
Mst Shapna Akter
msa46@uwf.edu
Department of Intelligence and Robotics Systems
University of West Florida, USA.

Hossain Shahriar
hshahriar@uwf.edu
Center of Cybersecurity
University of West Florida, USA.

Juanjose Rodriguez-Cardenas
Jrodr225@students.kennesaw.edu
Institute for Cyber Workforce Development
Kennesaw State University, USA.

Md Mostafizur Rahman
md.mostafizur.rn@gmail.com
Department of Information Technology
Kennesaw State University, USA

Akond Rahman
Akond@auburn.edu
Department of Computer Science and Software Engineering
Auburn University, USA.

Fan Wu
fwu@tuskegee.edu
Department of Computer Science
Tuskegee University, USA

Abstract

The field of DevOps security education necessitates innovative approaches to effectively address the ever-evolving challenges of cybersecurity. Adopting a student-centered approach, there is the need for the design and development of a comprehensive set of hands-on learning modules. In this paper, we introduce hands-on learning modules that enable learners to be familiar with identifying known security weaknesses, based on taint tracking to accurately pinpoint vulnerable code. To cultivate an engaging and motivating learning environment, our hands-on approach includes a pre-lab, hands-on and post-lab sections. They all provide introduction to specific DevOps topics and software security problems at
手，后由实践与现实世界代码例程有安全问题使用工具。初步评估结果自数门课程在多所学校显示，手上的模块充实利益学生对软件安全和网络安全，而准备他们来解决DevOps安全脆弱。

**Keywords:** DevOps安全教育，污点追踪，Bandit，脆弱性，真实学习。

### 1. INTRODUCTION

安全脆弱性是类型bug，它能攻击或利用计算机系统，程序，或移动和网络应用（Akter, Faruk, Anjum, Masum, Shahriar, Sakib, Rahman, Wu & Cuz, 2022）。DevOps是实践交付和管理软件，代码，基础设施和资源，高效率，根据组织的需要。DevOps安全脆弱性可以采取多种形式，包括设计漏洞，程序错误，或不正确的配置，而且能引起未经授权访问，数据流失，或服务中断。如果一个安全脆弱存在系统或应用程序，它可能被害有恶意行为者利用未经授权访问或系统行为，用户知识或同意（Akter, Shahriar & Bhuiya, 2023）。这些脆弱性可能从各种源出现，如不安全编码实践，弱认证机制，或输入不正确。因此，识别和解决安全脆弱性是至关重要，来保证整体安全性和计算机系统的可恢复。

污点追踪是识别漏洞或脆弱性更精确的一个有效方法。手上的追踪是跟踪特定数据输入作为它们进入系统，开发人员可以追踪它在系统中的传播和行为，与不同组件。这也为识别潜在安全问题或脆弱性提供了一个基础，可能被恶意行为者利用。

污点追踪提供有价值的洞察，了解数据在系统中被处理，操纵，而且可能被误用，使开发者能够更准确地识别和解决脆弱性。通过将污点追踪技术应用在安全分析过程中，学生可以学习如何检测和修复bug或脆弱性。污点追踪提供了一种更准确、更全面的安全评估方法，确保了潜在的安全风险。

在本文中，我们介绍手上学习模块，让学习者熟悉识别已知安全弱点，基于污点追踪准确识别脆弱代码。我们介绍各种步骤用于自动化检测安全弱点在Python代码。初步评估结果自数门课程在多所学校显示，手上的模块充实利益学生对软件安全和网络安全，而准备他们来解决DevOps安全脆弱。

手上的学习是教育领域中的一个广泛接受方法。它围绕学习者自我中心策略，促进互动，让学生主动参与，建立知识。Hand-on learning approach based on realistic scenarios closely resemble real-world examples (Herreid, 2007). In order to equip students with essential skills through practical experiences in addressing real-world security challenges, hand-on learning employs a distinctive hand-on methodology that comprises pre-lab, lab, and post-lab activities (Akter, Shahriar, Ahamed, Gupta, Rahman, Mohamed, Rahman, & Wu, 2023).

The proposed hand-on learning approach consists of the following steps (Figure 1 provides visual representations):

Step 1: Initiate /Understand the topic through Pre-Lab Instructions.

Step 2: Engage/analyze problems through hands-on lab activities involving real-life issues.

Step 3: Optimize the solutions obtained from the hands-on lab using various approaches.

Step 4: Repeat steps 1-3 with different algorithms or datasets.

Many institutions offer courses on cybersecurity in their curriculum. However, these courses often lack sufficient learning materials around DevOps security. DevOps is a software development approach that combines development (Dev) and operations (Ops) teams to streamline and
automate the software delivery process (Ebert, Gallardo, Hernantes & Serrano, 2016). Development of hands-on lab exercises pose several challenges, including a scarcity of knowledgeable instructors, complex configuration processes, the need for extensive resources and materials, and the commitment to completing all steps. In order to overcome these difficulties, we have developed an open-source, portable, modular, and easy-to-adopt hands-on learning modules for DevOps in the field of cybersecurity.

