Enhancing Cybersecurity Education Through Multi-Opposing-Role Gameplay and Simulations

Nipuna Hiranya Weeratunge and Rune Hjelsvold
NTNU, Gjøvik, Norway

nipuna.h.weeratunge@ntnu.no
rune.hjelsvold@ntnu.no

Abstract: This paper presents the development, implementation, and evaluation of The XSS Game (TXG), a game-based educational tool designed to teach Cross-Site Scripting (XSS) attacks through a multi-opposing-role-playing game. Inspired by cognitive concepts like Transfer Learning, previous cybersecurity educational games have incorporated techniques such as adversarial thinking and role-switching. In many such games, the playable roles are often limited to attacker and defender. Building upon these, TXG was developed with an approach where players can take on three distinct roles: Attacker, Defender, as well as User, each providing players with a different perspective on XSS attacks. This approach aims to deepen students' understanding of XSS attacks by allowing them to experience multiple perspectives, enhancing their ability to identify, prevent, and respond to such threats. In addition, simulations are often used in cybersecurity educational games to provide learners with practical, hands-on experiences that are crucial for understanding complex cybersecurity concepts. While the main gameplay in TXG centres on role-based narratives drawn from real-life cybersecurity scenarios, requiring players to answer questions based on those narratives, the game also includes a Simulation Zone. This zone offers an immersive environment where players can perform various actions and observe their outcomes, enhancing experiential learning. Even though quiz-based and simulation-based cybersecurity educational games exist separately, the combination of the two has not been widely studied. By integrating both narrative-driven quizzes and interactive simulations, TXG aims to enhance students' learning by reinforcing theoretical knowledge with practical, hands-on experience, leading to a deeper and more applied understanding of XSS concepts. TXG was evaluated within a computer science course with 162 students through pre- and post-game surveys. Student feedback indicated that the multi-opposing-roleplaying with real-life scenarios approach had a modest but meaningful and practical impact on their learning to understand XSS attacks holistically. The Simulator Zone showed promise as an immersive and reinforcing learning tool, but low engagement limited its impact, and future improvements, such as more varied tasks, additional game elements, enhanced interactivity, and better UI/UX, are planned to boost engagement and better assess its educational value. Several players highlighted the game's effective learning format, which combines immediate in-game feedback with reflective pre- and post-game surveys, which holds promise for broader applications in cybersecurity education and beyond.

Keywords: Game-Based learning, Multi-opposing-role-playing, In-Game simulations, Cybersecurity education, Web application security, Cross-Site scripting attacks

1. Introduction

Cybersecurity is a critical concern across industries, making it essential for students, professionals, and the general public to understand its importance. However, widespread gaps in awareness persist. For instance, a multitude of firms, including media companies, retailers, and financial institutions, have been affected by cybersecurity breaches (Chen et al, 2025). These incidents highlight the severe consequences of neglecting cybersecurity, including financial loss, reputational harm, and even threats to human safety. In response, countries such as the US, Canada, EU members and several others have launched public initiatives to promote better cybersecurity practices (Van Steen et al, 2020).

1.1 Goals and Scope of the Paper

This study outlines the design, implementation, and testing of The XSS Game (TXG), a multi-opposing-role-playing game developed to teach Cross-Site Scripting (XSS) attacks to second-year computer science undergraduates. Players take on one of three roles, including opposing roles:

- Attacker: A technically skilled role focused on exploiting web application vulnerabilities.
- Defender (Developer): A technically skilled role aimed at securing web applications against attacks.
- User: A less technical role that interacts with the developed web applications.

This study aims to explore how a multi-opposing-role-playing game can teach the harmful effects of XSS attacks and provide mitigation skills to both technical and non-technical audiences. By adopting attacker and defender roles, players can learn to analyse and build more secure web applications, while the user role raises awareness about XSS threats for everyday users. Grounded in cognitive concepts like transfer learning, this approach helps students understand XSS attacks holistically through real-life scenarios from multiple

viewpoints. In addition, TXG includes a Simulation Zone where players can interactively simulate actions based on these cybersecurity roles.

Specifically, this paper explores the following research questions:

- RQ1: How can a multi-opposing-role-playing game effectively support teaching XSS topics to students?
- RQ2: What could the impact of narrative-based simulations be in helping students learn XSS topics?

