CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 5, No. 2
October 2026
ISSN: 2832-1006

In this issue:

4. **Bridging the Cybersecurity Skills Gap by Leveraging Cybersecurity Clinics: Developing the Arizona Cybersecurity Clinic**
Paul Wagner, University of Arizona
Robert Honomichl, University of Arizona
Shengjie Xu, University of Arizona

34. **What is Cybersecurity (or Cyber Security)? Answer [Still] Loading…**
Maguire Parsley, University of North Carolina Wilmington
Luke Warpula, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Geoff Stoker, University of North Carolina Wilmington

59. **Enhancing Cyber Defense: A Federated Multi-Modal Deep Learning Framework for Privacy-Preserving Zero-Day Attack Detection**
Samuel Sambasivam, Woodbury University

78. **Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation**
Brandon P. Grech, Anderson University (SC)

104. **Federated Learning and Edge Computing for Privacy-Preserving Real-Time Predictive Maintenance in Industrial IoT Systems Semantic Technologies for**
Kiran Kumar Vejendla, City University of Seattle
Kyong (Jin) Chang, City University of Seattle
Brian Maeng, City University of Seattle
Sherin Aly, City University of Seattle

117. **Perceived Usefulness of Password Complexity: A Methodology Framework**
Kyle Herman, Georgia Southern University
Hayden Wimmer, Georgia Southern University

132. **Beyond Awareness: Building Digital Resilience Through Comprehensive Cybersecurity Foundations for K-5 Students**
Ellie Ebrahimi, University of North Carolina Wilmington
Yasin Emre Gokce, University of North Carolina Wilmington
Majorie Pare, University of North Carolina Wilmington
Berker Koyuncu, University of North Carolina Wilmington
Jude Vargas, University of North Carolina Wilmington
Jacob Blount, University of North Carolina Wilmington

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2026 ISCAP Board of Directors

Amy Connolly James Madison University President	Michael Smith Georgia Institute of Technology Vice President	Jeff Cummings Univ of NC Wilmington Past President
David Firth University of Montana Director	Mark Frydenberg Bentley University Director/Secretary	Leigh Mutchler James Madison University Director
RJ Podeschi Millikin University Director/Treasurer	Bryan Reinicke Rochester Institute of Technology / Director	Jeffry Babb West Texas A&M University Director/Curricular Matters
Eric Breimer Siena University Director/2026 Conf Chair	Tom Janicki Univ of NC Wilmington Director/Meeting Planner	Xihui "Paul" Zhang University of North Alabama Director/JISE Editor

Copyright ©2026 by Information Systems and Computing Academic Professionals (ISCAP). Permission to make digital or hard copies of all or part of this journal for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial use. All copies must bear this notice and full citation. Permission from the Editor is required to post to servers, redistribute to lists, or utilize in a for-profit or commercial use. Permission requests should be sent to editorcppj@iscap.us.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

Jeffrey Cummings
Co-Editor
University of North Carolina Wilmington

Anthony Serapiglia
Co-Editor
Saint Vincent College

Thomas Janicki
Publisher
University of North Carolina Wilmington

2026 Review Board

Brandon Brown
Coastline College

Shawn Clouse
University of Montana

Jeff Landry
Univ of South Alabama

Li-Jen Lester
Sam Houston State Univ

Jamie Pinchot
Robert Morris University

Samuel Sambasivam
Woodbury University

Shwadhin Sharma
California State University Monterey Bay

Sushma Mishra
Robert Morris University

Kevin Slonka
Saint Francis University

Geoff Stoker
Univ of NC Wilmington

Paul Wagner
University of Arizona

Paul Witman
California Lutheran University

Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation

Brandon P. Grech
bgrech@andersonuniversity.edu
Anderson University (SC)
Anderson, South Carolina, 29621, USA

Abstract

As cybersecurity college students prepare for the workforce, competing in cybersecurity competitions such as the National Cyber League continues to be a popular and growing endeavor. This research discusses the development of a brand-new undergraduate cybersecurity course 'Competitions in Cybersecurity' where students practiced in eleven online Capture-the-Flag (CTF) or similar cybersecurity learning platforms throughout the semester. Students completed an assessment of each online practice website. This research highlights the assessment results regarding which of the eleven websites were enjoyable, easy to get started, and believed to be applicable to prepare for National Cyber League (NCL) competitions. This research also identified multiple websites that students found to be challenging to get started and/or were not applicable to NCL preparation. Furthermore, this research noted eight of the eighteen students who successfully completed this course showed significant improvements within their National Cyber League Individual Game placements within the same semester and/or following semester. This research noticed that platform satisfaction and perspective differed between the eight students who showed significant NCL improvement and the other students who did not show as much significant improvement.

Keywords: Cybersecurity, Competition, Gamification, Student satisfaction

Recommended Citation: Grech, B.P., (2026). Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation *Cybersecurity Pedagogy and Practice Journal.* v5(n2) pp 78-103. DOI# https://doi.org/10.62273/FWOS1592

©2026 ISCAP (Information Systems and Computing Academic Professionals)

Evaluating Eleven Online CTF Platforms for Undergraduate Cybersecurity Competition Preparation

Brandon P. Grech

1. INTRODUCTION

An inaugural 'Competitions in Cybersecurity' course was developed and launched in Fall 2024 at a Christian institution of higher education in the Southeast region of the United States of America. Eighteen students passed this course. Throughout this course, students practiced within eleven available online cybersecurity CTF (Capture-the-Flag) or similar learning websites. Near the end of the semester, students participated in the National Cyber League Individual and Team Games. Besides the registration payment for the National Cyber League, which was covered by the institution, all other websites were free and accessible to the students. After students participated in each online platform during class and outside of class, each student completed an assessment form and answered questions regarding ease of access, platform technical difficulties, enjoyable experiences, and the effectiveness and applicability of the platform in preparation for the National Cyber League.

1.1 National Cyber League

The National Cyber League (NCL) is an online competition that is open to college students within the United States of America. The NCL also allows U.S. high schools to participate as well; however, the primary audience is at the collegiate level. The NCL consists of nine skill categories: open source intelligence, cryptography, password cracking, log analysis, network traffic analysis, forensics, web application exploitation, scanning, and enumeration and exploitation. The NCL consists of an Individual Game and a Team Game every semester. Each game is 56 hours long and typically starts on Friday (1 p.m. Eastern Time Zone) and ends on Sunday (9 p.m. Eastern Time Zone). The Team Game is typically hosted online two weeks after the Individual Game. The Team Game allows up to seven students to compete together. Registration for the NCL was $35 per student in Fall 2024; however, it has since been raised to $45 per student. Registration includes access to the NCL Gym, Practice Game, Individual Game, and Team Game. The NCL has been shown to be effective in preparing students for the workforce (Zeichick, 2024). Participation within the NCL has been growing. In Fall 2018, 2,450 students competed in the NCL Individual Game (National Cyber League, 2018). In Fall 2024, 4,585 students competed in the NCL Individual Game (National Cyber League, 2024a). The NCL Individual Game shows an increase of over 87% between Fall 2018 and Fall 2024.

The NCL does not have a maximum number of students that may participate from a specific institution (National Cyber League, n.d.-a). Other competitions, such as the Collegiate Cyber Defense Competition (CDCC) and Collegiate Penetration Testing Competition (CPTC), only allow one team from an institution to compete during the competition. CDCC allows for one team of eight competitors with four alternates (National Collegiate Cyber Defense Competition, n.d.). CPTC allows for one team of six competitors with two alternates (Collegiate Penetration Testing Competitions, n.d.). The National Cyber League does not have a limit on how many individuals can compete during the NCL Individual Games. The NCL also does not have a limit on how many different teams from the same institution may compete during the NCL Team Game. The NCL provides scalability and more opportunities for students to compete without having roster spots taken by other peers and classmates.

