University
Carlos III of Madrid

Distributed Systems Security

Lab Assignments
Module 3: Fakebook part II (b)
IT Security Group

Guillermo Suárez de Tangil
(guillermo.suarez.tangil@uc3m.es)

Remembering last session…

- **Web Server** (Apache-Tomcat)
  - Fakebook should be accessible for any user
  - Tomcat's configuration should allow the correct operation of the web application
  - Not reveal any critical information
  - SSL
- **Data Base** (MySQL)
  - Accessible only from the local machine
  - Web admin only tables related to the web

Web Application

- JSP Files
  - Any user can enroll in Fakebook
  - Input parameters must be specially treated
    - SQL Injection
    - XSS
    - Control Input parameters (forms & database)
  - Errors/Anomalies Control
  - Access Control
  - Identity Theft
  - Protection of Personal Information
- Optional
  - Profile Image
  - Privacy Control -> Friends

Practical Assessment

- Deadline: December the 14th, 2011
- Deliveries:
  - Written report, scripts and configuration files
  - Outline
    - Security analysis
    - Security vulnerabilities
    - Vulnerability risk: **Information Assurance** vs. **Information Availability**
      - □ Including existing **examples of SQL Injection and XSS Attacks**
    - Vulnerability exploitation
    - Countermeasures and BCP (*justifying decisions taken*)
- Oral and Written Assessment (Operation)
  - Assessment process
    - White box testing: Manual evaluation of each VM
    - Black box testing: Automatic scripts
  - Pair Assessment
- Written Assessment (Knowledge): Individual test

Tips and Useful Advises (I/II)

- Analyze and understand how the Web application operates
- Identify variables that take its value from user input.
  - *Matching* and *storage* **database**
  - **HTML code**
- Analyze the mechanisms used to store personal information of the user
- Perform additional modifications to improve the security of the Web application, always considering the established requirements

Tips and Useful Advises (II/II)

- Divide and conquer
  - Break the module down (smallest work scopes)
- Before implementing, **abstraction**!
  - Textual description of the changes to tackle
- Backup copies
- Criticize your own decisions
- Discuss in with other pairs
  - **Do not plagiarize! (Knowledge assessment)**

References

- Assignment description
- XSS and SQL Injection
  - On the Internet, *and*
  - At the laboratory.