

Web Application Security Newsletter - May 2005

A MESSAGE FROM THE EDITOR - Welcome to the May 2005 edition of the Web Application Security Newsletter. New data points from security industry experts once again show off the dramatic rise in web application hacking that continues to take place. Nearly 70% of attacks in 2004 were waged against the application as opposed to network infrastructure. We've heard this previously from leading industry analysts and again from zone-h as discussed below. Not surprisingly, one of the top attack techniques is SQL injection. For hackers looking to score quickly, the shortest path to a website's valuable data assets is through SQL injection. It's unfortunate that more web applications aren't secured against this relatively well known hacking technique.

Companies have until June 1 to comply with new data security requirements

Amidst increasing incidents of identity theft and fraud, companies that manage credit card information have until June 1 to comply with new data protection requirements being pushed by MasterCard Intl Inc. and Visa U.S.A. Inc. The Payment Card Industry Data Security Standard (PCI) lists 12 items that must be met by companies handling credit card data. Designed to set in place a common process for protecting credit card data, items include technology requirements as well as procedural mandates. Banks that issue credit cards must ensure that companies comply with the requirements and could face fines up to \$500,000 per incident if data is compromised.

[Read more...](#)

Firm says that PHP bugs and SQL injection attacks were used most often by hackers

According to zone-h, the Estonian security firm, web server attacks and website defacements rose 36 percent in 2004. The firm estimates that 2,500 web servers per day are successfully hacked out of a total population of 45m servers. The firm's founder, Roberto Preatoni, stated that PHP bugs and SQL injection attacks were used most often by hackers to gain access to vulnerable systems. Preatoni said that 70 per cent of attacks are based on exploiting application vulnerabilities regardless of OS platform.

[Read more...](#)

Unisys predicts that application software breaches could lead to lemon laws

The advent of the lemon law tops the list as one of this year's security challenges. Unisys predicts that customers will begin to sue software providers for damages sustained by security vulnerabilities. Lemon laws will protect the consumer against damages caused by a security breach, which will significantly level the playing field between software makers and consumers. Also predicted is that cyber attack styles will become virulent, with 2005 predicted to deliver the first worm or virus that alters or destroys information at the record level. Terry Hartmann of Unisys highlights that organizations will become more proactive security-wise. "Faced with accountability for compliance, management has begun to realize that security is 20% technology and 80% process," he states.


[Read more...](#)

Buyer beware: "Just say no" to software riddled with holes

Win a FREE
Assessment Product

Whitepaper: Enabling Security
in the Software Development
Lifecycle (PDF)

Product Info: Cenzic
Hailstorm automates
penetration testing for your
web applications



Despite the millions of dollars spent for the sake of security, as consumers, we are still under attack. Who really is to blame for application insecurity? Is it the programmers who write the code or the software companies who are rushing to be first to market, despite a defective product? According to one expert, around 40 different categories of vulnerabilities have been identified, from SQL injection to buffer overflows. So, why aren't the vulnerabilities being fixed? As mass consumers, can we drive change by insisting that security criteria are met, refusing to accept software riddled with holes?

[Read more...](#)

A focus on security and standards are often lacking

Security is often an afterthought left to system administrators who wield firewalls, intrusion detection software, and other defense tactics after an application is deployed. According to one expert, few organizations use a standardized approach to address security. Research from Gartner Inc. has found that fixing security flaws prior to production can generate significant cost savings, as high as a 75% reduction in configuration management and incident-response costs. Solutions range from development of business and user application profiles to focusing on security as part of testing and quality assurance. Blue Cross and Blue Shield of Massachusetts Inc. have integrated preemptive security efforts during development in their evaluation and testing and with the use of intrusion-detection technology to identify potential security holes.

[Read more...](#)

Highly critical flaws come to light

Servers running open-source programming language PHP are vulnerable to several serious security exploits, including malicious code execution and denial-of-service issues. The project has issued updates, which are available from the PHP website or directly from some OS vendors. The PHP Group advised, "All users of PHP are strongly encouraged to upgrade to this release."

[Read more...](#)

www.cenzic.com

+1 (866) 4-CENZIC

info@cenzic.com

You have received this email as a subscriber to the Cenzic Newsletter. If you have received this email by mistake or would like to be removed, [click here](#).