Gamification in Cybersecurity: Improving Employee Compliance through Game-Based Learning and Incentives.

MSc Research Project
MSc Cybersecurity

Efoseh Iliya Fachano
Student ID: x22198911

School of Computing
National College of Ireland

Supervisor: Dr. Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: …Efoseh Iliya Fachano………………………………………………………………………………

Student ID: ……x22198911…………………………………………………………………………………..……

Programme: …MSc Cybersecurity…………………………………… **Year:** ……2023………………..

Module: ……MSc Research Project…………………………………………………………….………

Supervisor: Dr. Vanessa Ayala-Rivera…………………………………………………………….………

Submission Due Date: 31 January 2024……………………………………………………………….………

Project Title: Gamification in Cybersecurity: Improving Employee Compliance through Game-Based Learning and Incentives……………………………………..

Word Count: ……5824……………………….. **Page Count**…22……………………………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: …………Efoseh Fachano………………………………………………………………

Date: …………14 December 2023……..…………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Gamification in Cybersecurity: Improving Employee Compliance through Game-Based Learning and Incentives.

Efoseh Iliya Fachano
x22198911

Abstract

Cybersecurity is the practice of protecting computer systems, networks, and data from cyber-attacks. To prevent attacks caused by human error, organizations must ensure that their employees are aware of security measures and follow relevant standards and protocols. While different security awareness programmes are available, the most effective ways for raising security awareness are still debatable. Nowadays, companies use various methods such as policies, procedures, and training sessions to increase security awareness. Traditional information security training sessions have relied heavily on presentation slides and videos. This study explores how gamification can be used effectively to improve employee compliance with cybersecurity practices. An experiment was conducted with two groups where there was an experimental group with gaming elements and a control group without gaming elements. A quiz was given to both groups at the end of the experiment to measure their knowledge retention on the topic of OWASP Top 10. The experimental group had an overall accuracy score of 63% while the control group had an overall accuracy score of 57%. The findings of the experiment suggests that gamified learning can be more effective than traditional slides and manuals as it can improve knowledge retention of participants taking part in cybersecurity awareness training. This indicates that making cybersecurity education more enjoyable, rewarding, and competitive, organizations can increase employee engagement and motivation to adhere to security measures, ultimately reducing the risk of cyber-attacks.

***Keywords*: Cybersecurity Compliance, Gamification, Cybersecurity Awareness, Cybersecurity Training, OWASP Top 10**

1 Introduction

According to Sharif & Ameen (2020), cybersecurity is not only about technology, but it is also about the people who use it, which means that they are responsible for the proper usage and operation of technology. This includes technological and procedural components, as well as computer users, system security managers, enforcement team members, and other information system resource personnel. Employee's knowledge, behaviours, views, personalities, talents, or interests typically influence the people working in information security. Employees are also aware of security standards and play an active role in defending systems. However, one of the most significant difficulties that organizations face is a lack of compliance with security policies.

DeCusatis et al. (2022) suggest that the majority of cybercrimes can be traced back to mistakes made by users. User errors continue to be the primary factor in 86% of all data breaches, with over 35% of all identified breaches are attributed to phishing attacks. The solution to these issues is by enhancing cybersecurity awareness training, which could enable users to identify and avoid actions that compromise cybersecurity. A 2021 survey revealed that only 27% of global information workers are familiar with their organisation's security policy, and 8% confessed to deliberately ignoring or bypassing security protocols.

Sharif and Ameen (2020), stated that the demand for cybersecurity awareness and training has grown significantly over time, leading to an increase in more companies implementing cybersecurity training for their employees. Despite using various strategies and techniques for training, these often fail as they do not necessarily teach employees how to conceptualize or apply cybersecurity principles (Cone et al., 2006). The lengthy manuals and documents used in cybersecurity training can be monotonous and time-consuming, this highlights the need for more efficient and sustainable training methods. There should also be more frequent reviews and evaluations, and possibly incentives, to keep employees engaged and motivated to learn and adhere to cybersecurity procedures.

Li et al. (2019) noted that numerous studies on cybersecurity have shown that security protocols are not always effective for employees. Even after receiving written security policies and guidelines, some employees choose to ignore their organization's information security standards, while others tend to overestimate the risks associated with information security. Interestingly, even those who have received sufficient cybersecurity training from their employers do not consistently show improved cybersecurity behaviour.

The research question derived from the research problem discussed above is: *How does incorporating gamification elements and incentives improve employee adherence to cybersecurity protocols?*

I proposed an experiment to discover how to improve compliance and to provide insights on how to tackle the research problem. The study examines how organizations that have adopted gamified approaches to cybersecurity awareness have fared in terms of employee behaviour and security outcomes. It also seeks to understand how various game elements, such as rewards, challenges, points, badges, levels, leaderboards, influence learning and compliance to cybersecurity principles.

The next part of the paper is divided into sections. Section 2 presents a literature review on various studies related to cybersecurity awareness, gamification, employee compliance, and incentives. Section 3 outlines the research methods and specifications that will be employed in the study. Section 4 covers the design specifications. Section 5 highlights the implementation, and Section 6 gives an evaluation of the results. Finally, Section 7 concludes with the Conclusion and Future Work.