The main contributions of this study include:

- TXG (The XSS Game): A web-based, multi-opposing-role-playing game designed to teach XSS attacks for all audiences.
- Analysis of results: Qualitative and quantitative insights from the first version of the game.
- An outline of a development framework: For creating educational games across various subject domains.

2. Background

2.1 Cross-Site Scripting (XSS) Attacks

Cross-Site Scripting (XSS) is an injection attack where malicious scripts are inserted into trusted websites. It occurs when a web application includes user input in its output without proper validation or encoding, allowing attackers to inject harmful code, typically JavaScript, into pages viewed by others (KirstenS, 2024). When a victim loads the compromised page, their browser executes the script, assuming it's from a trusted source. This can lead to exposure of sensitive data like cookies and session tokens, or even altered webpage content (KirstenS, 2024). Due to its severity, OWASP ranks XSS as the third highest risk in its Top 10 Web Application Security Risks list (The Open Worldwide Application Security Project, 2024).

2.2 Transfer Learning

In cognitive science and artificial intelligence research, transfer learning involves improving performance in one domain by applying knowledge from a related domain (Weiss et al, 2016). Blickensderfer et al (1998) describe a similar concept, cross-training, where training in multiple interacting roles enhances performance in each role. Similarly, Gonzalez et al (2013) mention that individuals perform better in competitive and team environments after experiencing the roles of teammates or rivals, as demonstrated in a role-switching simulation game.

2.3 Related Work

Recent studies highlight the effectiveness of game-based learning (GBL) in cybersecurity education by boosting engagement and understanding across diverse learners. For instance, Williams et al (2024) found that gamified Capture The Flag (CTF) events increased interest in cybersecurity careers among non-technical students. Similarly, Kim et al (2025) reported that gamified labs improved both learning outcomes and motivation over multiple semesters.

Moreover, existing educational games on XSS attacks have primarily focused on attacker/defender roles. Gaurav et al (2021) introduced four web-based games covering topics like SQL Injection, XSS, and more, aimed at system administrators and IT beginners. Adversarial thinking is another common element in cybersecurity games. For instance, [d0x3d!] (Gondree & Peterson, 2013) is a board game where players act as white-hat hackers combating adversarial networks. Moreover, MeetingMayhem (Huang et al, 2024) teaches asymmetric encryption by allowing players to assume adversarial roles.

In the context of role-playing and simulations, Jaffray et al (2021) introduced "SherLOCKED," a detective-themed serious game that effectively consolidated foundational security concepts among undergraduate students, highlighting the value of narrative-driven learning environments. Role-switching is also used in games like PenQuest (Luh et al, 2020), where players alternate between attacker and defender roles. Similarly, Zolotarev et al (2021) propose a game with diverse switchable roles including auditors, technicians, and managers. Bahrini et al (2020) developed a mobile game featuring opposing narratives, “Save My Home” and “Hacker War”, allowing players to act as both defender and attacker.

In summary, while there are several cybersecurity games that target XSS attacks, adversarial thinking and role-switching, there appear to be no educational games that involve multi-opposing-role gameplay, specifically

focused on XSS attacks. Moreover, many of the existing games focus on the attacker\defender dynamic and do not investigate the user role. Hence, this is the main research gap that this study aims to address.

3. Learning Outcomes

The primary intended learning outcomes of TXG are:

- Know how to identify the different types of XSS attacks from multiple perspectives
- Develop secure applications containing preventive measures to mitigate XSS attacks
- Providing an interactive and fun approach to learning cybersecurity

4. Implementation

TXG's implementation includes a frontend built with HTML, JavaScript, and CSS, and a backend using the Flask framework (Pallets Projects, 2010). For evaluation, players accessed the game via a shared application link. As shown in Figure 1, TXG follows a multi-opposing-role gameplay flow, where players take on Attacker, Defender, and User roles. Participants were also required to complete integrated pre- and post-game surveys for evaluation.

