

- ✓ API Design Roadmap
- ✓ Backend Roadmap
- ✓ System Design Roadmap
- ✓ Backend Performance Roadmap

Find the detailed version of this roadmap along with other similar roadmaps

roadmap.sh

API Security

Authentication

- ☐ Avoid 'Basic Authentication', use standard (e.g. JWT)
- ☐ Do not reinvent the wheel in authentication mechanisms
- ☐ Use 'Max Retry' and jail features in login
- ☐ Use encryption on all sensitive data

Access Control

- ☐ Limit requests (throttling) to avoid DDoS / brute force
- ☐ Use HTTPS on server side and secure ciphers
- ☐ Use HSTS header with SSL to avoid SSL strip attacks
- ☐ Turn off directory listings
- ☐ Private APIs should only be accessible from safe-listed IPs

Input

- ☐ Limit requests (throttling) to avoid DDoS / brute force
- ☐ Use HTTPS on server side and secure ciphers
- ☐ Use HSTS header with SSL to avoid SSL strip attacks
- ☐ Turn off directory listings
- ☐ Private APIs should only be accessible from safe-listed IPs

Output

- ☐ Send X-Content-Type-Options: nosniff header
- ☐ Send X-Frame-Options: deny header
- ☐ Send Content-Security-Policy: default-src 'none' header
- ☐ Remove fingerprinting headers (e.g. x-powered-by)
- ☐ Force content-type for your response
- ☐ Avoid returning sensitive data (credentials, tokens, etc)
- ☐ Return proper response codes as per the operation

Monitoring

- ☐ Use centralized logins for all services and components
- ☐ Use agents to monitor all requests, responses, and errors
- ☐ Use alerts for SMS, Slack, Email, Kibana, CloudWatch, etc
- ☐ Ensure you aren't logging any sensitive data
- ☐ Use an IDS and/or IPS system to monitor everything

JSON Web Tokens (JWT)

- ☐ Use good JWT Secret to make brute-force attacks difficult
- ☐ Do not extract the algorithm from the header, use backend
- ☐ Make token expiration (TTL, RTTL) as short as possible
- ☐ Avoid storing sensitive data in JWT payload
- ☐ Keep the payload small to reduce the size of the JWT

OAuth

- ☐ Always validate redirect_uri on server-side
- ☐ Avoid response_type=token and try to exchange for code
- ☐ Use state parameter to prevent CSRF attacks
- ☐ Have default scope, and validate scope for each application

Processing

- ☐ Check if all endpoints are protected behind authentication to avoid broken authentication process
- ☐ Avoid user's personal ID in resource URLs (e.g., users/242/orders)
- ☐ Prefer using UUID over auto-increment IDs
- ☐ Disable entity parsing if parsing XML to avoid XXE attacks
- ☐ Disable entity expansion if using XML, YAML, or similar
- ☐ Use a CDN for file uploads
- ☐ Avoid HTTP blocking when handling large amounts of data
- ☐ Make sure debug mode is off in production
- ☐ Use non-executable stacks when available

CI / CD

- ☐ Audit your design and implementation with unit/integration tests for known vulnerabilities
- ☐ Use a code review process and disregard self-approvals
- ☐ Continuously run security analysis on your code
- ☐ Design a rollback solution for deployments



AI Tutor

Have a question? Type here



Continue Learning with following relevant tracks

Backend Roadmap

DevOps Roadmap