API-Testing

##API-Testing

```
Definitions:
API:stand{application programming interface} set of rules that allows diffrerent software
application to communicate with each other

API-Documentation:"used to detect how use and integrate with api and contain important data"



Types of Api:
1. REST:widely used api and used http method {PUT,POST,GET,DELETE } and use URL to access
resource
2. SOAP:Syand {Simpleobject access protocol } use xml for messaging betwwen client and server
3. Graphql:query language for api that allows client to request specific
```

Methods to do Api-testing

1-API-Recon:

- ☐ identifiy api endpoints
- ☐ rate limits and authentication mechisms
- ☐ http method that api used {GET,POST,DELETE,PUT}
- ☐ Api documentation : EX: /api || /openapi.json || /swagger.json check this in target application
- ☐ use automated tools to get enpoints: dirsearch || postman || Asmass || WFUZZ
- ☐ Identify supported content-type

Testing Api

1-***Mass assigment Vulnerablitiy***:This vulnerability occurs when an application updates a set of properties in an object based on data sent by the user, without properly validating or restricting that data

2-**server-side parameter pollution**:is a vulnerability that occurs when a web application or API does not properly handle multiple parameters with the same name in a request

- ☑ impact:
  - ☐ The attacker can override existing parameters
  - ☐ modify the application behaviour
  - ☐ access unouthrized data

**where found it ?

found it in ==> in user_input || fields || url path || headers

Ex:
Suppose you have an API endpoint that accepts a `role` parameter to assign a role to a user:

```
POST /api/users/1234/role
Content-Type: application/x-www-form-urlencoded
role=user
```

Exploit: role=user&role=admin

Depending on how the server processes the parameters:

☐ if php will excute role=admin

☐ if ASP.NET combine both and return error

☐ if Node.js/express return role=user

How to prevent Vulnerablitiy in API:

☐ secure documentation if you don't to be public
☐ use allowlist of permitted http method
☐ validate content-type is expected for each request or response
☐ use generic error message
☐ use input validation and