The NCL ties into other educational frameworks, such as the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) and the NIST NICE Workforce Framework for Cybersecurity (NICE Framework) Work Roles. The NCL provides a detailed outline of how the nine skill categories (mentioned above) align with thirty-six NSA CAE-CD Knowledge Units (National Cyber League, 2024b). The NCL also provides a detailed outline of how the NCL's nine skill categories align with thirty-five NICE Framework Work Roles (National Cyber League, 2021) as each NICE Framework Work Role has between two – nine NCL skill categories supporting each work role.

1.2 Goals of This Paper

By analyzing the assessments of each student's responses to each platform, this research looks to gain a better understanding of how students believe each experience was and if it was applicable in preparing for the National Cyber

©2026 ISCAP (Information Systems and Computing Academic Professionals)

League. This research also aims to identify if positive trends and significant improvements in national rankings were seen after students participated in this course and the eleven CTF websites. Ultimately, this research aims to help institutions assess which of these practice websites may help their students improve within the National Cyber League. Specifically, the research questions are as follows:

- What are the students' perspectives of each Capture-the-Flag (CTF) website?
- Was there a significant improvement in the National Cyber League found within students after participating in each CTF website?
- What student perspective differences are found between students who showed significant growth and those who did not?

This paper will begin by addressing the first question by sharing the survey results of all eighteen students regarding each CTF website. Additionally, this paper will also share significant improvements seen in National Cyber League Individual Game performances after students completed this course. Lastly, this paper will share the survey results of those students who showed significant growth after taking this course and any differences between these students and the remaining students.

1.3 Contributions of This Paper

This research is focused on sharing student experiences across eleven available online CTF platforms in preparation for the National Cyber League. Over 500 United States institutions of higher education participate in the National Cyber League each semester (National Cyber League, 2025); however, little research exists discussing how students are preparing for these competitions. This research aims to show institutions examples of freely available CTF websites that may be a good selection to utilize for NCL preparation. This research will also share student feedback that discusses which CTF websites students did not find as valuable as other websites.

1.4 Structure of This Paper

This research paper contains eight sections. Section 1 is the introduction. Section 2 discusses the methodology. Section 3 shares the course schedule. Section 4 contains the responses of each website. Section 5 discusses the improvement seen in National Cyber League performances. Section 6 compares the assessments of those who showed significant improvement with those who did not. Section 7 is the conclusion. Section 8 contains references.

2. METHODOLOGY

This research utilized an experiential, quantitative research design where students were introduced to a new online CTF platform each week to practice within. At the conclusion of the week, each student completed a four-question Likert-style assessment reflecting on their experiences. The four questions were:

(Q1) Do you agree it was easy to get enrolled and start practicing?
(Q2) Do you agree there were platform-related technical difficulties?
(Q3) Do you agree it was enjoyable?
(Q4) If you competed in the NCL Individual or Team Game before, do you agree this practice site is applicable to prepare for the NCL Games?

Each question had the available choices: Strongly Disagree, Disagree, Neither Agree nor Disagree, Agree, and Strongly Agree. Each choice was assigned a score of 1 – 5 as follows: Strongly Disagree (1), Disagree (2), Neither Agree nor Disagree (3), Agree (4), and Strongly Agree (5). The average of all responses was calculated. If a student did not respond, a 'No Response' is indicated and is not considered within the average.

This experiential cycle repeated eleven times throughout the semester with a new online CTF platform each week. Students also competed within the National Cyber League Individual Game near the end of the semester and again the following semester. Student performances were measured to determine whether participation within this course led to National Cyber League Individual Game performance increases compared to prior to taking this course. Figure 1 illustrates how Kolb's Experiential Learning Theory (Kolb, 1984) was applied in this research study.

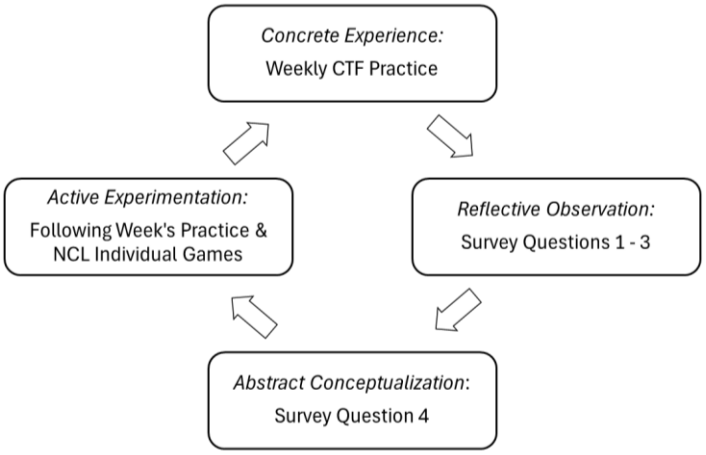


Figure 1. Application of Kolb's Experiential Learning Theory to Weekly CTFs

3. COURSE STUDENTS AND SCHEDULE

This section shares the schedule, tempo, and unexpected schedule changes of the 'Competitions in Cybersecurity' course.

3.1 Course Students

This inaugural course consisted of eighteen undergraduate students pursuing an undergraduate degree in cybersecurity at a Christian institution of higher education in the Southeast region of the United States of America. This course was a major elective that students could select; however, no students were required to enroll in this course. Students ranged from undergraduate sophomores to undergraduate seniors, as the only prerequisite for this course was a 100-level Linux course. Eleven of the eighteen students competed in the National Cyber League Individual Game in the previous semester. All eighteen students were traditional, in-person, undergraduate students who, at the time, had not yet gained full-time employment in a cybersecurity-related position.

3.2 CTF Practice Website Schedule

Each week, students practiced within an online CTF website and completed an assessment of their experiences. This course had in-person 75-minute classes each Tuesday and Thursday during the Fall 2024 semester. A majority of the students' time in class was spent working individually or in groups on each practice site; however, students spent even more time working on these practice sites outside of the class period. The schedule of the online CTF websites utilized is below.

Course Week	CTF Preparation Platform
Week 0	316ctf
Week 1	CTFlearn
Week 2	Bandit
Week 3	Natas
Week 4	picoGym
Week 5	247CTF
Week 6	Hacker101 CTF
Week 7	Root Me
Week 8	NCL Gym
Week 9	RingZer0 CTF
Week 10	Defend the Web

Table 1. CTF Practice Website Schedule

3.3 CTF Competition Schedule

Students also competed in six competitions throughout the semester. The first four competitions were utilized as further preparation for the National Cyber League Individual and Team competitions. The dates of each competition are below. Students had the option of PatriotCTF or ASIS CTF Quals as they were during the same week; however, all students chose to participate in PatriotCTF hosted online by George Mason's cybersecurity club. The official dates of the NSA Codebreaker Challenge were September 16th, 2024 – January 17th, 2025; however, the 'Competitions in Cybersecurity' course students were assigned to complete as much as they could within one week (October 8 – 14, 2024). Exploring experiences within the four non-NCL competitions as preparation for the National Cyber League is out of scope for this research and may be explored within future research.

