API testing information gathering

* Finding input data with compulsory and optional field
* Type of requests and supported methods like http or https including media types
  + Different type of requests are GET, PUT, POST, DELETE, PATCH
  + Same endpoint with different method can do different operation on the resource
  + Content-Type Header can be changed between json and XML to check for errors
    - application/json
    - application/xml
  + Identify hidden endpoint by changing the common word in API, For example, you could add a payload to the /update position of the path with a list of other common functions, such as delete and add
    - Create the word list from the API URLs only
    - Use Param miner to get 65K names per request
    - Content discovery tool ???
  + Mass Assignment:
    - Unintended binding of param like isAdmin
    - Hidden parameter if know also get binded
* Rate limit and authentication mechanism
* Review documentation if available
* Find all the parent endpoint to figure out using **intruder**
  + /api/swagger/v2
  + /api/swagger/
  + /api
    - If some request with removing some prefix still gives error but not 404 that means there are lot of endpoints available at that.
    - 302 means redirect
    - 400 means error occurred
* Server Side parameter pollution:
* JS link Finder which extracts all the links present from the js files also
  + <https://portswigger.net/bappstore/0e61c786db0c4ac787a08c4516d52ccf>
  + https://github.com/portswigger