Welcome and Introduction to SCT 2023

Gerard Frankowski – PSNC ICT Security Department
WP9T2

Secure Coding Training 2023 – Poznań, PSNC
25-27.10.2023

Restricted

Agenda

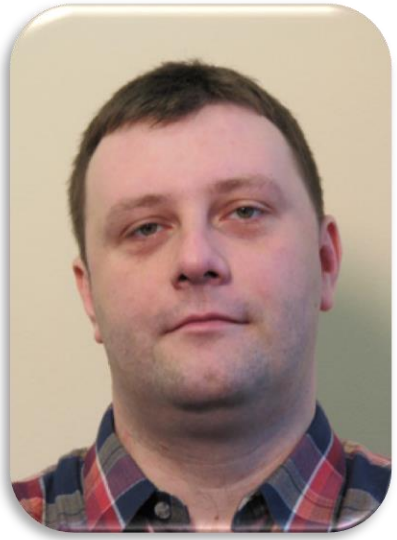
- Hello from the trainers and participants
- **Who and why do SCTs?**
  - PSNC experience on cybersecurity and secure coding
  - Why we are doing the SCTs?
- SCT goes back as F2F!
  - Main organizational issues
- The contents
  - New and updated topics since SCT 2022
  - SCT 2022 Agenda – days 1-3
- Useful details
  - Exercises and activities in breakout rooms
  - Coloring conventions and code snippets
  - Wisdom slides
  - Important links

SCT 2023 Trainers

Paweł Berus (PB)
In PSNC since 2010 – former developer, pentester and security code reviewer

Karolina Buchnat (KB)
Our new colleague, combining cybersecurity passion with Python development competencies

Mikołaj Dobski (MD)
In PSNC since 2010 – developer, CI/CD and ML expert, security analyst



Gerard Frankowski (GF)
In PSNC since 2003 – analyst, security code reviewer, former developer

Jarek Wieczorek (JW)
In PSNC since 2017 – cybersecurity analyst, code reviewer and Python developer

PSNC 30

SCT 2023 supporting squad and the GLAD Team

Marcin Wolski (MW)
WP9T2 Task Leader prepared the presentation of services offered by our task

Maciej Łabędzki (MŁ)
– will tell you about School for Software Engineering – **TBC**

Lisa Melrose

Dom Mayerl

Many thanks to the GLAD team!

Time for our Attendees!

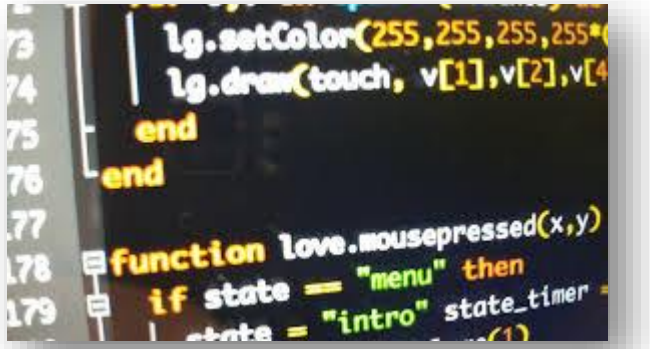
Cybersecurity in PSNC

- **P**oznań **S**upercomputing and **N**etworking **C**enter
- Polish NREN (**PIONIER**) operator
- Polish Optical Internet Research Center (**CBPIO**)
  - Over 20 laboratories, e.g. Laboratory of Cybersecurity and Critical Infrastructures Protection
- **PSNC Cybersecurity Department**: **29** colleagues as for now
- **ISO 27001** certified (ISMS)
- **ISO 9001** certified, concerning e.g. ICT consulting and cybersecurity audits
- **CyberSec**: Part of EDIH (**European Digital Innovation Hub**) network, including source code security services
  - More: https://cyber-sec.net.pl

CBPIO

EDIH
European
Digital Innovation
Hubs Network

PSNC experience on source code security



- Secure Coding Trainings
  - GÉANT: 12x (2010-2022) + 1 repetition (2018)
  - National Data Storage (2011-2012)
  - SECOR (2013)
  - E-textbooks: 3x (2013-2014)
  - SCADvance (2017)
  - Single presentations on different events, e.g. EGEE' 09, SECUREX international fair

- Code security reviews
  - Projects: EGEE-II, EGEE-III, GN3, GN3+, GN4/GN4-2/GN4-3, PL-Grid, PL-Grid+, PL-Grid NG, NDS, e-Textbooks, SCADvance, EDWIN, MEDICS
  - Others: e-banking services, Web applications, dLibra, internal reviews
  - Languages: mainly Java, C/C++/C#, PHP, Python

Why we are doing SCTs?