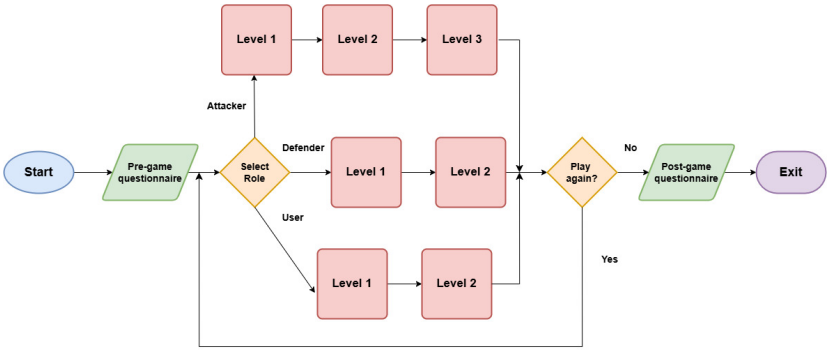

Figure 1: The XSS Game gameplay flowchart

5. Example Gameplay

TXG is a role-playing game where players assume different roles to answer questions based on specific XSS scenarios. As illustrated in Figure 2, the main gameplay involves players receiving an XSS-related question (box C), often paired with an image. To proceed, players must select answer(s) from the provided tiles (box E). In addition, box A offers access to external XSS information (KirstenS, 2024) and in-game guidance.

5.1 Simulator Zone

The Simulator Zone is a key feature of TXG, accessible through the crosshair button (Figure 2, box B) during specific questions. Within this zone (Figure 3), players can perform simulated actions such as navigating a target website, submitting test attack scripts, or defending against attacks by validating and sanitising inputs. These interactive elements aim to reinforce learning and provide a deeper understanding of XSS attacks, making TXG more than just a gamified quiz.

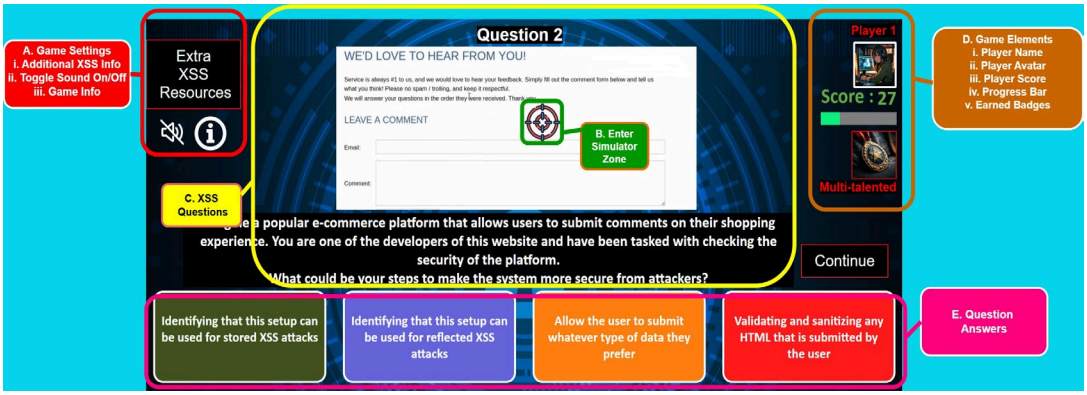

Figure 1: The XSS Game gameplay main components: A. Game Settings, B. Simulator Zone Button, C. XSS Questions, D. Game Elements, E. Question Answers