Course Week	Dates	Competition
Week 1	Aug 31 – Sep 4, 2024	CISA ICS CTF 2024
Week 2	Sep 6 – 8, 2024	CSAW CTF Quals
Week 4	Sep 20 – 22, 2024	PatriotCTF
Week 7	Oct 8 – 14, 2024	NSA Codebreaker Challenge
Week 9	Oct 25 – 27, 2024	NCL Individual Game
Week 11	Nov 8 – 10, 2024	NCL Team Game

Table 2. CTF Competition Schedule

The 'Competitions in Cybersecurity' course students were also assigned a final team project where students in groups of three created their own CTF competition with various categories and custom challenges. An in-class demonstration of each project occurred during Week 14 of the course, which included a live demo showcasing various challenges being solved. Exploring the submissions of each team project is also out of scope for this research; however, students shared positive feedback regarding creating their own CTF competition from scratch during their presentations.

3.4 Unexpected Schedule Adjustments

During the semester in which the 'Competitions in Cybersecurity' course was being held, Hurricane Helene impacted the Southeastern United States. This natural disaster cancelled in-person classes for this course on October 1, 2024 and October 3, 2024. These two cancelled in-person classes were during Week 6. Fall Break was not cancelled; therefore, students did not have class on October 10 (as planned). To adjust for Hurricane Helene, only one in-person class day (instead of two) was devoted to Hacker101 CTF and Root Me. The NCL Gym was already scheduled for only one day due to Fall Break. Students were given extensions as needed to ensure enough time was dedicated to each preparation site outside of class.

4. ASSESSMENT RESULTS

This section shares a description of each of the CTF websites. The averages of each CTF's assessment results are found near the end of this section. The individual response scores related to the four questions answered after completing each CTF practice site are found in the appendices:

(Q1) Do you agree it was easy to get enrolled and start practicing?

(Q2) Do you agree there were platform-related technical difficulties?

(Q3) Do you agree it was enjoyable?

(Q4) If you competed in the NCL Individual or Team Game before, do you agree this practice site is applicable to prepare for the NCL Games?

4.1 316ctf

During Week 0, students participated in 316ctf. 316ctf is a persistent and growing CTF website created by Anderson University (SC) and the faculty member responsible for creating the 'Competitions in Cybersecurity' course. 316ctf is intended for middle-school and high-school students to explore categories such as Password Cracking, Cryptography, Open Source Intelligence, Web, and Network Analysis; however, it is open to everyone. The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix A.

4.2 CTFlearn

During Week 1, students participated in CTFlearn. CTFlearn claims to be the most beginner-friendly way to learn cybersecurity (CTFlearn, n.d.). CTFlearn has been utilized in previous research and was noted to be accessible (Albaladejo-González, et al., 2025); however, this research disagrees with this claim as many students within this course claimed to have technical difficulties within the CTFlearn platform. Prior research states CTFlearn has pedagogical content related to Reverse Engineering, Cryptography, Web Vulnerabilities, Binary Exploitation, and Forensics and Networking (Votipka, 2021) while additional research states CTFlearn consists of challenges related to Software Security, Reverse Engineering, Cryptography, Exploitation, Forensics, and Web Security (Lazarov, 2023); however, this research shows that students did not find this content enjoyable. The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix B.

4.3 Bandit

During Week 2, students participated in Bandit. Bandit is a wargame created by the OverTheWire community. OverTheWire claims Bandit is aimed at absolute beginners to learn Unix/Linux basics (OverTheWire, n.d.). Bandit has been criticized for being "too public" due to having walkthroughs

easily accessible (Ruff & Giacobe, 2022). Bandit has also been used to assist with launching a cybersecurity club by showcasing the different Linux skill levels of students (Piazza & Olmsted, 2015). Bandit has also been utilized by undergraduate students at a polytechnic institute that did not have a course covering the usage of the Linux terminal (Winters, 2020). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix C.

4.4 Natas

During Week 3, students participated in Natas. Natas is another wargame created by the OverTheWire community. OverTheWire suggests Natas for learning web security after playing the Bandit wargame (OverTheWire, n.d.). The Natas platform has been effective as an introduction to hacking at collegiate hacking clubs (Radu & Thomas, 2015). Natas, and the previously mentioned Bandit, have also been utilized by faculty as additional content for students during cybersecurity labs (Singh et al., 2020). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix D.

4.5 picoGym

During Week 4, students participated in picoCTF's picoGym. The picoCTF platform is a computer security education program created by Carnegie Mellon University (picoCTF, n.d.). The picoGym is available on-demand which hosts prior picoCTF event challenges and other challenges. Throughout the year, picoCTF has various events that are only available during the event. The picoGym has been utilized at other institutions to improve cybersecurity education (Ken et al., 2025). Writeups for some picoGym challenges are also publicly available (Leka, 2023). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix E.

4.6 247CTF

During Week 5, students participated in 247CTF. 247CTF is a continuous security competition that offers challenges in various cybersecurity categories (247CTF, n.d.). The 247CTF platform has been utilized by institutions of higher education as one of the first steps towards building a competent CTF team (Goetgheluck et al., 2024). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix F.

4.7 Hacker101 CTF

During Week 6, students participated in Hacker101 CTF. The Hacker101 CTF is another free website that allows people to play and learn cybersecurity skills (Hacker101, n.d.). Hacker101 CTF has been utilized to assist with preparing future bug bounty hunters (Cuevas et al., 2022). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix G.

4.8 Root Me

During Week 7, students participated in Root Me. Root Me is another platform that allows people to learn computer security skills such as web security, network security, and reverse engineering (Paiva et al., 2023; Root Me, n.d.). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix H.

4.9 NCL Gym

During Week 8, students participated in the NCL Gym. The NCL Gym contains challenges from previous NCL competitions. The NCL Gym is typically open throughout the semester to students after they have paid and registered for the National Cyber League (National Cyber League, n.d.-b). During the Fall 2024 semester, the NCL Gym was open between August 19 – December 13 (National Cyber League, 2024c). Students noted that a majority of the NCL Gym challenges were the same as the previous semester and had minimal changes between semesters. The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix I.

4.10 RingZer0

During Week 9, students participated in RingZer0's Team online CTF (RingZer0, n.d.). RingZer0's CTF has been modeled by graduate institutions teaching cybersecurity (Knight et al., 2020). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix J.

CTF Platform	Q1	Q2	Q3	Q4
316ctf	4.72	1.78	4.39	4.11
CTFlearn	2.61	4.83	2.17	3.47
Bandit	4.33	1.89	4	3.53
Natas	4.61	1.72	4.22	4.44
picoGym	4.47	1.82	4.18	4.2
247CTF	4.43	2	3.57	3.83
Hacker101	4.13	2.19	3.75	3.71
Root Me	3.39	3.5	3.39	3.24
NCL Gym	4.61	1.39	4.28	4.47
RingZer0	4.25	2.12	3.47	3.44
Defend the Web	4.35	1.88	4	3.88

Table 3. Comparison of Practice Site Based on Course Order

4.11 Defend the Web

During Week 10, students participated in Defend the Web (Defend the Web, 2024). After the course, around early May 2025, the Defend the Web's home page claimed to be on hiatus due to running costs and personal commitments (Defend the Web, 2025). The responses of each (pseudonym) student and the average of each of the eighteen students' responses to all four questions can be found at Appendix K.

4.12 Comparing Each Eleven CTFs

Table 3 shows each of the eleven CTFs' average for each question in order of the course schedule.

