Software testing methods

Security testing

Jouni Juntunen, Jari Kiiskinen
University of Applied Sciences
Spring 2026

Contents

- Security and software
- Security testing
- Planning security testing
- Testing web security

About security and software

- Especially nowadays security is highly important, since number and usage of various online information systems containing confidential information has increased significantly
- Usage of third party and open source software is high, which poses a security risk
- Economical consequences for for security flaws can be high

Security testing

- Executed based on risk evaluation
- Purpose of the security testing is to reveal flaws in the security mechanisms of a software system that protect data and maintain functionality as intended
- Aspects, such as authentication, authorization, availability, confidentiality integrity, non-repudiation, resilience are tested
- Based on testing results developers are able to fix security problems
- **Privacy testing** is a process verifying that software meets privacy requirements

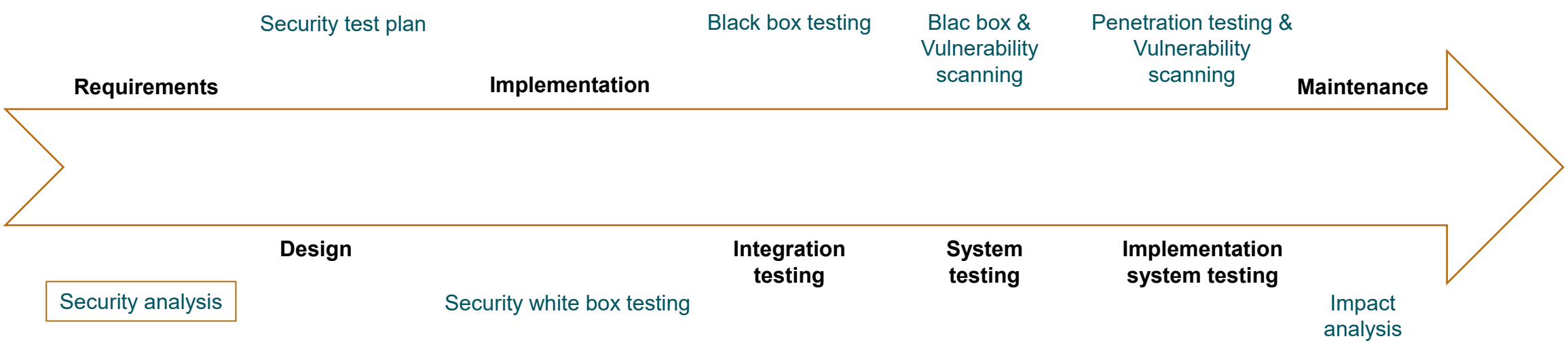
Executing security testing

- Assessment
- Review
- Manual testing
- Scanners
- Automated tests
  - Unit tests
  - E2E tests
  - ...