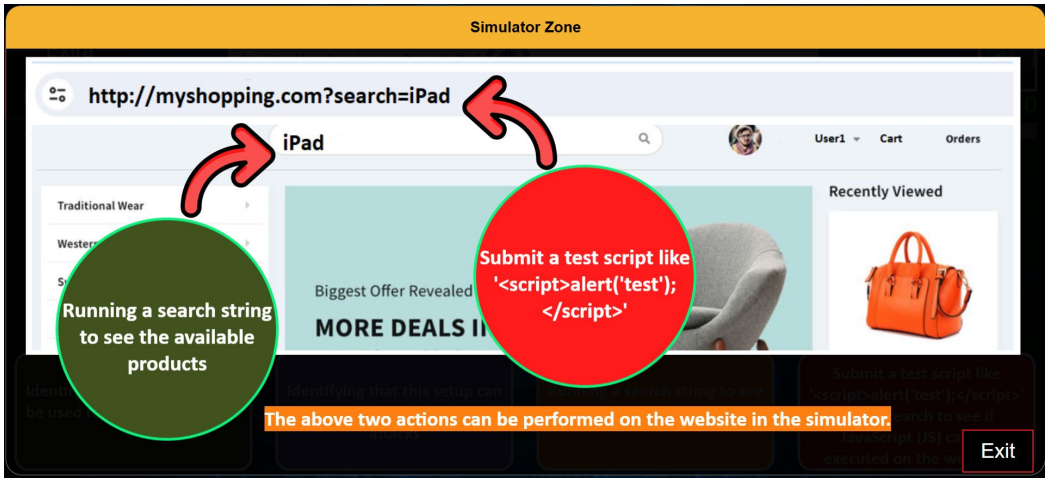

Figure 2: TXG Simulator Zone, where players can simulate actions

5.2 Game Elements

TXG contains several game elements aimed at increasing players' motivation and engagement, which can be seen in box D in Figure 2. Table 1 describes the elements in more detail.

Table 1: Game elements and description

Game element	Description
Player name	Allows players to personalise the gaming experience.
Player avatar	Allows players to personalise the gaming experience.
Player score	Rewards/penalises player actions. Players receive positive points for correct answers and negative points for incorrect answers. Adds a sense of accomplishment as well as competition.
Progress bar	Allows players to monitor game progression status.
Badges	Rewards player achievements. Players receive awards according to the number of completed roles: Expert badge for 1 completed role, Multi-talented badge for 2 completed roles, and All-rounder badge for 3 completed roles.
Leaderboard	Ranks player achievements, such as score and earned badges, to add a sense of competition and motivate players.

Moreover, interface features such as progress indicators, avatars, and badges were designed in line with Nielsen's usability heuristics (e.g., visibility of system status, user control) (Nielsen, 1994) and motivational principles from Malone and Lepper's framework, including challenge, control, and feedback (Malone & Lepper, 1987). These design choices aim to balance usability with meaningful learning engagement.

6. Data Collection

TXG was evaluated with a class of second-year undergraduate computer science students, where it was presented as an assignment in which the students would have to obtain a score of 80% or more to pass. The data for the evaluation were mainly collected from the pre-game and post-game surveys, as well as other in-game player behavioural data, such as the time spent completing the game, achieved scores and badges, and the time spent in the Simulator Zone.

Before data collection, the survey and data handling procedures were reviewed and approved by Sikt – the Norwegian Agency for Shared Services in Education and Research. The study primarily collected non-personal data, such as participants' age group, education level, cybersecurity knowledge, gaming experience, and opinions. The only personal data collected, participants' institutional email addresses, were used solely for assignment marking and were permanently deleted after grading to ensure anonymisation.

The research adhered to international standards for human-subject research, following General Data Protection Regulation (GDPR), National Committee for Research Ethics in the Social Sciences and the Humanities (NESH) guidelines, and Declaration of Helsinki. Participants were clearly informed about the study's purpose, the data collected, and their rights, including the right to withdraw at any time without

penalty. Since the study posed minimal risk and all personal data were anonymised, additional ethics committee approval was not required under national regulations.

7. Evaluation Results and Discussion

7.1 Data Overview

After initial data cleaning steps, 162 unique players were found to have participated in the evaluation. The average playtime to complete the game was 15 minutes and 47 seconds. In the pre-game survey, information such as demographic data, player familiarity with cybersecurity concepts, and previous gaming experience was also collected. This is summarised in Table 2.

Table 2: Pre-game survey data, N=162

Category	Data values
Gender	Female (F): 29.9% Male (M): 41.5% Prefer not to answer: 28.6%
Knowledge about Cybersecurity concepts (CSK)	No knowledge (NK): 3.8% Basic knowledge (e.g. regular web surfing) (BK): 62.3% Advanced knowledge (e.g. specialised cybersecurity education) (AK): 33.9%
Previous gaming experience (PGE)	No previous gaming experience (NGE): 6.2% Some gaming experience (SGE): 43.2% High level of gaming experience (HGE): 50.6%

It should be noted that the player comments that are presented in the following sections are presented as they were received to convey their original meanings and have not been edited for grammar.

The pre-game survey also obtained the players' views on gaming, which can be categorised as Positive, Neutral and Negative sentiments, as seen below.