The charts below show the data from all eighteen students ordered from highest to lowest regarding each question one through four.

In Figure 2, the average scores of responses regarding Question 1 'Do you agree it was easy to get enrolled and start practicing' are shown. The platforms 316ctf, NCL Gym, and Natas received a 4.6 or higher regarding easiness of enrolling and getting started. The majority of platforms scored an average of 4.0 or higher. The two platforms that showed enrollment and starting concerns were Root Me and CTFlearn.

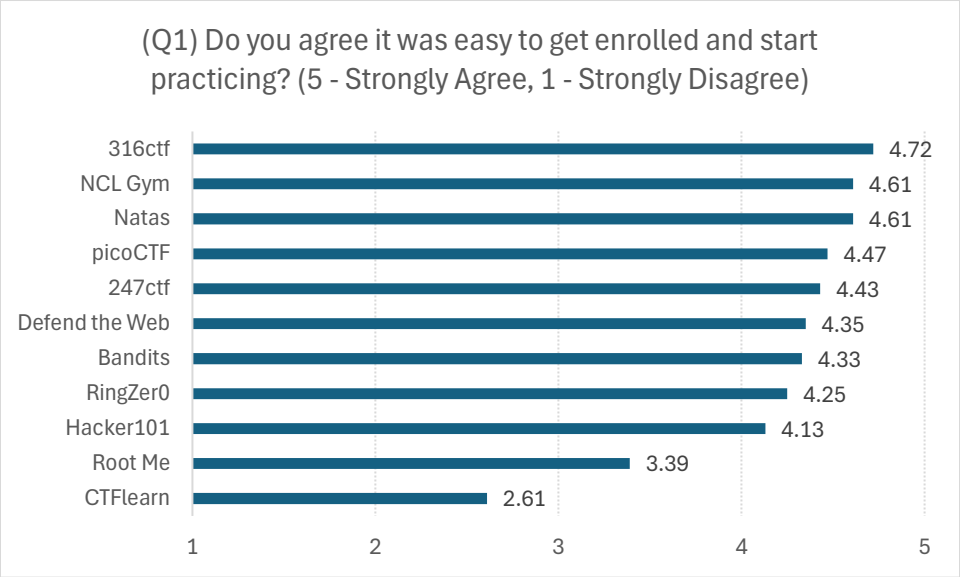


Figure 2. Comparison of Question 1 Averages Sorted Highest to Lowest (All Students)

In Figure 3, the average scores of responses regarding Question 2 'Do you agree there were platform-related technical difficulties' are shown. The students indicated there were technical difficulties within both CTFlearn and Root Me. Nearly all students strongly agreed there were technical difficulties within CTFlearn. The remaining nine platforms showed minimal technical difficulties.

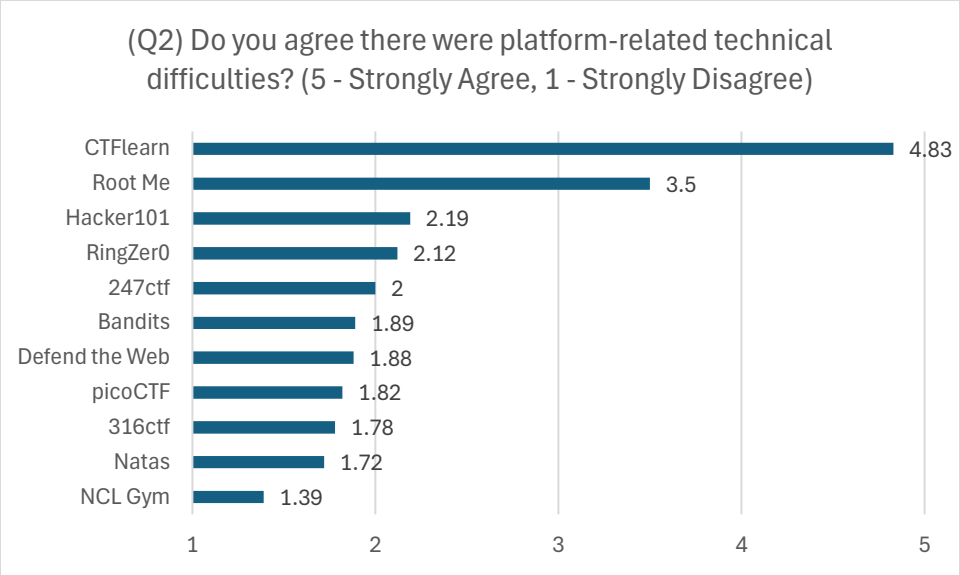


Figure 3. Comparison of Question 2 Averages Sorted Highest to Lowest (All Students)

In Figure 4, the average scores of responses regarding Question 3 'Do you agree it was enjoyable' are shown. Six of the eleven platforms scored a minimum of 4.0. These include 316ctf, NCL Gym, Natas, picoCTF, Defend the Web, and Bandit. The least enjoyable platforms were the same two that had platform-related difficulties (CTFlearn and Root Me).

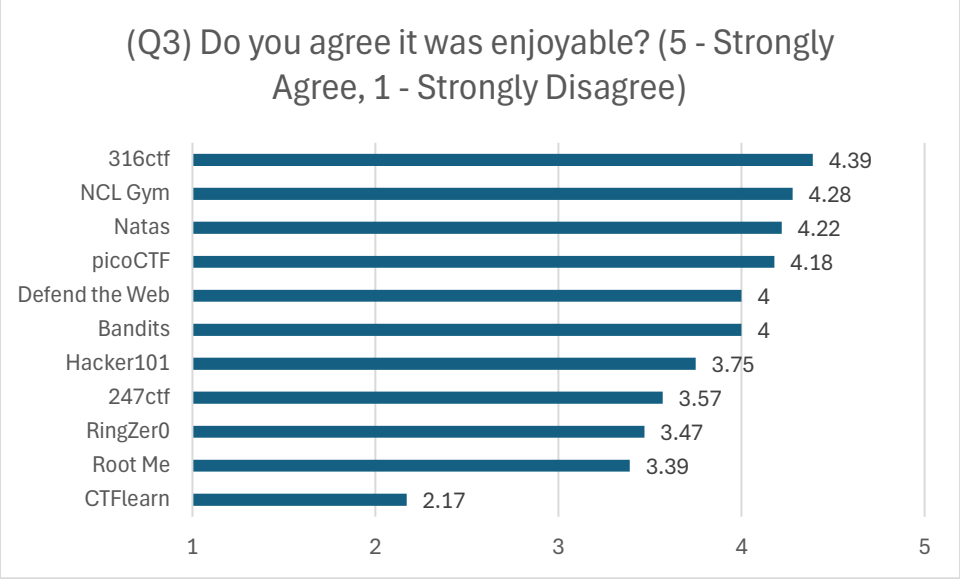


Figure 4. Comparison of Question 3 Averages Sorted Highest to Lowest (All Students)

In Figure 5, the average scores of responses regarding Question 4 'If you competed in the NCL Individual or Team Game before, do you agree this practice site is applicable to prepare for the NCL Games' are shown. Four of the eleven platforms scored a minimum of 4.0. These include NCL Gym, Natas, picoCTF, and 316ctf. The platform RingZer0 scored the second-lowest score and joined CTFlearn and Root Me as the three least agreed upon in preparing for the NCL Games.

