Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 25

9-6-2024

# Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning

Thitima Srivatanakul
*York College, City University of New York*, tsrivatanakul@york.cuny.edu



## Recommended Citation

Srivatanakul, Thitima (2024) "Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 25.
DOI: https://doi.org/10.62915/2472-2707.1192
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/25

# Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning


## Abstract

Gamification, including game-based learning (GBL), is a widely recognized pedagogical approach used for imparting and reinforcing cybersecurity knowledge and skills to learners. One innovative form of GBL gaining popularity across various educational levels, from secondary schools to professional development, is escape room-style education. This study is centered on the development and design of escape room activities tailored for teaching cybersecurity concepts, with a particular focus on web and software security, to undergraduate students at York College. The primary objectives of this research are twofold: firstly, to evaluate the effectiveness of educational escape room activities in reinforcing cybersecurity concepts taught in an undergraduate course; and secondly, to assess the potential of educational escape rooms in fostering teamwork and collaboration among undergraduate students.



## Keywords

escape room, cybersecurity, game-based learning, undergraduates, reinforcement, web security


## Cover Page Footnote

N/A

# Designing Cybersecurity Escape Rooms: A Gamified Approach to Undergraduate Learning

Thitima Srivatanakul
Mathematics and Computer Science Department
York College, City University of New York
New York, U.S.A.
tsrivatanakul@york.cuny.edu
https://orcid.org/0000-0002-0361-3377

***Abstract*— Gamification, including game-based learning (GBL), is a widely recognized pedagogical approach used for imparting and reinforcing cybersecurity knowledge and skills to learners. One innovative form of GBL gaining popularity across various educational levels, from secondary schools to professional development, is escape room-style education. This study is centered on the development and design of escape room activities tailored for teaching cybersecurity concepts, with a particular focus on web and software security, to undergraduate students at York College. The primary objectives of this research are twofold: firstly, to evaluate the effectiveness of educational escape room activities in reinforcing cybersecurity concepts taught in an undergraduate course; and secondly, to assess the potential of educational escape rooms in fostering teamwork and collaboration among undergraduate students.**

***Keywords— escape room, cybersecurity, game-based learning, undergraduates, reinforcement, web security***

## I. Introduction

With about 700,000 of cybersecurity positions remaining unfilled in the USA [1] and an estimated workforce gap of four million globally [2], there is a pressing demand for increased cybersecurity awareness, education, and training. For example, over the next decade, employment opportunities for a cybersecurity position such as the information security analysts are forecasted to experience a 32 percent growth, significantly outpacing the average growth rate for all other occupations [3]. As different forms of threats continue to escalate, the responsibility for cybersecurity becomes a shared commitment, involving everyone, not just the technical professions.

Promoting cybersecurity education and training remains a central factor in inspiring the younger workforce to pursue careers in cybersecurity. Different forms of cybersecurity education and training are accessible through diverse channels, encompassing formal settings, informal environments, co-curricular activities, and curriculum integration. However, teaching cybersecurity concepts to learners presents challenges such as the complexity of the material and the need for hands-on experience. The gamification of cybersecurity materials or game-based learning (GBL) addresses these challenges by introducing and reinforcing cybersecurity knowledge and skills to learners in an engaging manner.

Escape room-style education is a GBL approach that has gained popularity in recent years, encompassing various education levels, including secondary school, higher education, professional development, and the general audience.

In this paper, escape room activities were designed and implemented for an undergraduate-level cybersecurity course. The primary goals of this study were to 1) evaluate the effectiveness of educational escape room activities in reinforcing cybersecurity concepts taught in an undergraduate course; and 2) to assess the potential of educational escape rooms in fostering teamwork and collaboration among undergraduate students.

## II. Background On Educational Escape Rooms

Escape Rooms, sometimes referred to as Escape Games, are typically designed for groups of 4 to 6 players. The primary objective is to solve a series of puzzles with the aim of achieving a specific goal, most commonly to 'escape' from a themed room within a given time limit. A popular variant of the traditional escape room is when the game structure is centered on 'breaking in' rather than the traditional 'escaping'. This involves the discovery of correct codes for locked boxes or the solution of digital puzzles to uncover additional clues. The educational escape room, as referenced in the literature, employs themes and puzzles that are relevant to educational settings, designed as learning environments [4].

Escape rooms in education are supported by several learning theories that strengthen their pedagogical grounding. Constructivist Learning Theory [5] suggests that learners build knowledge through experiences, making escape rooms ideal for hands-on learning. Experiential Learning Theory [6], proposed by David Kolb, emphasizes learning through reflection on doing, which escape rooms facilitate by requiring practical application of knowledge. Collaborative Learning Theory [7] highlights the role of social interaction, with escape rooms fostering teamwork and communication. These theories collectively support the effectiveness of escape rooms as educational tools.

This section summarizes the features and characteristics found in typical educational escape rooms.

### *A. Puzzle Types*

Escape rooms feature a variety of puzzle types that challenge participants. *Cipher puzzles* involve deciphering encrypted ciphers to reveal clues or solutions. *Logic puzzles* require deductive reasoning to solve problems. *Pattern recognition*

involves participants recognizing patterns, symbols, and sequences to solve puzzles. *Physical puzzles* necessitate participants to manipulate physical objects to progress, such as assembling jigsaw puzzles or physically searching for hidden clues. *Word puzzles*, such as anagram and crossword-style challenges, and *math puzzles*, where participants must solve mathematical problems to make progress, are also frequently incorporated. *Riddles* are commonly presented in the escape room to encourage creative thinking for solving puzzles.

In recreational escape rooms, puzzles often revolve around general knowledge or theme-based content. In contrast, puzzles in educational escape rooms are intentionally designed to teach and reinforce content knowledge and content-related skills of learners. Here are a few examples of how content knowledge is incorporated into educational escape room puzzles:

- In a physics of fluids experiment, teams were tasked to use three different-sized glasses and surface tension principles to fill, measure, and overflow water to derive a three-digit code [8].
- Clues with names spelled as chemical elements, such as Ni, Co, La, and S, are mapped to the corresponding line numbers in the periodic table to form a four-digit combination. This approach is used to teach the Leblanc process in a chemistry course [9].
- The basics of cryptography are taught using the Caesar cipher mini-game, which helps raise awareness about data protection in cybersecurity [10].
- Use of logical deduction to eliminate the triangles that do not fit the description of the clues. The one remaining triangle provides the code to unlock the next clue, used in teaching mathematical concepts to secondary school students [11].

### *B. Puzzle Structure*

The puzzles are woven together, creating a structured path that allows participants to engage with them as they progress. This path typically falls into two main categories: linear and non-linear.

- **Linear (or sequential) path** - Puzzles are presented one after the other in a sequential manner, as shown in Fig. 1. Successfully solving a puzzle provides participants with a physical object or another clue, which, in turn, allows them to address the next puzzle.

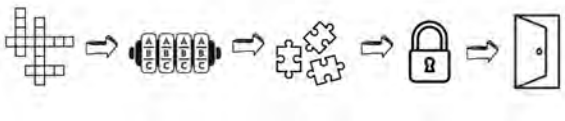

Fig. 1. Linear or sequential puzzle flow

- **Non-linear path –** Puzzles can be presented in parallel, allowing participants to work on multiple puzzles simultaneously or presented all at once for participants to find and solve them in any order. Additionally, some puzzles may be interconnected, meaning that solving one puzzle can initiate another. A single puzzle may require clues from two or more other puzzles to progress. After all the puzzles are solved, the clues will converge to the final puzzle or the meta puzzle, signifying that the participants have successfully 'escaped' the room.

  Fig. 2 shows an example of a non-linear path where three parallel paths lead to the final clue, whereas Fig. 3 shows a more random path with interconnected puzzles leading to the final clue.