Types of security testing

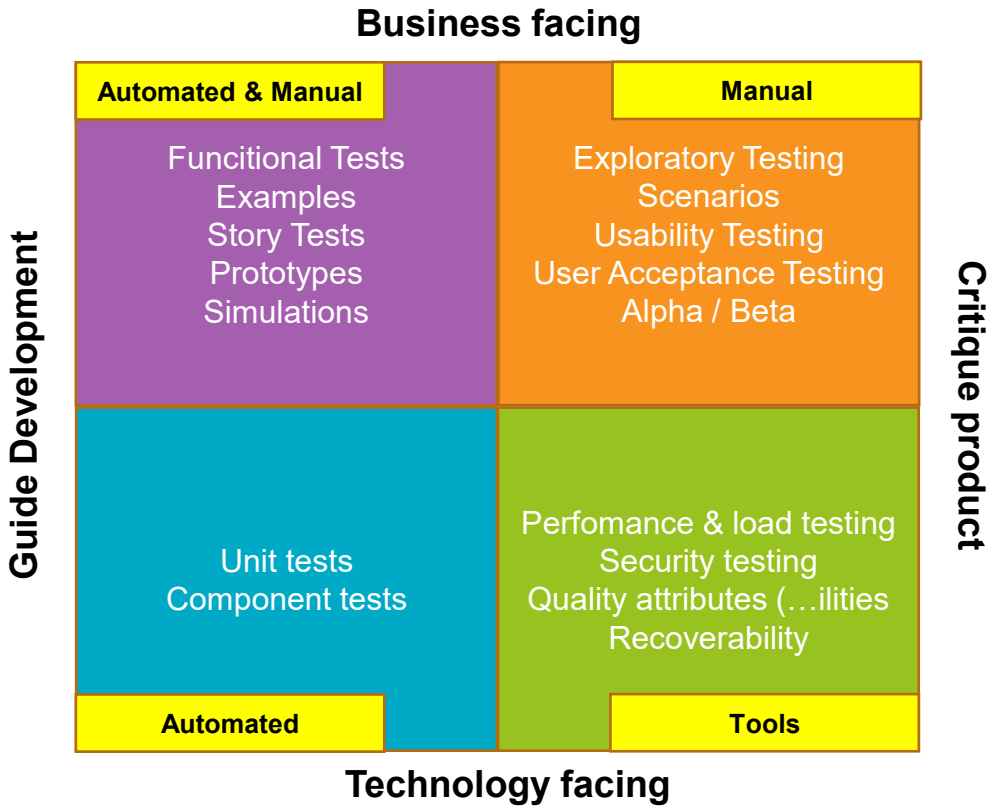
- Risk assessment(, third-party risk assessment)
- Vulnerability scanning
- Penetration testing
- Ethical hacking
- Posture assessment
- Security scanning
- Security auditing
- Social engineering
- Code review
- ..

Security testing and SDLC



Security testing in agile

- Shift security left, start testing and developing security early in the project
- Automate and integrate security testing (CI/CD)
- Prioritize security related requirements
- Test and implement incrementally



Planning security testing - conciderations

- Scope and objectives
- Testing methods and tools
- Security-related test scenarios
- Strategy
- Schedule
- Test environment
- Analysis
- Success criteria
- …

Planning security testing - conciderations

- Type:
  - black box
  - grey box
  - white box
- External/Internal
- Covert/non-covert
- Destructive/non destructive

Reporting security testing

- Executive summary
- Methodology, approach
- Findings
- Risk analysis
- Recommendations

Tools

- There are lot of tools (scanners etc.) available for security testing
- For example, ZAP by OWASP available on https://www.zaproxy.org
- Some tools (like ZAP) will help executing security tests even without having extensive background in security testing

Web attacks

- CSFR
- XSS
- Man in the middle (MitM)
- DoS
- Phishing
- Brute-force
- SQL injection
- …
- https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Tactics in attack and protection

- Minimizing attack vector/repeats/helpful information
- Sleepers in system vs reacting immediately
- Multilayer security, onion model
- Data value vs time to decipher, ”ROI”
- Security in physical resource, cloud resource, separated network resource

OWASP Top 10

- A01:2025 - Broken Access Control
- A02:2025 - Security Misconfiguration
- A03:2025 - Software Supply Chain Failures
- A04:2025 - Cryptographic Failures
- A05:2025 - Injection
- A06:2025 - Insecure Design
- A07:2025 - Authentication Failures
- A08:2025 - Software or Data Integrity Failures
- A09:2025 - Security Logging and Alerting Failures
- A10:2025 - Mishandling of Exceptional Conditions

https://owasp.org/Top10/2025/

What is tested

› x

- User accounts
- Passwords
- Session management
- URL address of the browser
- Configuration of server
- Software versions (browsers, frameworks, libraries etc.)
- Inputs of the application
- Database of the application
- Robots (i.e. what robots can get from the site)
- Denial of Service (DOS) and DDOS (distributed DOS)
- etc...

Resources

- OWASP. Web Security Testing Guide. https://owasp.org/www-project-web-security-testing-guide/stable/
- Korpela, Karina & Weatherhead, P. Planning for Information Security Testing – A Practical Approach. Isaca Journal Vol 5.