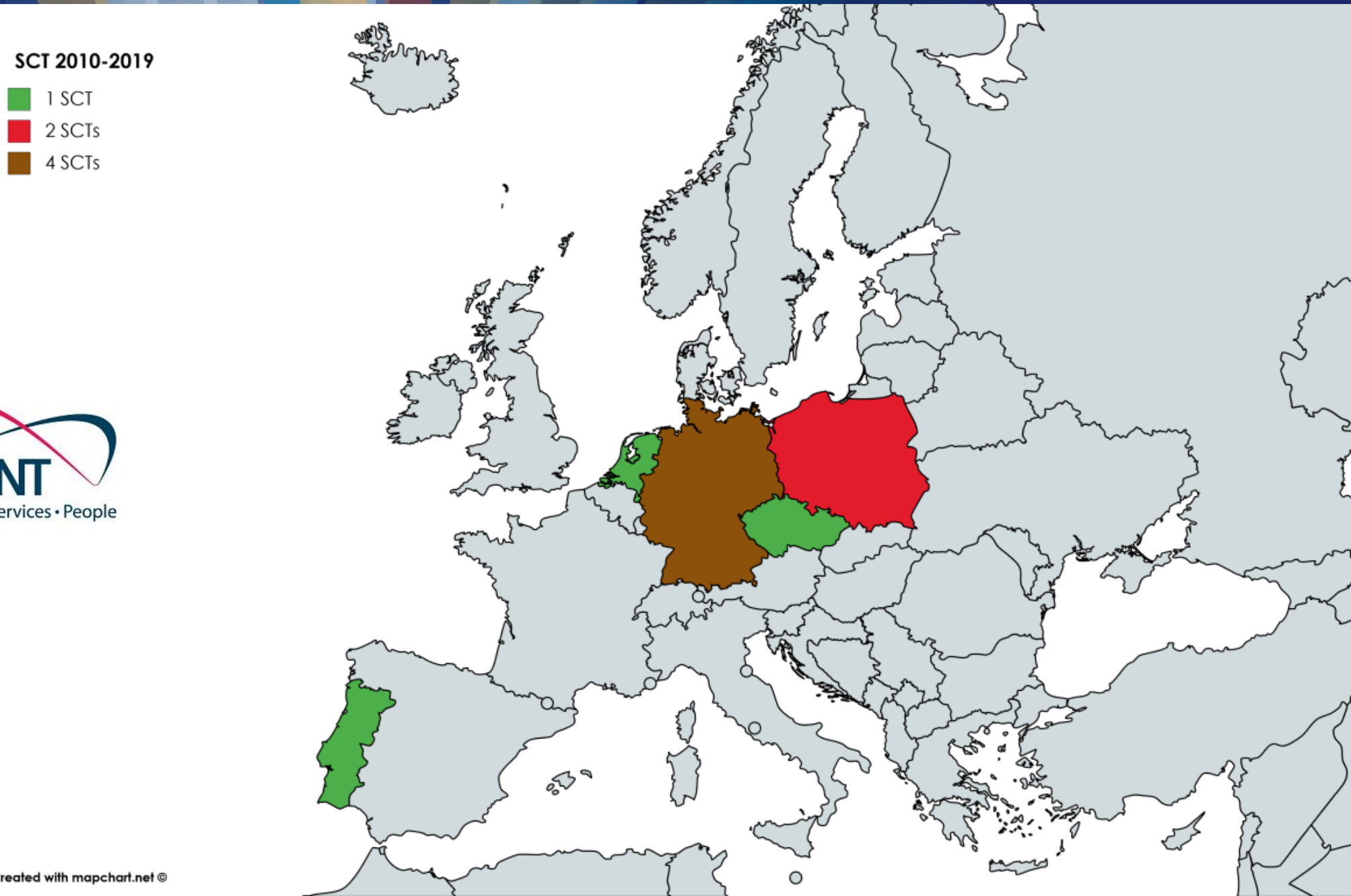
- The main purposes of the SCT trainings:
  - To **keep the awareness**
  - To **practice** good templates
  - To **explain particular issues** useful for secure development of GÉANT services

