Related Roadmaps

- Backend Roadmap
- DevOps Roadmap

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.

JWT (JSON Web Token)

- [ ] 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 token

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 to be only accessible from safe listed IPs

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

Input

- [ ] User proper HTTP methods for the operation
- [ ] Validate `content-type` on request header
- [ ] Validate user input to avoid common vulnerabilities
- [ ] Use standard Authorization header for sensitive data
- [ ] Use only server-side encryption
- [ ] Use an API Gateway for caching, Rate Limit policies etc

Processing

- [ ] Check if all the endpoints are protected behind authentication to avoid broken authentication process
- [ ] Avoid user's personal ID in the resource URLs e.g. users/242/orders
- [ ] Prefer using UUID over auto-increment IDs
- [ ] Disable entity parsing if you are parsing XML to avoid XXE attacks
- [ ] Disable entity expansion if using XML, YML or any other language
- [ ] Use CDN for file uploads
- [ ] Avoid HTTP blocking if you are using huge amount of data
- [ ] Make sure to turn the debug mode off in production
- [ ] Use non-executable stacks when available.

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 (i.e. x-powered-by etc)
- [ ] Force `content-type` for your response.
- [ ] Avoid returning sensitive data (credentials, sec. tokens etc)
- [ ] Return proper response codes as per the operation

CI & CD

- [ ] Audit your design and implementation with unit/integration tests.
- [ ] Use a code review process and disregard self-approval.
- [ ] Continuously run security analysis on your code.
- [ ] Check your dependencies for known vulnerabilities.
- [ ] Design a rollback solution for deployments.

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 that you aren't logging any sensitive data.
- [ ] Use an IDS and/or IPS system to monitor everything.

More Resources

Recommended Resources