HOW TO (RELATIVELY) SECURE WEB APPLICATIONS

AHMAD MUAMMAR WK, OSCE, OSCP, EMAPT

ME@AMMAR.WEB.ID

Why we need to secure it

- Financial & Valuation Risk
- Brand & Media Risk
- Customer & User Risk
- Technology Risk

Secure and Security

- There is no 100% Secure
- Security is the Defense of Digital Information and Assets against Threats.
- Security Is A Process and Not A Product

SECURE WEB APPLICATIONS

Know your web Applications

1. Know Your Web Management (meaning: Where its hosted, who manage it, etc)
2. Know Your Web Infrastructure (meaning: What server specs, internet/bandwidth specifications, Server OS)

Know your web Applications

3. Know Your Web Application Infrastructure (meaning: What Your Application server, database server, programming language/technology)

4. Know Your Web about (Dynamic web with 3 user level, with user personal page, there is (chat) feature, there is upload pic options (mostly needed to know the all users (legitimate and non) capability)

5. Know What you don't know about your web

DEFENSIVE SECURITY

Defensive Security

1. Keep Up-to-date
   - Hardware, Software, Firmware, Appliance
2. Use Security Product
   - Hardware/Appliance: Firewall, Web application Firewall
   - Software: Firewall, Antivirus, AntiMalware

Defensive Security

3. Doing Security Hardening
   - Configure base on Security Policy/Guideline
4. Implement Security Mechanism
5. Implement Secure Coding during Web Applications development.
   - Using (Relatively) Secure web framework
   - Using Secure class/function/module (csrf token, xss protection, sql injection protections)

OFFENSIVE SECURITY

Offensive Security

1. Security Vulnerability Assessment
    - Security Audit (base on checklist)
    - Vulnerability Assessment (Using Vulnerability Scanner)
    - Security Penetration Testing

Offensive Security

2. Check your defensive mechanism works! (optimally and as u need it)

- eg: 9 firewall done nothing to web applications attacks , since all 7 of them will allow port 80 to be accessed!
- eg: Check 2FA implementation. (eg: Using 2FA, password and token but both sent through emails in reset password functions)

DEFENSIVE SECURITY VS OFFENSIVE SECURITY

Security

- ☑ This is like Knowing your Enemy (Offensive Security and Know Yourself (Defensive Security)