infotex

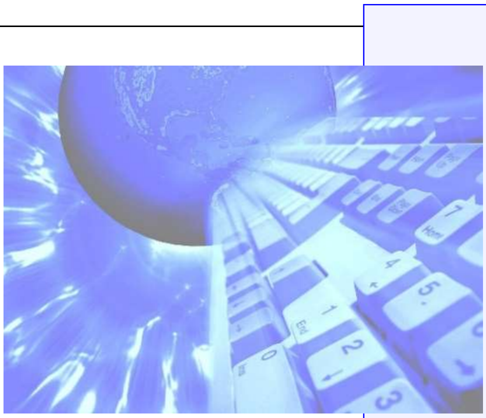
CISSPs, CISAs, CISMs, CRISCs, CPAs

Web Site Security Review

my.infotex.com

offerings.infotex.com

infotex Provides Web Application Security Review Services!



Many banks are proceeding with a false sense of security that, because they outsource their on-line banking processes, they are secure from a web defacement and/or even an information security breach perspective. They do not realize that, especially if they utilize "forms" ont heir websites, they are facing possible reputational, operational, even integrity risk. Our marketing sites, often maintained by non-technical personnel, now utilize forms, search engines, even connections into databases that all offer vulnerabilities to the bad guys.

According to the Federal Financial Institutions Examination Council (FFIEC), "financial institutions should establish appropriate systems and application development methodologies." This process should include "Quality assurance, risk management, and testing standards and procedures." Testing standards provide the best means to manage project risks and ensure software includes expected functionality, security, and operability.

infotex conducts our Web Site (and/or Web Application) Security Review using a phased approach. Not only do we look at technical controls, but also non-technical controls that your organization has in place. We test control processes, user interfaces, encryption, authentication, and infrastructure, as well as review code.

Our Reporting

During the process, we confirm and document results of findings, perform a risk analysis, and create a vulnerability matrix. In addition, we provide a report that includes an Executive Summary, a Vulnerability Matrix, and a CD with supporting documentation. Beyond that, we review the Executive Summary and Vulnerability Matrix with the appropriate members of your team.

Our Web Application Security Review

- **Phase I: Infrastructure Vulnerability Assessment** – We perform a technical vulnerability assessment in two phases (blind and internal) on your web application infrastructure (servers and network devices) using standard techniques for assessing networks with application security in mind.
- **Phase II: Infrastructure Configuration Audit** – **infotex** performs an assessment of your current network configuration including client and server applications and IT practices based on comparison to vendor and industry published best practices.
- **Phase III: Application Review** – We will scan all source code looking for vulnerabilities. This review will use as a standard the framework presented at owasp.org. In particular, each application will be checked for all vulnerabilities listed in the most current OWASP Top 10 list.
- **Phase IV: Development Controls Review** – Our process includes interviews with various personnel to test for appropriate knowledge of policies and procedures pertaining to development controls. In addition, we review the policies and procedures in place as they pertain to the Systems Development Lifecycle.

Top 10 "Current" Web Application Vulnerabilities (OWASP)

1. Cross Site Scripting (XSS)
2. Injection Flaws
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access