# 3.1 STRIDE Threat Analysis Matrix

|  |  |  |  |
| --- | --- | --- | --- |
| Threat Category | Risk Level | Mitigation | Implementation |
| Spoofing | Medium | Password Hashing | Werkzeug check\_password\_hash |
| Tampering | Low | AES-GCM Auth | Authentication tags |
| Repudiation | Low | Cryptographic Binding | Master Key derivation |
| Information Disclosure | Low | Client-side Encryption | Web Crypto API |
| Denial of Service | High | Operational Controls | Backup/Redundancy |
| Elevation of Privilege | Low | Key Separation | Hierarchical keys |

# 3.2 Attack Vector Analysis

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attack Vector | Probability | Impact | Risk Score | Mitigation |
| Server Compromise | Medium | Low | Medium | Zero-knowledge design |
| Password Brute Force | High | High | High | PBKDF2 + High iterations |
| Man-in-the-Middle | Low | Medium | Low | HTTPS/TLS |
| Client Malware | Medium | High | High | Out of scope |
| Code Injection | Low | High | Medium | CSP headers |

# 3.3 Cryptographic Primitive Comparison

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Algorithm | Key Size | Performance | Security Level | Browser Support |
| PBKDF2 | N/A | Fast | Good | Native |
| Argon2 | N/A | Medium | Excellent | Library Required |
| AES-GCM | 256-bit | Very Fast | Excellent | Native |
| ChaCha20-Poly1305 | 256-bit | Fast | Excellent | Limited |