

Can We use Authentic Learning to Educate Students About Secure Infrastructure as Code Development?

Akond Rahman^{*}, Shazibul Islam Shamim^β, Hossain Shahriar^δ, Fan Wu^α
akond.rahman.buet@gmail.com, mshamim42@tntech.edu, hshahria@kennesaw.edu, fwu@tuskegee.edu
Tennessee Tech University^{*β}, Kennesaw State University^δ, Tuskegee University^α
USA

ABSTRACT

Despite yielding benefits for organizations, infrastructure as code (IaC) scripts are susceptible to security weaknesses, such as hard-coded passwords. Existence of such security weaknesses necessitate integration of education materials related to secure development of IaC scripts. In this preliminary work, we describe our experiences of how application of authentic learning helped students learn about secure development of IaC scripts. Our paper shows education materials based on authentic learning to help students learn about secure IaC development.

CCS CONCEPTS

• **Software and its engineering** → *Empirical software validation.*

KEYWORDS

devops, devsecops, infrastructure as code

ACM Reference Format:

Akond Rahman^{*}, Shazibul Islam Shamim^β, Hossain Shahriar^δ, Fan Wu^α. 2022. Can We use Authentic Learning to Educate Students About Secure Infrastructure as Code Development? . In *Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol 2 (ITiCSE 2022)*, July 8–13, 2022, Dublin, Ireland. ACM, New York, NY, USA, 1 page. <https://doi.org/10.1145/XXXXXX.XXXXXX>

1 CONTENT

Infrastructure as code (IaC) is the practice of automatically provisioning computing infrastructure, such as Amazon EC2 instances, at scale [3]. Despite reported benefits, such as reduction in provisioning time, IaC scripts developed by practitioners are susceptible to contain security weaknesses, such as hard-coded passwords and use of weak cryptography algorithms [3]. For example, Rahman et al. [3] reported 67,801 occurrences of security weaknesses in open source software (OSS) IaC scripts that included 9,175 hard-coded passwords. The existence of such security weaknesses necessitate integration of security into IaC development in order to reliably deploy software to end-users.

In this preliminary work, we report our experience of using authentic learning [1] to educate students about IaC-related security

weaknesses. Authentic learning emphasizes on exposing students to real-world problem-based activities [1]. We take motivation from prior work, which has reported authentic learning to be effective in engaging students in web security-related courses [2]. As part of applying authentic learning we *first conduct concept dissemination with pre-lab content*, where we discussed what Ansible is, and how Ansible scripts can be parsed using the ‘pyyaml’ utility. *Second, we conduct a hands-on exercise*, on how a hard-coded password in Ansible script can be identified. *Finally, we assign a post-lab exercise* where students are asked to identify security weaknesses in multiple Ansible scripts automatically with static analysis. The exercise was designed and deployed for the ‘Software and Systems Security’ course at Tennessee Tech University in Fall 2021.

Student Feedback: Upon completion of the exercise, we sought feedback from the students using a survey questionnaire. Of the 33 students in the course, 23 responded. Amongst the 23 students, 78% reported to gain knowledge on static program analysis, as shown in the ‘STATIC_ANALYSIS’ row of Figure 1. Also, 73% of the 23 students reported to gain knowledge about secure IaC development, as shown in the ‘SECURITY’ row. Overall, results from Figure 1 show our authentic learning-based exercise to help students learn about secure IaC development.

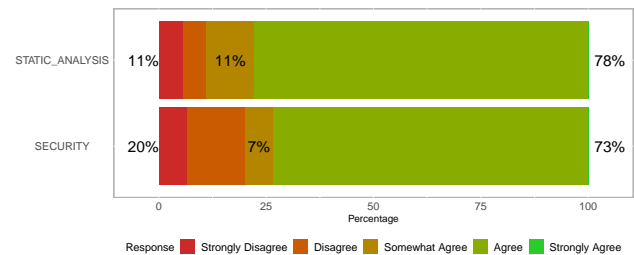


Figure 1: Summary of student feedback

ACKNOWLEDGMENTS

This research was partially funded by the U.S. National Science Foundation (NSF) award # 2026869.

REFERENCES

- [1] Faith W Maina. 2004. Authentic learning: Perspectives from contemporary educators. (2004).
- [2] Kai Qian, Dan Lo, Reza Parizi, Fan Wu, Emmanuel Agu, and Bei-Tsung Chu. 2018. Authentic Learning Secure Software Development (SSD) in Computing Education. In *2018 IEEE Frontiers in Education Conference (FIE)*. 1–9. <https://doi.org/10.1109/FIE.2018.8659217>
- [3] Akond Rahman and Laurie Williams. 2021. Different Kind of Smells: Security Smells in Infrastructure as Code Scripts. *IEEE Security Privacy* 19, 3 (2021), 33–41. <https://doi.org/10.1109/MSEC.2021.3065190>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ITiCSE 2022, July 8–13, 2022, Dublin, Ireland.

© 2022 Association for Computing Machinery.

ACM ISBN 978-1-4503-9200-6/22/07...\$15.00

<https://doi.org/10.1145/XXXXXX.XXXXXX>