Our approach is readily available at https://sites.google.com/view/alamose/home?authuser=0 and is structured into 10 learning modules, each consisting of three parts: Pre-lab, hands-on lab, and post-lab activities. These modules cover a wide range of topics related to DevOps and cybersecurity, including an Installation Overview (M0), Automated Requirements Validation (M1), Automated Detection of Known Security Weaknesses (M2), Automated Taint Tracking for Accurate Detection (M3), Automated Forensicability (M4), Git Hooks to Facilitate Automated Security Static Analysis (M5), Security Weakness Identification with Continuous Integration (M6), Security Weaknesses in Infrastructure as Code Scripts (M7), Security Weaknesses in Kubernetes Manifests (M8), Chaos Engineering with Whitebox Fuzzing (M9), and Automated Secret Management (M10). These learning modules provide students with comprehensive resources and practical exercises to enhance their knowledge and skills in applying DevOps principles to cybersecurity. By utilizing our open-source approach, students can gain hands-on experience and develop proficiency in addressing real-world security challenges within the DevOps framework.

This paper is organized as follows. Section 2 provides an overview of the related work in the field. Section 3 presents the design of the labware, divided into three parts: Pre-lab, Hands-on lab, and Post-lab. The student learning assessment is discussed in Section 4. Finally, Section 5 concludes the paper and summarizes the key findings and contributions.

2. RELATED WORK

Authentic learning is a teaching approach that immerses students in real-world tasks to develop practical skills and deeper understanding (Herrington & Oliver, 2000). In the realm of software security, authentic learning has gained significant traction in recent times (Qian, Parizi, Wu, Agu & Chu, 2018)(Lo, Qian, Chen, Shahriar & Clincy, 2014). For instance, Rahman et al. (Rahman, Shamim, Shahriar & Wu, 2022) utilized a learning platform to educate students on secure infrastructure-as-code development, while Lo et al. (Lo, Shahriar, Qian, Whitman, Wu & Thomas, 2022) pioneered authentic learning in the context of machine learning in cybersecurity, integrating portable hands-on labware.

From the literature review we have found that several studies have implemented case study-based (Akter, Shahriar, Ahmed, Gupta. Rahman, Mohamed, Rahman, Rahman & Wu, 2023), project-based, and authentic learning approaches in various disciplines, including cybersecurity and software engineering. For instance, Deng et al. (Deng, Lu, Huang, Chung & Lin, 2019) implemented a case-study-based learning approach for machine learning-based hands-on-lab exercises in cybersecurity. Similarly, Blanken et al. (Webb, Palmer, Deshaies, Burbules, Campbell & Bashir, 2018) performed a case-study-based module to engage learners in ethical dilemmas in cybersecurity, while Garg et al. (Garg & Varma, 2007) compared case study-based and lecture-based approaches in software engineering research. Frontera et al. (Frontera & Rodríguez-Seda, 2020) followed a project-based learning framework to evaluate cyber-attacks on a cyber-physical system, and Huang et al. (Huang, 2019) integrated applied machine learning technology.
with project-based learning in engineering programs.

In addition, Lo et al. (Lo, Qian, Chen, Shahriar & Clincy, 2014) conducted an authentic learning project in the field of cybersecurity, involving students in solving real-world cybersecurity challenges. Faruk et al. (Faruk, Masum, Shahriar, Qian & Lo, 2022) focused on the implementation of authentic learning in ML for cybersecurity, developing learning modules with hands-on activities for solving security problems. Qian et al. (Qian, Parizi, Wu, Agu & Chu, 2018) implemented an authentic learning approach in secure software development, providing students with hands-on laboratory practice in secure mobile app development.

Figure 3 shows the statistical trends of the percentage of web applications that contain high risk vulnerability from 2015 to 2019. It shows the high risk vulnerabilities fall significantly by 20% compared to that in 2015 [23].

Despite the valuable contributions of these studies, it is worth noting that none of them specifically addressed DevOps security education. While case study-based, project-based, and authentic learning approaches have been implemented in various disciplines, there is a gap in the literature regarding the application of these approaches in the context of DevOps security education. Therefore, our work fills this gap by developing authentic learning modules specifically tailored for DevOps security education.

3. LABWARE DESIGN

Portable labware has been developed, designed, and deployed on the open-source environment GitHub. This environment allows users to access and share resources from anywhere and at any time without installation and maintenance hassles. As a result, learners can collaboratively interact with their peers, practice, and run all modules. Each of our hands-on labware modules is developed using vulnerable codes. The structure of these modules comprises three components: a pre-lab section covering basic knowledge, a hands-on lab section providing in-depth explanations of experiments, and a post-lab section offering instructions for further optimizations.