2 Related Work

Numerous research has been done on cybersecurity awareness as well as the application of gamification in such training. This section dives into some of these studies, particularly those that have conducted surveys on existing cybersecurity games. Another study that this section examines is one that focuses on the importance of cybersecurity awareness for employees. Other studies that are included in this section relate to OWASP Top 10[1]. These studies also investigate whether employee compliance is driven by gaming elements and incentives.

2.1 Gamification in Cybersecurity

Gamification is integrating gaming elements and techniques into areas that typically do not have gaming elements to enhance engagement, motivation, and learning outcomes (Matovu et al., 2022). In addition to that, Oroszi (2020) proposed that by integrating gamification principles into cybersecurity education, businesses can transform the training process into a lively and engaging experience, thereby improving employee compliance and reducing security risks.

Sharif & Ameen (2020) found that 71% of companies employ gamification, while only 29% utilize other training methods. A survey conducted in 2020 explored various games designed to educate students and employees at different levels about cybersecurity topics such as malware, threats and attacks, internet safety, and more (Hill et al., 2020). The survey revealed that cybersecurity professionals have access to a lot of resources for educating employees in the workplace.

Gamification methods are useful because individuals enjoy competition and immediate feedback on their decisions, and employees understand that their actions can influence outcomes and they can experiment with the consequences of their decisions (Scholefield & Shepherd, 2019). One form of gamification is known as a serious game. Van Steen & Deeleman (2021) described a serious game stating that it is different from a traditional game because its main objective is not entertainment or enjoyment. Serious games aim to promote learning among participants. Hodhod et al., (2003) stated that serious games that incorporate learning theories can replicate learning-related behaviour and offer a way to improve the effectiveness of cybersecurity education, making it more interactive, engaging, and personalized for learners. Tirumala, Valluri, & Babu (2019) discussed how serious games apply to cybersecurity, ranging from wargames to safety and security games, which provide a valuable alternative to standard safety training and allow learners to explore various scenarios before encountering them in their daily lives.

Matovu et al. (2022) explored how freemium gamified platforms can be used to teach cybersecurity awareness, especially social engineering techniques and countermeasures, to students from different disciplines. Kahoot!, a widely used online platform for game-based learning, was used to deliver cybersecurity education, focusing on social engineering. Similar

[1] https://owasp.org/Top10/

to Kahoot!, another platform called Quizziz[2] also features various game mechanics, such as timing, rewards, leader board, etc., that enhance interactivity, learner's involvement, and understanding of the cybersecurity topic. In this study, both groups, an experimental and control group will take a quiz on the Quizziz platform to assess their knowledge retention and engagement on the cybersecurity topic.

2.2 Cybersecurity Awareness

Security awareness involves the user's capacity to identify and avoid activities that pose as cybersecurity threats, along with the ability to respond with intelligence and responsibly to enhance cyber safety (Sharif & Ameen, 2020). Achieving this goal requires continuous Cyber Security Awareness (CSA) training, emphasizing ongoing efforts and a commitment to constant improvement. Cybersecurity personnel must stay informed about the evolving cyber threat landscape, technological developments, and changes in an organisation's goals and priorities to stay relevant to their target audience and enhance organisational security (Chaudhary, Gkioulos, & Katsikas, 2022).

A recent study by Martin and Helebrandt (2022) highlights the importance of training individuals to ensure their safety and confidence in the digital environment. Effective security management training equips individuals with an understanding of the actions necessary to mitigate risks on the internet. It is crucial for them to possess both theoretical knowledge of threats and practical skills to defend against them. This comprehensive training approach aims to cultivate a new generation of cybersecurity specialists who can not only articulate their expertise but also lead or manage teams working on projects such as penetration tests and red team assaults for businesses. Ultimately, these professionals play a crucial role in defending both businesses and individuals in society.

Traditional training approach for information security have heavily depended on the use of slide presentations and videos. Abu-Amara & Tamimi (2021) proposed an interactive game called Cyber Shield to bring awareness to password complexity and physical security. This influenced the idea for this study to create a game about Open Web Application Security Project (OWASP) and a slide presentation, then compare and assess the two groups with a final quiz at the end.

2.3 Open Web Security Project (OWASP) Top 10

Web security is a big concern for both web developers and users due to the increased reliance on web applications. Intruders target web applications to launch various attacks such as browser attacks, cookie-session theft, cross-site scripting, and many others. Securing web applications, including all web services and functionality within the web app, can reduce the risk of data and customer breaches. The Open Web Application Security Project (OWASP) has created a ranking of critical web application security risks along with remediation

[2] https://quizizz.com/

guidance to help understand the various types of cybersecurity risks that could affect web applications (Aljabri et al., 2022).

According to the non-profit organisation OWASP, it aims to improve software security by providing free resources and tools to developers. The OWASP Top 10 is a list of the most critical web application security risks, updated every few years. The latest version, OWASP Top 10:2021, was released in June 2021.

