Secure API Design and Implementation

Kamran Khalid
Senior Backend Developer

Why API Security Matters

- APIs = Front Door to modern apps
- FinTech = Money, Identity, Trust
- Weak security → breaches, GDPR fines, reputation loss

Common API Attacks

- BOLA: change /user/123 → /user/124
- Broken Authentication: weak JWTs
- Token Theft & Replay
- Business Logic Abuse

AuthN vs AuthZ

- Authentication (AuthN): Who are you?
- Authorization (AuthZ): What can you do?
- Example: Login vs Role-based Access

OAuth 2.0 & OIDC

- OAuth 2.0: Delegated access
- OIDC: Authentication layer
- Flows: Authorization Code, Client Credentials

JWT — Pros & Pitfalls

- Pros: Stateless, scalable, holds claims
- Pitfalls: Hard to revoke
- Best: Verify signature & expiry

Token Storage & Rotation

- Web → HttpOnly cookies
- Mobile → Secure storage
- Rotation: Use refresh tokens & invalidate old ones

Transport & Network

- TLS 1.2/1.3 only
- HSTS, mTLS
- API Gateway & WAF for rate limiting & filtering

Request-Level Security

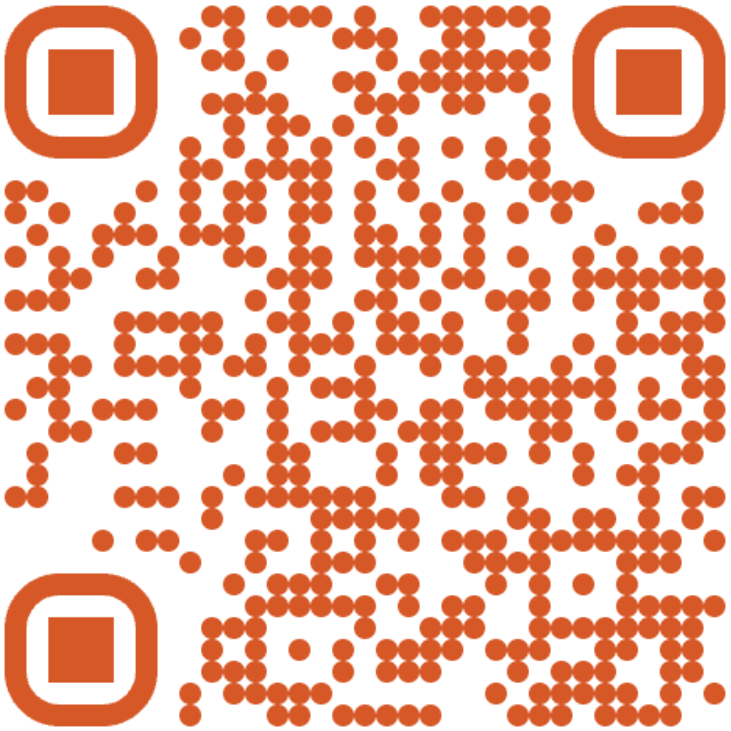
- Validate input & Content-Type
- Parameterized Queries
- Sanitize responses to avoid leaks

Rate Limiting & Throttling

- Prevents brute-force & abuse
- Use token bucket or sliding window
- Example: 5 logins / 15 min per IP

Secrets & CI/CD Security

- Never hardcode secrets
- Use AWS Secrets Manager or Vault




Kamran Khalid
Innovative Fullstack Developer with Proficiency in Backend Development and Agile Methodol...

Thank You!