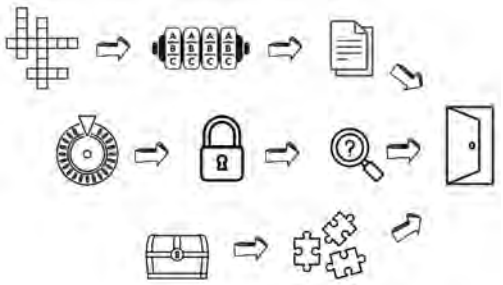

Fig. 2. Non-linear parallel puzzle paths converging to the final clue.

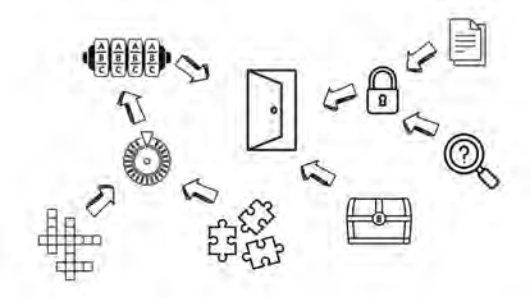

Fig. 3. Non-linear interconnected puzzles leading to the final clue.

When it comes to educational escape rooms, the implementation of paths does not vary significantly. The choice of path depends on the level of difficulty or complexity and the time available.

### *C. Gameplay*

Traditionally, recreational escape rooms are designed for a single group to play in one room at a time. The objective is to 'escape' from the room or successfully retrieve the final object. The usual scenario involves the entire group being locked inside the room, one group at a time. However, with the increasing popularity of escape rooms in various settings, where space and time might be limited, we are now witnessing a wide variety of formats, including those where multiple groups can participate simultaneously [4]. The following is a summary of the gameplay options for escape rooms:

- One Group: In this format, one group plays at a time, in a dedicated room.
- Multi-Groups: Two or more groups play simultaneously. This can be done in different escape rooms or within the same room, running parallel games.
- All Groups: This format provides a larger space (or virtual space) for all groups to participate at the same time.

- Boxes: In this style, all groups use a 'box with a lock,' which contains puzzles for each team. Groups can play simultaneously [4].

While there is limited research available regarding the potential benefits of different gameplay styles, practical considerations, such as limited resources in terms of available rooms and time, often dictate the chosen format, especially in educational settings.

## III. Educational Escape Rooms in Cybersecurity

Escape rooms have found applications in cybersecurity education across various levels and contexts in recent years. For instance, studies illustrated the implementation of the escape rooms to highlight potential risks and vulnerabilities associated with human behavior, focusing on raising employee cybersecurity knowledge and awareness [12, 13]. Oroszi [12] reported that security awareness escape rooms are an effective method for improving information security knowledge and awareness among employees. The study also found that participants were willing to change bad habits highlighted during the escape room activities [12]. The study noted, however, that designing and implementing escape rooms require significant time and effort, which might not be feasible for all organizations. Löffler et al. [13] transformed a physical escape room into a virtual setting, demonstrating that it can be done with minimal adjustments without sacrificing player immersion. However, the virtual format struggled to effectively teach some of the topics effectively such as targeted social engineering attacks.

DeCusatis et al. [10] designed a virtual cybersecurity escape room aimed at raising cybersecurity awareness across a broader audience and age groups. Playtesting with pre-college and college students revealed that the escape room was engaging and effective in enhancing cybersecurity knowledge. The study also identified potential enhancements, such as implementing an achievement system and customizable features to improve the sense of ownership and user engagement. Beguin et al. [14] created "Defend and Attack Scenarios" escape rooms to address vulnerabilities, teaching participants how to both exploit and defend against them, fostering an attacker mindset and helping individuals protect themselves from cyber threats. Their study noted that active participation in escape rooms led to better retention of cybersecurity principles and practices among players. However, one of the limitations is scalability; the escape room format may be difficult to scale for larger groups or institutions, potentially limiting its widespread adoption.

Streiff et al. [15] described the development of escape room challenges to teach cybersecurity technical skills such as Cryptography, Data security, Wireless protocol manipulation, and embedded systems attacks for grades 7 and up. Several others utilized the escape room activities to convey cybersecurity concepts, including cryptography [16] – [18], network security [17, 19] to students at undergraduate level.

While physical escape rooms may present space limitations for accommodating numerous participants, researchers have explored the development of virtual escape rooms to teach cybersecurity topics. For instance, Williams and El-Gayar [20] discussed the development of a virtual cybersecurity escape room as a substitute for physical versions. The aim is to instruct students in subjects such as social engineering, password security, and fundamental computer science concepts, including binary. Deeb and Hickey [18] introduced a computer game where the player's avatar searches for objects, finds clues, and solves a series of cybersecurity-related puzzles to escape a virtual room. Löffler et al. [13] discussed the transformation of a cybersecurity escape room to raise employee awareness into a virtual equivalent, maintaining player immersion. They developed a web-based game prototype for escape rooms, playable individually or in very small teams. Though virtual escape rooms can serve as an alternative when physical presence is restricted, it was observed that team collaboration is somewhat diminished in the virtual escape game experience.

From the literature review, challenges or limitations identified in these studies include the scalability of the escape room format, the significant time and effort required to develop them, and the limited representation of participants, which affects the generalizability of the results. Common topics like cryptography, social engineering attacks, and basic cybersecurity concepts are frequently covered. However, there is still a gap in addressing other crucial cybersecurity areas. Limited research has explored web and software security, despite their prevalence in causing several vulnerabilities and security risks, in the design and development of educational escape rooms in cybersecurity. In this study, the goals are twofold, firstly to evaluate the effectiveness of educational escape room activities in reinforcing cybersecurity concepts, particularly on web and software security, taught in an undergraduate course; and secondly, to assess the potential of educational escape rooms in fostering teamwork and collaboration among undergraduate students.

## IV. Methodology

The study aims to develop and design escape room activities to teach web and software security topics for undergraduate students. The objectives of this study are to discuss whether an educational escape room be used to effectively reinforce the learning materials taught in a cybersecurity class for undergraduate students and if the education escape room can be used to encourage teamwork and promote collaboration of undergraduate students. Thus, the driving questions of this research are:

RQ1: How do students perceive the effectiveness of educational escape rooms in reinforcing cybersecurity concepts taught in an undergraduate course?

RQ2: Can educational escape rooms help in fostering teamwork and collaboration among undergraduate students?

The escape room activities were conducted with undergraduate students enrolled in the 'Web and Software Security Course' in Fall 2023 at York College, CUNY. This course covers fundamental concepts and practical aspects of software and web applications security. The course emphasizes on common weaknesses in software as listed in CWE top 25 and the OWASP top 10 most common vulnerabilities in web applications. Countermeasures against various attacks – such as buffer overflows, cross site scripting, SQL injection and session hijacking are discussed with hands-on exercises and

assignments. The course also covers basic security principles behind the development of software systems. The course also covers both attackers and defender's mindset through exercises and assignments, which helps students to understand the design and implementation flaws that may lead to software security breaches.

The escape room activities were conducted twice during the course. The initial session took place mid-way through the semester, functioning as a pilot study to gather insights for refining the design and implementation of the escape room. The second implementation, conducted towards the end of the course, incorporated feedback from the pilot study and was aimed at directly evaluating the study's research questions.

### *A. Pilot Study*

A pilot study was undertaken to assess the design and development of escape game activities before their full implementation. Escape room puzzles were introduced a week prior to the midterm exam, mid-way through the course, with the aim of evaluating the design and implementation. During the pilot, students were informed that the escape game served as a review tool for the upcoming midterm exam. Twenty-six students participated in the escape room. Following the game, a post-game reflection survey was administered, with 20 students providing feedback, to gather insights on potential improvements to the process. Since the first implementation was conducted half-way through the course, not all the topics from the course were covered. Table I. depicts the learning objectives covered in the pilot study.