Some studies on OWASP are available, however, they mostly discuss Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) (Farah et al., 2016) and SQL Injection as they seem to be the most common attacks. Alazmi & De Leon (2022) evaluated the effectiveness of web vulnerability scanners (WVSs) in detecting vulnerabilities related to the OWASP Top Ten. The study evaluated 12 WVSs by 15 original evaluation studies. The evaluations tested mostly only two of the OWASP Top Ten vulnerability types: SQL injection (SQLi) and Cross-Site Scripting (XSS). The study suggests that WVSs should be improved to detect more vulnerabilities, especially those related to the OWASP Top Ten.

This research hopes to bring more awareness to the area of web security.

2.4 Employee Compliance and Incentives

Babatunde (2016) explained that adherence to security includes security governance and frameworks that ensure organizations comply with specific security policies and practices to strengthen data and security infrastructure. The majority of security compliance is determined by regulations in the country that they operate in as well as in their business sector. For example, in the United Kingdom, transactions in the banking industry payment operations and must comply with Payment Card Industry Security Standards Council (PCI DSS).

The Social Exchange Theory (SET) suggests that the reciprocal exchange of social and material resources is a key motivator for individuals and a basic aspect of human interaction. Also, a psychological contract, as described by Michaelides (2021), is an unwritten pact between an employee and an employer, containing interactions that could be transactional or relational and are based on certain assumptions. Incentives can be perceived as a transaction where employees are rewarded for actively learning about cyber safety. Various types of incentives such as badges, points, or even virtual currency can be earned by users as they progress, providing a sense of achievement and motivation. Employees who consistently follow security practices and exhibit good cybersecurity behaviours can be given incentives.

Scholefield & Shepherd (2019) discussed a study where gamified learning activities were used to teach C-programming at the university level. In this context, gamification enhanced knowledge acquisition by offering rewards like badges and points and enabling students to showcase their social status through a leaderboard. However, gamification did not prove effective for all students. For example, some students who earned a hundred points in the educational game stopped playing instead of continuing to engage in additional tasks. Perhaps, if provided with incentives, they might have continued to participate in the game.

3 Research Methodology

Several investigations into gamification have been conducted, including a case study examining the efficacy of escape rooms (Oroszi, 2020), a simulated phishing training exercise compared to gamified phishing education games (Davis & Grant, 2022), and a survey that focused on serious games for cybersecurity training and education (Hill et al., 2020). This paper is an experimental study where participants, are randomly allocated to separate groups, an experimental group and a control group. The key variable is the presence or absence of gamification and incentives in this cybersecurity awareness training. The experimental group receives rewards after completing training tasks, while the control group does not receive any reward. The results are analysed to evaluate the influence of incentives on behavior, measured through compliance with security protocols, engagement and knowledge retention.

3.1 Research Methods

Research Question: How does incorporating gamification elements and incentives improve employee adherence to cybersecurity protocols?
Hypothesis: Participants who experience gamification in this case it is the experimental group, will demonstrate higher compliance levels than those in the control group.

The research methodology is composed of the following steps:

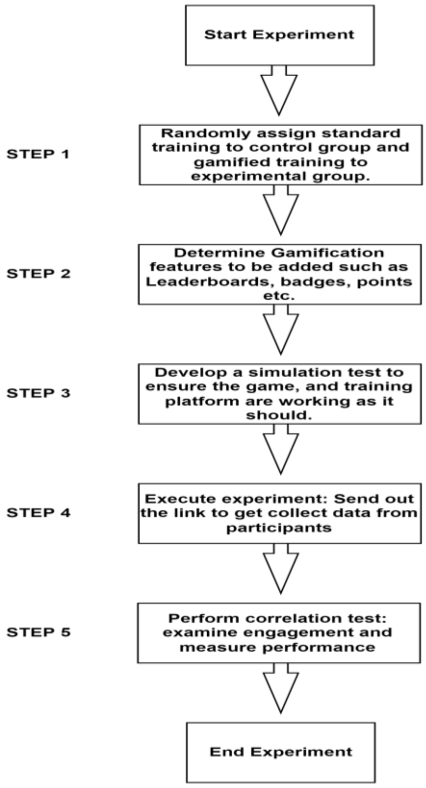

Start Experiment
STEP 1
Randomly assign standard training to control group and gamified training to experimental group.
STEP 2
Determine Gamification features to be added such as Leaderboards, badges, points etc.
STEP 3
Develop a simulation test to ensure the game, and training platform are working as it should.
STEP 4
Execute experiment: Send out the link to get collect data from participants
STEP 5
Perform correlation test: examine engagement and measure performance
End Experiment

Figure 1: Flow Diagram

Step 1: Design the experiment with a control group and an experimental group. For unbiased results, randomly assign participants to each group. The control group received standard cybersecurity training without gamification features, while the experimental group received the gamified version with incentives.

Step 2: Determine the gamification features to be included in the experimental group. These include badges, leaderboards, points, levels, and rewards for completing the game tasks. In this experiment the gamified version has levels in which the participant will have to pass and get to the next level.

Step 3: Develop a simulation test, where participants are introduced to scenarios on the gamified training to assess how effective it is and identify any potential issues. This will assist in refining the gamification elements before the main experiment.

Step 4: Create the questionnaire and send out the link to participants to gather data for the experiment. This was achieved through observations, recorded interactions, and data from the training platform.

Step 5: Send out the questionnaire to execute the main experiment, ensuring that participants in the two groups receive the same training content, except for the gamification features in the experimental group. However, the quiz content is the same for both groups.