Positive sentiments

> *"I think gaming is a fun way to spend time, as well as a good tool to learn while having fun!"*
>
> *"I like gaming and have been gaming since I can remember. It's both social and fun when shared with others."*

Neutral sentiments

> *"I am glad that gaming is an option for a hobby, however, I don't consider myself a gamer nor am I interested in working with game development in the future."*
>
> *"No opinion."*

Negative sentiments

> *"Gaming is not really that interesting to me."*
>
> *"It's boring at my age"*

Out of the 162 players, the majority of the players' game sentiments were positive (75%) followed by neutral and negative sentiments at 24% and 1% respectively. As shown in Table 2, almost all players (about 94%) have previous gaming experience. The table also shows that almost all players had some level of cybersecurity knowledge (about 96%), with a significant portion mentioning an advanced level of cybersecurity knowledge (about 34%).

7.2 UI/UX

One of the main aspects pointed out by the players was the UI/UX issues faced during gameplay. Before starting TXG, players could adjust the browser zoom to scale the game elements. However, by looking at the player comments, it seems that this approach needs to be redone, so that the game scales for all resolutions

and browsers. Moreover, some players mentioned that having sound effects for button clicks was somewhat distracting and annoying.

> *"The design of the website. I had to change the size of the browser (after adjusting it to the targets in the beginning) for every question in order to see all of the text."*
>
> *"The sound effects kinda drove me mad."*
>
> *"Only small nitpicky stuff about the visual style, the black background behind the text is a little jarring, make it a bit more opaque or something that fits the background picture better."*

7.3 RQ1: Effectiveness of Multi-Opposing-Role-Play for learning XSS topics

7.3.1 Multi-Opposing-Role-Playing

Several players commented that playing the game through multiple opposing roles was interesting and suggested adding more tasks and variety to the roles.

> *"Love these kinds of games and assignments. I really liked getting to pick an avatar, the scoreboard and getting to try out as both user, defender, and attacker."*
>
> *"More difference in the roles, maybe an input option where you can write additional scripts as an attacker, or click on a fake link as a user to show how you can be redirected to a site."*
>
> *"More questions, but let the player choose the same player role multiple times."*
>
> *"Maybe make the role of user a bit harder."*

7.3.2 Adversarial thinking

It was interesting to see that some players were actually trying to invoke XSS attacks on TXG itself, in order to find vulnerabilities. This goes to show that adversarial thinking can be a beneficial skill when it comes to cybersecurity education.

> *"<script>alert('XSS HEHEHE')</script>"*
>
> *"<script>alert('xss')</script> just had to lol."*

7.3.3 Student learning

Most of the players (about 56%) mentioned that TXG provided a good learning experience to learn complex subject matters, such as XSS.

> *"It was fun, motivating and it did not feel like a lecture, even though I learned a lot. I also liked that I got the answers to the questions right away, so that it was easy to understand where I went wrong."*
>
> *"Educational, I think the explanations are simple enough that regular people with no knowledge about cybersecurity would understand."*
>
> *"I really enjoy this way of learning and testing my understanding of the subject at hand. This shows that the lecturer takes their students enjoyment of the subject into consideration. This was fun and engaging, something that we rarely see in our everyday as university students."*

However, some players mentioned that adding more varied tasks could result in a better learning experience.

> *"More difference in the roles, maybe an input option where you can write additional scripts as an attacker, or click on a fake link as a user to show how you can be redirected to a site."*
>
> *"Maybe add some other types of tasks than just questions. For example tasks where we can test more scripts?"*

To evaluate the effectiveness of TXG in improving participants' understanding of XSS attacks, a Wilcoxon Signed-Rank Test was conducted on the total number of correct responses before and after gameplay. The hypotheses tested were: Null Hypothesis (H_o) — there is no difference in participants' XSS knowledge before and after playing TXG (median difference = 0); and Alternative Hypothesis (H_1) — there is a significant difference in participants' XSS knowledge after gameplay (median difference ≠ 0). The analysis revealed a statistically significant improvement, with a Z-score of 3.40 and a two-tailed p-value of 0.00067, indicating strong evidence against the null hypothesis. The mean difference in scores was 0.27 (SD = 1.02), suggesting a

modest gain in performance. The effect size (r = 0.52) indicates a large practical impact, and the surprisal value (S = 10.55) further emphasises the strength of the result. These findings demonstrate that TXG had a statistically significant and practical positive effect on participants' XSS knowledge, reinforcing its potential value as an effective tool for cybersecurity education through game-based learning.