TABLE I. LEARNING OBJECTIVES FOR EACH ESCAPE GAME PUZZLE

| **Learning Objectives** | **Escape Game Puzzle** |
|---|---|
| Understanding of CIA Triad and basics cybersecurity terminologies | Mapping terminologies with their description using crossword puzzle. |
| Understanding of symmetric key encryption | Exchanging a secret message between teams using simple symmetric key encryption |
| Understanding of asymmetric key encryption | Exchanging/creating a shared secret key with asymmetric key encryption |
| Understand SQL injection | Answering a set of questions to find the attack |
| Understand Password security – hashed password | Using a pre-computed hashed table to determine the corresponding plaintext password |
| Understand Identification & Authentication Failures | Identifying vulnerabilities and attacks from a list of questions. |

The design of the escape room has a combination of physical and digital puzzles, and it was designed for all students to participate simultaneously to accommodate the time constraint. The physical puzzles were designed for easy setup, involving simple printing, and cutting tasks. Fig. 4 and Fig. 5 illustrate a few examples of the physical puzzles used during the pilot study. Fig. 4 displays two puzzles where members of each group were separated and used the symmetric encryption technique to share their clues. Fig. 5 features a combination of a crossword puzzle and a jigsaw puzzle to reveal the next clue.

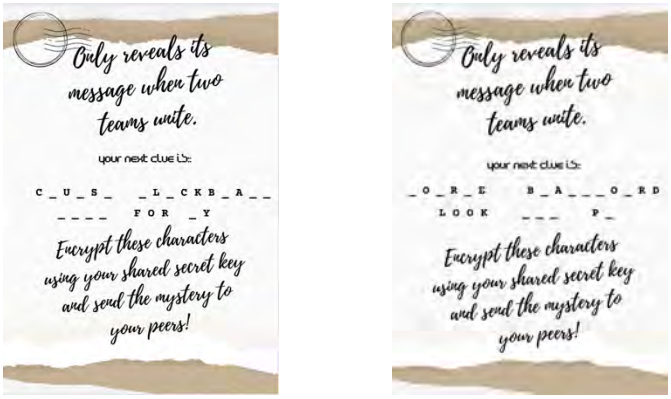


Fig. 4. Symmetric encryption puzzles for team clue sharing.

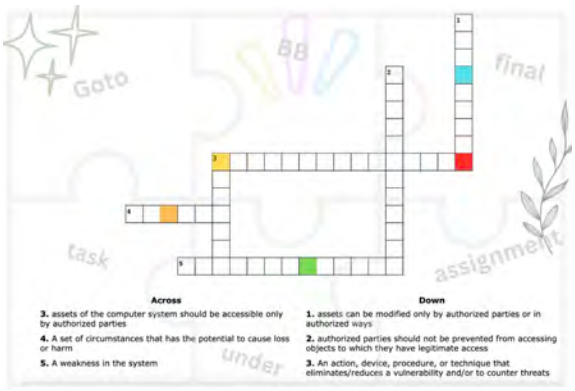


Fig. 5. Crossword and jigsaw puzzle combination for clue progression.

Successfully solving one puzzle provides clues to find others. For instance, solving SQL injection questions leads students to a hashed password, which they later need to determine its corresponding plaintext. Completing a crossword puzzle reveals colored characters that are used to unlock the next clue.

The class of 26 students was divided into seven groups, each consisting of 3-4 students. This is the same group for the semester-long group activities conducted in the class. Five groups successfully solved all the puzzles and reached the final state (escaping the room) within the 60-minute time limit. The remaining two groups were unable to complete the challenge within the allocated time but successfully did so afterward. A debriefing session followed the escape room activity, where the solutions were discussed, and explanations were provided for each puzzle for any questions from the students. Subsequently, a post-survey was conducted to gather students' opinions about their escape room experience.

All participants (100%) strongly agreed or agreed that the educational escape room activities were relevant to the course objectives and effectively promoted teamwork and collaboration among their peers. Moreover, 95% of participants found the escape room engaging and enjoyed the experience. When asked about improvements, a few suggested more time, additional hints, and fewer steps. The majority of students expressed interest in having more escape room activities later in the course.

Valuable insights were gathered from the pilot study, drawing from both the survey results and observations. It was identified that the initial puzzle, involving symmetric and asymmetric encryption, proved to be challenging for most students who have not yet grasp the concept. To enhance engagement and mitigate frustration at the early stage of the game, it is recommended to structure puzzles with increasing complexity, progressing from relatively straightforward challenges to more complex ones in the final stages. The approach is also utilized by [21]. Additionally, providing more time for groups to complete tasks within the set limit and implementing a systematic approach to offering hints were highlighted as important considerations. Encouraging students to review materials before participating in the escape room was also underscored for effective reinforcement of concepts.

### *B. Final Implementation*

The final implementation, which incorporated feedback from the pilot study, took place two weeks before the final exam, covering all the course materials. To ensure the final implementation remained unexpected and engaging, the puzzles were intentionally designed to cover topics different from those explored in the pilot study. For students, this activity served as a comprehensive review of all course materials, providing significant support in their final exam preparations. The detailed design and implementation are discussed in the next section.

## V. Our Escape Games

The design and development of this escape room are guided by Clarke's framework [22], focusing on six main areas: Participation, Objectives, Theme, Puzzles, Equipment, and Evaluation. Each of these areas is elaborated below.

**Participants:** Participants consisted of undergraduate students enrolled in the Web and Software Security course, who had acquired knowledge and skills in cybersecurity through lectures, lab exercises, and course assignments. The game was designed for cooperative play, tailored specifically for groups working together on their course project. It was structured to last approximately 80 minutes, featuring a mix of easy and more challenging puzzles to cater to a range of problem-solving skills, incorporating various puzzle styles.

**Objectives:** The goal is to design the game with intentionality, not merely as an afterthought to an existing game structure [22]. For undergraduate students in the course, the specific objectives were: 1) to reinforce knowledge and skills related to cybersecurity topics and materials covered in class, serving as a review for the final exam, and 2) to promote teamwork and collaboration among the students. The focused learning objectives from the course included in this escape room are:

1) Understand basics cybersecurity terminologies.
2) Demonstrate an understanding of symmetric key usage and proficiency in decrypting messages using a monoalphabetic cipher.
3) Able to read the buffer overflow memory dump
4) Able to craft an input to cause the buffer overflow
5) Able to break the access control by locating the hidden page on a website (insecure direct object references)
6) Understand the Common Vulnerability Scoring System (CVSS) scoring
7) Understand the risk of hard-coded credentials
8) Able to map the specific characteristics to the OWASP top 10

**Theme:** The theme revolves around forming a team to prevent destruction caused by an attacking group. Each puzzle represents a step in halting the breach before time expires. Due to cost and space constraints, the escape room's theme was embodied through the narrative embedded in the puzzles. Physical props were not utilized.

**Puzzles:** Each puzzle was carefully crafted to assess and challenge the students' recently learned cybersecurity knowledge and skills based on the focused learning objectives and featuring various levels of difficulty. Instructions were provided before commencing the escape room activities. A range of activities was implemented to maintain player interest and facilitate the achievement of numerous learning outcomes. The puzzles incorporate a mix of formats and puzzle types, including physical (e.g., jigsaw and crossword puzzles), digital (e.g., instructions in riddle and logical clues) formats, and a web-based escape room application. However, the main flow of the escape room puzzles was directed by the web-based escape room application, WebEsape, which was developed in PHP by the author. It was designed to present a series of puzzles and to offer a customized user interface tailored for each puzzle, thereby providing an interactive experience for the users. Hints were available through two methods: automatically from the web-based system after several unsuccessful attempts, and directly by requesting hints from the instructor. The purpose of offering hints is to avoid participant frustration and maintain positive team dynamics [11].

**Equipment:** The escape room activities were conducted in a classroom equipped with PCs, enabling students to access the web-based escape room application and digital clues. Given the limited space, students worked in groups, utilizing one or two PCs to solve the puzzles. To minimize confusion and enhance the experience, no red herrings were employed in the final implementation.

Fig. 6. Computer lab where the escape room activities took place.