Step 6: Carry out a correlation test to examine the relationship between engagement measures in gamification such as points earned and completion rates. This experiment will determine whether increased engagement with gamification elements correlates with higher compliance.

3.2 Ethical Considerations

This section tackles the ethical considerations of the research, including getting consent from participants, ensuring confidentiality and privacy, and addressing any potential risks to participants. This means adequately informing participants about the purpose of the study, the implications of their participation, and their rights as research subjects. Participants can voluntarily give their consent, free from coercion or undue influence. The process of informed consent is documented, and participants have the right to ask questions and withdraw their participation at any point without any negative consequences. The privacy and confidentiality of participants is upheld, and their personal information is kept confidential. All data collected during the study is anonymous and securely stored to prevent unauthorized access.

Firstly, approval from the college was obtained by filling and submitting the Declaration of Ethics Consideration Form and the Ethics Application Form. Then, the participants are presented with an opening statement that informs them about the purpose of the study, what information is collected, the researcher’s contact details and an Opt-In checkbox to obtain informed consent. If the participant gives their consent, then the first part of the questionnaire will appear asking general background questions such as if the participant is either a student or employee, what area of IT they are familiar with, how many years of experience in the area, and how familiar they are with the OWASP Top 10 vulnerabilities.

Finally, the participants will take the training material in one of the two ways available. Once they complete the training, a final knowledge quiz is given to the participants to take. The quiz will ask questions about the topic they learned in the training. Then the quiz results are analysed and the findings are included in the Evaluation.

4 Design Specification

The material that was used for providing the cybersecurity training is centered around OWASP (Open Web Application Security Project) Top 10 vulnerabilities (Berisford et al., 2022). This was chosen to bring more awareness on OWASP Top 10, specifically the 2021 update. The design includes two groups, one control group and experimental group. The results will be used to compare participants knowledge retention and other factors such as experience in the field of web application security. The design for the control group includes a participation form created with Microsoft Forms, which asks about the participants knowledge and experience level then they proceed to read slides. After the slides there is a quiz to test what they have learned by reading through the slides to learn about the OWASP Top 10. The design for the gamified course also includes a participation form, then the participants proceed to start the game and completes the quiz after the game. The Scratch[3] game has 10 levels starting with A01:2021 - Broken Access Control and ends with A10:2021- Server-side Request Forgery.

The first step was to design a course outline about the OWASP Top 10, which gives an overview of OWASP and its mission, then the next part discusses common attack vectors and potential consequences. Additionally, it discusses the mitigation strategies to reduce the risk of the OWASP Top 10 web vulnerabilities. The next step was to create the course slides then create the gamified training. Lastly the quiz was created to include multiple choice questions and answers based on the course content.

4.1 Training Design

1. Training Objectives:

- To ensure participants understand the OWASP Top 10 web application security risks.
- To equip them with the knowledge and skills to recognize and mitigate these risks.
- To promote a culture of security awareness and responsibility within the organization.

2. Target Audience:

[3] https://scratch.mit.edu/

All participants who work with or have access to web applications, including developers, testers, administrators, and non-technical individuals. The control group receives basic training course in this case a slide presentation while the experimental group receives a gamified training on Scratch platform.

3. Training Content:

a. Introduction to OWASP Top 10:

- Overview of OWASP (Open Web Application Security Project) and its mission.
- Explanation of why web application security is important.

b. Brief Coverage of the OWASP Top 10:

- Explanations, examples, and real-world scenarios for each vulnerability.
- Common attack vectors
- Best practices and countermeasures to prevent and mitigate risks.

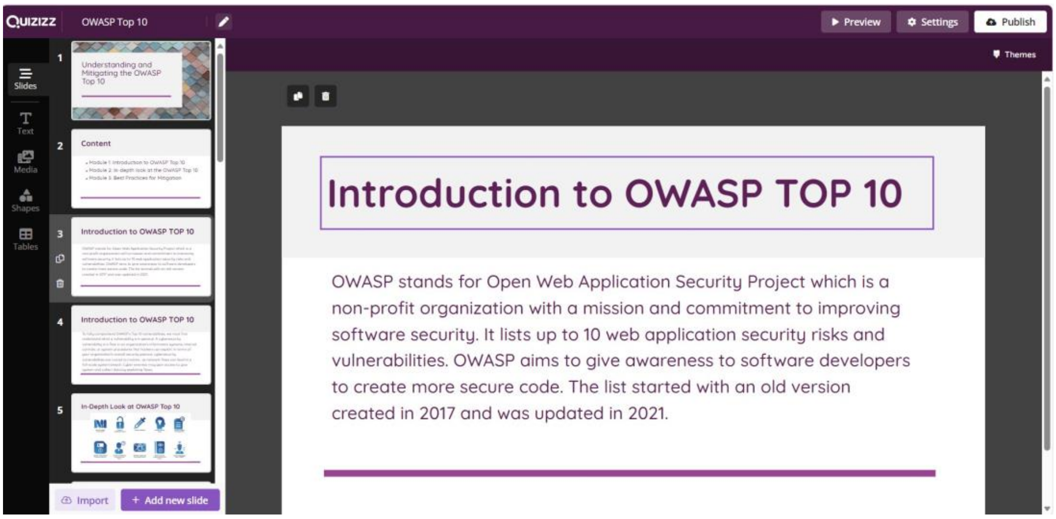
4. Training Delivery:

Online Training Modules:

- Web-based module for self-paced learning.
- Interactive quizzes and assessments.

