Basic Techniques for Securing the Apps

1. Filter input
    a. trim()
    b. Prepared statements
    c. filters
        i. filter_var()
        ii. Validate filters
        iii. Sanitize filters + strip_tags()

2. Escape/Sanitize output – *Pay attention to not escape the data more than once, you must escape only when you received it or when you need to output it!*
    a. htmlentities()
    b. htmlspecialchars()
    c. addslashes()

    The problem with *htmlentities()* is that it is not very powerful, in fact, it does not escape **single quotes**, cannot detect the character set and does not validate HTML as well. **To solve this problem –**

    - The first argument that this function accepts is the string we need to sanitize.
    - The second one must include a flag, in our case we want to use the ***ENT_QUOTES*** constant - **It prompts the function to encode single quotes.**
    - Eventually, the last argument allows you to specify **the character set** you are using in your application.
      A basic example would look like this:

```
echo htmlentities($string, ENT_QUOTES, 'UTF-8');
```

3. Encrypt sensitive data – *user passwords are never saved in the data base without encryption!*
    a. *password_hash()*

more