Pre-Lab
The Pre-Lab outlines DevOps solutions to software security, including prevention and detection, and introduces a specific software security study scenario with the root causes of security threats, attack plans, and their effects. Students can gain perspective and insight by observing a simplified "hello world" example for the software security case and its corresponding DevOps solution. This prepares students with a specific software security case for conceptual understanding and provides them with a starting point to experience DevOps solutions for such software security cases. By utilizing the DevOps technique, it helps students develop a fundamental understanding of why these software security vulnerabilities need to be addressed. Figure 3 shows a screenshot of the Pre-Lab for Module 2's Automated Detection of Known Security Weaknesses.

Hands-on Lab
The open-source GitHub platform, which is an in-browser environment accompanied by a free Google Cloud service, is utilized for designing, creating, and deploying the hands-on activity laboratories. Upon completion of the practical activity lab, students will gain valuable first hand experience in problem-solving. Students can further enhance their understanding by utilizing visual cues and screenshots provided for each stage.

©2023 ISCAP (Information Systems and Computing Academic Professionals)
Post-Lab
Students are encouraged to use their newly acquired knowledge and skills to address actual problems in the Post add-on lab. It encourages critical reflection on the provided example and practical application for improving problem-solving, such as raising the prediction and detection accuracy rate with new innovative concepts and active testing and experiments. Students can share their original work with others in the Colab. Colab, short for Google Colaboratory (https://colab.research.google.com), is an online platform that provides free access to a Jupyter notebook environment along with GPU support, enabling users to write, share, and run code collaboratively (Bisong & Bisong, 2019).

IV. STUDENT LEARNING ASSESSMENT
We implemented the module in three schools during spring 2023. A preliminary survey collected from a total of seventy-two undergraduate Engineering students at Kennesaw State University, Auburn University, Tuskegee University. Surveys are represented in quantitative and qualitative views. We conducted both a prelab and post-lab survey, where we asked various questions.

It’s easy to fall into a technology-first approach when thinking about analytics. A common cause of failed analytics projects is not the wrong tools.

Pre-Lab Survey:
Among the 74 students surveyed, the majority (55) considered themselves to be in the age group between 18 and 25 years. A few of them (16) fell into the age group between 26 and 35, two of them between 36 and 45, and one of them between 46 and 55. We asked the participants to describe their level of education in the field of DevOps Security in Figure 4.

Additionally, we inquired about their preferences regarding (a) project-based lab work versus listening to lectures, (b) personally doing or working through examples, and (c) having a learning/tutorial system that provides feedback. The responses from prelab survey are displayed in Figures 4 and 5.

In Fig 4, we posed four questions: (a) Which course are you enrolled in? (b) What is your gender? (c) What is your race? And (d) Do real-world relevant applications engage your learning in cybersecurity? For question (a), 25 participants were enrolled in Programming I and II at Tuskegee University, 10 in IT 4823 – Information Security Concepts, 7 in Physical IT System Security at KSU, 2 in Data Analytics, and 2 in IT 6413 at KSU. All the participants come from a STEM (Science, Technology, Engineering, and Mathematics) background, indicating they have a foundational knowledge of technology. For question (b), 44 participants responded as male, while 30 participants responded as female. For question (c), 44 participants identified themselves as African American, 21 as Asian, and 5 as white. For question (d), 34 participants agreed, 12 strongly agreed, and 12 were neutral.

In Fig 5, three questions are presented: (a) “I learn better by listening to lectures.” (b) “Please indicate the extent to which you have received education in the following areas based on the given scale: i. DevOps Security or IaC security, ii. Software Engineering, iii. Software Cybersecurity.” (c) “For each of the following statements, indicate the extent to which you agree or disagree: i. I learn better by engaging in hands-on lab work, ii. I learn better by listening to lectures, iii. I learn better by personally doing or working through examples, iv. I learn better by reading the material on my own, v. I learn better by having a learning/tutorial system that provides feedback.” For question (a), most respondents indicated they had no experience in programming languages (35 to 40 participants).

A few had “limited or moderate experience, 5 to 10 had good experience, and none identified as expert programmers. For question (b), most participants reported having no education in DevOps security, while only a few had experience in Software Engineering and Software Cybersecurity. For question (c), the majority of participants strongly agreed with statements I, iii, and v.

