anchor@anchor-cyber:~$ man asvs-5.0

ANCHOR CYBER SECURITY LLC

OWASP ASVS 5.0 — Field Reference

17 chapters, ~350 requirements across three Levels. Level 2 is the right default for most production web and API applications — this is the chapter index, not a substitute for running the actual checklist.

VERSION NOTE

ASVS 5.0.0 (May 2025) replaced 4.0.3 and restructured 14 chapters into 17 — if you see an older reference to "V1 Architecture" or "V2 Authentication," that's 4.0.3's numbering, not this one. Re-check anything written against the old structure before treating it as current.

The 17 Chapters

V1	Encoding and Sanitization
V2	Validation and Business Logic
V3	Web Frontend Security
V4	API and Web Service
V5	File Handling
V6	Authentication
V7	Session Management
V8	Authorization
V9	Self-Contained Tokens
V10	OAuth and OIDC
V11	Cryptography
V12	Secure Communication
V13	Configuration
V14	Data Protection
V15	Secure Coding and Architecture
V16	Security Logging and Error Handling
V17	WebRTC

$ asvs --levels

Three Levels, Not a Ladder Everyone Climbs

Level 1 is opportunistic-attacker baseline — the minimum for any app handling anything sensitive. **Level 2** is for apps handling significant business, financial, health, or otherwise sensitive data against a skilled, motivated attacker — this is where most web and API applications handling sensitive data should default to. Level 3 is for the highest-value targets (critical infrastructure, high-value financial systems) — don't scope a client there by default just because "more secure" sounds safer; it's a real cost/effort step up, not a strictly-better setting.

$ asvs --triage

Picking Chapters by Architecture Shape

Let the architecture tell you where to start, not the chapter numbering. A product with a local client agent, a network-inspection component, and a cloud-hosted commercial portal should check, in order: **V6** (auth on the portal), **V8** (authorization — one customer's data must not leak across tenants), **V12** (secure communication — anything inspecting or terminating traffic by design makes this chapter unusually load-bearing), **V14** (data protection — policy/evidence data at rest), **V16** (logging — audit evidence integrity matters most for exactly this kind of product).

src: OWASP ASVS 5.0.0 (May 2025) exit 0