- Through this SCT, we want you to:
  - Become familiar with **security requirements** for development of Web applications in several areas
  - Experience the nature of certain types of Web applications **security vulnerabilities**

SCT on the road again!

- First time F2F since 2019!
- People got accustomed to VCs but F2F workshops are more effective
  - …And how to organize social events via Zoom?
- Thus after…
  - Poznań
  - Prague
  - Berlin
  - Utrecht
  - Lisbon

- …we have invited you to Poznań again!



GÉANT

GÉANT
Networks • Services • People

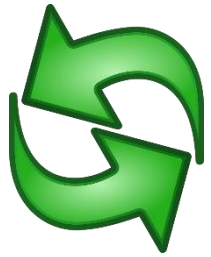
GÉANT

SCT 2023 – main organizational issues

- We return to the usual F2F SCT schedule
- 3 days
  - Day 1: afternoon (13:00-17:00 CEST)
    - More high level issues + ASVS
  - Day 2: the whole day (9:00-17:00 CEST)
    - Python secure programming day!
  - Day 3: morning (9:00-13:00 CEST)
    - A bit of ASVS + HackMe
- Two main workshops finalize Days 2 and 3
  - Day 2 – Python secure programming workshop
  - Day 3 – HackMe contest
- Social event – Day 2
- Feedback collection – Day 3

New and updated topics since SCT 2022

- Added:
  - **Python secure programming**
  - OWASP ASVS
    - V3 – Session Management
    - V12 – Files and Resources
  - Technical dinner ☺
- Updated or adjusted:
  - HackMe contest
  - CI/CD and SDLC issues



SCT 2023 Agenda – day 1 (Wednesday, 25th October)

Time	Topic	Who
13:00-13:40	Welcome and introduction to SCT 2023	GF
13:40-13:55	WP9T2 - Software Governance for the GÉANT community	MW
13:55-14:00	Invitation to School of Software Engineering 2024	MŁ
14:15-15:45	**Continuous Integration / Continuous Development and Secure Development Life Cycle**	MD
16:00-17:00	**Writing Hacker Proof Code - Files and Resources**	GF

Breaks not shown

SCT 2023 Agenda – day 2 (Thursday, 26th October)

Time	Topic	Who
9:00-9:50	**Secure Programming in Python – Introduction**	KB, JW
9:50-11:00	**Secure Programming in Python – Python gotchas (1)**	KB, JW
11:15-12:00	**Secure Programming in Python – Python gotchas (2)**	KB, JW
12:00-13:00	**Secure Programming in Python – secure coding practices (1)**	KB, JW
13:45-15:00	**Secure Programming in Python – secure coding practices (2)**	KB, JW
14:20-15:00	**Secure Programming in Python – tools and conclusions**	KB, JW
15:15-17:00	**Secure Programming in Python – practical workshop**	KB, JW

Breaks not shown

SCT 2023 Agenda – day 3 (Friday, 27th October)

Time	Topic	Who
9:00-10:20	**Writing Hacker Proof Code - Session Management**	GF
10:30-10:50	HackMe – Preparations and Instructions	PB
11:00-12:30	**HackMe contest**	PB
12:40-12:50	HackMe Evaluation and Solutions	PB
12:50-13:00	SCT 2023 Summary and Closing	GF

Breaks not shown

In-place exercises

- You will be shown an exercise (sometimes plus the expected time to provide a solution)
- You will be asked to present your solutions and we will be discussing them
  - Our exemplary solutions do not have to be neither the only nor the best ones
- The presentations will contain solution slides, possibly with additional comments
- Later you will be provided full PDF slides

Coloring of code snippets and good / bad patterns Convention 1 (the old one)

```
This is the background to present a bad coding (configuration) pattern
```

```
And this is to present a proper template or pattern
```

```
This is neutral, just to show some example
```

```
And this is the way we denote an important part of the source code in a larger listing
```

Coloring of code snippets and good / bad patterns Convention 2 (Python Secure Programming part)

Code fragments containing errors or other problems have been marked with a pink dashed box.

