# MindAPI

## Reconnaissance

### Identify architecture

#### Architecture

- REST APIs
  - RESTful
  - OData
- GraphQL
- SOAP
  - Transfered data in XML format
- XML-RPC
  - Transfered data in simpler XML format `<users><user><firstName>David</firstName>`
- JSON-RPC
  - Transfered data similar to XML-RPC but in JSON format `{"users":[{"firstName":"David"}]`
- gRPC-Protobuf
  - Identify `grpc`
    - Accept request header
    - Content-Type request header
    - Access-control-expose-headers in the response header

#### Documentation

- https://smartbear.com/blog/soap-vs-rest-whats-the-difference/
- https://www.odata.org/documentation/
- https://www.howtographql.com/basics/1-graphql-is-the-better-rest/
- https://www.smashingmagazine.com/2016/09/understanding-rest-and-rpc-for-http-apis/
- https://www.soapui.org/docs/rest-testing/working-with-rest-services/
- https://cloud.google.com/blog/products/api-management/understanding-grpc-openapi-and-rest-and-when-to-use-them

### Check for documentation

#### Automatic

##### Swagger

- https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/swagger.txt

##### OData

- `/$metadata`

#### WADL

- `/application.wadl`
- `/application.wadl?detail=true`
- `/api/application.wadl`

#### WSDL

- ?wsdl or ?singleWsdl
  - wsdl-wizard
  - SoapUI
  - Wsdler

#### GraphQL

- https://graphql.org/learn/introspection/
- https://github.com/prisma-labs/get-graphql-schema

### Manual

- site:target.tld intitle:api | developer

## Search for APIs

### Traffic Analysis

- REST
  - Burp CE
  - ZAP
  - mitmproxy
- OData
  - Burp CE
  - ZAP
  - mitmproxy
- GraphQL
  - Burp CE
  - ZAP
- SOAP
  - Burp CE
- XML-RPC
  - Burp CE
  - mitmproxy
- JSON-RPC
  - Burp CE
  - mitmproxy
- gRPC-Protobuf
  - mitmproxy
  - Wireshark

        - `echo HEX_STREAM | xxd -r -p | protoc --decode_raw`
        - protoc

### Wayback Machine

- https://archive.org/web/
- waybackurls
- gau

### Path Manipulation

- /api/v1
- /api/v2
- /api/v3

### Dorks

#### Google

- `site:target.tld inurl:api`
- `intitle:"index of" "api.yaml" site:target.tld`
- WADL
    - `inurl:/application.wadl`
    - `user filetype:wadl`
    - `ext:wadl`
- WSDL
    - `user filetype:wsdl`
    - `ext:wsdl`
- Odata
    - inurl:/%24metadata

#### Github

- https://github.com/search?q=target.tld+%2Bapi
- WADL
    - https://github.com/search?q=target.tld+application.wadl&type=code
- WSDL
    - https://github.com/search?q=target.tld+*.wsdl&type=code

### Secrets

- `intitle:"index of" intext:"apikey.txt" site:target.tld`
- `allintext:"API_SECRET*" ext:env | ext:yml site:target.tld`
- truffleHog
- shhgit

### API Directories

- https://apis.guru/browse-apis/
- https://apilist.fun/
- https://apiharmony-open.mybluemix.net/public

## Enumerate endpoints / methods

### Endpoints

#### GraphQL

- https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/graphql.txt

#### Swagger

- https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/swagger.txt

#### Other

- https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/api/api_endpoints.txt
- https://s3.amazonaws.com/assetnote-wordlists/data/automated/httparchive_apiroutes_2020_11_20.txt

#### WADL

- https://github.com/dwisiswant0/wadl-dumper

### Tools

#### ffuf

- `ffuf -w wordlists/WORDLIST -u https://TARGET.TLD/FUZZ`
- https://github.com/ffuf/ffuf

#### Amass

- `amass enum -active -d TARGET.TLD -config /root/amass/config.ini`
- https://github.com/OWASP/Amass

#### nuclei

- `nuclei -target TARGET.TLD -t exposures/apis/`
- https://github.com/projectdiscovery/nuclei

#### Jaeles

- `jaeles scan -s /jaeles-signatures/sensitive/swagger-ui-probing.yaml -u TARGET.TLD`
- https://github.com/jaeles-project/jaeles

#### Arjun

- `arjun -u https://api.TARGET.TLD/endpoint`
- https://github.com/s0md3v/Arjun

#### ParamSpider

- `python3 paramspider.py --domain TARGET.TLD`
- https://github.com/devanshbatham/ParamSpider

#### param-miner

- https://github.com/PortSwigger/param-miner

#### TnT-Fuzzer

- `tntfuzzer --url https://TARGET.TLD/v2/swagger.json --iterations 100 --log_all`
- https://github.com/Teebytes/TnT-Fuzzer

#### Kiterunner

- `kr scan TARGET.TLD -w routes.kite -A=apiroutes-210228:20000 -x 10 --ignore-length=34`
- https://github.com/assetnote/kiterunner

## Supported Content Types

- Play with request URL
    - Requested resource extension e.g. replacing `.json` by `.xml`
    - Query string e.g. replacing `?json` by `?xml` or `?format=json` by `?format=xml`
- Play with `Content-Type` request header and payload
    - Without `Content-Type`, submit either `json`, `xml`, ...
    - Changing `Content-Type` and payload accordingly

# Testing

## Broken Object Level Authorization

### Endpoint receives an ID?

#### Understand the pattern

- Sequential
- Encoded
- Other

#### Tamper

##### Change

- Next value

- Previous value
- Data Type
  - Is it a number? Change it to a string
  - Is it a string? Change it to a number
- Method -> GET to POST