5. Assessment and Certification:

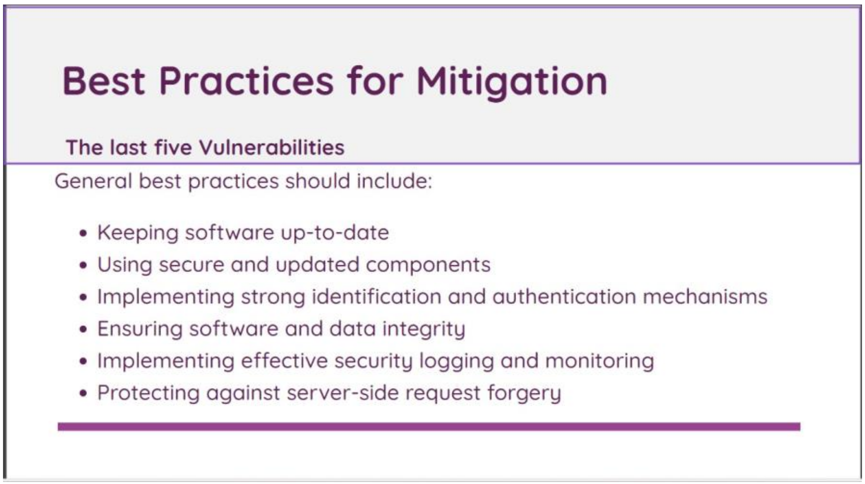
- A final quiz or assessment to gauge participants' knowledge.
- Award badges to successful participants.


Quizizz
OWASP Top 10
Preview
Settings
Publish
Themes
Slides
Text
Media
Shapes
Tables
1
Understanding and Mitigating the OWASP Top 10
2
Content
• Module 1: Introduction to OWASP Top 10
• Module 2: In-depth look at the OWASP Top 10
• Module 3: Best Practices for Mitigation
3
Introduction to OWASP TOP 10
4
Introduction to OWASP TOP 10
5
In-Depth Look at OWASP Top 10
Import
+ Add new slide

Introduction to OWASP TOP 10

OWASP stands for Open Web Application Security Project which is a non-profit organization with a mission and commitment to improving software security. It lists up to 10 web application security risks and vulnerabilities. OWASP aims to give awareness to software developers to create more secure code. The list started with an old version created in 2017 and was updated in 2021.

Figure 2: Slide presentation introducing OWASP Top 10.



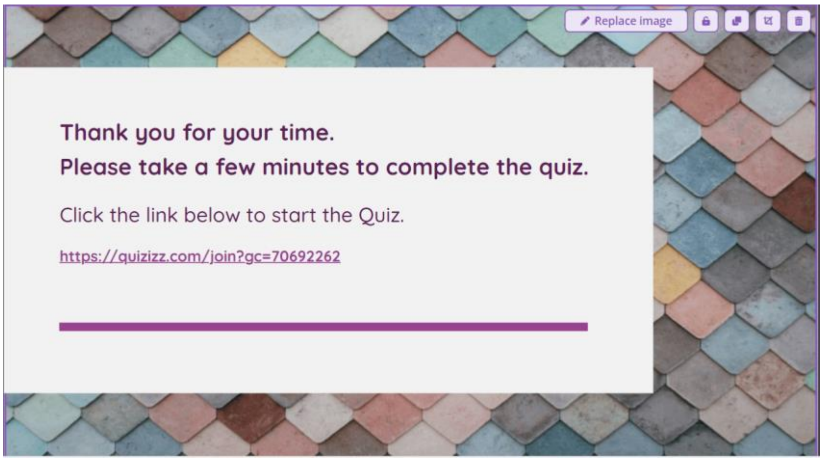
Best Practices for Mitigation

The last five Vulnerabilities

General best practices should include:

- Keeping software up-to-date
- Using secure and updated components
- Implementing strong identification and authentication mechanisms
- Ensuring software and data integrity
- Implementing effective security logging and monitoring
- Protecting against server-side request forgery

Figure 3: Slide presentation on Mitigating the last five OWASP Top 10 vulnerabilities.



Thank you for your time.
Please take a few minutes to complete the quiz.

Click the link below to start the Quiz.

https://quizizz.com/join?gc=70692262

Figure 4: Slide presentation prompting participant to start the quiz.

4.2 Scratch Game Design

The gamified training is based on Scratch which was developed by MIT. The reason for selecting Scratch is because it is an easy tool to use to create games, stories and animation. There are 10 mini games about the OWASP Top 10 vulnerabilities. The third screen has levels where the player selects level 1, A01-2021: Broken Access Control (Berisford et al., 2022). The player starts the game and follows the instructions on how to play the game. The first game has a silver door in which the player walks close to it to gain access to the room. Once they gain access, they player gets an explanation to what broken access control is and how to mitigate it. The player is taken to level 2, A02-2021: Cryptographic Failures and this time the player must deliver a secret encrypted message by dragging it to the destination to prevent a hacker from accessing the message and the same process occurs where the player receives an explanation of Cryptographic failures and how to mitigate them. This process is repeated for the other 8 levels. Once the player completes the game, they receive a completion badge and are reminded to take the quiz on the Quizziz platform.

