all applications. At the same time, global settings applied indiscriminately can interfere with individual applications, so companies should also be able to define per-application rules as needed. And regardless, policy management and data collection should remain granular.

✔ **Adapt policies for dynamic application environments**

A positive security model that can't anticipate and accommodate dynamically generated traffic from a client could potentially block legitimate traffic. The only reliable approach to making sure that dynamic content is properly handled while still enforcing client-to-application behavior is adaptive application learning—which learns corrective behavior through analysis of the content in actual client requests.

Not-So-Sweet 16

Comprehensive protection is critical in today's network environment. Without it, applications face undue risk from any one of the 16 classes of application exploits. Here are the most common Web application attacks and vulnerabilities:

1	Cross-site Scripting (XSS)	An attack on the trust relationship between a user and a Web application, XSS is an attempt to trick the user or the user's browser into sending a hacker confidential information that can be used to steal that user's identity.
2	Buffer Overflow Exploits	This common input validation attack overflows a buffer with excessive data. Successfully executed, it can help a hacker run a remote shell on the machine and gain the same system privileges granted to the application being attacked.
3	CGI-BIN Parameter Manipulation	Another type of input validation attack, in which data that's passed to a server-side script is illegally modified. If query parameters passed to CGI scripts aren't properly validated, hackers have a better chance of gaining unauthorized system privileges to modify files, run commands and execute other operations.
4	Form/Hidden Field Manipulation	An attack in which contents of a hidden field are modified to trick the application into accepting invalid data and tampering with user sessions.
5	Forceful Browsing	An attempt to access unauthorized and unadvertised URLs to gain entry to the root directory of a Web server or other off-limit areas.

6	Cookie/Session Poisoning	Reverse-engineering weak cookies to steal a user's session or to impersonate a legitimate user of an application.
7	Command Injection	Inserting system commands into program variables like form fields, which are inadvertently executed on the server.
8	SQL Injection	An input validation attack that sends SQL commands to Web applications, which are then passed to a back-end database. A successfully executed SQL injection attack can give a hacker access to sensitive information.
9	Error-triggering Sensitive Information Leaks	An attack in which malformed, illegitimate data is fed to an application with the goal of generating errors and gaining sensitive information about the application environment.
10	Web Site Defacement	Malicious modification of Web pages.
11	Zero-day Exploits	A vulnerability that's exploited before it's publicly known and before vendor-developed patches, signatures, or other fixes are available.
12	Back Doors and Debug Options	Exploiting application back doors or debug code on production systems.
13	Broken Access Control Lists/Weak Passwords	Circumventing an application's access control system by requesting resources for which the user should not have access.
14	Insecure Use of Cryptography	Exploiting an application's use of a weak cryptographic algorithm in digitally signing cookies.
15	Server Misconfiguration	Hackers can exploit server misconfigurations—including the failure to fully secure the Web server, disable default accounts and services, or remove unnecessary functionality—to gain unauthorized application access.
16	Well-known Platform Vulnerabilities	Exploiting publicized weaknesses in Web servers or operating systems to gain unauthorized access to an application.

The Citrix Solution

The “Not So Sweet 16” are clearly the kind of threats your business doesn’t need. But with Citrix Application Firewall™, companies can deploy the industry’s highest-performing Web application security solution to protect Web applications and servers without degrading throughput or application response times.

Citrix Application Firewall delivers complete application security functionality. Deep-stream inspection ensures correct application behavior and the validity of user and machine inputs. Its positive security model ensures that all suspicious application behavior can be blocked, with no need for attack signatures or pattern matching.. Adaptive learning enables Citrix Application Firewall to protect complex Web applications. And multi-layer cloaking hides sensitive details about the application environment—keeping hackers from harvesting information they could use to launch an attack.