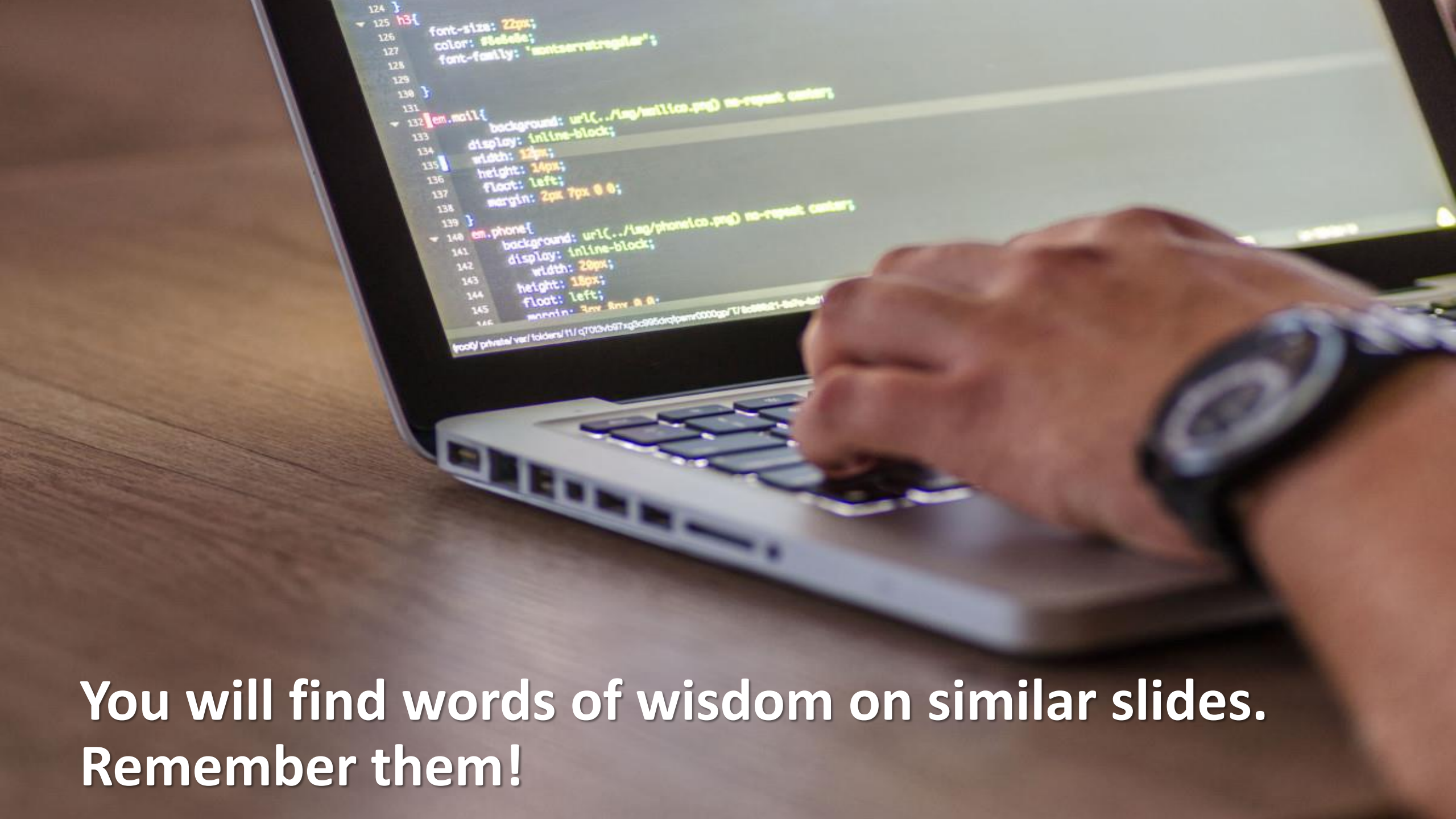
Code fragments that are correct and do not contain errors are marked with a green box.