<table>
<thead>
<tr>
<th>#</th>
<th>Answer</th>
<th>%</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt; 18 years</td>
<td>0.00%</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Between 18 and 25 years</td>
<td>74.32%</td>
<td>55</td>
</tr>
<tr>
<td>3</td>
<td>Between 26 and 35 years</td>
<td>21.62%</td>
<td>16</td>
</tr>
<tr>
<td>4</td>
<td>Between 36 and 45 years</td>
<td>2.70%</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Between 46 and 55 years</td>
<td>1.35%</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>&gt; 55 years</td>
<td>0.00%</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1: Display the responses of students on age group
**Post-Test Survey:**

We asked students if the tutorials in the pre-lab helped them understand more about the topics; in a post-test survey we completed it after involvement in the practical lab. Figures 6 and 7 display the responses.

In Figure 6, feedback on the secure DevOps materials revealed a predominantly positive response. For the statement, "I like being able to work with the secure DevOps hands-on materials," 28 participants agreed, 14 strongly agreed, 18 were neutral, 1 disagreed, and 1 strongly disagreed. For the statement, "The tutorials help me learn more on the topic," 34 agreed, 10 strongly agreed, 16 remained neutral, and 5 disagreed. For the statement, "hands-on labs help in understanding DevOps security better," 32 agreed, 12 strongly agreed, 16 were neutral, and 5 disagreed. For the statement, "The hands-on labs enhance my learning on secure DevOps coding and best practices," 32 participants agreed, 14 strongly agreed, 16 were neutral, and 2 disagreed.

In Figure 7, the feedback on the secure DevOps materials indicated an overall positive sentiment. For the statement "The real-world relevant applications engage my learning on cybersecurity," 34 participants agreed, 14 strongly agreed, 14 were neutral, and 1 strongly disagreed. Regarding the assertion, "The learning modules help me apply learned knowledge to solve cybersecurity problems in the future," 32 participants agreed, 10 strongly agreed, 15 were neutral, 2 disagreed, and 2 strongly disagreed. In response to "The post-lab motivates and promotes me to continue studying," 29 participants agreed, 10 participants strongly agreed, 17 were neutral, 5 disagreed, and 2 strongly disagreed.

The feedback gathered from students post their engagement with the secure DevOps hands-on materials and real-world relevant applications showcases a notably affirmative inclination towards the efficacy and impact of these materials. As seen in Figure 6, a significant majority of the participants acknowledged the value of the secure DevOps materials, particularly in aiding their understanding of the subject matter. A standout observation is that more than 80% of the participants either agreed or strongly agreed that the hands-on labs and tutorials were beneficial to their learning, especially in the realm of secure DevOps coding best practices and understanding DevOps security.

In Figure 7, the sentiment continues to be positive, underscoring the relevance and effectiveness of the provided materials. A substantial 48 out of 74 participants (over 70%) agreed or strongly agreed that real-world applications enhanced their cybersecurity learning. Similarly, a combined total of 42 participants confirmed the efficacy of the learning modules in applying their acquired knowledge to future cybersecurity challenges. The post-lab feedback also suggests that the lab experience serves as a motivational tool, with a majority expressing that it encourages them to delve deeper into their studies. online. Five questions to assess students’ learning are included and the responses were collected using the Likert scale that uses a 5-point scale, 1 (Highly disagree) to 5 (Highly agree).

These findings emphasize the crucial role of practical hands-on materials and real-world applications in fostering an enriched and engaged learning experience for students, enhancing not only their comprehension but also their enthusiasm to continue their studies in the field of cybersecurity and DevOps.
Figure 4: (a), (b), (c), and (d) display the responses from the pre-survey questions.
Figure 5: Figure (a), (b), and (c) displays the responses from the pre-survey questions.

The survey results show that students are interested in learning by doing, and the plugin-based tool helps student learn developing secure mobile applications. Fig. 6: Figure (a), (b), (c), and (d) displays the responses from the post-survey questions.

Figure 6: Feedback on the Secure DevOps materials

Q7. Please indicate the extent to which you have received education in the following areas on the scale indicated:

Q2. The outline tutorials in the pre-lab help me learn more on the topics

Q1. I like being able to work with the secure DevOps hands-on materials.

Q3. The hands-on labs help me understand better on DevOps security.
Figure 7: (a), (b), and (c) displays the responses from the post-survey questions.

5. CONCLUSION

This labware aims to address the challenges and requirements of learning DevOps for security by utilizing effective and engaging authentic learning techniques, as well as filling the gap in pedagogical resources and hands-on learning environments. The project introduces a novel teaching approach that utilizes DevOps to proactively resolve security issues. Based on preliminary feedback, students not only grasp the concepts but also practice the skills through the hands-on labs.

ACKNOWLEDGEMENT

The work is supported by the National Science Foundation under NSF Award #2100134, #2100115, #2209638, #2209637, #1663350, #2310179. Any opinions, findings, recommendations, expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES


M. S. Akter, H. Shahriar, and Z. A. Bhuiya, “Automated vulnerability detection in source code using quantum natural language processing,” in Ubiquitous Security: Second


