Research notes

IDOR Hunting

Three different types of IDORS

- BOLA - Broken Object Level Authorization
    - You can access a resource, while being logged in but where the resources belongs to another user
- BODA - Broken Function Level Authorization
    - You can access a resource, while logged in but where the resource requires a greater level of access than you have
- Lack of authentication
    - You can access a resource without being logged in

Authorisation is what you can do, what you have permission to do, you vs another person (THIS IS AN IDOR)

Authentication who you are? (THIS IS **NOT** AN IDOR)

IDORS are about if the session ID your provide, matches **and** is check against the one in the database

Sessions are stored on the **s**erver

Cookies are stored on the **c**lient

Sessions are destroyed regularly

- When you close your browser (done locally)
- When it expires (client and the server)

- when you logout (client and server)

Even if you use the "correct" session ID, the server wont recognise it.

Changing a working cookie for another accounts *working* cookie, tells us if the ID is validated. And then we can tell if its possible to exploit

To test for IDORS test with:

- Another user's cookies - BOLA
- No cookies - lack of authentication

You know you have an IDOR when you can perform an action on AccountA with the cookies of AccountB using repeater