SANS
SECURITY
AWARENESS

The Open Web Application Security Project, or OWASP, is a nonprofit organization focused on improving software security. One of the major contributions to application security that the OWASP Foundation provides is the "OWASP Top 10", a globally recognized list of the ten most critical security concerns for web applications.

In the latest iteration of the OWASP Top 10, published in 2021, the foundation solicited organizations to provide the number of applications tested for a given year and the number of applications with at least one instance of a Common Weakness Enumeration, or CWE, found in that testing.

This updated list is comprised of: Broken Access Control, Cryptographic Failures, Injection, Insecure Design, Security Misconfiguration and XML External Entities, Vulnerable and Outdated Components, Identification and Authentication Failures, Software and Data Integrity Failures, Security Logging and Monitoring Failures, and Server-Side Request Forgery.

Based on the data provided, there have been significant changes from previous years, including three new categories, four categories with naming and scoping changes, and some category consolidation. For example, for the first time in a decade, injection is no longer the top concern, as broken access control and cryptographic failures have a higher percentage of applications vulnerable to them based on the population tested and reported on.

Being aware of these application security risks will help you stay vigilant when developing and reviewing applications. In the coming modules, we'll discuss what each category is, why it is relevant, how it works, and what we can do to help safeguard against attacks focused on exploiting these vulnerabilities.