| **#** | **Control Area** | **Status** | **What’s in place** | **Gaps / Next Actions (priority)** |
| --- | --- | --- | --- | --- |
| 1 | Access control (route/object/property level)\* | **Partial** | Role/menu-based checks; controller-level auth | Add **object- and property-level** checks in services/repos; enforce tenant/owner filters on every query; add unit/integration tests for BOLA/BOPLA. |
| 2 | Tokens & sessions | **Yes** | JWT with secure cookies; refresh flow | rotate refresh tokens with **reuse detection**, validate iss/aud/nbf/exp/jti, and enable **key rotation** (kid/JWKS). |
| 3 | Input/output hardening\*\* | **Partial** | Input data validation | Add DTO **allow-lists** (avoid mass assignment), request **size/depth** limits, strict content types, upload **magic-number** checks & AV scan, consistent error handling w/o PII. |
| 4 | Rate limiting & abuse controls\* | **No** (IP on FE, user on BE) | -- | Add server-side **.NET rate limiter** per IP/user/endpoint (fixed/sliding window), plus **global** and **login** burst limits; protect expensive endpoints. FE IP throttling, per-user checks in BE |
| 5 | Transport & security headers | **No** | — | Enforce **TLS 1.2+**, **HSTS** in prod, set X-Content-Type-Options, Referrer-Policy, X-Frame-Options/frame-ancestors, and CSP if any HTML is served. |
| 6 | CORS | **Yes** | Configured | -- |
| 7 | Secrets & keys | **Yes** | Centralized secrets | Ensure **automated rotation**, per-env separation, and access logging; if using parameter encryption, use **AEAD** and versioned keys—not just “obfuscation”. |
| 8 | Data layer protections\* | **Yes (configured), not used in dev** | RLS/column encryption/TDE configured | Enable for **prod** paths; verify ORM parameterization, **immutable audit** trail for admin & auth events. |
| 9 | Observability & logs (privacy)\* | **Yes** (file & DB, no cloud) | Central logs on disk/DB | Mask PII/tokens; define **retention & purge**; add integrity checks; consider on-prem stack (e.g., **ELK/Loki+Promtail**) for correlation without cloud. |
| 10 | GDPR program controls | **Partial** | Data minimization & purpose limitation, subject right capabilities, | Confirm DPIA where needed; ROPA, DSR endpoints (access/export/delete), breach process; align **retention** across services. |
| 11 | Assurance & testing | **No** | — | Adopt **OWASP ASVS L2** as DoD; add **SAST/DAST** and **dependency/SBOM** scans in CI; pen-test high-risk flows; regular key/cert rotation drills. |