SSDLC Training — How-To Guide

How to Write Security Requirements Using OWASP ASVS

Deriving testable security requirements from ASVS

Step 1: Select Your ASVS Level

OWASP ASVS defines three verification levels based on risk:

- Level 1: Opportunistic — minimum for all applications
- Level 2: Standard — for applications handling sensitive data
- Level 3: Advanced — for critical applications (financial, healthcare, infrastructure)

Most enterprise applications should target Level 2. Choose based on your data classification and regulatory requirements.

Step 2: Map ASVS Sections to Features

Review each ASVS section against your application's features. Focus on sections relevant to your technology stack and data types.

- V2: Authentication — login, MFA, password policies
- V3: Session Management — token handling, timeout, invalidation
- V4: Access Control — RBAC/ABAC, object-level authorization
- V5: Validation — input sanitization, output encoding
- V8: Data Protection — encryption, key management, PII handling
- V13: API Security — rate limiting, schema validation, auth

Step 3: Write Testable Requirements

Use the SHALL/ACTION/CONSTRAINT pattern for each requirement:

- Example: 'The system SHALL enforce MFA for all administrative accounts using TOTP or WebAuthn'
- Example: 'The API SHALL validate all request bodies against the published JSON schema and reject non-conforming requests with HTTP 400'
- Example: 'The system SHALL encrypt all PII at rest using AES-256-GCM with keys managed in AWS KMS'

Each requirement must be testable — if you can't write a test for it, rewrite it.