Authors' Response to the Review of EMSE-D-20-00300: "Fixing Vulnerabilities Potentially Hinders Maintainability"

Sofia Reis, Rui Abreu, Luis Cruz

Editor

> Many thanks for submitting your revision to Empirical Software Engineering journal. All reviewers and I thank you for the effort you have put in preparing the detailed revision which successfully addresses all points raised earlier. Accordingly, I am happy to recommend the acceptance of your manuscript to the EiCs. Please note that reviewers highlight some editing issues, so please clarify Reviewer #2's points and conduct an overall proof read in preparing your final proofs.

Response:
We thank the editor and reviewers for their valuable feedback and acceptance. In the following, we answer the questions raised by the reviewer 2.

Reviewer 2

Reviewer comment 2.1:

> What is meant by "20 person years"? How would one obtain this measure?

Response:
A person-year is the equivalent to 12 person-months. A person-month is a standard measure of source code volume where the total volume in a codebase is the volume in lines of code converted to person-months. BCH uses person-years instead of volume because it facilitates the comparisons of source code volume between technologies (different programming languages have different levels of of verbosity). We do not consider this metric on our study. However, according to the "Building Maintainable Software" book, 20 person-years of rebuild value is the equivalent to at most 1750000 lines of code in Java.

Reviewer comment 2.2:

> The bullet for automated tests. Can you think of another work instead of "contemplate"? I'm not sure of what you are trying to say.

Response:
Thank you for pointing this out. We changed the work for "consider". This metric only considers unit testing, which is usually not applied for security testing but rather to functionality testing.