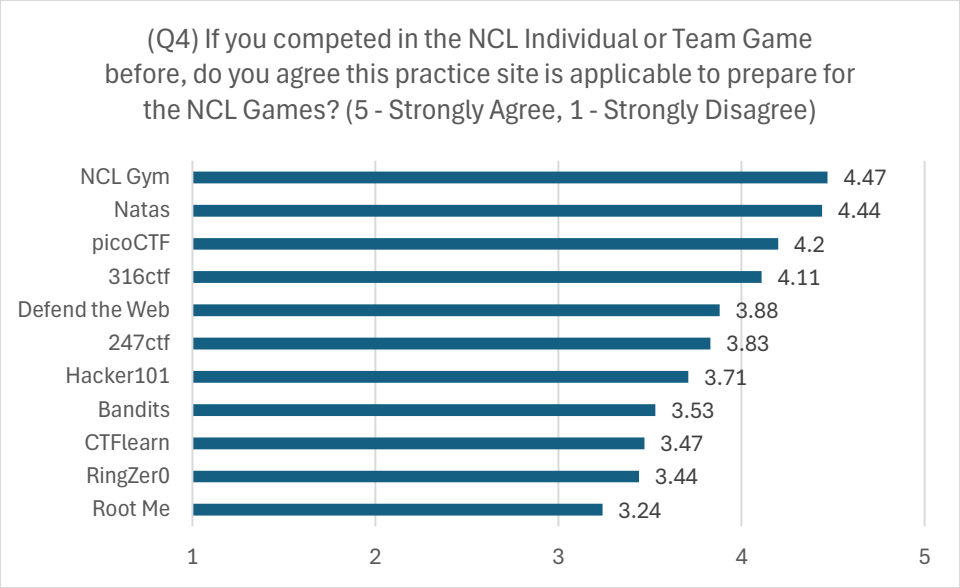


Figure 5. Comparison of Question 4 Averages Sorted Highest to Lowest (All Students)

5. IMPROVEMENTS IN NCL COMPETITION

Out of the 18 students who successfully completed this course in Fall 2024, 11 competed in the National Cyber League Individual Game in Spring 2024 (the semester prior to the course being offered).

During the course's semester, 17 students competed in the Fall 2024 National Cyber League Individual Game. During the following semester, 13 students competed in the Spring 2025 National Cyber League Individual Game.

The statistics below share how many students placed in each tier. These numbers are non-cumulative; for example, a student ranked in the Top 100 is not also considered in the Top 500. A few students who did not participate were ineligible to compete due to graduating before the competition(s).

This research data shows that prior to taking the course, zero course students placed in the Top 50, four placed in the Top 100, and an additional two placed in the Top 500. Within the semester, immediate improvements were made as one student placed in the Top 50, three placed in the Top 100, and two placed in the Top 500. During the following semester, the largest improvement occurred, as four students placed in the Top 50 and an additional four students placed in Top 500. This data and positive trend are shown below.

NCL Ind. Ranking	Spring 2024	Fall 2024	Spring 2025
Top 50	**0**	**1**	**4**
Top 100	**4**	**3**	**0**
Top 500	**2**	**2**	**4**
Top 1000	2	2	1
Outside Top 1000	3	9	4
Did Not Participate	7	1	5

Table 4. NCL Individual Rankings Before, During, and After the Course

6. COMPARISON OF STUDENT ASSESSMENT

Out of the 18 students who successfully completed this course, eight showed significant improvement. A student is considered to have shown significant improvement if they placed in the Top 500 during or after completing the 'Competitions in Cybersecurity' course and if they improved their ranking in Fall 2024 and/or Spring 2025 compared to their Spring 2024 placement, if available (prior to the course).

As previously stated, eleven students competed in the Spring 2024 NCL Individual Game and seven did not. These students may have competed in a previous NCL Team Game or an even earlier NCL Individual Game which would fulfill the requirement to answer Question 4. Placing in the Top 500 is a challenging feat, as over 4,600 students competed in the Spring 2025 National Cyber League Individual Game. The National Cyber League awards the individuals who place in the Top 500 in the standard bracket during Individual Games by mailing them a physical challenge coin as an award. This research will now explore if these eight students' experiences differ from the remaining ten students who did not make such a significant improvement and did not place in the Top 500 in any of their NCL Individual competitions. The eight students who made significant improvements (Top 500 and improved their ranking, if available) will be referred to as 'Group A' and the remaining ten students will be referred to as 'Group B'.

6.1 Question 1 Comparison

The table and figure below visually represent the differences between Group A and Group B's experiences getting enrolled and beginning practicing. The data has been ordered from highest to lowest based on Group A's experience. Group A showed much more dissatisfaction with CTFlearn compared to Group B.

CTF Platform	Group A	Group B
picoGym	4.86	4.2
Natas	4.75	4.5
NCL Gym	4.75	4.5
316ctf	4.63	4.8
247CTF	4.6	4.33
Bandit	4.38	4.3
Defend the Web	4.29	4.4
RingZer0	4.29	4.22
Hacker101	4	4.25
Root Me	3.13	3.6
CTFlearn	1.63	3.4

Table 5. Question 1 Comparison Between Group A and Group B (Table)

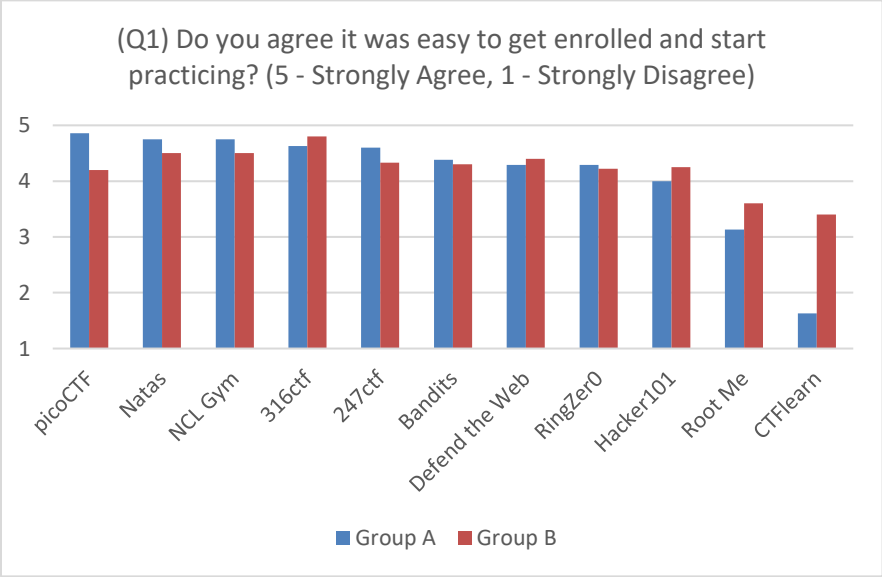


Figure 6. Question 1 Comparison Between Group A and Group B (Bar Chart)

CTF Platform	Group A	Group B
CTFlearn	5	4.7
Root Me	3.75	3.3
Hacker101	2.13	2.25
Defend the Web	2	1.8
RingZer0	2	2.2
Bandit	1.63	2.1
247CTF	1.6	2.22
316ctf	1.38	2.1
picoGym	1.29	2.2
Natas	1.25	2.1
NCL Gym	1.13	1.6

Table 6. Question 2 Comparison Between Group A and Group B (Table)

6.2 Question 2 Comparison

The table and figure below visually represent the differences between Group A and Group B's experiences with platform-related technical difficulties. The data has been ordered from highest to lowest based on Group A's experience.