7.3.4 Overall rating

The post-game survey also featured a 1–5 Likert scale where players could rate the TXG playing experience along several dimensions. This is shown in Figure 4, which illustrates that TXG has performed relatively well in the different categories. For instance, it is encouraging to see that about 52% of the players stated that they would recommend TXG to others. However, many neutral responses suggest that there is much room for improvement.

Table 3 presents the average overall ratings across the categories shown in Table 2, such as gender, previous cybersecurity knowledge, and previous gaming experience. Both females and males have rated TXG similarly across the different categories, with a difference of only 0.1 in some of the categories. The main exception is in the category, Game elements made TXG more engaging, where males have rated TXG slightly lower than females (3.0 vs 3.2, respectively).

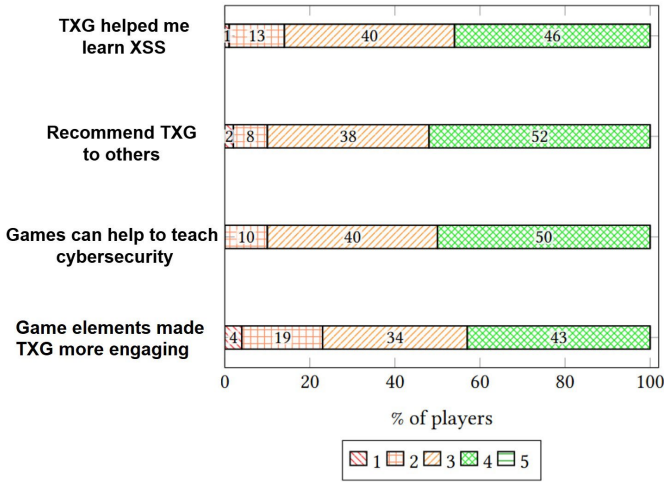

Figure 3: Survey responses represented by the Likert scale chart, where 1–5 represents strongly disagree, disagree, neutral, agree, and strongly agree, N=162

In the CSK group, players with no prior cybersecurity knowledge rated TXG more positively than those with basic or advanced knowledge in areas such as recommending the game (3.7 vs. 3.3 and 3.4), its value in teaching cybersecurity (3.8 vs. 3.4 and 3.4), and the engagement provided by game elements (3.5 vs. 3.1 and 3.2). A similar trend was seen in the PGE group, where non-gamers rated the game slightly higher in terms of recommendation and engagement. However, as these groups made up only 3.8% and 6.2% of participants respectively, firm conclusions cannot be drawn. Minimal rating differences were observed between players with some or high prior knowledge and experience, suggesting a generally consistent reception among more experienced users. Issues such as limited interactivity and UI/UX shortcomings may have influenced overall ratings.

Table 3: Average overall 1–5 Likert scale ratings analysed by the categories given in Table 2

Category	Average Overall Rating							
	Gender		CSK			PGE		
	F	M	NK	BK	AK	NGE	SGE	HGE
TXG helped me learn XSS	3.3	3.3	3.3	3.3	3.3	3.2	3.3	3.3
Recommend TXG to others	3.3	3.2	3.7	3.3	3.4	3.6	3.4	3.3
Games can help to teach cybersecurity	3.3	3.4	3.8	3.4	3.4	3.4	3.4	3.4
Game elements made TXG more engaging	3.2	3.0	3.5	3.1	3.2	3.4	3.2	3.2

Despite these limitations, TXG demonstrated its effectiveness in supporting learning outcomes and addressing RQ1. The multi-opposing-role-playing format promoted engagement, adversarial thinking, and improved understanding of XSS attacks. Players responded positively to the role diversity and suggested greater task variety, with learning outcomes showing a modest but meaningful and practical improvement. Future iterations should enhance interactivity and UI/UX design to further increase effectiveness and user satisfaction.

7.4 RQ2: Impact of Narrative-Based Simulations on XSS Concept Reinforcement

7.4.1 Simulation zone

Several players mentioned that the Simulator Zone made the game immersive and supported their learning. However, only about 22% of the players had utilised the Simulator Zone, with an average of 1 minute and 28 seconds spent within it.

