Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21602605

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Review Article

Volume-06|Issue-04|2026

Using OWASP Juice Shop in Cybersecurity Education: A Literature Review

Sarah Rukhmuddin Rajgoli[1], Niharika Prasanna Kumar[2], Aditya Prakash[3], Shresth Modi[4], Yashash Mathur[5], Utsav Upadhyay[6]

[1,2,3,4,5,6]Department of Information Science and Engineering, RV Institute of Technology and Management, Bengaluru, India

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
Rajgoli, S. R., Kumar, N. P., Prakash, A., Modi, S., Mathur, Y., Upadhyay, U. (2026). Using OWASP Juice Shop in Cybersecurity Education: A Literature Review. *Indiana Journal of Multidisciplinary Research, 6*(4), 225-230.

Abstract: Hands-on experience is essential in cybersecurity education. Without it, students learn the vocabulary but not the practical skills. OWASP Juice Shop is an intentionally vulnerable web application that enables learners to practice real-world attack techniques—such as SQL injection, broken authentication, and Cross-Site Scripting (XSS)—without affecting live production systems. This review examines how Juice Shop has been incorporated into university courses, Capture the Flag (CTF) competitions, capstone projects, and hybrid learning environments. Drawing upon published studies, it evaluates what educational practices improve learning outcomes and which approaches are less effective. Existing research indicates that students generally demonstrate greater engagement, improved practical understanding, and better knowledge retention. However, integrating an open-ended penetration testing platform into a structured academic curriculum remains challenging, and not every implementation has produced consistent success. This review identifies effective practices, highlights current research gaps, and outlines future directions for cybersecurity education research.

Keywords: OWASP Juice Shop, cybersecurity education, hands-on learning, vulnerable web applications, web application security, gamified learning, Capture the Flag (CTF), blended learning, pedagogical strategies.

INTRODUCTION

Cybersecurity education continues to face a significant gap between theoretical instruction and practical skill development. Universities typically emphasize concepts such as threat models, attack taxonomies, and secure software design principles, yet many graduates enter industry without the ability to perform basic penetration testing or analyze web application vulnerabilities effectively. This challenge has been repeatedly documented in previous studies [1]–[3]. Although the disparity between academic curricula and industry expectations is well recognized, many educational programs still rely heavily on lectures and textbook-based exercises [15], [18].

Experiential learning addresses this limitation. When students interact with a genuinely vulnerable application rather than merely studying theoretical examples, they develop both technical competence and practical problem-solving abilities that traditional classroom instruction cannot provide [12], [20]. **OWASP Juice Shop** was specifically developed to support this learning approach. It is an intentionally vulnerable e-commerce application containing SQL injection vulnerabilities, authentication bypasses, and more than eighty challenges aligned with the **OWASP Top Ten**. The platform runs locally using Docker and can be easily reset whenever required [4], [11]. Unlike earlier educational platforms, Juice Shop utilizes a modern technology stack—including Angular, Node.js, and SQLite—that closely reflects contemporary industrial web applications [24], [25]. This review consolidates findings from existing studies to examine how Juice Shop has been integrated into cybersecurity education, what students learn from using it, and where current research remains limited.

MATERIALS AND METHODS

Cybersecurity education has evolved considerably over the past decade; however, the balance between theoretical knowledge and practical application remains a continuing challenge. Passive instructional methods effectively develop conceptual understanding but rarely produce practical cybersecurity skills. Consequently, researchers and educators have increasingly adopted interactive learning environments, among which **OWASP Juice Shop** has become one of the most extensively studied platforms [11], [13], [19], [20].

Traditional Cybersecurity Teaching Methods

Historically, cybersecurity education relied primarily on lectures, textbook case studies, and carefully controlled laboratory exercises where students rarely encountered unexpected situations [1]. Although these approaches successfully teach foundational concepts—and those fundamentals remain important—students educated predominantly through passive learning frequently

***Corresponding Author:** Sarah Rukhmuddin Rajgoli

struggle when confronted with real-world cybersecurity tasks, including vulnerability assessments, incident response, and exploit development [5]. Frameworks such as **SPARTA** advocate competency-based learning that aligns educational exercises with measurable industry skills rather than simply covering theoretical course content [6], [7].