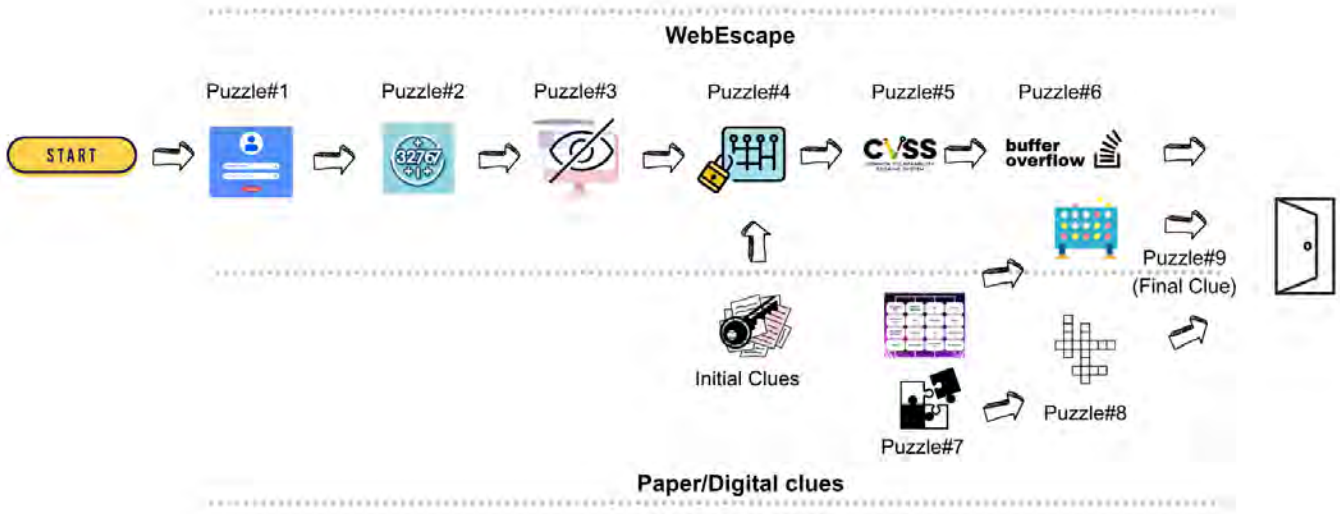


Fig. 7. The flow of the educational escape room, showcasing the paths between paper/digital clues to the WebEscape.

**Evaluation:** Feedback collected from the pilot study was utilized to refine the design and execution of the escape game's final implementation within the course. Additionally, students were asked to complete a 15-minute survey aimed at assessing whether the established learning objectives were met. Following the activity, a debriefing session was organized. During this session, detailed instructions were provided on the strategies for tackling each puzzle, along with explanations to ensure participants understood how each puzzle was linked to the course materials. This session aimed not only to reinforce the educational objectives of the escape room experience but also to offer insights into the practical application of the course content, thereby enhancing the overall learning experience for the students.

## VI. Escape Room Puzzles

Fig. 7 illustrates the visual representation of the flow of the escape room activity. It shows a non-linear path that participants would follow, starting with a welcome page of the WebEscape and initial clues, moving through a series of puzzles that are both digital and physical in nature, and ending with the final goal, represented by a door.

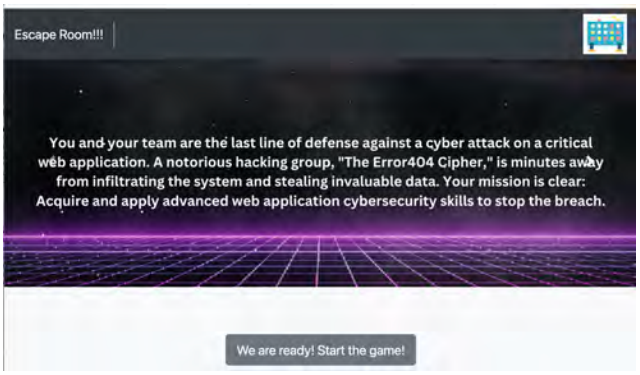


Fig. 8. A welcome message with a mission from WebEscape.

**Game Start:** Students were presented with a mission of the escape game, which is to acquire and apply advanced web application cybersecurity skills to stop a notorious hacking group from infiltrating the system, as shown in Fig. 8. They were also presented to an envelope consisting of clues and puzzles to be used later in combinations with other puzzles, as shown in Fig. 9, depicted as 'Initial Clues' in Fig. 7. Students initiate gameplay and the timer by clicking a button from the WebEscape welcome page.


Fig. 9. Paper clues provided at the start of the game.

**WebEscape Puzzle#1 - Bypassing Authentication:** The first challenge starts with a login page (Fig. 10), where participants must try to gain access. If they enter the wrong username three times, the system offers a clue (Fig. 11). Similarly, if they repeatedly fail at the password entry, another prompt appears, advising them to inspect the source code for hints (Fig. 12). As shown in Fig. 13, the source code inspection reveals the password hidden in comments containing sensitive information. Upon solving this, participants are directed to the next puzzle.

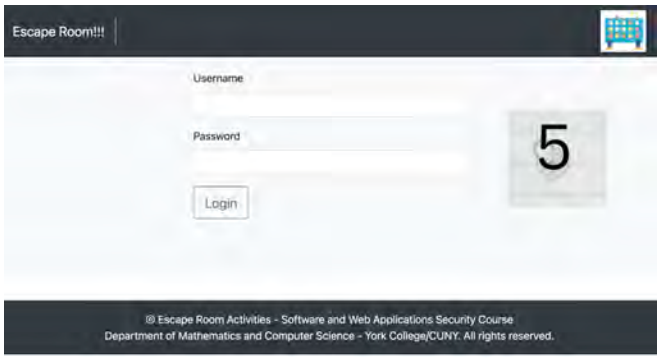


Fig. 10. A login page to bypass authentication.

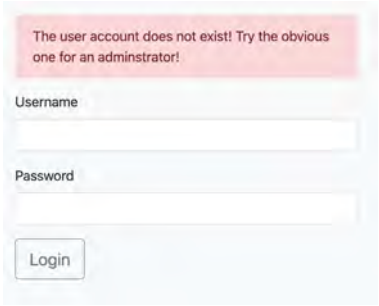


Fig. 11. A clue provided when a wrong username is entered.

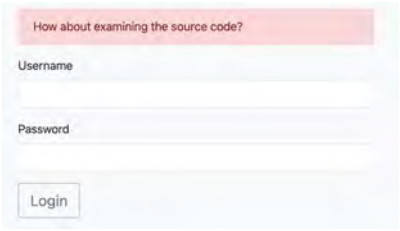


Fig. 12. Another clue provided for multiple failed attempts.

```
<br><br>

<!— admin's password is: 123456789 don't forget to remove—>
<section class="bg-light">
    <div class="container  pt-md-0">
        <div class="row align-items-center">
        <div class="col-md-3" >

</div>
            <div class="col-md-6 my-5 text-center text-md-left">

            <form method="post">
                    <div class="form-group">
                        <label for="username">Username</label>
                        <input  class="form-control" id="username" name="username" >
```

Fig. 13. Source code revealing a hidden password.

**WebEscape Puzzle #2 – Integer Overflow:** Participants face the next challenge in the form of a riddle (Fig. 14), which tasks them with identifying the smallest positive integer that causes an integer overflow in a specified program. The code relevant to this task is accessible via an external link provided to the participants.

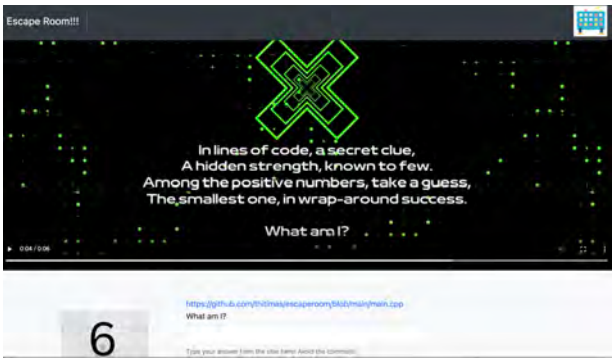


Fig. 14. A riddle designed to test knowledge of integer overflow.