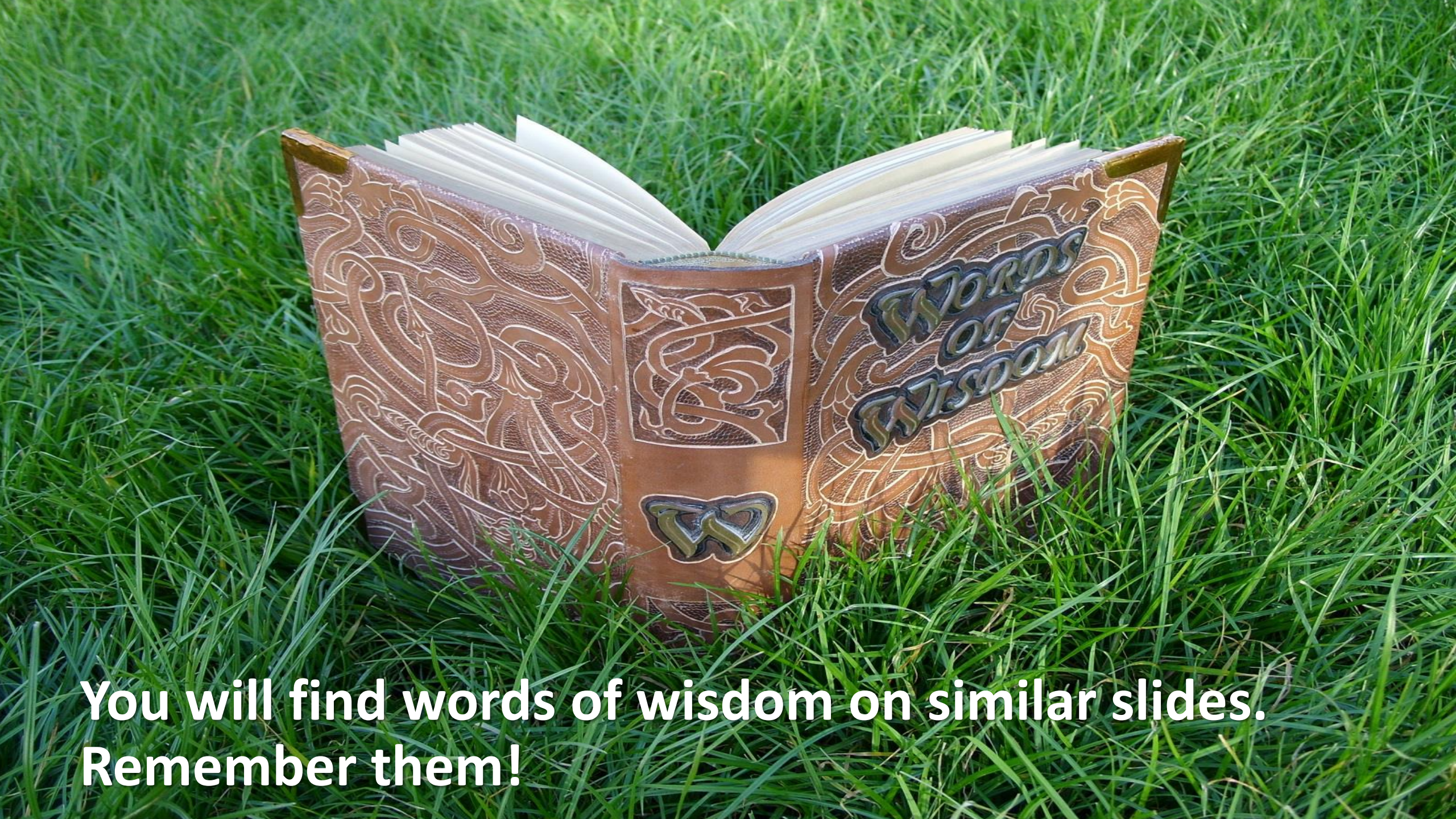
Neutral code fragment, i.e. not marked (as good or bad).

```
variable1 = 10
variable2 = "Hello"
variable3 = [1, 2, 3]
# code coloring follows the IDE editor
```

The content of code snippets

- Remember that even the recommended code patterns may not be the full solution!
  - They present a particular isolated issue and then address it
  - But the real, full pattern could exceed one or several slides…
- **So do not copy this code directly into your project, just use the provided good patterns**


You will find words of wisdom on similar slides.
Remember them!