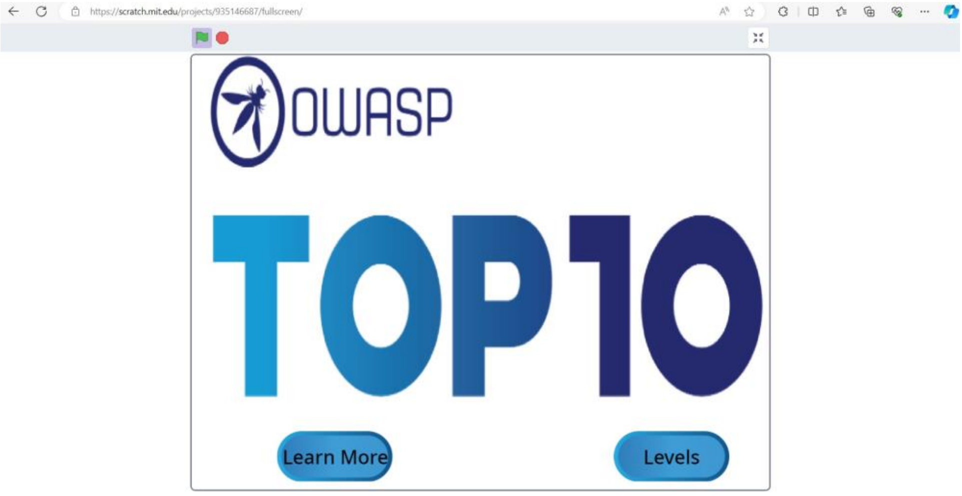
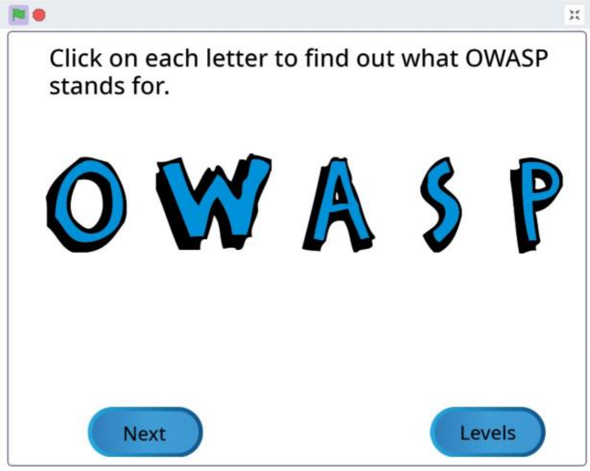
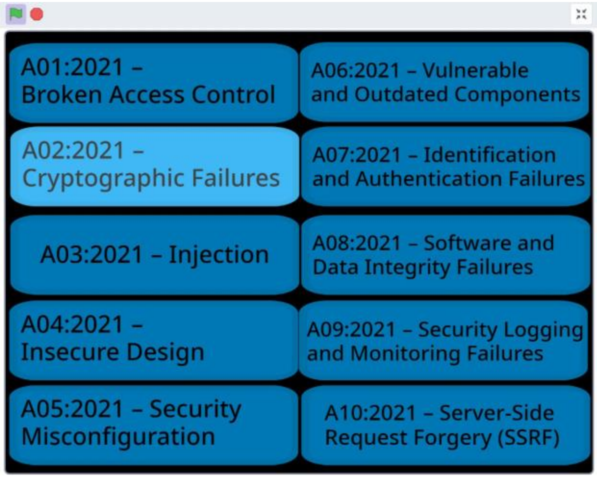


Figure 5: Scratch Interface



Click on each letter to find out what OWASP stands for.

Figure 6: Scratch Interface on OWASP



A01:2021 – Broken Access Control

A02:2021 – Cryptographic Failures

A03:2021 – Injection

A04:2021 – Insecure Design

A05:2021 – Security Misconfiguration

A06:2021 – Vulnerable and Outdated Components

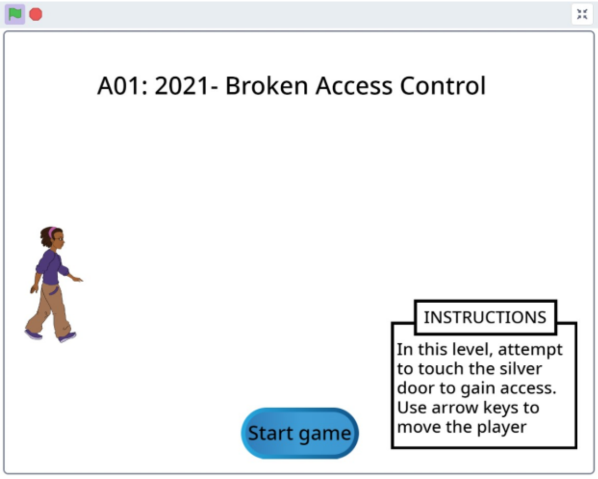
A07:2021 – Identification and Authentication Failures

A08:2021 – Software and Data Integrity Failures

A09:2021 – Security Logging and Monitoring Failures

A10:2021 – Server-Side Request Forgery (SSRF)

Figure 7: Scratch game showing the levels.

