Input/output

* Kiểm tra đọ dài/kich thước
* Chuyển đổi kiểu dữ liệu,
* Whitelist-blacklist

Kiểm tra name file. đuôi file, kich thước, trùng tên(đặt lại tên)

Access control

* Authen

+ capcha weak – pas word checks, log all failures

+các phiên lám viêc khác nahu, kết thưc logout càn kết thúc phiên lm việc

* Author
  + Phân quyền người dung

Bảo vệ dữ liệu

* Phân loại: kiểu gì, bao nhiêu, public,
* Lưu trữ mã hóa dữ liệu, dữ liệu nhậy cảm
* Pass cần sủ dụng hàm băm
* Lựa chọn các thuật toán đủ mạnh đủ mới: AES, RSA (NOT MD5…)
* Key coment

Kết nối sủ dung các kết nối có mã hóa

* Htttp hacker có thể tặn lấy dữ iệu, https có mã hóa ngăn chặn lấy cắp tt

**Mobile app**

Validate activity, deep link, schema ẽported

Webview disnabale javascript

Kiểm tra chứng chỉ : kiểm tra giao tiếp

Ko cần login + debug

Anti root/jailbreak/emulator

Anti reverse + hackint tool

**Back**

Sql injection (sử dụng sql prepared statement)

**Xml** bật tắt cái gì? Cho ai.

Đảm bảo deserialize

* Sources checks
* Integrity checks
* Giám sát exception

http security header

X content typeoption …

**Fontend**

Tấn công Xss

Xử lý :input validation on all data, Resoure integrity

**0981881674 hung**