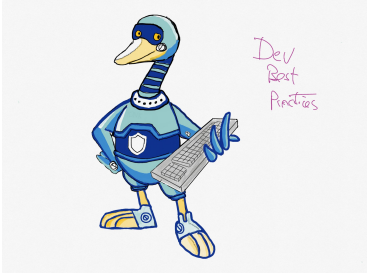


Best Practices Make Perfect!

How the OSSF is improving secure development education

Marta Rybczynska and CRob

OpenSSF Day EU, 2022

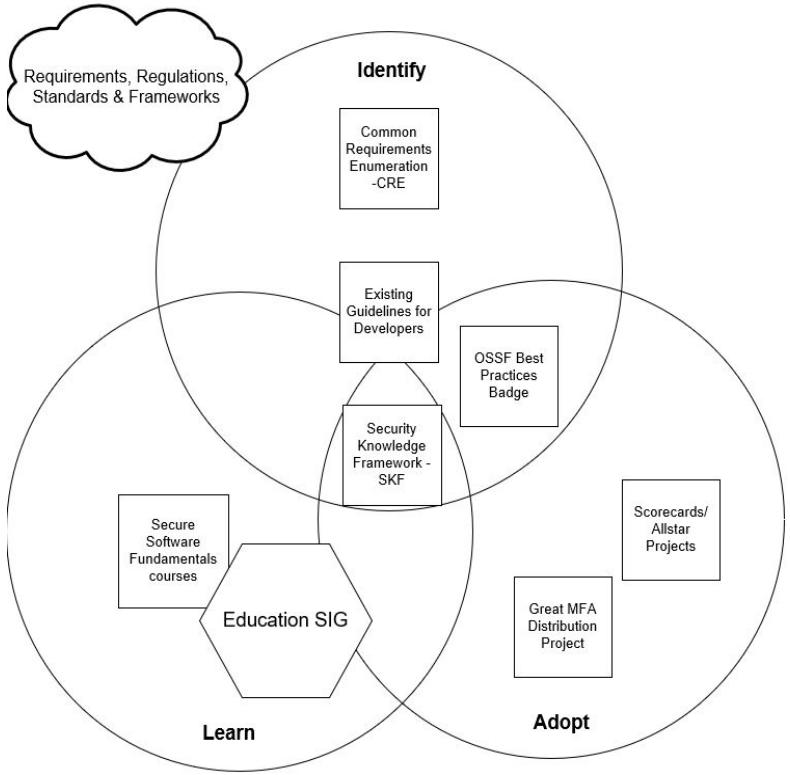
Why do we need best practices?

Our vision is to make it easy for developers to adopt best practices, thanks to:

- **Identifying** good practices, requirements, and tools that help open source developers create and maintain more secure software
- Helping maintainers **Learn** to write secure software
- Provide tools to help developers **Adopt** these good practices into their daily work

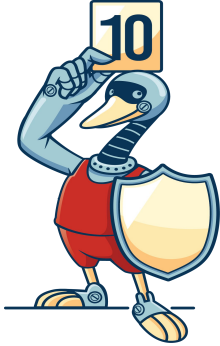
Recently published two concise guides:

- Concise Guide for Developing More Secure Software
- Concise Guide for Evaluating Open Source Software



https://github.com/ossf/wg-best-practices-os-developers

Evaluating projects with Scorecards



- Automated tool to assess project's security practices
- Gives:
  - Aggregate score
  - Scores for different areas
  - Ideas for improvement
- Example checks:
  - Is the project free of checked-in binaries?
  - Does the project run tests in CI?
  - Does the project contain a security policy?
- Currently working with GitHub, more planned
- New features: badges, REST API

https://github.com/ossf/scorecard

Choosing software with the Best Practices badge

Open Source Security Foundation (OpenSSF) Best Practices badge is a way for Free/Libre and Open Source Software(FLOSS) projects to show that they follow best practices.

Reviews project processes around Project Basics (website, licensing, documentation,etc), Change Control, Reporting, Quality,Security, and Analysis. Full criteria list

Graduated tiers of more stringent criteria for higher level badge qualification

New: covers more than 5,000 projects!

Some badge earners:

https://bestpractices.coreinfrastructure.org/en

Learning the basics

The “Developing Secure Software” (LFD121) course is available on the Linux Foundation Training & Certification platform. It focuses on the fundamentals of developing secure software. Both the course and certificate of completion are free. It is entirely online, takes about 14-18 hours to complete, and you can go at your own pace. Those who complete the course and pass the final exam will earn a certificate of completion valid for two years.

Available through edX Platform, LF Training, and via SCORM Connect to connect to popular LMS systems

https://openssf.org/training/courses/

NEW Concise Guides

Concise Guide for Developing More Secure Software

25 suggestions with short explanation and links - shows how to improve development

Example (point 11): *Prominently document how to report vulnerabilities & prepare for them.*

Concise Guide for Evaluating Open Source Software

9 question to ask before adapting a dependency, with additional suggestions and steps to follow

Example (point 2): *Are you evaluating the intended version?*

The Education initiative

As part of the OSSF's Mobilization Plan, the BEST WG adopted Stream 1 and created the Education SIG and is working to deliver a proposal to bring more secure development training to all types of learners around the globe

https://github.com/ossf/education

https://openssf.org/oss-security-mobilization-plan/

Closing - what are we looking for in the next 1 year?