S. Becker, I. Bogicevic, G. Herzwurm, S. Wagner (Hrsg.): SE/SWM 2019,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 133

How is security testing done in agile teams? A cross-case analysis of four software teams

Daniela Soares Cruzes [1], Michael Felderer[2], Tosin Daniel Oyetoyan[3], Matthias Gander[4], Irdin Pekaric[5]

Abstract: This summary refers to the paper 'How is security testing done in agile teams? A cross-case analysis of four software teams' [Cr17]. The paper was published as a full research paper in the proceedings of the 18th International Conference on Agile Software Development (XP 2017). It presents a multiple case study on how security testing is done in agile teams.

Keywords: Security testing; agile processes; agile testing; case study research; software testing; software processes; software security

1 Overview

In agile software development, there is a focus on the feature implementation and delivery of value to the customer. Therefore, non-functional aspects like security are often neglected. This holds for software constructions and even more for testing in agile teams. Security testing [Fe16a] can broadly be described as (1) the testing of security requirements that concerns confidentiality, integrity, availability, authentication, authorization, non-repudiation and (2) the testing of the software to validate how much it can withstand an attack. It is challenging for agile teams to systematically apply security testing in their development processes. There is in general a lack of systematic approaches and guidelines for agile security testing as well as of related empirical studies in real-world projects on agile security testing. The paper 'How is security testing done in agile teams? A cross-case analysis of four software teams' fills this gap and for the first time provides a multiple case study on security testing in agile projects based on four agile teams, two in Austria and two in Norway. We investigated how the security engineering process is managed/organized in agile teams, how security testing is performed in each testing phase, and how security testing techniques are generally used in the secure software development lifecycle. The main contribution of this paper is to deepen relevant knowledge and experience on the characterization of security testing in an agile context and to derive respective recommendations.

[1] SINTEF Digital, Trondheim, Norway danielac@sintef.no
[2] Universität Innsbruck, Innsbruck, Austria michael.felderer@uibk.ac.at
[3] SINTEF Digital, Trondheim, Norway tosin.oyetoyan@sintef.no
[4] Universität Innsbruck, Innsbruck, Austria matthias.gander@uibk.ac.at
[5] Universität Innsbruck, Innsbruck, Austria irdin.pekaric@uibk.ac.at

doi:10.18420/se2019-40

2 Results

The findings from investigating four agile teams show a lack of knowledge on security by agile teams in general, a large dependency on incidental penetration testers, and the ignorance of static testing of security. These are clear indicators that security testing is highly under-addressed and that more efforts should be invested for more proper security testing in agile teams. Although the study is based only on the insights of a limited amount of agile teams, we could derive recommendations for research and practice. Software engineering research can help to increase knowledge and application of security testing in several respects. First, knowledge can be increased by the development of suitable courses and guidelines based on empirical evidence showing which approaches work in which context. Then, with regard to model-based security testing [Fe16b], lightweight approaches are needed. Finally, also for penetration testing and security risk assessment suitable automation support and innovative techniques are required. In software development practice, there is a need to better use guidelines for secure coding and testing like from the OWASP. Within teams, there should be more systematic approaches of spreading knowledge in general and integrating static security analysis and penetration testing in particular. Furthermore, project owners should have more security awareness and take security issues into account when refining, prioritizing and validating the product backlog.

3 Conclusion

We summarized the paper 'How is security testing done in agile teams? A cross-case analysis of four software teams' [Cr17] that was published as a full research paper in the proceedings of the 18th International Conference on Agile Software Development (XP 2017). It presents a multiple case study on how security testing is done in agile teams. In the future, we plan to replicate this study and to develop and evaluate suitable security testing approaches to support the adoption of security testing in agile teams through action research studies with industry.

References

[Cr17] Cruzes, Daniela Soares; Felderer, Michael; Oyetoyan, Tosin Daniel; Gander, Matthias; Pekaric, Irdin: How is security testing done in agile teams? a cross-case analysis of four software teams. In: International Conference on Agile Software Development. Springer, pp. 201–216, 2017.

[Fe16a] Felderer, Michael; Büchler, Matthias; Johns, Martin; Brucker, Achim D; Breu, Ruth; Pretschner, Alexander: Security testing: A survey. In: Advances in Computers, volume 101, pp. 1–51. Elsevier, 2016.

[Fe16b] Felderer, Michael; Zech, Philipp; Breu, Ruth; Büchler, Matthias; Pretschner, Alexander: Model-based security testing: a taxonomy and systematic classification. Software Testing, Verification and Reliability, 26(2):119–148, 2016.