You will find words of wisdom on similar slides.
Remember them!

Other SCT 2023 tips

- Please ask questions at once!
- Tell us when you need an extra break
  - The agenda is subject to change when the actual pace needs it
  - But we will finish on time

Your feedback is crucial!

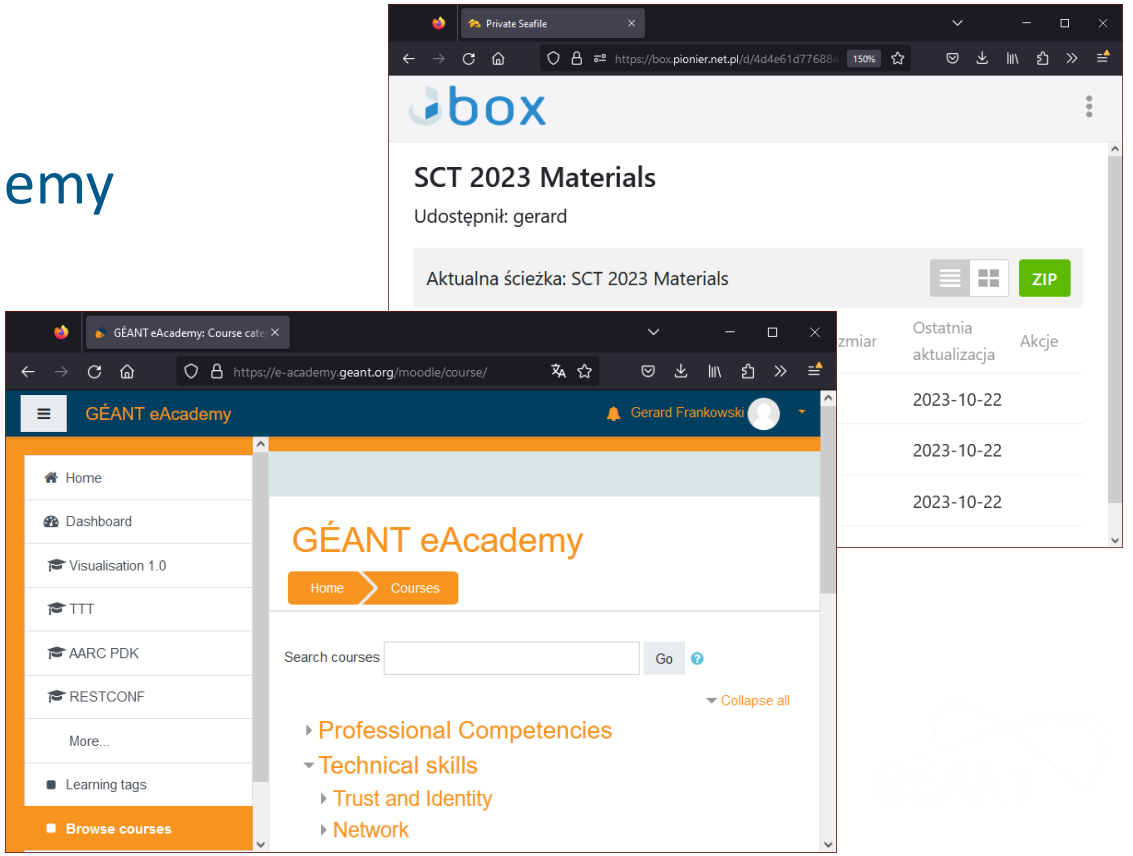
- This year we will have a printed-out evaluation form
  - Our experience says this is the most effective form of feedback collection :)
- Evaluation form is **anonymous**
- We suggest to fill the form during the timeframe for HackMe contest results evaluation
  - Friday between 12:40-12:50
  - Should take no more than 5 minutes

- You may also suggest your favorite topics for future SCTs!

