MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

SECURITY DEEP-DIVE · 2026 EDITION

OWASP Top 10:2025
Web Vulnerabilities Deep-Dive

Root causes, testing questions, secure design controls, and remediation checklists for modern web applications.

10	40+	2025
Risk categories	Review questions	Current edition

mnatech.in @mna_tech_academy +91 9216110094

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

How to use this guide

Use each category as an awareness and review framework. Start with architecture and data flows, validate controls through approved testing, and turn findings into engineering actions.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

Inside this resource

01 **The 2025 Risk Landscape**
Understand what changed and how to use the Top 10 responsibly.

02 **Access, Configuration & Supply Chain**
A01–A03: prevent unauthorized actions, unsafe defaults, and compromised dependencies.

03 **Crypto, Injection & Insecure Design**
A04–A06: protect data, separate code from data, and model abuse before implementation.

04 **Authentication, Integrity & Logging**
A07–A09: make identity resilient, updates trustworthy, and attacks observable.

05 **Exceptional Conditions & Test Plan**
A10: fail predictably, preserve security controls, and recover safely.

06 **Remediation & References**
Convert findings into durable engineering improvements.

The 2025 Risk Landscape

Understand what changed and how to use the Top 10 responsibly.

A01 Broken Access Control

Authorization failures remain the leading category; SSRF is included here in 2025.

A02 Security Misconfiguration

Review architecture, implementation, telemetry, and recovery controls together.

A03 Software Supply Chain Failures

Review architecture, implementation, telemetry, and recovery controls together.

A04 Cryptographic Failures

Review architecture, implementation, telemetry, and recovery controls together.

A05 Injection

Review architecture, implementation, telemetry, and recovery controls together.

A06 Insecure Design

Review architecture, implementation, telemetry, and recovery controls together.

A07 Authentication Failures

Review architecture, implementation, telemetry, and recovery controls together.

A08 Software or Data Integrity Failures

Review architecture, implementation, telemetry, and recovery controls together.

A09 Security Logging & Alerting Failures

Review architecture, implementation, telemetry, and recovery controls together.

A10 Mishandling of Exceptional Conditions

Review architecture, implementation, telemetry, and recovery controls together.

Key change: The 2025 edition adds Software Supply Chain Failures and Mishandling of Exceptional Conditions, and focuses more strongly on root causes.

Access, Configuration & Supply Chain

A01–A03: prevent unauthorized actions, unsafe defaults, and compromised dependencies.

Object authorization
Check ownership and permission on every server-side object request.

Function authorization
Enforce role and privilege rules server-side; deny by default.

Configuration baseline
Remove debug features, sample accounts, directory listing, and unnecessary services.

Headers and cloud controls
Review security headers, storage exposure, CORS, and infrastructure-as-code.

Dependency integrity
Inventory dependencies, lock versions, verify provenance, and protect build credentials.

Build pipeline
Require reviews, isolated runners, signed artifacts, and controlled release promotion.

Crypto, Injection & Insecure Design

A04–A06: protect data, separate code from data, and model abuse before implementation.

Area	Review	Preferred control
Data in transit	TLS configuration and certificate lifecycle	Modern TLS, automated renewal, strict transport
Passwords	Storage and reset workflow	Adaptive password hashing, single-use reset tokens
Queries	Untrusted data entering interpreters	Parameterized queries and safe APIs
Commands/templates	Dynamic construction	Allow-lists and context-aware encoding
Business logic	Abuse cases and unsafe state transitions	Threat modeling, limits, server-side invariants
Sensitive workflows	High-impact action design	Re-authentication, approval, audit trail

Authentication, Integrity & Logging

A07–A09: make identity resilient, updates trustworthy, and attacks observable.

Session lifecycle
Rotate identifiers after login, expire safely, revoke on risk, and protect cookies.

MFA and recovery
Protect enrollment and recovery as strongly as sign-in.

Deserialization and updates
Verify signatures and avoid unsafe object reconstruction.

Audit events
Record authentication, authorization, administrative, and sensitive-data events.

Alert quality
Create actionable alerts with owner, severity, context, and tested response.

Privacy
Never log passwords, full tokens, or unnecessary personal data.

Exceptional Conditions & Test Plan

A10: fail predictably, preserve security controls, and recover safely.

Error handling

Use centralized exception handling and safe user messages while retaining diagnostic context securely.

Resource limits

Bound input size, recursion, retries, queues, decompression, and expensive operations.

Fail-safe defaults

Timeouts and dependency failures must not bypass authentication, validation, or approval.

Recovery tests

Exercise unavailable databases, partial writes, malformed data, and downstream timeouts.

Release gate

- Threat model reviewed for material changes
- Automated security tests passed
- Dependencies and secrets scanned
- Authorization tests cover roles and objects
- Logging and alert path verified
- Rollback and incident owner confirmed

Remediation & References

Convert findings into durable engineering improvements.

Finding field	What good looks like
Evidence	Reproducible observation without unnecessary sensitive data
Impact	Business outcome and affected assets
Root cause	Design or implementation condition, not only payload
Fix	Specific control with owner and deadline
Verification	Negative and positive tests plus regression coverage

Official references

- OWASP Top 10:2025 — https://top10.owasp.org/2025/
- OWASP ASVS — https://owasp.org/www-project-application-security-verification-standard/
- OWASP Cheat Sheet Series — https://cheatsheetseries.owasp.org/



Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.