



SECNAP® Network Security has been a trusted partner to clients in a broad range of industries since 2001 for our ability to effectively address and remediate their evolving needs.

Leveraging our comprehensive portfolio of services, CIOs, CISOs, IT directors and network managers have been able to dramatically reduce vulnerabilities and enhance the protection of sensitive data. Regulated institutions have been able to substantially improve their compliance positions.

### **The High Price of Vulnerability**

Security breaches have far-reaching impacts that range from remediation costs and damages payable to victims, to the incalculable toll of negative publicity and lost business. A recent *Security Trends Report* published by Cenzic indicates that 70% of vulnerabilities reported in Q1 2008 affected web applications, servers and browsers—and roughly 65% of those were classified as easily exploitable.

The SECNAP Web Application Assessment identifies vulnerabilities before they have a chance to become security breaches (and public statistics).

### **Industry-Leading Tools and Expertise**

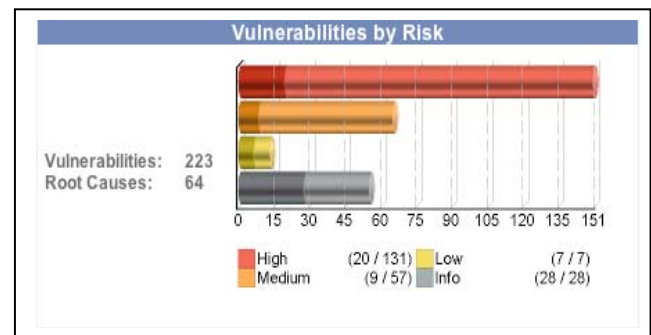
In addition to extensive hands-on experience, our professionally certified network security auditors leverage a complete tool kit in order to evaluate security weaknesses in your web applications, with a focus on SQL injection vulnerability.

Extensive automated and manual tests are conducted, including penetration testing that attempts to gain access to sensitive data. Reviews of applicable policies, procedures and processes are included as needed.

### **What You Gain from the SECNAP Assessment**

One of the most significant benefits of our Web Application Assessment is the peace of mind you'll enjoy knowing your web applications are free of weaknesses that could enable unauthorized intrusion or compromise sensitive data. In addition to helping you rest easier, the assessment will:

- **Verify applications are properly configured to prevent unnecessary data from being revealed**
- **Validate user authentication processes, password reset mechanisms and session management schemes**
- **Identify strengths and weaknesses of web applications in terms of overall security**
- **Prioritize exposures that present greatest risk**
- **Deliver an actionable report including executive summary and remediation recommendations.**



SECNAP offers a full complement of network security solutions designed to meet your needs today and tomorrow. Please see the reverse side for more information about our Web Application Assessment services, or give us a call.

**866-732-6276**

### **Award-Winning Security Solutions**

Our technological leadership in intrusion detection and prevention earned the 2008 *Shaping Information Security Award* from Info Security Products Guide and the *2008 Best Products and Services Award* in the Intrusion Prevention class from Network Products Guide.



### Overview of Assessment Process

The Web Application Assessment leverages a set of automated and manual tests designed to find weaknesses in the application. Initial steps include identifying application layout and locations where the greatest risks appear to reside. Once the site is mapped, appropriate attacks are initiated to discover vulnerabilities in the application, leveraging SQL vulnerability detection and penetration testing. Findings are compiled and a thorough report delivered, including useful graphs and charts.

### Assessment Components

Designed to verify that your organization is utilizing external web applications that are free of vulnerabilities which could cause sensitive data to be compromised, the assessment encompasses a variety of components, tools and tests.

Fault injectors are just one example. These tools insert strings into a target application that are most likely to cause the application to fail. Hackers typically use these strings to probe the application for weakness that can be exploited. Following are injectors typically employed during the assessment:

- Windows Command Injection
- Unix Command Injection
- SQL Parser
- SQL Disclosure
- Relative Path
- Cross-Site Scripting
- Buffer Overflow
- Insecure Configuration
- Unvalidated Input
- Denial of Service

*A growing body of regulation imposes enormous burdens on institutions to exercise constant vigilance and implement safeguards to protect their information systems, transaction processes and sensitive databases.*

*Cybercriminals become bolder and more creative each day, and the burgeoning volume of cyberthreats can originate from sources as mundane as email and online forms.*

*These and other factors have created an environment in which IT staff routinely operate on overload. By leveraging third-party support for specific projects—such as security audits, penetration testing, and intrusion detection and prevention solutions—IT management can ensure staff are able to remain focused on mission-critical responsibilities.*

### Testing to Identify Areas of Risk

The security assessment examines multiple levels of potential vulnerability—from field-level, to form or page-level, to cross-frame scripting vulnerabilities.

In addition, tests are conducted to discover other areas of risk, such as:

- Unvalidated parameters
- Broken access control
- Broken account and session management
- Cross-site scripting flaws
- Buffer overflows
- Command injection flaws
- Error handling problems
- Insecure use of cryptography
- Remote administration flaws
- Web and application server misconfiguration

### Final Report and Briefing

Our final report provides a thorough assessment of web application vulnerabilities, accompanied by expert recommendations to help you begin to address them. Findings may also be presented to key stakeholders, including C-level executives, IT management, web applications development and systems staff.

In addition, optional work, security equipment or security solutions may be recommended to assist you in addressing priority risks expeditiously.



*Useful graphics are included in the Web Application Assessment report to illustrate specific findings.*

