GamaSec

Web Application Security Testing White Paper

1. Web Applications: An attractive target for hackers

How do you cost effectively defend web applications from hackers? Your organization relies on mission critical business applications that contain sensitive information about customers, business processes and corporate data. Moving away from proprietary client/server applications to web applications gives you a simpler, cost-effective, highly extensible delivery platform. These applications are more than a valuable tool to power your business operations; they are also a valuable and vulnerable target for attackers.

Web applications are increasingly the preferred targets of cyber-criminals looking to profit from identity theft, fraud, corporate espionage, and other illegal activities. The impact of an attack can be significant, and include:

- Costly and embarrassing service disruptions
- Down-time
- Lost productivity
- Stolen data
- Regulatory fines
- Angry users
- Irate customers
-

In addition to protecting the corporate brand, federal and state legislation and industry regulations are now requiring web applications to be better protected.

As you take action to protect web applications in a timely and effective manner, you must balance the need for security with availability, performance and cost-effectiveness. Protecting web applications requires both zero-day protection and rapid response with minimal impact to operations without impacting performance or changing system architectures.

2. Web applications are increasingly vulnerable.

Rapid growth leads to emerging problems

The number of corporate web applications has grown exponentially and most organizations are continuing to add new applications to their operations. With this rapid growth come common security challenges driven by complexity and inconsistency. New awareness into web application vulnerabilities, thanks to organizations such as the Open Web Application Security Project (OWASP), has helped organizations identify application security as a priority. But according to a June, 2006 survey (www.symantec.com/about/news/release/article.jsp?prid=20060919_01), while 70 percent of software developers indicated that their employers emphasize the importance of application security, only 29 percent stated that security was always part of the development process.

Overlooked online application vulnerabilities

Unfortunately, it is not just application flaws that are leaving systems vulnerable. In addition to application issues, every web application relies on a large stack of commercial and custom

software components. The operating system, web server, database and all the other critical components of this application stack, have vulnerabilities that are regularly being discovered and communicated to friend and foe alike. It is these vulnerabilities that most organizations overlook when they're considering web application security.

As new vulnerabilities are found, patches become a critical part of managing application security. The process of patch management is complex and difficult to do successfully. Even the most proactive IT team must often reassign critical resources to deploy urgent patches, disrupting normal operations. The time required to patch responsibly lengthens the window of time a hacker has to exploit a specific vulnerability. With thousands of vulnerabilities and patches being announced each year the problem continues to grow. Even organizations with the most efficient patching processes in place can't rely on this alone to protect them from attacks targeting web application vulnerabilities.

Hackers look for the path of least resistance

Today's sophisticated attackers target corporate data for financial and political gain. They know they can more easily exploit vulnerabilities in web application stacks versus trying to defeat well built network and perimeter security. Hackers have a myriad number of vulnerabilities techniques to use including:

- SQL Injection
- Cross Site Scripting
- Buffer Overflow,
- Denial of Service

The number of application vulnerabilities in commercial applications and open source applications is growing at an alarming pace; anywhere from 200 to 400 new vulnerabilities are identified every month.

According to zone-h.org, 45% of attacks make use of vulnerabilities rather than configuration issues or use brute force. Attackers are working hard to find and exploit new vulnerabilities in web applications faster then they can be patched. The window of time, from when a hacker identifies a vulnerability to when it is communicated and eventually patched, makes a fast response defence- strategy critical to prevent a potentially damaging intrusion.

3. Required: A remote online web application security-testing service

Web applications are increasingly vulnerable and protecting them requires a system that can:

- Ensure compliance today
- meet the evolving needs of an organization for tomorrow
- Respond quickly

To meet this challenge, by the optimal solution should locate these vulnerabilities as they are seen from the hacker's point of view. Therefore a remote online Web application security testing service will best address those needs.

A web application security scan should reveal vulnerability for these attacks:

- SQL Injection
- Blind SQL Injection
- Installation Path Disclosure
- .Net Exception

- Command Execution
- PHP Code Injection
- Xpath Injection
- CRLF Injection
- Directory Traversal
- Script Language Error
- URL Redirection
- Remote File Inclusion
- LDAP Injection
- Cookie Manipulation
- Source Code Disclosure
- Cross-Site Scripting
- Cross-Frame Scripting

The security scan must test vulnerabilities for a wide variety of website components:

- Web Servers
- Web Server Technologies
- HTTP Methods
- Backup Files
- Directory Enumeration
- Directory Indexing
- Directory Access
- Directory Permissions
- Sensitive/Common Files
- Third Party Application

The online web application security service must:

- Remotely crawl the entire website.
- Analyse each file.
- List the vulnerabilities found along with the severity levels of each vulnerability.
- Launch a series of web attacks to discover security.
- Include option to make a tailor made attack
- Be able to adapt to any web site configuration.
- Produce dynamic tests, which will create relevant reports of online scan findings.
- Provide a constantly updated vulnerability assessment
- Include an automatic False Positive Prevention Engine.
- Provide Enhanced Report Generation for Scanning Comparison. – Must include the ability to create comparison and trend analysis of your web applications vulnerabilities based on scan results generated over a selected time periods.
- Recommend solutions in order to fix, or provide a viable workaround to the identified vulnerabilities

A website application security service which includes all these components will help you prevent hackers from attacking you site and disrupting your business. For a longer version of this article. http://www.gamasec.com/pdf/WhitePaper.pdf

GamaScan provides website application security testing. A robust set of reports and charts provide a clear and concise view of security vulnerabilities, as well as recommended solutions. For further information see:info@gamasec.com. The Vulnerability Report identifies all services and open ports, with known vulnerabilities listed, as well as descriptions and patches provided. The Security Notification Report provides vulnerability details and subsequent issues, as well as recommended remedies.

Author:
Avi D. Bartov – Co-Founder and CEO of GamaSec, Avi is a graduate of law from Nanterre University in Paris, France with over 12 years of experience & management in IT security. He is a technology executive who has led several companies to success in Europe and Israel.

Abstract
Web Application Security Testing White Paper
Author: Avi D. Bartov
The need to provide web security and defend web applications from hackers due to software and hardware vulnerabilities requires remote an online web vulnerability-assessment service to combat maximum vulnerabilities. The risks must be continually updated and the tests tailor-made to provide optimal solutions.

Keywords
website security test, protect application, server, hacker, vulnerability check, web security seal, application security, security assessment software, vulnerability assessment,