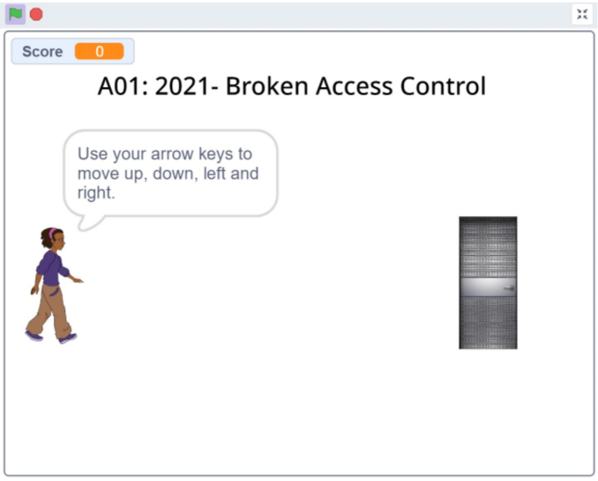


A01: 2021- Broken Access Control

INSTRUCTIONS

In this level, attempt to touch the silver door to gain access. Use arrow keys to move the player

Figure 8: Level 1 Game with instructions



A01: 2021- Broken Access Control

Use your arrow keys to move up, down, left and right.

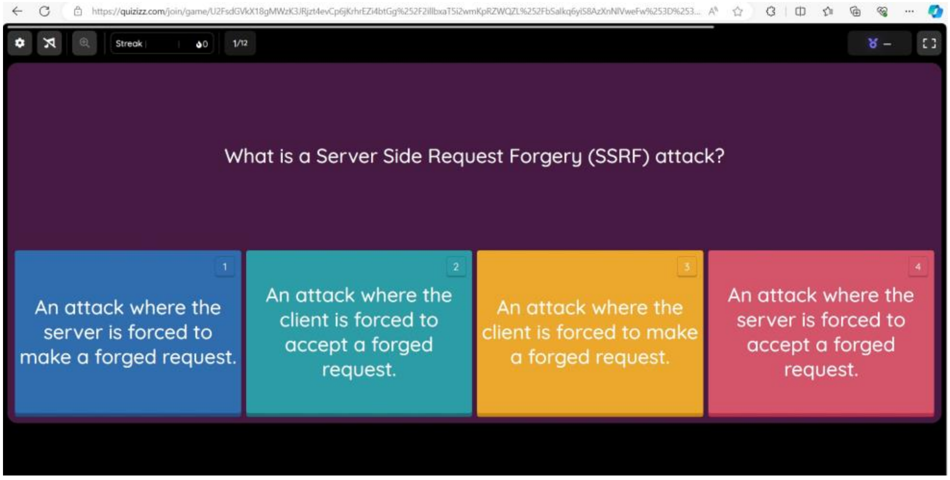
Figure 9: Level 1 Game showing the silver door

5 Implementation

The platform used for this step in the research is Quizziz, as the platform allows anonymity for each participant and provides detailed reports of each participant’s performance. It also allows competition amongst the participants with the leaderboard feature. Both groups had the same quiz questions, however, the control group did not have much engagement such as memes to motivate the participant to complete the quiz and attempt to be first on the leaderboard.

The proposed solution is that the experimental group will have a higher overall accuracy score compared to the control group. This is evaluated using the quiz report and it provides insights on how the participants performed and the questions they understood and those they did not understand well enough. Also factors such as experience or lack of are analysed together with the result from the quiz.

Some challenges were encountered creating the mini games as it had to be interactive and also should not be too technical in the short explanation to avoid appearing as long as the slide presentation. Another challenge is that it was also time consuming having to create all 10 mini games that is why some of the games are very short in other not to deter participants from playing the game which could take up to 15 minutes.



https://quizizz.com/join/game/U2FsdGVkX18gMWzK3JRjzt4evCp6jKrhrEZi4btGg%252F2illbxaT5i2wmKpRZWQZL%252FbSalkq6yiS8AzXnNlVweFw%253D%253...

Streak 0

1/12

What is a Server Side Request Forgery (SSRF) attack?