Use of Vulnerable Applications in Education

Purposefully vulnerable applications represented an important advancement in cybersecurity education. **DVWA (Damn Vulnerable Web Application)** provides students with practical exposure to SQL injection and Cross-Site Scripting (XSS) vulnerabilities in a simplified environment, while **WebGoat** introduces insecure design patterns, broken authentication, and access control vulnerabilities [8], [9]. Although both platforms effectively demonstrate specific security flaws, they generally present vulnerabilities in isolation rather than within realistic application workflows. **OWASP Juice Shop** differs by embedding vulnerabilities within a fully functional e-commerce application, requiring students to first understand the application's intended functionality before identifying and exploiting security weaknesses.

Research on OWASP Juice Shop in Training and Academia

Research on **OWASP Juice Shop** has produced largely positive findings. Studies report improvements in students' problem-solving capabilities and threat analysis skills, while its open-source configuration framework enables instructors to customize challenges according to specific learning objectives [14], [15]. Gamification features—including scoreboards, achievement badges, and CTF integration—have consistently been shown to improve student engagement when compared with conventional laboratory environments [12], [13]. Several studies also report positive outcomes regarding professional certification preparation, although the available evidence supporting certification performance is less extensive than the evidence for learner engagement.

Gaps in Existing Studies

Most published research involving Juice Shop has been conducted within individual academic courses or over a single semester, providing limited evidence regarding long-term knowledge retention [13], [14]. Comparative evaluations between Juice Shop and other intentionally vulnerable learning platforms remain relatively scarce [16]. Furthermore, very little research has explored the use of Juice Shop for **AI security**, **secure machine learning**, or **DevSecOps** education, despite these areas becoming increasingly important within modern cybersecurity practice [17]. This review consolidates current knowledge while identifying research questions that remain unanswered.

RESULTS

Architecture and Technology Stack

OWASP Juice Shop is implemented as a **Single Page Application (SPA)** using **Angular** and **Node.js/Express**. The frontend follows **Material Design** principles, while the backend provides a RESTful API supported by **SQLite** and **MarsDB**, enabling students to interact with both SQL and NoSQL database paradigms within a single educational environment [11]. WebSocket-based notifications provide immediate feedback whenever challenges are successfully completed. The complete platform can be deployed using **Docker**, **Vagrant**, **Heroku**, or conventional local installations, providing substantial flexibility for classroom environments [4], [8], [25].

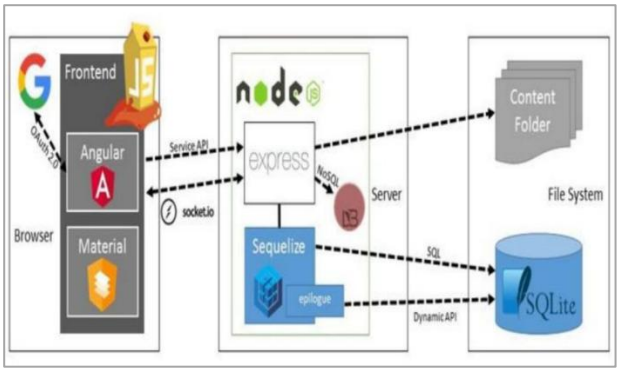

Fig. 1: Architecture Diagram of OWASP Juice Shop

Simulated Real-World Security Issues

OWASP Juice Shop contains more than **eighty-five** security challenges covering SQL injection, Cross-Site Scripting (XSS), broken authentication, security misconfiguration, sensitive data exposure, XML External Entity (XXE) attacks, race conditions, insecure deserialization, and numerous additional vulnerability categories [2], [4]. What distinguishes Juice Shop from platforms such as **DVWA** and **WebGoat** is not merely the range of vulnerabilities provided but the manner in which those vulnerabilities are embedded within a fully functional e-commerce application. Successfully exploiting these weaknesses requires students to first understand the application's legitimate behavior, thereby transforming abstract cybersecurity concepts into realistic problem-solving exercises [5].