**WebEscape Puzzle #3 – Hidden Page:** Participants receive a clue prompting them to deduce the name of a concealed webpage. To proceed, they must directly navigate to the page using the name they infer, thereby gaining direct access to essential resources. The purpose is to test students understanding of an insecure direct object reference vulnerability. Correctly identifying and visiting the hidden page moves them forward to the next puzzle.

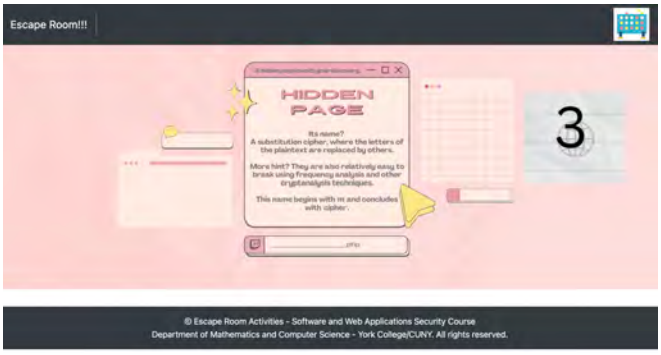


Fig. 15. A clue to test students' understanding of an insecure direct object reference vulnerability (hidden page)

**WebEscape Puzzle #4 – Decrypting Monoalphabetic Ciphertext:** This challenge provides participants with an encrypted message, where the participants need to decrypt it to answer the question to proceed to the next stage. The monoalphabetic key is partially provided, as shown in Fig. 16. The remainder of the key can be assembled from the paper clues provided at different stages of the escape game. As demonstrated in Fig. 17, laying the two clues reveals the rest of the key.


Fig. 16. Clue for a monalphabetic cipher.

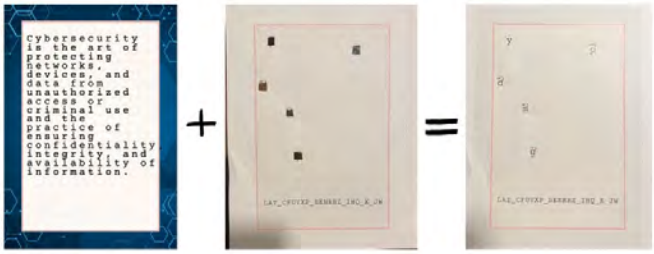


Fig. 17. Two paper puzzles layered on top of each other to reveal missing letters for the key.

**WebEscape Puzzle #5 – Calculating CVSS Scores:** This challenge requires participants to engage with the Common Vulnerability Scoring System (CVSS) by interpreting a provided CVSS vector string. Their task is to analyze the vector string, which describes the properties of a hypothetical security vulnerability, and then calculate and input the correct CVSS scores, as shown in Fig. 18.

This process involves understanding the various components that make up the CVSS vector, such as the level of access required to exploit the vulnerability, the complexity of the attack, and the potential impact on confidentiality, integrity, and availability. By completing this challenge, participants will gain practical experience in assessing cybersecurity risks, using a standardized framework that's critical for identifying and prioritizing system vulnerabilities.


Fig. 18. A puzzle to test students' understanding of the CVSS.

**WebEscape Puzzle #6 – Understanding Buffer Overflow**: This puzzle focusses on the critical concept of buffer overflow, a common vulnerability in software development. Participants are tasked with understanding how a buffer can exceed its allocated space, impacting adjacent memory areas such as the saved EBP (Base Pointer) and the return address within the stack frame. The challenge is to identify the specific word that results in the saved EBP being overwritten, as shown in Fig. 19. To assist in this task, participants are provided with a physical clue: a hexadecimal to character mapping.

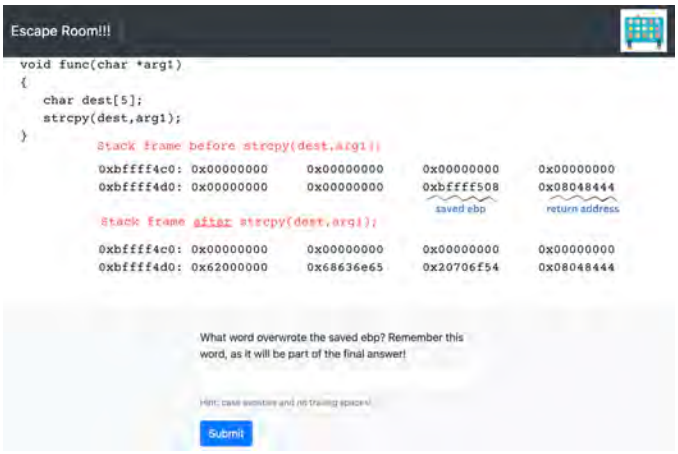


Fig. 19. A puzzle to test students' understanding of buffer overlow.

**Paper Puzzle #7 – Linking Common Terms**: Inspired by the well-known game of Connect 4, this puzzle challenges participants to match course-related terminologies with their corresponding groups, as shown in Fig. 20. Participants must then arrange these terms into a sequence of numbers representing each group. This sequence is entered into WebEscape as one of the three essential clues needed to unlock the final puzzle.


Fig. 20. A paper puzzle of Connect 4.

**Paper Puzzle #8 – Crossword on OWASP Top 10**: This crossword puzzle, as shown in Fig. 21, is designed to be a supplemental activity for participants to engage with alongside the main challenges in WebEscape. It centers on deepening the participants' understanding of the OWASP Top 10. Each crossword clue is a riddle that corresponds to one of the OWASP Top 10 security risks (Fig. 22), prompting participants to apply their knowledge in a fun and interactive format.

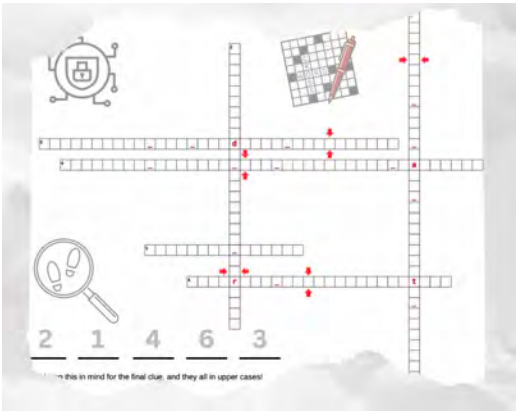


Fig. 21. OWASP Top 10 Crossword puzzle.


Fig. 22. A digital clue for the crossword puzzle.

**WebEscape Puzzle #9 (Final Clue) –** This serves as the culminating challenge of the escape room (Fig. 23). To unlock it, participants must combine the answers derived from three distinct sources: WebEscape Puzzle #6, Paper Puzzle #7, and Paper Puzzle #8. Upon successful completion, the final congratulatory message is displayed in Fig. 24 confirming that they have accomplished the mission.

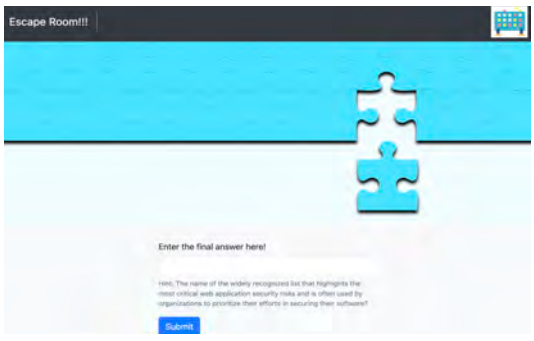


Fig. 23. The final puzzle.

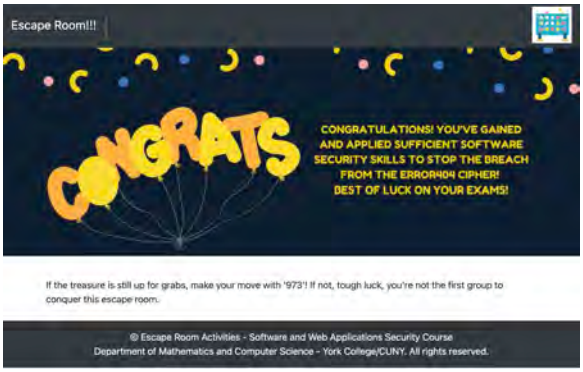


Fig. 24. The final congratulatory message.