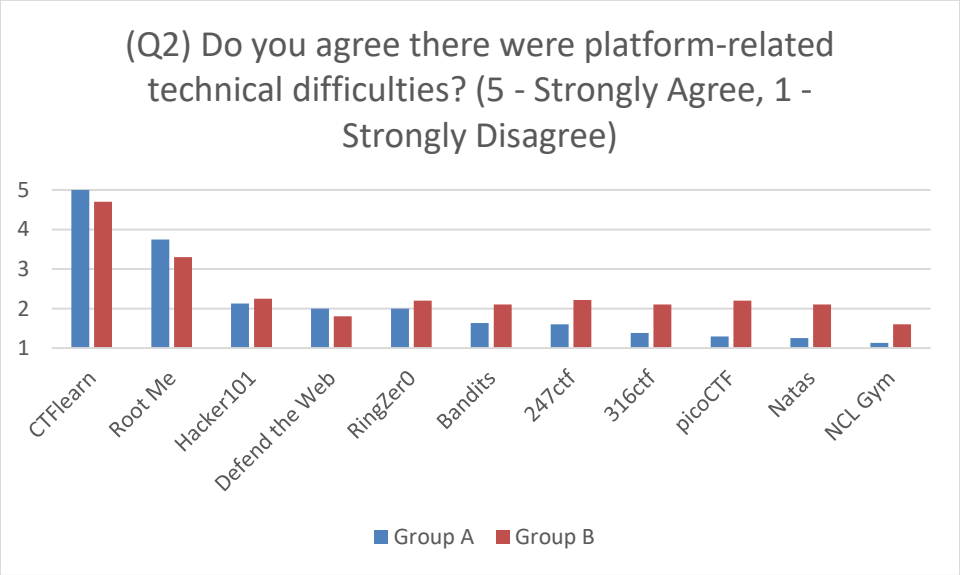


Figure 7. Question 2 Comparison Between Group A and Group B (Bar Chart)

6.3 Question 3 Comparison

The table and figure below visually represent the differences between Group A and Group B's enjoyment of each platform. The data has been ordered from highest to lowest based on Group A's experience.

CTF Platform	Group A	Group B
picoGym	4.57	3.9
Natas	4.5	4
NCL Gym	4.5	4.1
316ctf	4.25	4.5
RingZer0	4	3.1
247CTF	4	3.33
Hacker101	3.88	3.63
Bandit	3.88	4.1
Defend the Web	3.71	4.2
Root Me	3.5	3.3
CTFlearn	2	2.3

Table 7. Question 3 Comparison Between Group A and Group B (Table)

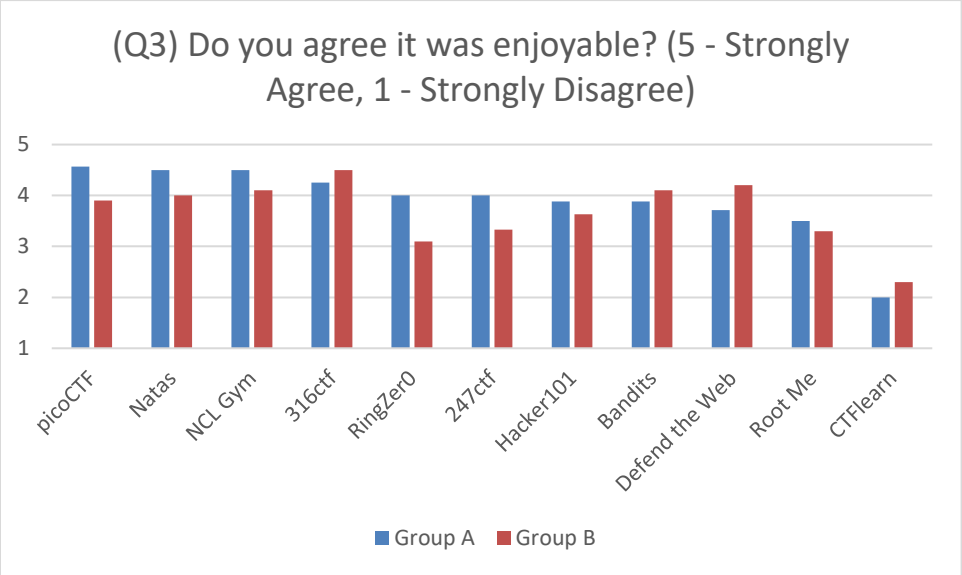


Figure 8. Question 3 Comparison Between Group A and Group B (Bar Chart)

6.4 Question 4 Comparison

The table and figure below visually represent the differences between Group A and Group B's opinions on whether the platform is applicable in preparing for the National Cyber League. The data has been ordered from highest to lowest based on Group A's experience.

CTF Platform	Group A	Group B
Natas	4.88	4
picoGym	4.57	3.88
NCL Gym	4.5	4.44
316ctf	4.25	4
247CTF	4.2	3.57
Defend the Web	4.14	3.7
Hacker101	3.88	3.5
RingZer0	3.86	3.11

Bandit	3.5	3.56
CTFlearn	3.25	3.67
Root Me	3.13	3.33

Table 8. Question 4 Comparison Between Group A and Group B (Table)

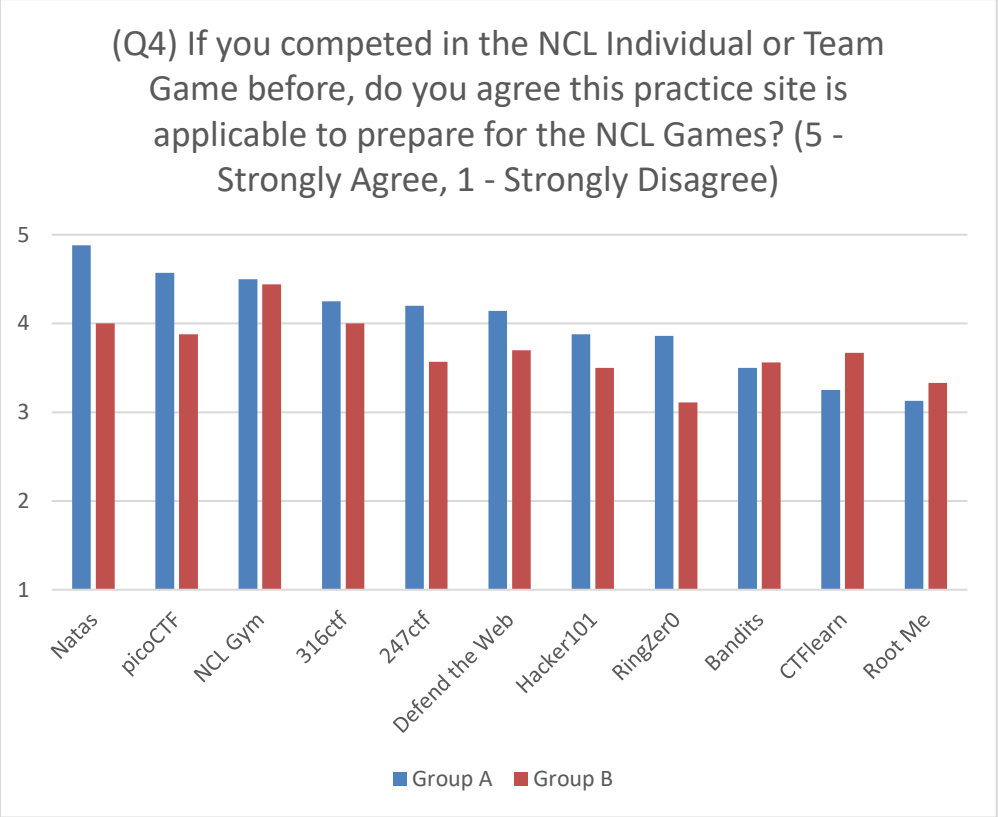


Figure 9. Question 4 Comparison Between Group A and Group B (Bar Chart)

