

SSL/TLS Configuration Report SSL/TLS Configuration Report Target: localhost:8082 | Generated: 2025-09-09\_04-59-20 Findings: 3 (High risk: 1) Vulnerabilities / Findings

| Issue                        | Status     | Risk | Evidence   | Mitigation   |
|------------------------------|------------|------|--|--|
| Certificate Retrieval Failed | Error      | Low  | [SSL: WRONG_VERSION_NUMBER] wrong version number (_ssl.c:1007) | Ensure port 443 reachable and proper TLS handshake possible.                     |
| Missing TLS 1.2 Support      | Vulnerable | High | TLS 1.2 handshake failed                                       | Ensure TLS 1.2 is enabled (modern clients require it).                           |
| No TLS 1.3 Support           | Info       | Low  | Negotiation did not use TLS 1.3                                | (Info) Enable TLS 1.3 for better security & performance if platform supports it. |

Protocol Supported TLSv1.0 ■ TLSv1.1 ■ TLSv1.2 ■ TLSv1.3 ■ Certificate Info Subject Issuer Valid From Valid To Days Until Expiry Wildcard No Self-Signed No Host Match No