

AUDIT

Verifizieren der OAS
Spezifikation nach
Sicherheitskriterien

Modul 3

Themen

- Welcher Teile der Open API Spec sind Sicherheitsrelevant ?
- Was kann ich als API Entwickler sie sicherer machen.
- Wie überprüfe ich meine Anpassungen?

```
"securityDefinitions": {  
  "access-token": {  
    "type": "apiKey",  
    "in": "header",  
    "name": "x-access-token"  
  }  
}
```

/api/admin/user/search?

Input Parameter ?

..

SETUP

- Laden des Plugins
- Token von der 42c Plattform holen
- Forken von <https://github.com/apiaxl/secure-sdlc-api-developer>

Übung

- Importieren einer Open API Spec Datei in die IDE
- Ist sie sicher ??
- Was sollte angepasst werden ?
- Ein AUDIT fahren.
- Was wurde angemahnt ?
- Wie muss ich es ändern ?

Modul 3 - AUDIT: Was haben wir gesehen ?

- Konsequentes API Design-First hilft früh in Entwicklungszyklus
- Entwickler fokussierte AUDIT Tools helfen besser zu werden
- Automatisierte Audits sind ein guter Bestandteil des SDLC