Table II. illustrates the alignment of the learning objectives and the game puzzles used in the final implementation.

TABLE II. ALIGNMENT OF GAME PUZZLES WITH LEARNING OUTCOMES

| **Learning outcomes** | **Puzzles** |
|---|---|
| 1) Understand basics cybersecurity terminologies. | Paper Puzzle #7 |
| 2) Demonstrate an understanding of symmetric key usage and proficiency in decrypting messages using a monoalphabetic cipher. | WebEscape Puzzle #4 |
| 3) Able to read the buffer overflow memory dump | WebEscape Puzzle #6 |
| 4) Able to craft an input to cause the buffer overflow | WebEscape Puzzle #2 |
| 5) Able to break the access control by locating the hidden page on a website (insecure direct object references) | WebEscape Puzzle #3 |
| 6) Understand the Common Vulnerability Scoring System (CVSS) scoring | WebEscape Puzzle #5 |
| 7) Understand the risk of hard-coded credentials | WebEscape Puzzle#1 |
| 8) Able to map the specific characteristics to the OWASP top 10 | Paper Puzzle #8 |

## VII. EVALUATION

The survey was completed by all 23 students who took part in the escape room activities, accounting for 100% of those involved in the final implementation. Participation in the survey was voluntary and conducted in compliance with IRB guidelines. The demographic breakdown of the participants was 70% male and 30% female. Among them, 39.1% were Asian, 34.8% were Black or African American, and 26.1% were Hispanic/Latino. Furthermore, the survey results showed that 83% of the students had never participated in an escape room experience before this course, whether for recreation or education. Meanwhile, 13% had experienced Escape Rooms recreationally, and a mere 4% had previously engaged with them in an educational context.

To analyze the survey responses, we employed a combination of quantitative and qualitative methods. The survey included a mix of Likert scale, multiple-choice, and open-ended questions. For the quantitative data, descriptive statistics were used. The survey options ranged from 1 (strongly disagree) to 5 (strongly agree), with the mean (M) values indicating the average level of agreement. The standard deviation (SD) reflects the variation or spread of responses around the mean. For the qualitative data from open-ended questions, quotes from students were analyzed for sentiment and thematic content.

Table III. presents the results of the Likert-scale survey, which was designed to assess students' perceptions and attitudes towards using escape rooms in an educational setting.

TABLE III. STUDENTS EVALUATION (N = 23)

| Question | M (SD) | SA or A |
|---|---|---|
| 1) I found the educational escape room activities engaging. [*Engagement*] | 4.87 (0.34) | 100% |
| 2) The educational escape room effectively promoted teamwork and collaboration among my peers. [*Promotion of Teamwork*] | 4.83 (0.39) | 100% |
| 3) The escape room activities enhanced my problem-solving skills. [*Enhancement of Problem-solving skills*] | 4.65 (0.57) | 96% |
| 4) I found the educational escape room challenging in relation to the course material. [*Challenge & Relevance to Course Materials*] | 3.91 (1.08) | 70% |
| 5) I am very satisfied with the use of escape room in an educational context. [*Satisfaction*] | 4.78 (0.42) | 100% |
| 6) The educational escape room activities were relevant to the course objectives. [*Relevance*] | 4.87 (0.34) | 100% |
| 7) I am very likely to recommend the inclusion of escape rooms in educational settings to my peers. [*Likelihood to Recommend*] | 4.65 (0.71) | 87% |
| 8) The instructions and guidance provided for the escape room activities were very clear. [*Clarity of Instructions*] | 4.57 (0.73) | 87% |
| 9) I enjoyed this educational escape room experience. [*Enjoyment*] | 4.96 (0.21) | 100% |
| 10) I found the escape room activities to be more effective for reinforcing materials compared to other in-class exercises we've used before. [*Effectiveness for Reinforcing Materials*] | 4.65 (0.65) | 91% |
| 11) I understand the course materials better through the escape room activities than I would with other types of in-class exercises we've used before. [*Understanding of Course Materials*] | 4.43 (0.73) | 87% |

*RQ1: How do students perceive the effectiveness of educational escape rooms in reinforcing cybersecurity concepts taught in an undergraduate course?*

The survey results indicate a highly positive student reception to the educational escape room activities, with exceptional levels of engagement, enjoyment, and perceived value in reinforcing course material and enhancing problem-solving skills. Survey responses indicate that students found the escape room activities to be more effective for reinforcing materials compared to other in-class exercises, with a high approval rating (mean score of 4.65, SD = 0.65, 91% agreement). Additionally, students reported a better understanding of course materials through escape room activities over other methods used in the class (mean score of 4.43, SD = 0.73, 87% agreement).

Enjoyment of the experience was extremely high (mean score of 4.96, SD = 0.21), indicating a very positive reception with little variation in responses. Students found the escape room activities highly engaging, with a mean score of 4.87 and very low variability (SD = 0.34). The level of satisfaction among respondents was high (mean score of 4.78, SD = 0.42), indicating that all participants expressed satisfaction with the use of escape rooms in an educational context. Everyone (100%) agreed or strongly agreed to the statements in these areas. The activities were deemed highly relevant to course objectives (mean score of 4.87, SD = 0.34).

Although students generally found the activities beneficial, the relatively lower score and greater variance regarding the challenge level in relation to course material (mean score of 3.91, SD = 1.08) suggest that the difficulty of the escape room activities may need to be calibrated to better suit the entire class needs. The slight variability in perceptions of instruction clarity also highlights an area for improvement.

Table IV. shows the evaluation results, using Likert-scale, in which the students believe escape game activities contribute to the course learning outcomes.

TABLE IV. STUDENTS FEEDBACK ON LEARNING OUTCOMES

| Learning outcomes | M (SD) | SA or A |
|---|---|---|
| 1) Understand basics cybersecurity terminologies. | 4.7 (0.56) | 96% |
| 2) Demonstrate an understanding of symmetric key usage and proficiency in decrypting messages using a monoalphabetic cipher. | 4.48 (0.59) | 96% |
| 3) Able to read the buffer overflow memory dump | 4.09 (1.04) | 70% |
| 4) Able to craft an input to cause the buffer overflow | 4.22 (0.8) | 78% |
| 5) Able to break the access control by locating the hidden page on a website (insecure direct object references) | 4.39 (0.66) | 91% |
| 6) Understand the Common Vulnerability Scoring System (CVSS) scoring | 4.78 (0.42) | 100% |
| 7) Understand the risk of hard-coded credentials | 4.78 (0.42) | 100% |
| 8) Able to map the specific characteristics to the OWASP top 10 | 4.61 (0.58) | 96% |

The survey data, captured in Table IV., offers insightful feedback on the effectiveness of escape room activities in enhancing cybersecurity learning outcomes among students. Using a Likert-scale format, the responses indicate a generally

high level of approval, with students particularly acknowledging their improved understanding of basic cybersecurity terminologies and the risk associated with hard-coded credentials, both of which saw a unanimous agreement on their learning gains. Specifically, students felt confident in understanding the CVSS scoring system and in mapping characteristics to the OWASP top 10, reflecting a strong grasp of critical cybersecurity concepts. Although students also reported increased ability in practical skills such as crafting inputs to cause buffer overflow and identifying insecure direct object references, there was a slightly lower confidence in reading buffer overflow memory dumps. This suggests while the escape room activities significantly contributed to comprehending theoretical knowledge and applying some practical skills, certain areas, particularly those requiring detailed technical analysis, might benefit from further instructional support or tailored activities to enhance understanding.

*RQ2: Can educational escape rooms help in fostering teamwork and collaboration among undergraduate students?*

The escape rooms were almost equally effective in promoting teamwork and collaboration, with a mean score of 4.83 and slightly higher variability (SD = 0.39), as shown in Table III (question no. 2). All respondents agreed or strongly agreed it promoted teamwork.

