



A business case for Application Security Testing

Introduction

More and more companies are relying on Web-based applications to provide online services to their employees, to support e-commerce sales and to leverage portals, discussion boards and blogs that help staff better communicate with customers, partners and suppliers. However, as the number and complexity of Web applications have grown, so have the associated security risks. With increasing frequency, incidents of Web application breaches resulting in data theft are popping up as front-page news.

Some of news you can't ignore

World story

- 40 Million Credit Cards Compromised
- 55 Million Customer Records Exposed, 130+ Security Breaches in 2005
- \$105 Billion In Cyber crime Proceeds in '04, More than Illegal Drug Sales

There have been quite a few Govt and FSS security breaches in India recently.

- Hacker breaks into 17 bank a/cs
- Bank of India site hacked, served up 22 exploits
- Maharashtra govt website hacked
- Goa govt's info website hacked

Evolving Security Needs

Close to 80% of web sites are vulnerable to Cross-site scripting, which can be executed even by a novice hacker. Your website could be one as well.

Table below lists just a few of the potential threats to Web applications, the effect they could have on your business, and the average percentage of Web sites that are vulnerable to this type of attack.

Threat	Gives attackers the ability to ...	Average percentage of vulnerable Web applications
Cross-site scripting	... impersonate a trusted user to gain access to your sensitive business data	80%
Structured query language (SQL) injection	... access all the data in your database, resulting in a complete data compromise	62%
Parameter tampering	... navigate your database and retrieve or modify its contents	60%
Cookie poisoning	... steal one or more of your customers' identities	37%

Emerging regulations and requirements

As the number of Web application security breaches has increased, regulatory and industry requirements have become more stringent. Such measures dictate that companies protect all Web-facing applications against attacks by engaging an application security organization to review all custom application code for vulnerabilities. Here is a list of popular industry standards and regulatory compliances.

Standard/Compliance	Description
OWASP Top 10	<p>The OWASP Top Ten provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are.</p> <p>The U.S. Federal Trade Commission strongly recommends that all companies use the OWASP Top Ten and ensure that their partners do the same. In the commercial market, the Payment Card Industry (PCI) standard has adopted the OWASP Top Ten, and requires (among other things) that all merchants get a security code review for all their custom code.</p>
Payment Card Industry Data Security Standard	<p>It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, cracking and various other security vulnerabilities and threats. A company processing, storing, or transmitting payment card data must be PCI DSS compliant or risk losing their ability to process credit card payments and being audited and/or fined.</p>
ISO 27001	<p>..is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It lists security control objectives and recommends a range of specific security controls.</p>
FISMA	<p>The Federal Information Security Management Act of 2002 is a United States federal law enacted in 2002. The act was meant to bolster computer and network security within the federal government and affiliated parties (such as government contractors) by mandating yearly audits.</p>

Establishing proper security practices in your company

To combat the growing threat of Web application breaches, it's important to address three key areas of your business: your people, your processes and your technology.

Your people

It is imperative that the people developing and deploying your Web applications—whether they are staff members or external contractors—understand the fundamentals of secure design principles and security threats. In the past, security was viewed as an IT problem, not a development problem. But now, security experts have realized that security starts at the code level. Therefore, it's important to provide your developers with the training they need to stay on top of changing security threats and learn about existing and emerging methods for mitigating them.

Your processes

As almost anyone who's ever developed software can tell you, it's both easier and significantly cheaper to get it right the first time. That's why integrating Web application security testing into the software development lifecycle from the very start is essential for establishing good risk management. And while it's important to have a dedicated and knowledgeable security assessment teams perform a final review, it's equally important to integrate security into the early stages of application development to focus on security issues as they appear. By approaching the issues proactively, you can save time and reduce your development costs.

Your technology

There are a number of ways to implement proper security protocols in your Web-based applications. Although effective, manual penetration testing alone can be time consuming, labor intensive and costly. Supplementing manual testing procedures with an automated Web application security tool can help you gain a consistent, reliable and scalable analysis of your Web application security vulnerabilities—even across large, diverse IT environments. And such tools can help drive down testing costs by automating many manual tasks. Further, today's scanning tools are very sophisticated, capable of providing complete coverage of the latest application technologies including Web 2.0, which can greatly extend your manual testing capabilities.

Conclusion

As incidents of Web application breach continue to increase, so too does the threat to your business. If you rely on Web applications to support any part of your business, it's time to take control of your application security. We can help you examine your existing security practices and make recommendations that can help you protect your enterprise from the devastating consequences of a security breach.

CresTech has considerable experience of security testing of web applications and can increase the success of your project through early involvement in the planning process, and a rigorous implementation of these methods.