Citrix Application Firewall also offers comprehensive protection for specific kinds of customer data. Its SAFE Commerce Protection Module prevents unauthorized transmission of credit card numbers by Web applications, either by blocking the transmission entirely or by masking the majority of digits in the credit card number itself. Meanwhile, the SAFE Object Module keeps user-defined data objects—such as customer account, patient record identification, and driver’s license numbers—under wraps. Even billing codes and EDI (electronic data interchange) tags can be protected with the SAFE Object Module. All together, that adds up to 16-for-16 protection against today’s most dangerous classes of application vulnerabilities.

But protection is only part of the picture. Citrix Application Firewall also offers flexible deployment options, and the system can be up and running in as little as 30 minutes. It can be used as a standalone device or in conjunction with Citrix® NetScaler® application delivery systems, which have been shown to improve application performance by up to 15 times.

Overall, Citrix Application Firewall delivers best-fit performance for any enterprise or data center installation.

- Full protection against known and emerging Web application threats
- Plug-and-play appliance that can be up-and-running in less than 30 minutes
- High-performance security for both Web and XML Web services applications without performance degradation
- Full protection against identity theft, and theft of credit card numbers and other sensitive data
- Positive security model that requires no application security expertise to maintain
- Advanced learning capabilities to protect more sophisticated Web applications
- Greater protection against attacks that target specific user sessions (mandatory for e-commerce, secure extranet, and online banking applications)
- More granular control over application security policies
- Advanced features for preventing the loss of confidential Web site information

Citrix Application Firewall delivers everything today’s businesses need to safeguard critical Web applications—and reap benefits ranging from brand protection and the continued trust of customers to regulatory compliance and lower administrative costs.

Conclusion

With Web applications extending the boundaries of the enterprise, companies have no choice but to deploy technology that specifically secures these critical resources, and the sensitive information behind them, from attack. Network-layer defenses like firewalls and intrusion prevention systems don't protect at the application layer, which makes application firewalls the only viable option.

"[Citrix Application Firewall] scores highest in attack protection and boasts the best combined scores in attack detection, traffic throttling and blocking."

— Forrester Research; Forrester Wave:™ Web Application Firewalls, Q2 2006

Citrix Application Firewall blocks all known and emerging Web and Web services application attacks, thanks to comprehensive core technology that includes deep-stream inspection and a positive security model. By specifically safeguarding applications and sensitive data, this hardened, high-performance solution from Citrix lets companies conduct their Web-based business processes competitively and without worry. In fact, Forrester Research recently designated Citrix Application Firewall the solution that "scores highest in attack protection and boasts the best combined scores in attack detection, traffic throttling and blocking" in the recent Forrester Wave:™ Web Application Firewalls, Q2 2006.

More than 180,000 customers look to Citrix to provide the best access experience to their business applications. Now Citrix can help protect these applications with the industry's highest-performing Web application security solution: Citrix Application Firewall.



Best Access Experience. Anytime. Anywhere.

About Citrix: Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and most trusted name in on-demand access. More than 180,000 organizations around the world rely on Citrix to provide the best possible access experience to any application for any user. Citrix customers include 100% of the Fortune 100 companies and 98% of the Fortune Global 500, as well as hundreds of thousands of small businesses and individuals. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Citrix annual revenues in 2005 were \$909 million. Learn more at <http://www.citrix.com>.

©2006 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler® and Citrix Application Firewall™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and other countries. All other trademarks and registered trademarks are property of their respective owners.

Citrix Worldwide

WORLDWIDE HEADQUARTERS

Citrix Systems, Inc.

851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Tel: +1 (800) 393 1888
Tel: +1 (954) 267 3000

EUROPEAN HEADQUARTERS

Citrix Systems International GmbH

Rheinweg 9
8200 Schaffhausen
Switzerland
Tel: +41 (52) 635 7700

ASIA PACIFIC HEADQUARTERS

Citrix Systems Hong Kong Ltd.

Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
Tel: +852 2100 5000

CITRIX ONLINE DIVISION

5385 Hollister Avenue
Santa Barbara, CA 93111
Tel: +1 (805) 690 6400

www.citrix.com