7. CONCLUSION

This research has shown that a cybersecurity course dedicated to competitions in cybersecurity can have a significant positive impact on students' placements in National Cyber League competitions. This research has discovered that students who showed significant improvement believe that Natas, picoGym, and the NCL Gym were the most applicable in preparing students for the National Cyber League Games. The same students found the same three platforms (picoGym, Natas, and NCL Gym) were also the most enjoyable. The platforms 316ctf and 247CTF also had a 4 or higher in both enjoyability and applicability to the NCL Games, according to students who showed significant improvement (Group A). It is also of interest that Group A's top four enjoyable platforms were in order picoGym, Natas, NCL Gym, and 316ctf; however, Group B's top four enjoyable platforms were the same in reverse order with 316ctf followed by NCL Gym, Natas, then picoGym. Students also found platform-related technical problems and enrollment/starting issues in the CTFlearn and Root Me platforms. The Defend the Web platform is currently inaccessible since this inaugural course's research. Faculty members, cybersecurity competition coaches, and students who are looking for enjoyable and applicable platforms for the National Cyber League should strongly consider looking at picoGym, Natas, and the NCL Gym and explore the remaining platforms within this research as additional potential preparation sites for the National Cyber League. This research can and should be replicated at other schools within a course or a cybersecurity club to identify if similar significant improvements are found with National Cyber League individual performances. The findings of this research have been applied to the following year's second iteration of the 'Competitions in Cybersecurity' at this institution, which is being offered in Fall 2025.

8. REFERENCES

247CTF. (n.d.). *Home*. https://247ctf.com/

Albaladejo-González, M., Nespoli, P., Gómez Mármol, F., & Ruipérez-Valiente, J. A. (2025). A multimodal and adaptive gamified system to improve cybersecurity competence training. *Cluster Computing, 28*(9). https://doi.org/10.1007/s10586-025-05264-6

Collegiate Penetration Testing Competition. (n.d.). *Overview*. RIT ESL Global Cybersecurity Institute. https://cp.tc/overview

CTFlearn. (n.d.). *Learn cybersecurity*. https://ctflearn.com/

Cuevas, A., Hogan, E., Hibshi, H., & Christin, N. (2022). Observations from an online security competition and its implications on crowdsourced security. *arXiv*. https://doi.org/10.48550/arXiv.2204.12601

Defend the Web. (2024). *An interactive cyber security platform*. Wayback Machine. https://web.archive.org/web/20241013223256/https://defendtheweb.net/

Defend the Web. (2025). *Goodbye*. Wayback Machine. https://web.archive.org/web/20250507233154/https://defendtheweb.net/

Goetgheluck, Y., Mernit, S., & Pereira, J. (2024). Gamification of IT for training in information systems management. *Colloque International Game Evolution 2024*. https://hal.science/hal-04579392/

Hacker101 CTF. (n.d.). *Home*. HackerOne. https://ctf.hacker101.com/

Ken, C. L., Juremi, J., Alizadeh, S., & Sulaiman, S. (2025). Enhancing cybersecurity education through gamified learning and capture the flag (CTF) platform. *Communications in Computer and Information Science*, 69–82. https://doi.org/10.1007/978-3-031-98003-9_6

Knight, G. S., Leblanc, S., Devendorf, E., & Shuck, M. (2020). Design it, build it, defend it: Using cyber exercises in the education of cyber forces. In G. Austin (Ed.), *National cyber emergencies: The return to civil defence* (Chapter 13). Routledge.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development*. Prentice-Hall.

Lazarov, W., Stodulka, T., Schafeitel-Tähtinen, T., Helenius, M., & Martinasek, Z. (2023). Interactive environment for effective cybersecurity teaching and learning. *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES)*, 1–9. https://doi.org/10.1145/3600160.3605007

Leka, C. (2023). *CTFLib / A collection of writeups of capture-the-flag challenges for beginners*. University of Piraeus. https://dione.lib.unipi.gr/xmlui/handle/unipi/15290

National Collegiate Cyber Defense Competition. (n.d.). *NCCDC rules and requirements*. National CCDC. https://www.nationalccdc.org/rules.htm

National Cyber League. (n.d.-a). *Rules of conduct*. Cyber Skyline. https://nationalcyberleague.org/competition/rules

National Cyber League. (n.d.-b). *Competition*. https://nationalcyberleague.org/competition

National Cyber League. (2018). *Leaderboard: Fall 2018*. Cyber Skyline. https://cyberskyline.com/hosted_events/ncl-fall-2018

National Cyber League. (2021). *NCL category alignment: How NCL cybersecurity skill categories align to the NIST NICE cybersecurity work roles and CompTIA certifications*. Cyber Skyline. https://drive.google.com/file/d/1sC-eeRyclL0qV-mOf-hB1kqu3SmXZZZc/view

National Cyber League. (2024a). *Leaderboard: Fall 2024*. Cyber Skyline. https://cyberskyline.com/hosted_events/ncl-fall-2024

National Cyber League. (2024b). *How NCL skill categories align to the NSA Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units (KUs)*. Cyber Skyline.

https://drive.google.com/file/d/1Z8khijDbNRC_wOx5Z89re03Rns82UcWD/view

National Cyber League. (2024c). *Competition*. Wayback Machine. https://web.archive.org/web/20241206033728/https://nationalcyberleague.org/competition

National Cyber League. (2025). *Cyber power rankings: Spring 2025*. Cyber Skyline. https://cyberskyline.com/data/power-ranking/spring-2025-national

OverTheWire. (n.d.). *Wargames*. https://overthewire.org/wargames/

Paiva, J. C., Queirós, R., & Gasiba, T. (2023). Sifu reloaded: An open-source gamified web-based cybersecurity awareness platform (short paper). *Proceedings of the 4th International Computer Programming Education Conference (ICPEC), 112*, 5:1–5:8. https://doi.org/10.4230/OASIcs.ICPEC.2023.5

Piazza, M., & Olmsted, A. (2015). Herding cats: How to launch a cyber security club in an academic setting. *International Journal for Information Security Research, 5*(2), 559–564. https://doi.org/10.20533/ijisr.2042.4639.2015.0064

picoCTF. (n.d.). *Home*. Carnegie Mellon University. https://picoctf.org/

Radu, A., & Thomas, S. L.. *Organising monkeys or how to run a hacking club*. University of Birmingham. https://inaradu.com/publications/Organising_Monkeys.pdf

RingZer0. (n.d.). *RingZer0 team online CTF*. https://ringzer0ctf.com/

Root Me. (n.d.). *CTF all the day*. https://www.root-me.org/en/Capture-The-Flag/CTF-all-the-day/

Ruff, M., & Giacobe, N. A. (2022). Leveraging browser-based virtual machines to teach operating system fundamentals. *Journal of The Colloquium for Information Systems Security Education, 9*(1), 7. https://doi.org/10.53735/cisse.v9i1.150

Singh, M., Singh, P., & Kumar, P. (2020). An analytical study on cross-site scripting. *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 1–6. https://doi.org/10.1109/iccsea49143.2020.9132894

