ARTÍCULO

Best Practices for Web Developers in Security (Unified Version)

In today's fast-moving cybersecurity landscape, web developers play a critical role in protecting business applications and sensitive data. Reports such as Verizon's DBIR and studies from OWASP indicate that more than 50% of breaches originate from code vulnerabilities or insecure configurations, making security an essential part of the development lifecycle.

A key practice is adopting a **security-by-design mindset**. This means validating and sanitizing all user inputs to prevent common attacks like XSS or SQL Injection, as well as managing secrets and credentials through secure vaults instead of storing them in repositories or visible variables. Strengthening authentication with MFA and modern standards like OAuth2 or JWT adds an additional protection layer.

Proper **session management**, default **TLS 1.3 encryption**, and security headers such as *Content-Security-Policy* and *Strict-Transport-Security* also help significantly reduce the attack surface.

Continuous testing—through static analysis (SAST) and dynamic analysis (DAST)—detects weaknesses before deployment. Finally, real-time monitoring with tools like **NetGuard Pro** allows teams to identify unusual behavior and respond quickly to potential incidents.

By integrating these practices, web developers strengthen application security, protect their users, and contribute to the operational resilience of their organizations.