# Secure Software Development – Course Review Workshop

## Version 1.0

| Author(s)/Organisation(s): |
|---|
| Žarko Stanisavljević / UB<br><br>Pintér Róbert, Sanja Maravić-Čisar / VTŠ<br><br>Milan Stojkov, Nikola Luburić, Imre Lendak / UNS |
| **Date of final release:** |
| April 12th, 2019 |
| **Relevant Work Package(s):** |
| WP2 – Course Development |
| **Short Description:** |
| Review of the 2.2. Secure Software Development course content prepared by the UNS. |
| **Keywords:** |
| Secure Software Development, review |

| Revision History: | | | | |
|---|---|---|---|---|
| Revision | Date | Author(s) | Status | Description |
| V1.0 | Apr 12, 2018 | Imre Lendak | Working draft | First edition |

**ISSES** – Information Security Services
Education in Serbia

*Supported by the Erasmus+ Capacity Building in
the field of Higher Education (CBHE) grant
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP*

**CONTENTS**

**ISSES** – Information Security Services
Education in Serbia

*Supported by the Erasmus+ Capacity Building in
the field of Higher Education (CBHE) grant
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP*

# 1   Introduction

Imre Lendak introduced the meeting with his report about:

- project status,
- course development,
- lab development,
- program development
- next meeting(s).

**ISSES** – Information Security Services
Education in Serbia

*Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP*

## 2 Course Content Presentation

- 10:20 – 10:40: Nikola Luburic, Secure Software Development introduction
  - Discussion about additional standards – Zarko suggested to include NIST as they are free standards
  - Discussion about course content put online
- 10:40 – 11:00: Nikola Luburic, Security Requirements
- 11:00 – 11:15: Nikola Luburic, Secure software design
- 11:15 – 11:35: Nikola Luburic, Threat modeling
- 11:35 – 11:50: Nikola Luburic, Web application vulnerabilities
- 11:50 – 12:00: Nikola Luburic, Web-based client vulnerabilities
- 12:00 – 12:25: Milan Stojkov, Application Programming Interface vulnerabilities
- 12:25 – 12:40: Milan Stojkov, Security of Managed Languages
  - Maybe include one additional slide with Web.config primer
- 12:40 – 12:50: Milan Stojkov, Security Testing
  - Add relevant tools in SAST, DAST, IAST, e.g. based on the relevant Gartner reports.
  - Missing content: present the free tools and compare them to the commercial ones.
- 12:50 – 13:15: Milan Stojkov, Secure Deployment
- 13:15 – 13:30: Milan Stojkov, Penetration Testing

**ISSES** – Information Security Services
Education in Serbia

*Supported by the Erasmus+ Capacity Building in
the field of Higher Education (CBHE) grant
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP*

# 3  Laboratory Exercise Content Review

- The general idea is to develop lab. exercise content which can be delivered on any general computer equipment, i.e. no special equipment is needed.
- Milan & Nikola suggested to not use the Avatao platform in this course, because we currently do not have the human resources and knowledge the develop the additional, new challenges for Avatao, which would be our 'payment' against their service, i.e. the use of the Avatao service.

# 4    Course Content Discussion

In the second part of the workshop we discussed various topics. Some were closely related to the SSD course, while others were more general and relevant in the context of other project outputs as well.

## 4.1   SSD Course-related

- **Positioning** of the SSD course @ the UNS. The course will be introduced on the BSc level on the FTN/E2/SIIT in its future BSc program → How to link to link to the new MSc program? What about the students who took BSc elsewhere and did not have SSD on the BSc level? → **Decision:** Include SSD as an optional course in the new MSc for those who did not have this content on the BSc level
- Will we map the topics to the project **Repository of Information Security Concepts** (RISC)? We should extend the RISC based on the latest version of the course content. That will be necessary for the quality assessment of the course.
  - o  TODO: Nikola & Milan will review and update the SSD part of the RISC based on the latest course content.
- Who will/should do the **quality assessment** of this course? Not the UNS &/| CrySyS as they are the partial source and/or developer. → Maybe the ETF, as they will be one of the direct beneficiaries of this content, i.e. use it in their future study program.
  - o  TODO: Imre will find who is responsible for the QA of the SSD course. The decision was made in Nis, in October 2018.
  - o  TODO: Imre will communicate with Stefano & Stevan to proceed with the QA process.

## 4.2   Work package 3: Course Development (WP3)-related

- Course content will be put **online** for open access (presentations in PDF & Wiki). Thereby the content will be available to the members of the consortium.
  - o  TODO: Imre will manage the Wiki creation and send user credentials.
  - o  TODO: Milan, Nikola will upload Wiki content, PPTs (PDFs) and references.
- Course content in **textbooks** – nominate subjects which we would like to cover by textbooks, i.e. project team members should volunteer to align and include their book development efforts with the ISSES project execution.
  - o  TODO: Imre will communicate with the project team that we should nominate textbooks.
- List of **references** at the end of each lecture content (e.g. Wiki) should include ~10 items. Preferably not textbook, but blogs.
  - o  TODO: Imre will communicate with the project team that these are necessary for the Wiki.
- When will we organize the **additional course content reviews** (i.e. internal workshops) for the Advanced Network & Systems Security and Cybersecurity Strategies courses?
  - o  We agreed that this format is useful. Zarko mentioned that it could be optional and done for those courses where it is deemed necessary.