***Corresponding Author:** Sarah Rukhmuddin Rajgoli

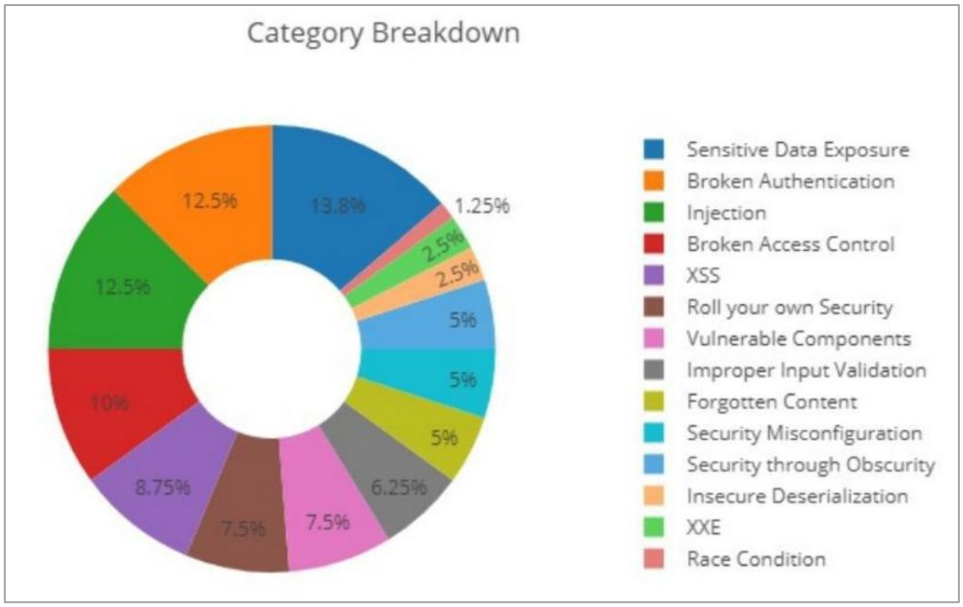

Fig. 2: Vulnerability Categories

Key Technical Features

The integrated scoreboard tracks challenge completion in real time while allowing instructors to filter completed tasks according to vulnerability category and difficulty level. **Capture the Flag (CTF)** mode generates unique flag values for every successfully completed challenge, making competitive cybersecurity events straightforward to organize [6]. Platform components—including branding, product catalogs, and available hints—can be customized through YAML configuration files, allowing instructors to emphasize specific vulnerability categories without unnecessary distractions [3]. A self-healing database reset mechanism automatically restores corrupted environments, which proves particularly valuable when multiple students simultaneously attack the same application instance.

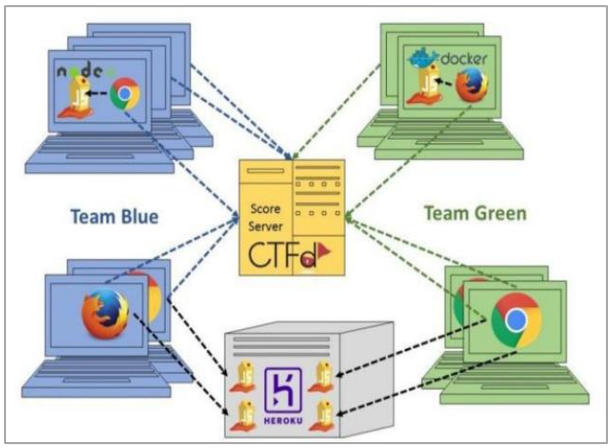

Fig. 3: CTF Mode in OWASP Juice Shop

Lab-Based Learning

Within university cybersecurity courses, **OWASP Juice Shop** is commonly integrated with structured laboratory exercises that guide students toward vulnerability categories aligned with weekly instructional topics—for example, authentication vulnerabilities following lectures on broken authentication or input validation exercises after instruction on Cross-Site Scripting (XSS) [1], [2]. The controlled environment enables students to experiment extensively without risking unintended consequences. Challenge difficulty gradually increases, while the integrated scoreboard enhances student motivation more effectively than conventional worksheet-based activities. Multiple studies consistently report that students completing Juice Shop laboratory exercises perform better on practical cybersecurity assessments and demonstrate greater confidence when performing web application security tasks [3].