#### Duplicate

- ?id=1&id=2

#### Add as an array

- ?id[]=1&id[]=2

#### Wildcard

- GET /users/id -> GET /users/*

#### cross-deployments IDs

- Identify other deployments (hosts) of your target API
- Enumerate resources IDs (often non- numerical/sequential ones)
- Test those IDs on your target API host

### Check the response

### Tools

- REST APIs
  - Astra
  - apidor
  - AuthMatrix
  - Autorize
  - Auth Analyzer
- GraphQL
  - InQL

## Broken Authentication

### Test

#### URL sensitive data

- Passwords
- Tokens

#### Brute force attacks

- Login
- Forget Password
- Forget Username

#### Authenticity of tokens

#### Password

##### Strength

- Changing Password
- Registration

##### Type

- Plain text
- Weak encryption
- Weak hash algorithm

##### API Keys

- Predictable
- Weak hash algorithm

### Types of Authentication

#### JWT

##### Test JWT secret brute-forcing

- jwt_tool
- jwt_cracker
- jwtcat
- apicheck

##### Abusing JWT Public Keys Without knowing the Public Key

- rsa_sig2n

##### Test if algorithm could be changed

- jwt.io
- jwtcat
- apicheck
- JSON Web Token Attacker

##### Test token expiration time (TTL, RTTL)

###### Test if sensitive data is in the JWT

- jwt.io

###### Check for Injection in "kid" element

###### Check for time constant verification for HMAC

###### Check that keys and secrets are different between ENV

#### OAuth

- Test redirect_uri
  - Open redirects
    - Common issues
      - `?redirect_uri=https://atttacker.com`
      - `?redirect_uri=https://ATTACKER.TARGET.TLD`
      - `?redirect_uri=https://ALLOWED_HOST.com/callback?redirectUrl=https://attacker.com`
      - `?redirect_uri=https://TARGET.TLD.attacker.com`
      - `?redirect_uri=https://TARGET.TLD%252eattacker.com`
      - `?redirect_uri=https://TARGET.TLD//attacker.com/`
    - Fuzz
      - `?redirect_uri=https://TARGET.TLD§FUZZ§`
      - `?redirect_uri=https://§FUZZ§TARGET.TLD`
  - XSS
- Test the existence of response_type=token
- Testing state
  - Missing state parameter?
    - CSRF
      - Generate a valid `authorization_code` and don't use it
        - Send the crafted CSRF page to TARGET
  - Predictable state parameter?
  - Is state parameter being verified?
- If you revocate access, will code be also revocated?

#### Basic Auth

## Excessive Data Exposure

### Check if the API returns full data objects from database with sensitive data

- apicheck

### Compare client data with the API response to check if the filtering is done by client side

### Sniff the traffic to check for sensitive data returned by the API

- Burp CE
- ZAP
- mitmproxy

## Lack of Resources & Rate Limiting

**Execution timeouts**

- Regexploit

**Test brute-force attacks**

**Max allocable memory**

**Number of file descriptors**

**Number of processes**

- racepwn
- Race The Web

**Request payload size (e.g. uploads)**

**Number of requests per client/resource**

- Astra
- API Fuzzer

**Number of records per page to return in a single request response**

- API Fuzzer

## Broken Function Level Authorization

- Can a regular user access administrative endpoints? (MindAPI recon can help you here)
- Testing different HTTP methods (GET, POST, PUT, DELETE, PATCH) will allow level escalation?
- Enumerate/Bruteforce endpoints for getting unauthorized requests (MindAPI recon can help you here)

## Mass Assignment

**Enumerate object properties**

- API documentation (Reconnaissance)
- Inspect available API clients' network traffic
  - Desktop
  - Mobile
  - Web
- Exercise data retrieval endpoints
  - watch-out for `?include=user.addresses,user.cards`-like parameters

- Uncover hidden properties
  - Guessing, based on API context
  - Reverse engineering available API clients
  - Fuzzing
    - GraphQL
      - ShapeShifter (demo)

**Craft request payloads**

- Include augmented objects
  - One additional property at a time
  - Possible combinations of properties
  - All enumerated properties at once
- Vary properties data types/values
  - Number, String, Array, Object
  - State values: `to-do` -> `in-progress` -> `done` (keep in mind possible state transitions)
- Test different operation types
  - Create
  - Update

## Security Misconfiguration

**The latest security patches are missing, or the systems are out of date.**

**Can you use other HTTP verbs?**

**Test if Transport Layer Security (TLS) is missing**

- testssl

**Test for security headers**

- API Fuzzer

**CORS is well configured?**

- Astra
- API Fuzzer

**Force an error to see if any sensitive information is exposed**

**GraphQL**

- Introspection Query and/or GraphiQL is enabled
- GraphQL server provides fields name hints
- Query batching is enabled without limit
- Unlimited Depth and/or Amount

## Injection

#### Test if user input is validated, filtered, or sanitized by the API

- REST APIs
  - Astra
  - API Fuzzer
  - TnT-Fuzzer
  - APIFuzzer
- GraphQL
  - GraphQLmap

#### Test if client data is used or concat into DB queries, OS commands, etc

- REST APIs
  - Astra
  - API Fuzzer
  - TnT-Fuzzer
  - APIFuzzer
- GraphQL
  - GraphQLmap

#### Check if incoming data from external systems is validated, filtered, or sanitized by the API

### Improper Assets Management

- Check for the API documentation (MindAPI recon can help you here)
- Hosts inventory is missing or outdated.
- Integrated services inventory, either first- or third-party, is missing or outdated.
- Old or previous API versions are running unpatched.