TP Class Assignment - 08/Apr/2019

Each group must answer the questions of the following exercises in the Github area of their group until the end of 23/Apr/2019. For each day of delay, 0.15 points will be deducted from the grade of this assignment.

Exercises

1. Risk

As seen in the last lesson, the goal of secure software development is to reduce the risk to acceptable levels.

Remember the risk formula of the previous class:

> risk = probability of attack to succeed * impact

where

> probability of attack to succeed = level of threat * degree of vulnerability

Question P1.1

Consider a home PC and a bank's *homebanking* server. Which one is at greater risk on the Internet? Justify by using the risk formula.

Experience 1.1

Consider that company's A application has the risk level R. Which factors of the risk formula would be affected by:

1. Discovery and incarceration of cybercriminals that threatened the application.
2. The company discovers and removes various vulnerabilities of the application.

2. Secure Software Development Lifecycle (S-SDLC)

Experience 2.1

At what pahse of the waterfall model should the European GDPR regulation be taken into account?

Question P2.1

At what pahse of the *Microsoft Security Development Lifecycle* model should the European GDPR regulation be taken into account?

Experience 2.2

1. In what business function, security practice and SAMM activity should the European GDPR regulation be taken

into account?

2. At what level of maturity of this safety practice does the company have to be, to take into account the GDPR European regulation in its projects? Justify.

Question P2.2

This question should be answered by even-numbered groups.

In any of the S-SDLC it is fundamental in the Requirements phase to identify the security requirements, which must be based on the current legislation and international recommendations and standards (ISO 27000 family), as applicable, and must be translated into specific requirements for the software to be developed.

The ISO / IEC 27002: 2013 *Information technology - Security techniques - Code of practice for information security controls* provides guidelines for information security standards and information security management practices in an organization, including the selection, implementation and management of security controls, taking into account the environment of information security risk of the organization.

Analyse the safety controls in the following sections:

- 14.2 *Security in development and support processes*
- 10.1 *Cryptographic controls*

What can you conclude about the use of these controls in the software development project that your group is developing for this discipline or for other disciplines?

Note: You can find ISO / IEC 27002: 2013 here.

Question P2.3

This question should be answered by odd-numbered groups.

The *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64, Security Considerations in the System Development Life Cycle*, was developed to assist Federal Government Agencies to integrate the IT security components into the software lifecycle development (SDLC) that they use.

Analyse section 2.3 (*Key Roles and Responsibilities in the SDLC*). What can you conclude about the SDLC security roles and responsibilities compared to the software development projects in which you have participated?

Note: You can find NIST Special Publication (SP) 800-64 in the directory Aula10.

3. SAMM (*Software Assurance Maturity Model*)

In this section you are asked to use the SAMM continuous improvement cycle applied to your Security Engineering project.

To do this you must use the Toolbox (excel file) provided in the directory [Aula10](Class 10), where you will find more information regarding SAMM.

Note that:

- For the *Assess* Phase you must fill in the *sheet* "*Interview*";
- For the *Set the Target* Phase, the group should discuss the *score* objective of the identified security practices. If

you need assumptions, indicate them in the justification of the decision made;
- For the *Define the Plan* Phase you should fill in the *sheet* "*Roadmap*", assuming that each phase is 3 months long. Take into account the effort required and the possible dependence between activities in each of the phases.

Note that there are no right or wrong answers.

Question P3.1

Identify the maturity of three security practices (of your choice) that you use in the development of the Security Engineering project (SAMM *Assess* phase)

Question P3.2

For each of the security practices identified in the previous question, set the target for it (SAMM *Set the Target* phase), i.e. the desired maturity level;

Question P3.3

Develop the plan to achieve the desired maturity level identified in the previous question, in four phases (SAMM *Define the Plan* phase).