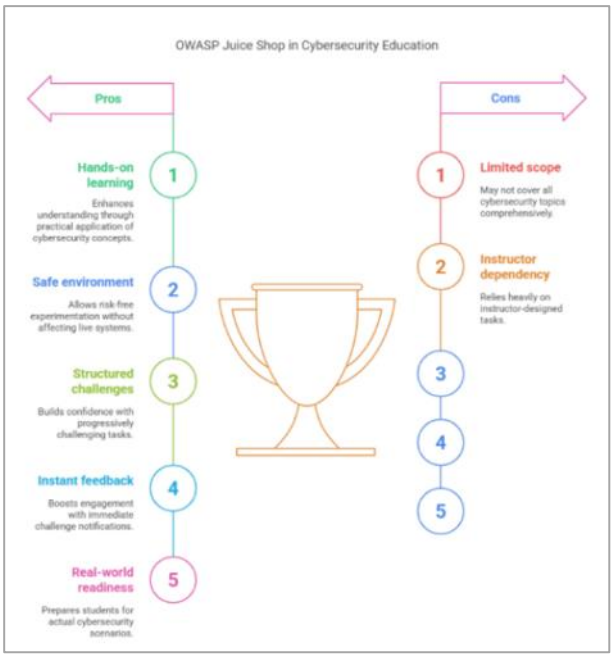

Fig. 4: OWASP Juice Shop in Cybersecurity Education – Pros and Cons

***Corresponding Author:** Sarah Rukhmuddin Rajgoli

Project-Based Learning

Several instructors have adopted a more open-ended instructional approach by providing students with the complete Juice Shop platform and requiring them to conduct comprehensive vulnerability assessments, document identified weaknesses, and propose mitigation strategies with minimal instructional guidance [4]. This project-based methodology encourages independent decision-making regarding assessment scope and vulnerability prioritization, more closely resembling professional penetration testing and cybersecurity consulting practice than structured laboratory exercises. Research evaluating these instructional approaches reports stronger long-term knowledge retention and improved professional preparedness, although such outcomes are inherently more difficult to quantify than traditional laboratory assessment scores [5].

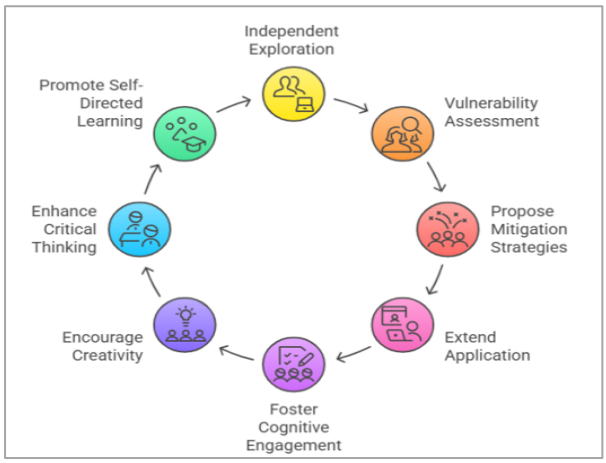

Fig. 5: Project-Based Learning with OWASP Juice Shop

CTF Challenges and Gamification

Juice Shop's **CTF mode** transforms a training platform into a competitive learning environment. Teams solve challenges to collect flags, while a live scoreboard tracks rankings in real time. These competitions develop not only technical skills but also practical habits that traditional static exercises cannot foster—working under time pressure, prioritizing challenges, and collaborating effectively when difficulties arise [6]. Institutions that have organized Juice Shop CTF competitions report higher student satisfaction and, anecdotally, stronger collaboration and community among cybersecurity students [7].

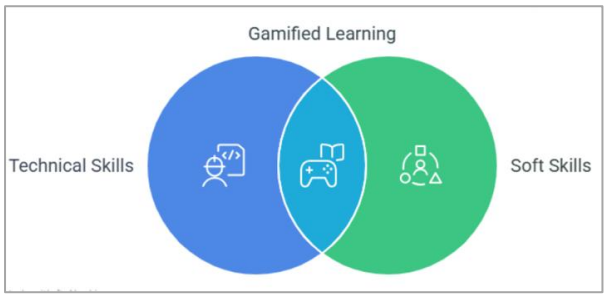

Fig. 6: Enhanced Learning through Gamification

Blended Learning

Juice Shop integrates seamlessly into blended learning environments. A common instructional approach begins with a lecture covering topics such as the **OWASP Top Ten** or **Secure Software Development Lifecycle (SDLC)** security principles, followed immediately by Juice Shop challenges that reinforce the concepts discussed during the lecture [3], [5]. This direct connection between theory and practical application significantly reduces the traditional gap between learning cybersecurity concepts and applying them. The platform supports fully online, hybrid, and face-to-face teaching environments, making it particularly valuable following the widespread changes in course delivery after 2020.

