API Audit checklist

[www.apiopscycles.com v.](http://www.apiopscycles.com/) 3.0 10.12.2018 CC-BY-SA 4.0

**Criteria OWASP**

**criteria**

**Implemented, yes?**

**API Management**

API is published via API management

API is visible in a Developer portal

API can only be accessed via API management gateway

Rate limits are enforced when requesting API

Specification is maintained automatically when changes are done to API

Specification for endpoints is validated on every change against standard specification

Specification contains schema for the requests and responses

Request and response schema and examples are validated for format and examples pass the schema validation

**URIs**

API uses HTTPS (or in special cases other stateless protocol with encryption)

The API published under the organization’s official domain

Visible domain is shared with other APIs (i.e the domain the API

consumers see?)

Endpoints are max 2-resources deep (Example

/projects/123/tasks/345)

Other naming styles in style guide have been applied

API has versioning

Versioning strategy is best for the selected API management platform and for the primary API consumers? Major version is in URI (only if API management platform doesn't support versioning based on client subscription)

API uses stateless processing (no sessions, OpenID connect tokens are ok)

There is no special processing (asynchronous events)

**HTTP-methods**

GET -requests don't have request bodies POST is used for creating and updating data? POST is used only in standard ways.

PUT is used to create or replace entire resource? DELETE is used only to remove a resource? **HTTP status codes**

404 is used for wrong URL

400 -responses have additional information of the specific error

(for example missing required attribute)

401 -response is used when API consumer is using wrong credentials

403 using endpoint which is valid but not accessible by the requesting API consumer or trying to use operation they are not allowed to do

true true

500 -response when there is an internal processing problem which API consumer can not fix by changing the request

500 -responses have application specific error code but not a very clear plain message about exact error (stack trace or error text) which could expose internal implementation to API consumer

GET: 200 OK and items -array as empty array

GET: 204 empty response, nothing in the body

POST: 200 OK for updates or submits without creating new resources

201 -response is combined with the identifier of the created resource

DELETE: 204 OK when removing resource was successful

**Localization**

Date- and time formats in UTC with time zone (ISO standard) Language and country codes used with ISO -standard codes? Other standard codes applied?

Geocoordinates in ISO standard if used?

Payload localization supported or localized values accessible with

API?

Error message localization supported?

**Additional security**

All endpoints are protected by at least a client specific API key even if they are publicly available (anti-farming)?

OpenID connect and JWT supported (session based authentication)?

Protect against CFRS? (allow API management developer portal as origin to allow developers to try out the API via the portal user interface)

true

true true true

Inputs are validated? true

Inputs are validated automatically by the coding framework used? true

Outputs are escaped? true

Outputs are escaped automatically by the coding framework used?

Need for encrypting data has been evaluated before implementation? (country-specific privacy and other legal requirements and business confidential requirements) Encryption of data in transit and data in storage has been implemented according to the evaluated need?

Need to detect message integrity has been evaluated before implementation (typically using signed and encrypted JWT - tokens as authentication and integrity ensured)?

Message integrity has been implemented according to the evaluated need?

true true

true true

true

UUID used to identify object instead of internal ID? true

Secured direct object references i.e. no sensitive information like bank account numbers, social security numbers, person names etc. in URL as resource names or query parameters? Specification contains examples in the standard format of the requests and responses and API documentation is generated automatically based on the specification, schema and examples

true

POST, PUT: 201 Created for creating new resource true

400 bad requests from the client, for example a required query parameter was missing

Whitelisting: POST, PUT and DELETE are only available for resources which API consumer can manipulate?

GET requests with longest endpoint-hierarchy and multiple query parameters with long values don't exceed 2000 of URI length? (Some older clients and browsers may have this type of limit, although it is not official limit and newer clients can handle it well)