> *"I like quiz type games and find them fun and interesting, and the simulator zones help with making it feel more like an immersive game."*
>
> *"I liked that it was a quiz, and with the simulation zone, it was a great idea to make the game more immersive."*
>
> *"I like the concept, the gamification makes the concepts easier and having the simulation zone helps solidify the concepts."*
>
> *"Loved being able to learn through a game, and loved the simulation area! Great that one can get more insight into a topic if needed."*
>
> *"The simulator zone was a great addition to The XSS Game, it truly makes the game feel unique and engaging. Definitely the best mechanic."*

Although there were positive comments about the Simulation Zone, several players mentioned existing weaknesses and potential improvements that can be made to it.

> *"Simplicity, easy to follow, and not a need for entering the simulation zone to complete the assignment."*
>
> *"A bit more interactive simulation zone."*
>
> *"The simulator was not very useful and often forgotten/ ignored."*

Given these findings, it is clear that while the Simulator Zone holds potential, the current version was underutilised, and its educational impact is difficult to assess reliably. Therefore, the conclusions related to RQ2 remain preliminary, with this study identifying the Simulator Zone as a promising but currently limited feature.

7.5 Educational Game Development Framework

Many of the players mentioned that this style of learning was enjoyable and effective.

> *"It is still a bare bones game but that's about it for me, so I am hopeful that with more dev time this game will become a fun tool for learning."*
>
> *"Interactivity is always fun and useful to ensure engagement. Nice to have both a pre-game and post-game questionnaire to help reflect over what was learnt throughout the game."*
>
> *"This was honestly one of the best learning experiences I've had. Incredibly fun and learning a lot along the way!"*
>
> *"I like that this game has an interactive learning approach with different scenarios that could happen in the real-world. I also like that there's somewhat an explanation of the wrong and correct answers. The visual examples are a plus too, made it more engaging."*

The educational game development framework presented in this study offers a flexible and interactive foundation for creating quiz-based learning games that incorporate multi-opposing roles, scenario-based tasks/simulations, and layered complexity. Specifically, the framework consists of a conceptual model, source code, UI designs, and evaluation data, which can be used to accelerate similar educational game development. Designed to enhance engagement and understanding, the framework allows players to take on roles such as

attacker, defender, and user, promoting critical thinking and real-world application. It also includes built-in pre- and post-game surveys to assess learning outcomes, making it suitable for researchers and educators across various disciplines. By adapting the content and roles, others can use this framework to develop educational games tailored to their specific teaching goals.

8. Limitations and Future Work

8.1 Control Group Evaluation

A key limitation of this study is the absence of a comparison with a control group. Future research plans include conducting an evaluation with one group interacting with TXG and a control group engaging in traditional learning activities, such as lectures, to compare outcomes. In addition, future studies will incorporate interviews as a data collection method, as interviews provide greater flexibility and allow for a deeper exploration of topics of interest, such as how playing different roles influenced the learning process, compared to surveys.

8.2 UI/UX Improvements

It is also planned to improve the UI/UX issues addressed by the players in the next iteration of TXG. This will focus on adding more visually appealing interfaces and options to control the sound effects. In addition, more varied tasks and XSS scenarios will be added to the different roles for a better learning experience. Specifically, it is planned to investigate why fewer players entered the Simulator Zone and whether improvements, such as increased interactivity, task variety, better game integration, multiplayer features, extra points and badges, and narrative-based simulations, along with UI/UX enhancements, would motivate players to utilise it more.

9. Conclusion

This study presents The XSS Game, a multi-opposing-role-playing game to learn XSS attacks for all audiences, which was evaluated with a group of second-year undergraduate computer science students. The initial evaluation results show that TXG was able to achieve the intended learning outcomes and is a promising tool to teach XSS attacks and other topics. Regarding RQ1, the player comments suggest that they found the multi-opposing-role-playing with real-life scenarios approach useful to their learning and proposed to have even more varied interactions, multiplayer, and replayability functionalities. Even though the study could not effectively answer RQ2, several players indicated that the TXG Simulator Zone provided an immersive experience and proposed more tasks and additions to it. UI/UX improvements, along with increased interactivity and task variety, are planned as future work to investigate RQ2 and beyond.