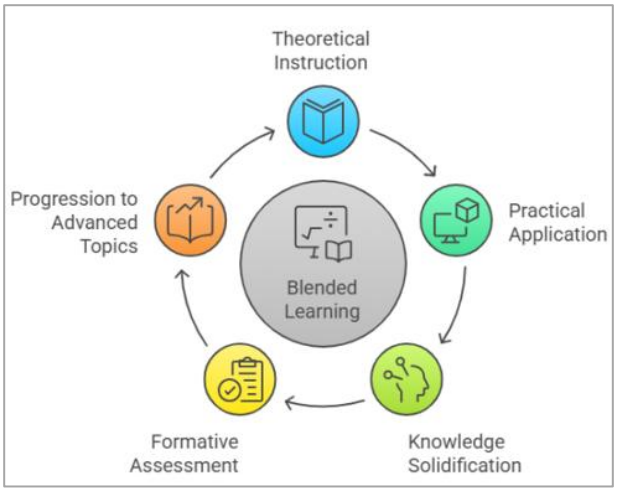

Fig. 7: Blended Learning with Juice Shop

DISCUSSION

Engagement and Skill Development

Student engagement represents one of the strongest arguments supporting the adoption of OWASP Juice Shop in cybersecurity education. Compared with conventional laboratory environments, students using Juice Shop consistently report higher satisfaction, spend more time actively engaged with learning tasks, and demonstrate greater persistence when facing difficult security challenges [1], [2]. Triplett [3] reported a 25% improvement in vulnerability identification accuracy following a sequence of Juice Shop laboratory exercises. Hajny *et al.* [4] documented measurable improvements in both technical proficiency and critical thinking skills. Furthermore, surveys conducted across multiple educational institutions found that more than 80% of participating students reported increased confidence in performing web application security assessments after completing Juice Shop exercises [5], [6].

Comparative Analysis with Traditional Teaching

Students trained using **OWASP Juice Shop** consistently outperform peers taught exclusively through traditional lecture-based instruction on practical penetration testing exercises, secure code review tasks, and security auditing activities. Knowledge retention also appears to improve substantially, with students using intentionally

***Corresponding Author:** Sarah Rukhmuddin Rajgoli

vulnerable applications retaining up to 30% more information three months after course completion than students taught through conventional instructional methods [5], [6]. The underlying explanation is straightforward: actively performing security tasks creates stronger learning experiences than simply hearing or reading about them.

Challenges

Despite its educational advantages, integrating OWASP Juice Shop into academic curricula is more challenging than proponents sometimes acknowledge. The platform's open-ended structure does not always align well with rigid academic schedules or standardized grading systems. Beginner students may encounter advanced topics such as JSON Web Token (JWT) manipulation or Server-Side Request Forgery (SSRF) and experience cognitive overload [4]. Successful deployment also requires appropriate IT infrastructure, and institutions lacking dedicated technical support often face maintenance challenges. A more subtle concern is that students who concentrate exclusively on accumulating scoreboard points may complete numerous challenges without fully understanding the underlying security concepts. Effective mitigation strategies include embedding Juice Shop within structured learning pathways, requiring reflective reports after completing challenges, and employing competency-based educational frameworks such as SPARTA to map each exercise to measurable learning outcomes.

CONCLUSION

OWASP Juice Shop has proven to be an effective educational platform for cybersecurity training. Research consistently demonstrates improvements in student engagement, practical skill development, and knowledge acquisition, while the platform's flexibility enables instructors to adapt it to a wide variety of course levels and instructional formats. However, Juice Shop should not be viewed as a plug-and-play educational solution. Successful implementation requires thoughtful pedagogical design rather than simply deploying the application through Docker. Overall, existing research strongly supports experiential learning with Juice Shop as being more effective than lecture-and-textbook approaches for developing practical cybersecurity skills. Future research should focus on longitudinal studies evaluating long-term knowledge retention, direct comparisons with alternative vulnerable application platforms, and the integration of Juice Shop into emerging educational domains such as **AI security** and **DevSecOps**, where demand for high-quality training platforms continues to grow.

CONFLICT OF INTEREST

The authors declare that they have no financial interests or conflicts of interest.

ACKNOWLEDGEMENTS

The authors would like to thank the faculty of the Department of Information Science and Engineering, RV Institute of Technology and Management, Bengaluru, for their continuous support and encouragement throughout this work.

