Web Application Security – Ensuring Critical Data Protection

**Issue**

Web applications¹ are a growing platform for providing information to mobile clients. Organizations, and their clients and customers, expect these mission-critical applications to be as robust, scalable and secure as traditional server-based applications. Because the assumption is that they are, many companies allow sensitive information to be processed in them.

Unfortunately, web applications are relatively easy to gain unauthorized access to, due to their often insecure configurations. This, along with the sensitive data they contain, has made them a frequent target for malicious hackers. Since 2013, the Open Web Application Security Project (OWASP) has seen a steady rise in SQL injection attacks, broken session management and cross-site scripting. These three types of attacks have been used in almost every high-profile web application breach recently. Typical malicious actions include session ID hijacking and not destroying cookies properly, allowing for simultaneous session logons. The risk posed by an insufficiently secure web application to your clients' and customers' information and your organization cannot be underestimated.

**Challenges and Opportunities**

Web application security is frequently compromised during migration from traditional in-house hosting to cloud-based platforms, as well as during application upgrades. Sound web application development and security involves a number of areas, including authentication, validation, session management, sensitive data exposure, cross-site scripting (XSS), SQL injection and function-level access control. Only when these areas are properly addressed can a web-based application be considered protected.

The following factors contribute to the challenges and security concerns around web applications:

- Lack of secure coding guidelines and practices during the development of the web application
- Absence of proper system development lifecycle (SDLC) processes, from development to quality assurance and production release
- Lack of formal testing and validation to confirm that security vulnerabilities are not present
- Improper evaluation, from a regulatory compliance standpoint, of what constitutes sensitive data within a web application

**Our Point of View**

The best way to address these challenges is proactively, by assigning an experienced team focused on assessing, testing and reporting on web application security, to ensure a secure network and application environment for the organization. The keys to successfully managing web application security include:

- Developing and implementing web security standards and policies that encompass all business applications and data
- Establishing a governance process for application development that can anticipate security flaws and allows for rapid escalation and resolution of issues
- Identifying gaps within existing IT development processes and developing measures to address them
- Establishing clear coding standards and guidelines and reviewing them periodically to identify opportunities for improvement
- Maintaining proper security testing procedures and performing routine vulnerability testing, including of scheduled upgrades, using leading industry tools and techniques
- Implementing proper session attack detection mechanisms
- Ensuring compliance of all web applications with the regulations that govern the data held within each application, based on the data’s classification

¹ An application program that is stored on a remote server and delivered over the Internet through a browser interface.
How We Help Companies Succeed
Protiviti’s IT Security and Privacy practice delivers a wide range of security architecture, transformation and management services to help organizations identify and address security and privacy exposures before they become problems. We advise and support our clients in all aspects of their IT transformation using proprietary methodologies and up-to-the-minute insight from our experts in the field.

Our cross-disciplined teams bring broad perspectives and deep technical skills, along with industry-leading tools and project management expertise. We have a demonstrated track record of helping companies establish security programs, deal with identity and access management, and handle industry-specific data security and privacy issues, including PCI and HIPAA. Our project and industry expertise combines with our commitment to your future-state vision to ensure your success and realization of expected value.

Example
Protiviti was engaged by a national insurance organization to conduct a web application assessment and evaluate the overall security posture, controls and potential risk exposures associated with the client’s marketplace. The web application had a user pool of 30 million and growing. Client emphasis was placed on evaluating configurations and controls that restrict unauthorized users from accessing sensitive user information, as well as on escalating access into other systems in the client’s IT environment.

Our security experts performed a thorough application security assessment by analyzing the web framework, crawling the site for possible points of attack, attacking parameters to manipulate application output, and manually confirming findings through testing. Following the assessment, we summarized our findings and presented strategic recommendations to our client.

As a result of our efforts, the client was made aware of a security flaw that allowed users to access other users’ information while logged in with their own credentials. This was a significant PII violation that would have continued to compromise customers' privacy and discredit the organization if left undiscovered. Protiviti diagnosed the vulnerability, and then provided detailed recommendations to remediate the issue. Our analysis aided the client in enhancing and enforcing existing configuration management and session management processes to create a more secure web application.

In addition, the recommendations and concluding metrics that we developed brought attention to the fact that the client was utilizing insecure coding practices and was not performing periodic testing of web applications within its software development lifecycle process. While the client’s perception of its application environment was that it was secure, our web application assessment revealed otherwise. Addressing the weaknesses we identified helped our client avoid the potential expense and loss of goodwill associated with exposure of sensitive personal information.

Contacts

**Tom Andreesen**  
+1.312.476.6318  
thomas.andreesen@protiviti.com

**Tom Stewart**  
+1.312.931.8901  
tom.stewart@protiviti.com

About Protiviti
Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.