Table V. shows the results from the survey when asked about the soft-skill benefits gained from participating in the escape room.

TABLE V. STUDENTS FEEDBACK ON SOFT-SKILLS GAINED

| Soft-skills | % |
|---|---|
| Group collaboration/interaction | 87% |
| Communication | 83% |
| Team building | 83% |
| Creativity | 78% |
| Leadership | 57% |
| Time management | 52% |
| Negotiation | 30% |
| Conflict resolution | 30% |

Group collaboration and interaction were highlighted by 87% of the participants, emphasizing the escape room's effectiveness in fostering cooperative engagement. Similarly, communication and team building were both acknowledged by 83% of respondents. Creativity was also a significant benefit, with 78% of students recognizing its development through the escape room challenges. Leadership skills were identified by more than half of the participants (57%) while time management was noted by 52% of respondents. Negotiation and conflict resolution were identified by 30% of the respondents, suggesting these areas were less directly impacted from the escape room experience.

Open-ended questions were used to gather feedback from participants about their escape room experience. When asked about the aspects they enjoyed most, participants emphasized the activity's team-oriented and interactive nature. They appreciated the hands-on learning approach, which not only reinforced course material but also cultivated skills such as time management, creativity, and problem-solving. The mix of engaging puzzles and practical tools offered varied challenges, enriching their experience. Quotes from participants reflect this sentiment:

- "Really working as a team and learning the material together for a better understanding."
- "I liked how interactive it was! It was very great to solve the different riddles."
- "The escape room has allowed me to build new relationships and learn to ask for help when needed."
- "I like the fact that I could communicate with my groupmates especially since a lot of people in the STEM field may be too shy to speak."
- "I liked that every aspect of it [as it] was related to the actual materials we learned in class and it was just a matter of using that knowledge."
- "It was very challenging but finding out steps to solve the problem was very beneficial."
- "The parts I like the most was the little physical things like the crossword puzzles because they were something I was familiar with."
- "It allowed me to be more open minded to try different methods to problem solve."
- "Group work, since it is a race to first place. Everyone helps each other and share ideas how to solve the problem."
- "Team collaboration and reinforcement of the concepts through exercises."
- "The fact that it felt real, and this was [a] competition."
- "The inclusiveness and sharing of personal knowledge and experience."

In response to which puzzles effectively reinforced learning, participants noted that the escape room challenges were instrumental in solidifying key concepts for the participants, with hands-on tasks such as sifting through source code, decrypting monoalphabetic ciphers, and understanding the repercussions of buffer overflows. Specific puzzles that stood out included the buffer overflow, the OWASP Top 10 crossword, and exercises focused on integer overflow and SQL

injections, which translated abstract cybersecurity principles into tangible problem-solving experiences. Some responses for this question include:

- "I think I found that learning about integer overflow and hexadecimals were much easier than doing the learning it normally."
- "I would say the buffer overflow problem helped a lot in remembering what exactly gets affected when it occurs."
- "The parts that required us to actually read and edit code were the most effective to me since it reinforced what we were learning at the time."
- "Buffer overflow memory dump was hard to understand yet with escape room helped me understand it a bit more."
- "Yes, the activity where we learned about asymmetric encryption."
- "Finding hard-coded password to log in."
- "The SQL puzzle cemented the concept for me."

For suggestions on improving the escape room experience, participants offered a range of ideas aimed at enhancing engagement and educational value. These included requests for more challenges, clearer guidance, and the introduction of incentives. Highlighted suggestion include:

- "More escape room challenges, maybe even a take home assignment."
- "You can include more hints in the games so that players can solve problems sooner."
- "Winner gets 10% towards the final."
- "Some ideas tend to sound similar so trying to figure out what we have to do is slightly challenge. I would say differentiation as well as more detail without giving the answer."
- "I think the second one was more content heavy than the first one which I liked so I think it's good to continue to include more problems that actually require you to use the knowledge you learned in the course."
- "The only suggestion I have is to either make the instruction clearer or provide an extra hint if a group is struggling for a very long time."
- "I think having a variety of challenges and difficulties could be good."
- "For one, I think having a clear order, like steps 1 to 10, would be helpful. The escape room was good, but there was no clear order [sequence], and some clues were not needed as they were answered in another problem."
- "[A] room that are spaced so students can walk around to see clues and figure them out on papers rather than on computers."
- "I think it was awesome the way it was conducted. The only thing I would is have them more often!"

Overall, the feedback indicates a strong appreciation for the escape room as an educational tool, with participants valuing its ability to merge learning with interactive and fun challenges. The suggestions for improvement reflect a desire for even more engagement, clearer instructions, and varied challenges to cater to a broader range of learning styles and preferences.

WebEscape tracks the time each group takes to complete the puzzle. Out of 7 groups, 6 managed to 'escape' within the allotted 80 minutes. The average 'escape' time was 72 minutes. The quickest puzzle to be solved was WebEscape Puzzle #5 – Calculating CVSS Scores, with an average completion time of 1.5 minutes. In contrast, the most time-consuming task was finding the hidden page and solving the monoalphabetic cipher (WebEscape Puzzle #3 - #4), which took groups an average of 24 minutes.

## VIII. Discussion

In this section, we examine how educational escape rooms support cybersecurity learning for undergraduates. We consider their effectiveness in aligning with educational goals, adapting to resource limitations, addressing learning misconceptions, and fostering knowledge sharing. These findings offer insights into the potential of escape rooms as a tool for enhancing student engagement and comprehension in complex subject areas. The following subsections detail our analysis and its implications for future educational strategies.

### *A. Aligning the puzzles with learning objectives*

The challenge of connecting puzzles to learning outcomes, rather than merely for entertainment, is highlighted in [11]. The task of transforming cybersecurity content into an engaging gameplay, particularly in areas beyond the naturally fitting cryptography puzzles, was a complex task. The successful alignment of each puzzle with specific learning objectives ensured that the puzzles served their educational purpose effectively. Considerable effort was invested in creatively converting educational material into puzzles that also entertain. The escape room's gamified setting made concepts like integer overflow and hexadecimal values more accessible, while the inclusion of monoalphabetic encryption and code analysis deepened understanding. The buffer overflow task effectively showcased the implications of such vulnerabilities, and the challenges involving usernames and passwords improved the comprehension of authentication processes. Activities that

involved direct code manipulation, inspecting web page elements for credentials, and SQL injection tasks provided practical experience that reinforced the coursework. While some participants found the puzzles straightforward, others benefited from the complexity offered by tasks like the buffer overflow memory dump, which clarified complex topics. Additionally, an activity focused on asymmetric encryption provided valuable insights into modern encryption methods.

### *B. Adapting Group Gameplay in Confined Spaces with Limited Resources*

Building on [21], this work demonstrates that escape room-style activities can be effectively conducted with large-enrollment classes simultaneously. The limitations posed by available resources and space often necessitate creative adaptation in the design of educational escape rooms. Although these constraints may require certain trade-offs, such as giving up extensive physical setups, this study has found that the core benefits of an engaging and educational experience are still achievable. Students divided into teams of 3-4 participated simultaneously in one classroom, yet this setup did not detract from the enjoyable experience. The theme and immersive environment can be effectively conveyed through a web-based application, along with physical and digital clues, allowing for seamless integration of theme and immersion in a resource-efficient manner. This approach not only circumvents the logistical challenges posed by limited space but also offers a scalable and flexible framework for implementing escape rooms in various educational settings.

### *C. Addressing Misconceptions Through Targeted Teaching*

The first escape room, which also served as our pilot study, was conducted midway through the course, revealing unique challenges, particularly in the application of asymmetric cryptography to generate a shared secret key for symmetric encryption, for example. Participants were physically separated and required to exchange clues via a digital padlet accessible to all. The task demanded that each group communicate their clues using symmetric encryption, derived from a secret key generated through asymmetric cryptography. This activity revealed, as observed by the instructor, a gap in the students' understanding of the concept—an insight that would likely have remained unnoticed in a traditional lecture setting. Consequently, this experience enabled the author to identify areas of difficulty for the students and to reteach these concepts in class. This finding aligns with [11], who observed that using escape rooms as a teaching tool provides educators with the opportunity to directly identify misconceptions in specific topics, thereby facilitating adjustments in their upcoming instructional strategies.

