**Unit 10 Secure Web development**

Web application vulnerabilities, including OWASP Top 10 threats SQL injection, XSS, and CSRF, account for more than 80% of all vulnerabilities.1 Based on this high rate of application vulnerabilities, organizations should invest significant resources in secure Web development. Unfortunately, many do not. According to a 2010 Ponemon report, 70% of organizations do not allocate sufficient resources to secure Web applications and 55% of respondents believe developers are too busy to address security issues.

While Web security may seem like an insurmountable challenge, organizations can follow application coding best practices, scan applications for vulnerabilities and deploy virtual patching solutions to minimize the window of exposure and the risk of a data breach.

Implement Secure Coding Best Practices and Vulnerability Scanning

Secure Web development is an iterative process that comprises application design, implementation, vulnerability testing, and monitoring. According to OWASP Secure Coding Principles, application design should incorporate confidentiality, integrity and availability, contain necessary controls to prevent unauthorized activity and enforce separation of duties. Once applications have been written, they should be rigorously tested for vulnerabilities using a combination of application scanning tools and code review.

Minimize the Window of Exposure with Virtual Patching

Fixing discovered vulnerabilities takes time—on average two to four months per vulnerability.2 Virtual patching can reduce the window of exposure and the disruption of emergency fix and test cycles. Organizations that use vulnerability assessment tools can import the scan results into a Web application security solution such as a Web Application Firewall (WAF). The WAF will create granular policies that block attempts to exploit known vulnerabilities. This integration instantly mitigates vulnerabilities, enabling organizations to fix applications on their own schedule.

Monitor Web Applications for Attacks

To effectively address Web application security, developers must understand how their applications are used. Application monitoring reveals the areas of the Web site that are targeted by hackers, illustrates attack trends, and uncovers exploit techniques in real time. Application developers can leverage this knowledge to identify and prioritize vulnerability fixes and to architect more resilient Web applications.

Accelerate Application Defect Analysis and Reporting

Application defects, such as broken links and server errors, can hinder online purchases--reducing revenues—or even damage company brand. Application flaws can also lead to detrimental leaks of sensitive data such as credit card numbers or financial records. To remediate application defects, developers must be able to access reports of broken links, URL response times, application errors, and sensitive data and code leakage. To further isolate errors, reports should pinpoint which SQL queries slowed Web page response times. Defect reports inspect Web and database traffic to reveal real, user-encountered errors.