Presentations and recordings

- **Links** for content to download or access after SCT 2023
  - PSNC cloud shared folder for presentations, recordings, etc.
    - https://box.pionier.net.pl/d/4d4e61d776884e03bf1a/, or
    - https://tinyurl.com/SCT23-repo

- We also will upload SCTs contents to eAcademy
  - https://e-academy.geant.org/moodle/



Thank You

Any questions?

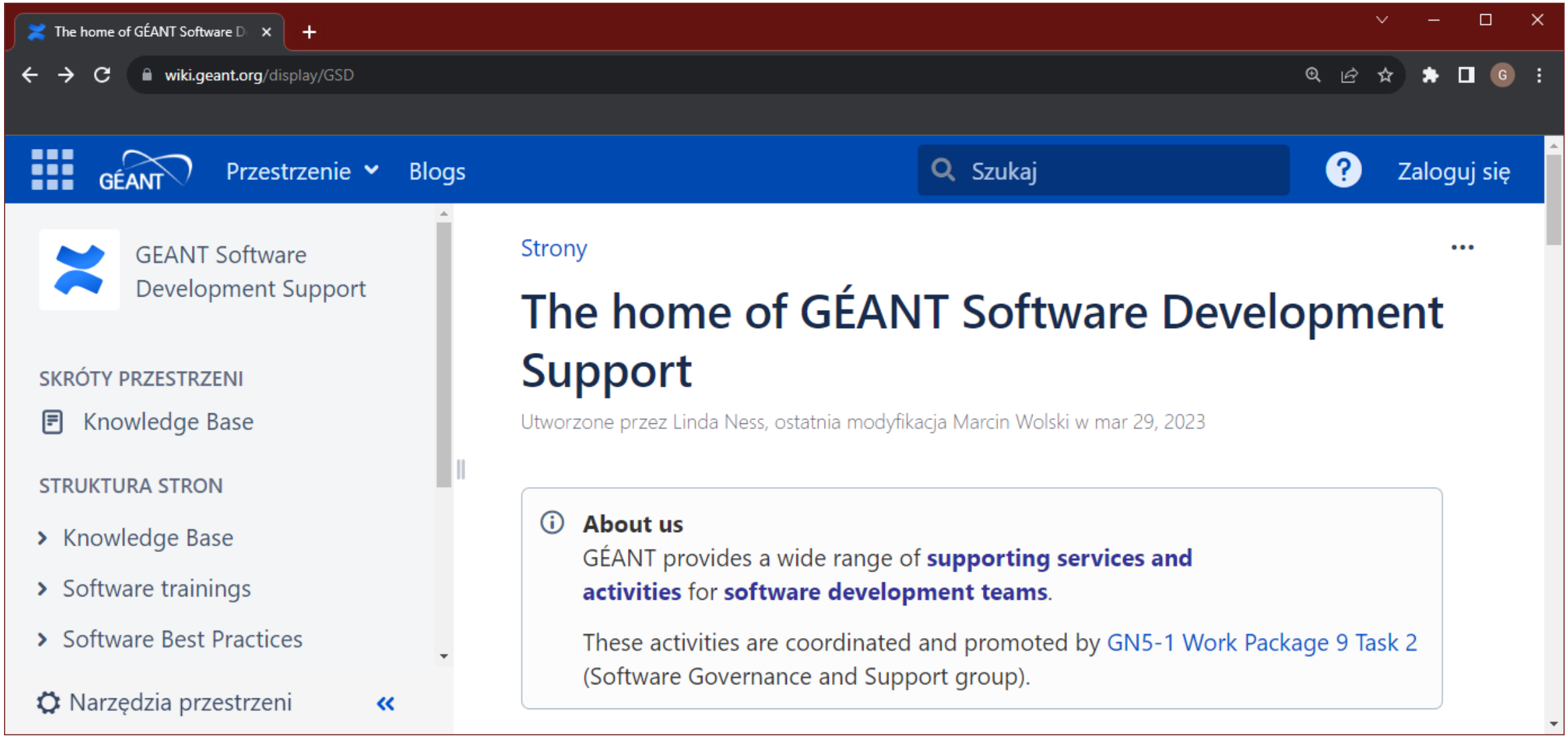