### *D. Knowledge Sharing through Peer Teaching*

Participants in the escape room experience expressed great appreciation for the team-oriented and interactive nature of the activity. This educational approach helped build new relationships, encouraged communication especially with reserved students, and provided a platform for sharing knowledge and experiences. Observations revealed that students collaborated closely to solve puzzles, emphasizing teamwork in tackling complex challenges. The efficiency of problem-solving increased with more contributors, showing a clear exchange of knowledge during the activities.

Overall, the strong endorsements of the escape room activities suggest that they are an effective game-based learning strategy for engaging with content-rich cybersecurity materials, though there is potential for further refinement to enhance educational results.

## IX. Conclusion

This study explores the creation and design of escape room activities tailored to teach cybersecurity concepts, with an emphasis on web and software security, to undergraduate students at York College. Midway through the course, an escape room activity was tested as a pilot study. The final version, which introduced the WebEscape platform, included puzzles that targeted specific learning outcomes and acted as a comprehensive review of the course's topics for the enrolled students. Results from this study, derived from survey feedback, show a highly positive reception among students to the educational escape room activities. These activities demonstrated exceptional levels of engagement, enjoyment, and perceived effectiveness in reinforcing course materials and enhancing problem-solving abilities. Additionally, the study observed that escape room activities effectively promoted teamwork and collaboration, critical soft skills for undergraduate students. A principal contribution of this research is showcasing how educational escape rooms can be designed to balance enjoyment with the fulfillment of learning objectives effectively. Overall, the experience was seen as a beneficial departure from traditional learning, making the class more enjoyable and promoting a more open-minded approach to tackling challenges.

This study has a few limitations. Participants were students enrolled in the course for one semester, making the sample size relatively small and potentially unrepresentative of the broader population, thus limiting the generalizability of the findings. This may also result in participation bias, as students who chose to enroll in this elective course may have different levels of interest or proficiency in cybersecurity compared to the general student population, which could influence the results. Additionally, the reliance on self-reported data could affect the accuracy and reliability of the findings. This study could be enhanced by providing students with clearer, more detailed, and standardized instructions. Utilizing multimedia formats such as videos and infographics would help ensure all students have a consistent and thorough understanding of the tasks.

As for future work, given that the time and effort invested in designing escape rooms are significant, the author plans to explore the creation of a web application that automatically generates puzzles and clues aligned with the learning objectives of common cybersecurity topics taught at the undergraduate level. The flexibility of generated puzzles in digital and virtual games would also help in executing escape game activities in large-enrollment classes or those limited in space. Additionally, exploring the integration of Artificial Intelligence (AI) in cybersecurity education to further enhance personalized learning experiences and adaptability to different difficulty levels is worth investigating. Another avenue for further research involves examining the effectiveness of these generated puzzles in enhancing students' understanding and knowledge

retention of cybersecurity concepts, as well as their impact on students' engagement and motivation in learning environments.

## REFERENCES


[1] "Announcement of White House National Cyber Workforce and Education Summit," The White House. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/18/announcement-of-white-house-national-cyber-workforce-and-education-summit/

[2] ISC2, "ISC2 Cybersecurity Workforce Study: Looking Deeper into the Workforce Gap," Nov. 2023. [Online]. Available: https://www.isc2.org/Insights/2023/11/ISC2-Cybersecurity-Workforce-Study-Looking-Deeper-into-the-Workforce-Gap.

[3] "Information Security Analysts - Occupational Outlook Handbook," U.S. Bureau of Labor Statistics. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[4] A. Veldkamp, J. Daemen, S. Teekens, S. Koelewijn, M. C. P. Knippels, and W. R. van Joolingen, "Escape boxes: Bringing escape room experience into the classroom," British Journal of Educational Technology, vol. 51, no. 4, pp. 1220-1239, 2020.

[5] S. O. Bada and S. Olusegun, "Constructivism learning theory: A paradigm for teaching and learning," *Journal of Research & Method in Education*, vol. 5, no. 6, pp. 66-70, 2015.

[6] D. A. Kolb, R. E. Boyatzis, and C. Mainemelis, "Experiential learning theory: Previous research and new directions," in *Perspectives on Thinking, Learning, and Cognitive Styles*, Routledge, 2014, pp. 227-247

[7] K. A. Bruffee, *Collaborative Learning: Higher Education, Interdependence, and the Authority of Knowledge*. Baltimore, MD: Johns Hopkins University Press, 1999.

[8] A. I. V. Vörös and Z. Sárközi, "Physics escape room as an educational tool," in AIP Conference Proceedings, vol. 1916, no. 1, Dec. 2017, AIP Publishing.

[9] N. Dietrich, "Escape classroom: The leblanc process—An educational 'escape game'," Journal of Chemical Education, vol. 95, no. 6, pp. 996–999, 2018.

[10] C. DeCusatis et al., "A cybersecurity awareness escape room using gamification design principles," in Proc. IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2022, pp. 0765–0770.

[11] J. Andrews and O. Bagdasar, "Escape Rooms for Secondary Mathematics Education: Design and Experiments," Open Education Studies, vol. 5, no. 1, pp. 20220194, 2023. Available: https://doi.org/10.1515/edu-2022-0194

[12] E. D. Oroszi, "Security awareness escape room—a possible new method in improving security awareness of users," in Proc. Int. Conf. on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), June 2019, pp. 1–4.

[13] E. Löffler, B Schneider, T Zanwar, and P.M. Asprion, "Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness," Int. J. Serious Games, vol. 8, no. 1, pp. 59–70, 2021.

[14] E. Beguin et al., "Computer-security-oriented escape room," IEEE Secur. & Privacy, vol. 17, no. 4, pp. 78–83, 2019.

[15] J. Streiff, C. Justice, and J. Camp, "Escaping to Cybersecurity Education: Using Manipulative Challenges to Engage and Educate," in Eur. Conf. on Games Based Learn., Oct. 2019, pp. 1046–XXII.

[16] S. Seebauer, S. Jahn, and J. Mottok, "Learning from escape rooms? A study design concept measuring the effect of a cryptography educational escape room," in Proc. IEEE Global Eng. Educ. Conf. (EDUCON), Apr. 2020, pp. 1684–1685.

[17] C. Borrego, C. Fernández, I. Blanes, and S. Robles, "Room escape at class: Escape games activities to facilitate the motivation and learning in computer science," JOTSE, vol. 7, no. 2, pp. 162–171, 2017.

[18] F. A. Deeb and T. J. Hickey, "Teaching introductory cryptography using a 3D escape-the-room game," in Proc. IEEE Front. in Educ. Conf. (FIE), Oct. 2019, pp. 1–6.

[19] C. C. Taladriz, "Flipped mastery and gamification to teach Computer networks in a Cybersecurity Engineering Degree during COVID-19," in Proc. IEEE Global Eng. Educ. Conf. (EDUCON), Apr. 2021, pp. 1624–1629.

[20] T. Williams and O. El-Gayar, "Design of a Virtual Cybersecurity Escape Room," in Nat. Cyber Summit (NCS) Res. Track 2021, Springer Int. Publishing, pp. 60–73, 2022.

[21] S. López-Pernas, A. Gordillo, E. Barra, and J. Quemada, "Examining the use of an educational escape room for teaching programming in a higher education setting," IEEE Access, vol. 7, pp. 31723–31737, 2019.

[22] S. Clarke, D. Peel, S. Arnab, L. Morini, and O. Wood, "EscapED: A framework for creating educational escape rooms and interactive games for higher/further education," International Journal of Serious Games, vol. 4, no. 3, pp. 73-86, 2017.