System Architecture - Authentication System

🔒 Trust Boundary: Internet

Web Browser

- User Agent (JavaScript, Cookies)
- Secure, HttpOnly, SameSite cookies (app_auth.py:24)
- Client-side PKCE (code_verifier)

External OAuth Provider

- Google, GitHub, etc.
- Future integration

HTTPS Request

🔐 TLS/HTTPS Layer (Port 5001)

HTTPS termination, HSTS enforcement (utils/security_headers.py:36)

Decrypted

🌐 Flask Application (app_auth.py:20)

Middleware Stack

- 🛡️ CSRF Protection (app_auth.py:29)
- 🔒 Security Headers (app_auth.py:53)
- ⏱️ Rate Limiter (5 req/min)

Route Handler

Route Blueprints:

auth_bp (routes/auth_routes.py:12)

- /register
- /login (line 60)
- /logout
- /change-password

oauth_bp (routes/oauth_routes.py:22)

- /oauth/authorize (line 35)
- /oauth/token (line 133)
- /oauth/userinfo (line 214)
- /oauth/revoke (line 242)

twofa_bp (routes/twofa_routes.py:12)

- /setup-2fa (line 21)
- /verify-2fa (line 82)
- /backup-codes
- /disable-2fa (line 171)

AuthService

OAuth2Service

TOTPService

Service Layer (Singletons):

AuthService

(services/auth_service.py:13)

Argon2id: t=2, m=19456, p=1

Timing-safe authentication

OAuth2Service

(services/oauth2_service.py:14)

PKCE (S256) line 98

Token Rotation line 290

TOTPService

(services/totp_service.py:16)

pyotp, QR Code line 36

Replay Prevention line 130

RateLimiter

(services/rate_limiter.py:11)

Database-backed

BEGIN IMMEDIATE line 96

SecurityService

(services/security_service.py:9)

3 failures → 15min lockout

CAPTCHA after 3 failures

EncryptionService

(utils/encryption.py:16)

Fernet (AES-128 CBC)

PBKDF2: 100k iterations

Database Queries

💾 SQLite Database (database_auth.py:9)

- users (line 22, 16 columns, totp_secret encrypted)
- login_attempts (line 87, 7 columns, 2 indexes)
- account_lockouts (line 113, 7 columns)
- rate_limits (line 133, 6 columns)
- security_events (line 153, 9 columns)
- oauth2_clients (line 180, 13 columns)
- oauth2_authorization_codes (line 209)
- oauth2_tokens (line 235, family tracking)
- sessions (line 274, fingerprinting)

reCAPTCHA

HaveIBeenPwned

External Services:

🤖 Google reCAPTCHA v2 (utils/recaptcha.py:10)

Triggered after 3 login failures (routes/auth_routes.py:78)

Site key in template context

🔍 HaveIBeenPwned API (utils/validators.py:82)

k-anonymity password breach checking

SHA-1 prefix query (5 hex chars) - line 88

Legend: -- Trust Boundary | 🔐 TLS/HTTPS | 🌐 Middleware | 🛣️ Routes | ⚙️ Services | 💾 Database | 🌍 External API

Trust Boundaries:

1. Internet to Application: HTTPS, HSTS, CSP, CSRF tokens, Rate limiting
2. Application to Database: Parameterized queries, Transaction isolation (BEGIN IMMEDIATE)
3. OAuth2 Client to Server: PKCE, Client auth, Redirect URI exact match