Part 3: Security testing

1. According to the slides, which three main areas affect data security and how?

Infrastructure security, that type of security includes access control mechanisms, availability, and confidentiality protection. Security devices and the configuration of the network is an important part of infrastructure security. Without infrastructure security, the system would be easily accessible from the outside.

Application security, that type of security is like a process of making applications more secure by finding, fixing, and exchanging the security of apps. Without application security, three CIA goals: confidentiality, integrity and availability would be easily vulnerable.

Organization security, that type of security includes the development and publication of policies, standards, procedures, and guidelines, also security awareness training, the monitoring of system activity, and changing of control procedures. If it were not for this, then chaos would prevail in the organization.

2. What types of applications is security testing particularly important for and why?

Applications that is accessed by large number of users;
Applications that contain personal user data;
Applications that contain company - specific confidential data;
Application availability is crucial;
Applications that integrate with 3-rd party components;
Application is a critical part of your business

Security testing is very important for applications listed above. Otherwise,it would violate three important CIA goals: confidentiality, integrity, and availability.

This can be detrimental to both the company and the customer of the company. Losses would be incurred by both parties Data has become very secure. GDPR was published in May 2018.

3. How can we integrate Security Testing in the life cycle of a software development project?

Security testing can be integrated into every stage of software development. A security engineer could be a responsible person. One of these solutions could be scanning application and infrastructure by using scanning tools. For example, OWASP ZAP. Another one could be using security test automation frameworks, for example, BDD-security. Also no less important is functional security testing which can show whether a software system behaves is as it should. There are many tools, so it is important to do a needs analysis in order to select the right tools.

4. **SAMSUNG Smart TV**

4.1 In 2018 consumer reports found the problem during a broad evaluation of privacy and security practices in the smart-TV platforms used by Samsung. Millions of Samsung televisions could potentially be controlled by hackers exploiting easy-to-find security flaws.

4.2 The security hole was detected by using consumer reports findings.

4.3 Using Components with know vulnerabilities was discovered (ninth in the list of the risks on OWASP's risks)

4.4 Important data can be stolen and can be used to cause harm, the system may malfunction, also can lead to financial distress or even increased consumer distrust.

4.5 Web-services testing, for example, ReadyAPI;

Functional TA tools, like Selenium, TestComplete, SOAP UI, etc.

Continuous security (monitoring) is crucial for these kind of vulnerabilities.