Chapter 8 - Attacking Access controls

Attacking Access Controls

- When attacking access controls it is important to understand the access requirements of each page you attack, if/what cookies you need.

Testing with different user accounts

- you should use both, two different accounts with the same access, and two different accounts with different levels of access.
- To test for priveledge escelation, navigate the site with the highest priviledge you can, and then repeat those requests (you can use autorize or autorepeater) with no,low, or different priveledge.

Testing Multistage Processes

- The method mentioned prior will not work for multistage processes, this is because actions will need to be done in specific orders, as the app will build up your state with info in a specific way.
- Sometimes a later stage will not verify access as it will assume that if you have passed the prior, you are legitiment. This can be used to bypass auth
- Sometimes auth is done by the `Referer` header, try removing this.