Many players also indicated that the TXG game format provided an effective learning experience with immediate answer feedback, while the pre- and post-game surveys helped to reflect on the lessons learned. This ultimately suggests that other game developers may consider using the TXG game format to develop educational games or even adding similar “training zones” to their games.

Acknowledgements

This work was supported by the Centre for Excellent IT Education (Excited), cofounded by the Norwegian Directorate for Higher Education and Skills (HK-Dir), project no. 528526.

Ethics Declaration: As stated in Section 6, the survey questions and data collection methods were reviewed and approved by the Sikt – the Norwegian Agency for Shared Services in Education and Research – before data gathering.

AI Declaration: Grammarly was used to check and correct the grammar of the study. This was the extent of AI use in the study.

References

Bahrini, M. et al., 2020. *Good vs. evil: Investigating the effect of game premise in a smart home security educational game.* s.l., Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play.

Blickensderfer, E., Cannon-Bowers, J. A. & Salas, E., 1998. Cross-training and team performance.. *American Psychological Association*.

Chen, C.-Y., Goh, B. W., Lee, J. & Li, N., 2025. The Effect of Cybersecurity Breaches on Analysts’ Earnings Forecasts. *European Accounting Review,* pp. 1--27.

Gaurav, D. et al., 2021. *Cybersecurity training for web applications through serious games.* s.l., IEEE International Conference on Engineering, Technology & Education (TALE).

Gondree, M. & Peterson, Z. N., 2013. *Valuing Security by Getting {[d0x3d!]}: Experiences with a Network Security Board Game.* s.l., 6th Workshop on Cyber Security Experimentation and Test (CSET 13).

Gonzalez, C., Saner, L. D. & Eisenberg, L. Z., 2013. Learning to stand in the other's shoes: A computer video game experience of the Israeli--Palestinian conflict. *Social Science Computer Review,* Volume 31, pp. 236--243.

Huang, S. et al., 2024. *A User Experience Study of MeetingMayhem: A Web-Based Game to Teach Adversarial Thinking.* s.l., Innovation and Technology in Computer Science Education.

Jaffray, A., Finn, C. & Nurse, J. R., 2021. *Sherlocked: A detective-themed serious game for cyber security education.* s.l., International Symposium on Human Aspects of Information Security and Assurance.

Kim, J. B., Zhong, C. & Liu, H., 2025. The Impact of Gamification on Cybersecurity Learning: Multi-Study Analysis. *Communications of the Association for Information Systems,* Volume 56, p. 6.

KirstenS, 2024. *Cross Site Scripting (XSS).* [Online] Available at: https://owasp.org/www-community/attacks/xss/ [Accessed 10 04 2025].

Luh, R. et al., 2020. PenQuest: a gamified attacker/defender meta model for cyber security assessment and education. *Journal of Computer Virology and Hacking Techniques,* Volume 16, pp. 19--61.

Malone, T. W. & Lepper, M. R., 1987. *Making learning fun: A taxonomy of intrinsic motivations for learning.* s.l.:Routledge.

Nielsen, J., 1994. *10 Usability Heuristics for User Interface Design.* [Online] Available at: https://www.nngroup.com/articles/ten-usability-heuristics/ [Accessed 03 05 2025].

Pallets Projects, 2010. *Welcome to Flask — Flask Documentation (3.1.x).* [Online] Available at: https://flask.palletsprojects.com/en/stable/ [Accessed 05 04 2025].

The Open Worldwide Application Security Project, 2024. *OWASP Top Ten | OWASP Foundation — owasp.org.* [Online] Available at: https://owasp.org/www-project-top-ten/ [Accessed 08 04 2025].

Van Steen, T., Norris, E., Atha, K. & Joinson, A., 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use?. *Journal of Cybersecurity,* Volume 6.

Weiss, K., Khoshgoftaar, T. M. & Wang, D., 2016. A survey of transfer learning. *Journal of Big data,* Volume 3, pp. 1--40.

Williams, L., Anthi, E., Cherdantseva, Y. & Javed, A., 2024. Leveraging gamification and game-based learning in cybersecurity education: engaging and inspiring non-cyber students. *Journal of The Colloquium for Information Systems Security Education,* Volume 11, pp. 8--8.

Zolotarev, V. V. et al., 2021. *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT & QM &IS).* s.l., IEEE.