Application Security

Introduction to IT Security

Otago Polytechnic
Dunedin, New Zealand

Application Security

Application Security is about the set of practices we adopt to assure the security of an application throughout the project lifecycle.

- Design
- Development (including testing)
- Deployment
- Upgrade
- Maintenance

I like to think of it as setting security goals/policies and making sure they are met.

Design

- Identify security requirements
- Identify threats
- Plan responses to identified threats

Development

Possible security concerns that need to be addressed during development include

- **A**uthentication, **A**uthorisation, **A**ccounting
- Session management
- Input validation
- Network communication
- Exception handling
- Data storage
- Configuration

Development: testing

Security should be addressed in your test plans[1].

- Black box/Penetration testing
- Code analysis

[1] You do have test plans, right?

Deployment

- Secure deployment platform
- Integrity of installation sources, including 3rd party components

Upgrade

- Basically the full development lifecycle in miniature
- Additionally, we have to check whether our upgrade breaks the existing system.

Maintenance

- Backups
- Log management
- Encryption key/certificate management
- Host security
- Disseminating and receiving security notices and updates

More information

- OWASP : https://www.owasp.org/
- WASC : http://www.webappsec.org/
- SANS : http://www.sans.org/security-resources/