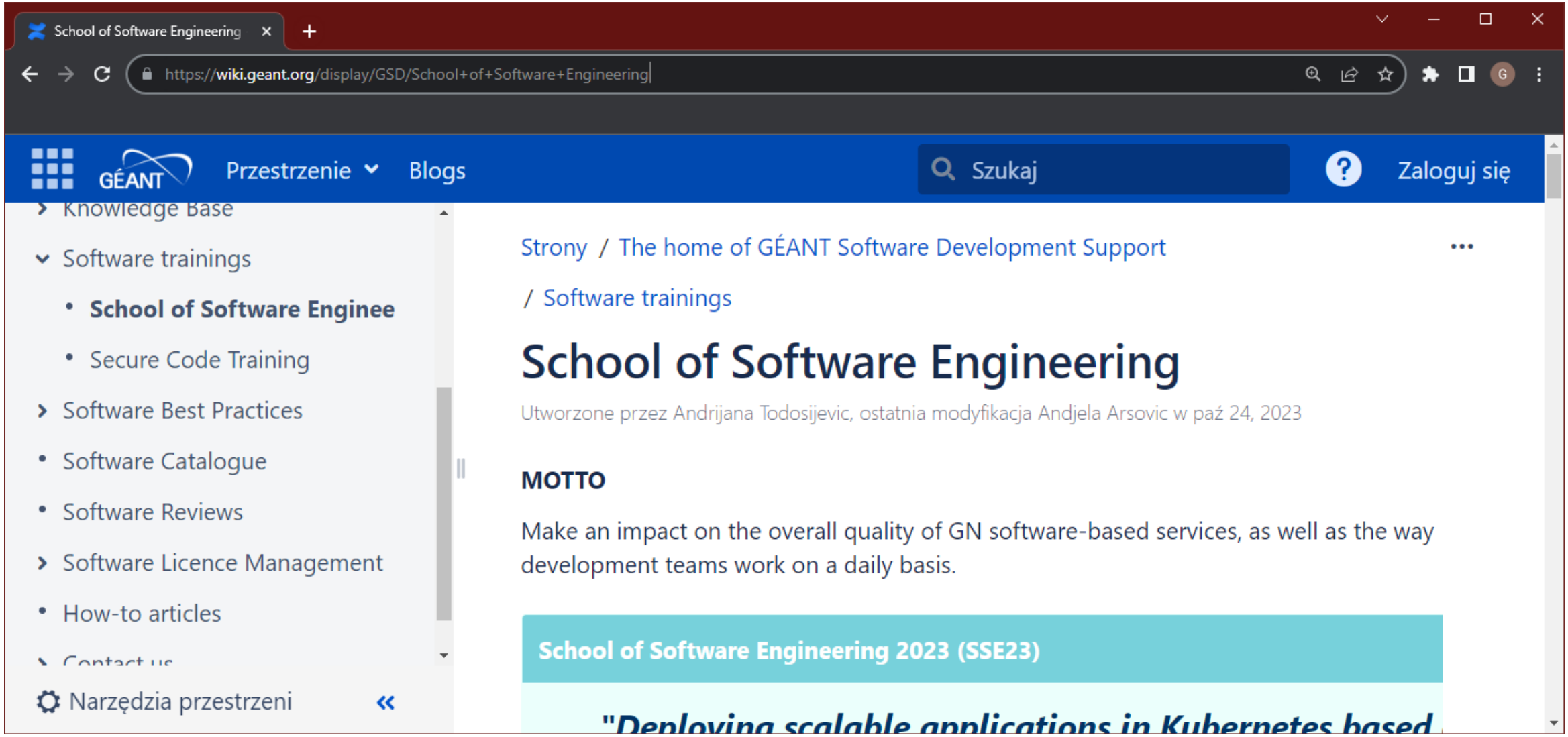
gerard@man.poznan.pl

www.geant.org

Co-funded by the European Union

The project co-financed by Polish Ministry of Science and Higher Education from financial resources of the programme entitled "PMW"

GN5-1 WP9T2 Landing Page - https://wiki.geant.org/display/GSD



School of Software Engineering Landing Page - https://wiki.geant.org/display/GSD/School+of+Software+Engineering