REFERENCES

1. Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., De Nicola, R. *Framework, Tools and Good Practices for Cybersecurity Curricula.* IEEE Access, **9**, 94723–94747 (2021).
2. Triplett, W. J. *Addressing Cybersecurity Challenges in Education.* International Journal of STEM Education Sustainability, **3**(1), 47–67 (2023).
3. Ismail, M., *et al. Cybersecurity Activities for Education and Curriculum Design: A Survey.* Computers in Human Behavior Reports, **16**, 100501 (2024).
4. Alazmi, S., De Leon, D. C. *A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners.* IEEE Access, **10**, 33200–33219 (2022).
5. Grover, S., Broll, B., Babb, D. *Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula.* In *Proceedings of the ACM SIGCSE Conference* (2023).
6. Wood, R. *DVWA.* GitHub (2021). https://github.com/digininja/DVWA
7. *WebGoat.* GitHub (2020). https://github.com/WebGoat/WebGoat
8. Darojat, E. Z., Sediyono, E., Sembiring, I. *Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP.* Jurnal Sistem Informasi Bisnis, **12**(1), 36–44 (2022).
9. Kingma, D. P., Welling, M. *Auto-Encoding Variational Bayes.* arXiv:1312.6114 (2013).
10. Griets DC. *Pwning – Juice Shop.* https://grietsdc.in/downloads/nasscom161121/pwning%20-%20JuiceShop.pdf (accessed 28 Apr. 2025).
11. Kimak, B., Ellman, J. *OWASP Juice Shop: Implementing Modern Web Security in Educational Environments.* IEEE International Conference on Cyber Security, pp. 1–8 (2022).
12. Legg, P., Mills, A., Johnson, I. *Teaching Offensive and Defensive Cyber Security in Schools Using a Raspberry Pi Cyber Range.* Journal of College Information Systems Security Education, **10**(1), Article 9 (2023).
13. Samonte, M. J. C., *et al. CyLearn: An Assistive Web-Based E-Learning System for Cybersecurity Skills Course.* International Journal of Information and Education Technology, **13**(6), 932–941 (2023).
14. Lee, D., Kim, D., Lee, C., Ahn, M. K., Lee, W. *ICSTASY: An Integrated Cybersecurity Training System for Military Personnel.* IEEE Access, **10**, 62232–62246 (2022).

***Corresponding Author:** Sarah Rukhmuddin Rajgoli

15. Ahmed, A., Watterson, C., Alhashmi, S., Gaber, T. *How Universities Teach Cybersecurity Courses Online.* Frontiers in Computer Science, **6** (2024).
16. Grover, S., Broll, B., Babb, D. *Cybersecurity Education in the Age of AI.* In *Proceedings of the ACM SIGCSE Conference* (2023).
17. Thapaliya, S., Adhikari, D. *The Future of AI in Cybersecurity Education.* International Journal of Multidisciplinary Innovation Research, **2**(4) (2025).
18. Harris, G. *How State Universities Are Addressing the Shortage of Cybersecurity Professionals.* Journal of Cybersecurity Education, Research and Practice, **2024**(1) (2024).
19. Ng, C. Y., Hasan, M. K. B. *Cybersecurity Serious Games Development: A Systematic Review.* Computers & Security, **150**, 104307 (2025).
20. Beuran, R., *et al. Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms.* Computers & Security, **128**, 103120 (2023).
21. Rana, S., Chicone, R. *Revolutionizing Cybersecurity Training.* In *2024 2nd International Conference on iMETA*, pp. 222–237. IEEE (2024).
22. Alnajim, A. M., *et al. Exploring Cybersecurity Education and Training Techniques.* Symmetry, **15**(12), 2175 (2023).
23. Giaretta, A. *Security and Privacy in Virtual Reality: A Literature Survey.* Virtual Reality, **29**, Article 10 (2025).
24. Svabensky, V., *et al. Applications of Educational Data Mining on Cybersecurity Training Data.* Education and Information Technologies, **27**(9), 12179–12212 (2022).
25. Ismail, M., *et al. Cybersecurity Activities for Education and Curriculum Design.* Computers in Human Behavior Reports, **16**, 100501 (2024).
26. Muhusina, I., *et al. Cybersecurity Activities for Education and Curriculum Design.* Computers in Human Behavior Reports, **16**, 100501 (2024).
27. Alhamdani, W. A. *Adopting the Cybersecurity Curriculum Guidelines.* Journal of Cybersecurity Education, Research and Practice, **2019**(1) (2019).
28. Aoyama, D., Yonemura, K., Shiraki, A. *Effective Methods in Cybersecurity Education for Beginners.* In *2024 12th International Conference on Information and Education Technology (ICIET)*, pp. 372–375 (2024).
29. Mierzwa, S. *National Centers of Academic Excellence in Cybersecurity.* Center for Cybersecurity, **5** (2022).

***Corresponding Author:** Sarah Rukhmuddin Rajgoli