# Web Application Security

OWASP Top 10

By

Ayush Bhandari

# OWASP Top 10

1. Broken Access Control – Enforce RBAC and validate permissions.
2. Cryptographic Failures – Use HTTPS/TLS, encrypt sensitive data.
3. Injection – Parameterized queries and input validation.
4. Insecure Design – Apply secure SDLC and threat modeling.
5. Security Misconfiguration – Disable defaults and patch systems.
6. Vulnerable Components – Update dependencies regularly.
7. Auth Failures – Implement MFA and strong password policies.
8. Integrity Failures – Verify code signing and package authenticity.
9. Logging Failures – Centralize logs and monitor activities.
10. SSRF – Validate outbound requests and restrict access.

# Web Security Principles

- **Confidentiality** – Keep sensitive info private.
- **Integrity** – Prevent unauthorized modifications.
- **Availability** – Ensure reliable system access.
- **Authentication** – Verify user identity.
- **Authorization** – Control user permissions.
- **Non-repudiation** – Ensure accountability.

# Web Security Best Practices

- Validate and sanitize all user inputs.
- Use HTTPS everywhere.
- Enforce strong authentication (MFA, OAuth2, JWT).
- Apply Least Privilege Principle.
- Keep dependencies updated.
- Use secure error handling.
- Maintain detailed logs.
- Perform regular pentests and code reviews.
- Backup data and prepare incident response plans.

# Visual Overview