OWASP Top 10 Application Security Overview

2025-10-24

OWASP Top 10 Application Security Overview

Prepared for Applied Information Assurance Projects
Date: October 2025

---

1. Executive Summary

This report provides an applied overview of the **OWASP Top 10 (2021 Edition)**—a globally recognized awareness document for web application security.
It identifies the most critical risks impacting software assurance and maps them to the **NIST Cybersecurity Framework (CSF) 2.0** to demonstrate how developers and organizations can align vulnerability management with governance and risk-based controls.

> **Objective:** To bridge technical security testing with information assurance practices, emphasizing prevention, detection, and response maturity.

---

2. Overview of the OWASP Top 10 (2021)

The OWASP Top 10 represents data-driven insights into the most prevalent and severe web vulnerabilities.
It serves as a living benchmark for secure development and auditing activities.

ID	Risk Category	Description
A01: Broken Access Control	Authorization enforcement failures enabling unauthorized actions or data access.	
A02: Cryptographic Failures	Misuse or absence of encryption, leading to exposure of sensitive data.	
A03: Injection	Unsanitized input passed to interpreters (e.g., SQL, OS commands).	
A04: Insecure Design	Fundamental flaws in architecture or threat modeling.	
A05: Security Misconfiguration	Default accounts, open S3 buckets, or verbose error messages.	
A06: Vulnerable & Outdated Components	Use of obsolete or unpatched software dependencies.	
A07: Identification & Authentication Failures	Weak credentials or poor session management.	
A08: Software & Data Integrity Failures	Unverified code updates or compromised CI/CD pipelines.	
A09: Security Logging & Monitoring Failures	Insufficient detection and response visibility.	
A10: Server-Side Request Forgery (SSRF)	Improperly validated external resource requests.	

3. Mapping OWASP Risks to NIST CSF Functions

This alignment highlights how OWASP technical vulnerabilities correlate with the **Identify, Protect, Detect, Respond, and Recover** functions of the NIST Cybersecurity Framework.

NIST CSF Function	Example OWASP Categories	Focus Area
Identify (ID)	A06	Inventory and management of assets and components.
Protect (PR)	A02, A04, A07	Secure system design, cryptography, and access control.
Detect (DE)	A09	Log monitoring and anomaly detection.
Respond (RS)	A03, A08	Incident response and mitigation of exploited components.
Recover (RC)	A01, A05	Configuration restoration and process resilience.

> **Insight:** Integrating OWASP principles into a CSF-based security program supports both compliance alignment and real-world operational defense.

---

4. Risk Reduction Strategies

Risk Type	Mitigation Strategy
Injection (A03)	Validate all inputs using whitelisting and parameterized queries.
Security Misconfiguration (A05)	Implement configuration baselines and hardening checklists.
Outdated Components (A06)	Track dependencies and enforce patch management through CI/CD pipelines.
Authentication Failures (A07)	Adopt MFA and session timeout enforcement.
Logging Failures (A09)	Centralize logs and enable real-time alerting.

---

5. Key Takeaways

- The OWASP Top 10 should be used as a **baseline** for security testing and code review.
- Each risk maps directly to **CSF categories**, allowing for enterprise-level risk reporting.
- Continuous training and vulnerability assessment tools (e.g., OWASP ZAP, Burp Suite) strengthen control assurance.
- Emphasis on **secure design and monitoring** closes the gap between technical defense and organizational assurance.

---

6. References

1. OWASP Foundation. *OWASP Top 10 – 2021.* https://owasp.org/Top10/
2. National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF) 2.0 Draft.* https://www.nist.gov/cyberframework
3. OWASP Application Security Verification Standard (ASVS) v4.0.
4. ISO/IEC 27001:2022 – Information Security Management Systems.

Appendix (Optional: For PDF Export)

For readability when exporting to PDF, add your organization or portfolio branding at the top and adjust margins to fit two pages using your PDF generator's "narrow" or "compact" page settings.

 Download PDF Report