Votipka, D., Zhang, E., & Mazurek, M. L. (2021). Hacked: A pedagogical analysis of online vulnerability discovery exercises. *2021 IEEE Symposium on Security and Privacy (SP)*, 1268–1285. https://doi.org/10.1109/sp40001.2021.00092

Winters, T. (2020). *Evaluation of effective teaching materials and techniques for software security engineering* [Master's thesis, Worcester Polytechnic Institute]. https://digital.wpi.edu/downloads/k643b3960

Zeichick, D. (2024). Confidence and competence: The impact of National Cyber League participation on career development in cybersecurity. *Journal of Computing Sciences in Colleges, 39*(10), 40–47. http://ccsc.org/publications/journals/SW2024.pdf

APPENDIX A

316ctf Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	2	4	4
Student02	5	1	4	4
Student03	5	1	5	4
Student04	5	5	5	5
Student05	5	1	4	3
Student06	5	2	4	4
Student07	5	1	5	5
Student08	5	2	5	4
Student09	5	2	4	4
Student10	4	4	4	4
Student11	5	1	5	4
Student12	5	1	5	4
Student13	4	2	4	3
Student14	4	2	4	3
Student15	4	1	4	5
Student16	4	2	4	5
Student17	5	1	4	5
Student18	5	1	5	4
Average	4.72	1.78	4.39	4.11

APPENDIX B

CTFlearn Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	2	5	1	4
Student02	3	5	4	4
Student03	2	5	3	3
Student04	2	5	2	4
Student05	4	5	1	3
Student06	1	5	2	2
Student07	5	5	2	4
Student08	4	5	4	No Response
Student09	4	5	3	4
Student10	4	3	4	4
Student11	1	5	1	3
Student12	1	5	2	4
Student13	3	5	2	4
Student14	4	4	2	4
Student15	1	5	2	3
Student16	1	5	2	4
Student17	2	5	1	2
Student18	3	5	1	3
Average	2.61	4.83	2.17	3.47

APPENDIX C

Bandit Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	2	4	4
Student02	5	1	4	4
Student03	4	2	5	4
Student04	5	1	4	3
Student05	5	1	4	3
Student06	4	4	3	3
Student07	5	2	4	5
Student08	4	2	5	No Response
Student09	3	1	4	4
Student10	5	5	3	3
Student11	4	1	3	3
Student12	5	1	5	4
Student13	4	2	4	5
Student14	3	2	4	3
Student15	4	1	4	2
Student16	5	2	4	4
Student17	4	1	4	3
Student18	4	3	4	3
Average	4.33	1.89	4	3.53

APPENDIX D

Natas Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	1	4	5
Student02	5	1	4	5
Student03	4	2	4	4
Student04	5	1	4	4
Student05	5	5	4	3
Student06	5	1	5	5
Student07	5	1	5	4
Student08	4	2	4	No Response
Student09	3	1	2	4
Student10	5	4	4	3
Student11	5	2	5	5
Student12	5	2	5	5
Student13	4	1	5	5
Student14	4	2	4	No Response
Student15	4	1	4	4
Student16	5	1	4	5
Student17	5	1	4	5
Student18	5	2	5	5
Average	4.61	1.72	4.22	4.44

APPENDIX E

picoGym Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	4	4
Student02	5	1	5	5
Student03	4	2	4	4
Student04	5	1	4	4
Student05	4	2	3	3
Student06	5	1	5	5
Student07	5	1	5	4
Student08	4	2	4	No Response
Student09	4	2	4	4
Student10	5	4	4	4
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	2	5	4
Student14	4	2	4	No Response
Student15	5	1	4	4
Student16	5	2	4	5
Student17	5	1	5	5
Student18	3	4	3	4
Average	4.47	1.82	4.18	4.2

APPENDIX F

247CTF Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	2	4
Student02	5	1	5	5
Student03	4	2	4	4
Student04	5	1	4	4
Student05	4	1	3	3
Student06	No Response	No Response	No Response	No Response
Student07	5	1	3	3
Student08	4	2	4	No Response
Student09	4	4	3	3
Student10	5	5	3	4
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	2	4	4
Student14	4	2	4	No Response
Student15	4	2	4	4
Student16	5	2	3	4
Student17	No Response	No Response	No Response	No Response
Student18	No Response	No Response	No Response	No Response
Average	4.43	2	3.57	3.83

APPENDIX G

Hacker101 Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	No Response	No Response	No Response	No Response
Student02	5	1	4	4
Student03	4	2	4	3
Student04	4	2	3	4
Student05	4	1	4	3
Student06	3	2	4	4
Student07	5	2	4	4
Student08	4	2	4	No Response
Student09	4	4	3	4
Student10	5	3	4	3
Student11	4	1	4	4
Student12	4	3	3	4
Student13	3	2	4	4
Student14	4	2	3	No Response
Student15	4	4	4	3
Student16	5	2	4	4
Student17	4	2	4	4
Student18	No Response	No Response	No Response	No Response
Average	4.13	2.19	3.75	3.71

APPENDIX H

Root Me Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	3	2	4	4
Student02	5	4	5	4
Student03	4	3	2	2
Student04	3	4	2	2
Student05	4	5	4	3
Student06	5	4	4	4
Student07	4	4	4	4
Student08	4	2	4	No Response
Student09	4	3	2	3
Student10	4	4	4	4
Student11	1	5	2	2
Student12	2	4	4	2
Student13	4	2	5	4
Student14	4	2	4	4
Student15	3	4	4	3
Student16	4	2	3	3
Student17	1	5	1	3
Student18	2	4	3	4
Average	3.39	3.5	3.39	3.24

APPENDIX I

NCL Gym Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	5	3	4	5
Student02	5	1	5	5
Student03	4	2	5	4
Student04	5	1	5	5
Student05	4	1	2	3
Student06	4	1	4	3
Student07	5	1	4	5
Student08	4	2	4	No Response
Student09	4	2	4	5
Student10	5	1	5	5
Student11	5	1	5	5
Student12	5	1	4	5
Student13	4	2	4	3
Student14	4	2	4	3
Student15	5	1	5	5
Student16	5	1	5	5
Student17	5	1	4	5
Student18	5	1	4	5
Average	4.61	1.39	4.28	4.47

APPENDIX J

RingZer0 Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	4	4
Student02	4	2	4	4
Student03	No Response	2	4	4
Student04	5	1	4	3
Student05	4	2	1	3
Student06	5	2	5	4
Student07	5	2	4	4
Student08	4	2	4	No Response
Student09	4	2	1	1
Student10	4	4	2	3
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	4	4	4
Student14	4	2	4	4
Student15	4	1	4	4
Student16	4	2	4	4
Student17	4	2	3	3
Student18	4	3	3	2
Average	4.25	2.12	3.47	3.44

APPENDIX K

Defend the Web Survey Results

Pseudonym	Q1	Q2	Q3	Q4
Student01	4	2	4	4
Student02	5	1	5	5
Student03	4	2	4	4
Student04	5	1	3	3
Student05	5	1	5	3
Student06	4	2	3	4
Student07	5	1	5	5
Student08	5	2	4	4
Student09	3	2	4	3
Student10	5	3	5	3
Student11	No Response	No Response	No Response	No Response
Student12	5	1	4	4
Student13	4	4	2	4
Student14	4	2	4	4
Student15	4	1	4	4
Student16	4	4	4	4
Student17	4	1	4	4
Student18	4	2	4	4
Average	4.35	1.88	4	3.88