Business logic flaws

BY UNCLE RAT

Agenda

- What is it
- Impact
- Examples

What is it

What is it

- Flawed assumptions about user behavior
- Leads to flaws in the design and implementation of the logic
- Will not be exposed by normal use of the application
- Are normally invisible
- By passing unexpected values to the server we try to induce unwanted behavior

Impact

Impact

- Can range from trivial to critical
- Depends on the related functionality
- I.e. flawed logic in money transactions is much more impactfull than flawed logic signing up for a newsletter

Examples

Examples

- The best way is to learn by example
- https://portswigger.net/web-security/logic-flaws/examples
  - Client side calculations of prices in a webshop
  - Existing users return another status code from non-existing ones when user brute forcing
  - Negative amounts of items on a webshop lead to negative prices
  - If price = integer and amount = integer and total price = interger we can overflow total price when we price * amount
  - Very very long input might get cut off allowing for unintended behaviour when registering an account