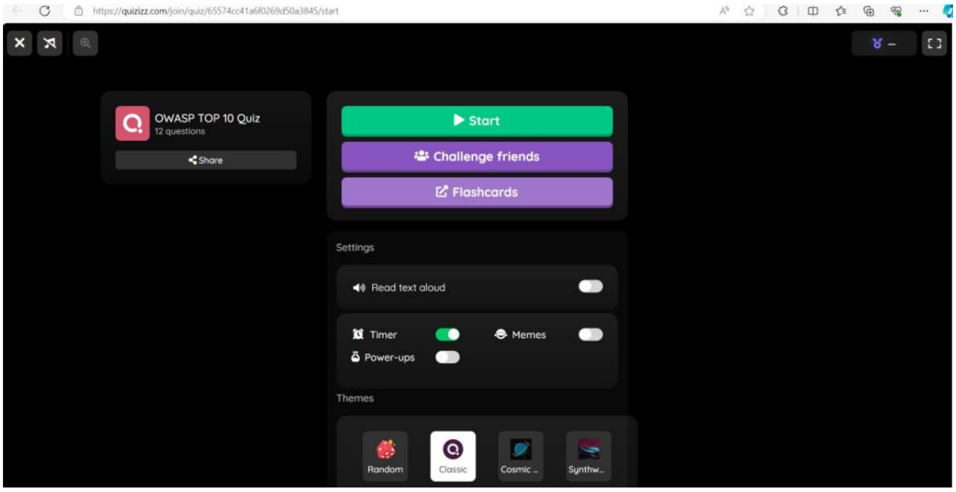
1 An attack where the server is forced to make a forged request.

2 An attack where the client is forced to accept a forged request.

3 An attack where the client is forced to make a forged request.

4 An attack where the server is forced to accept a forged request.

Figure 10: Quiz multiple choice question on Quizziz



https://quizizz.com/join/quiz/65574cc41a6f0269d50a3845/start

OWASP TOP 10 Quiz
12 questions

Share

Start

Challenge friends

Flashcards

Settings

Read text aloud

Timer

Memes

Power-ups

Themes

Figure 11: Control group quiz start screen

6 Evaluation

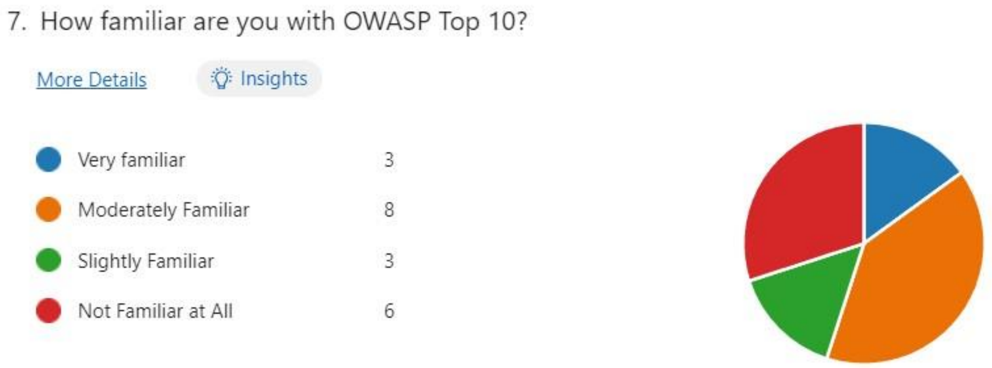
The aim of this experiment is to assess which participant group performed best in the quiz, the group with gamified training or the group with the standard traditional training. There were a number of factors which could have influenced the results such as prior knowledge on the topic and experience in the field.

The findings from the participation form and the quiz are evaluated below. 20 responses were received from the experimental group participation form while 16 responses were received from the control group. Despite the unequal number of responses there were only 10 participants from each group that successfully completed the steps and took the final quiz, which was analysed and discussed in the next section.

6.1 Participants' Prior Knowledge on OWASP Top 10.

Experimental group

The participants' knowledge or lack of knowledge on OWASP Top 10 is likely to influence how the participants score in the quiz. 15% of the participants were not familiar with the OWASP Top 10, 40% were moderately familiar, 15% were slightly familiar and 30% of the participants were not familiar at all.



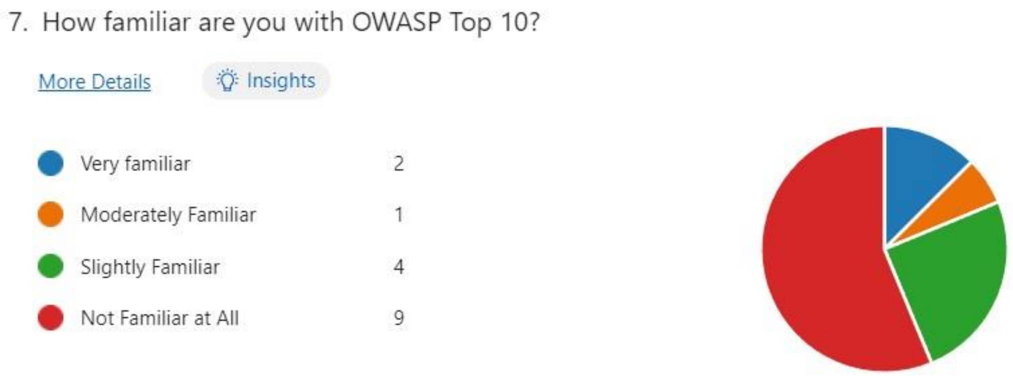
7. How familiar are you with OWASP Top 10?

● Very familiar	3
● Moderately Familiar	8
● Slightly Familiar	3
● Not Familiar at All	6

Figure 12: Distribution of familiarity with OWASP Top 10 of Experimental Group

Control group

Contrary to the experimental group, 13% of the participants were very familiar with the OWASP Top 10, 6% were moderately familiar, 25% were slightly familiar, and 56% were not familiar at all.


7. How familiar are you with OWASP Top 10?

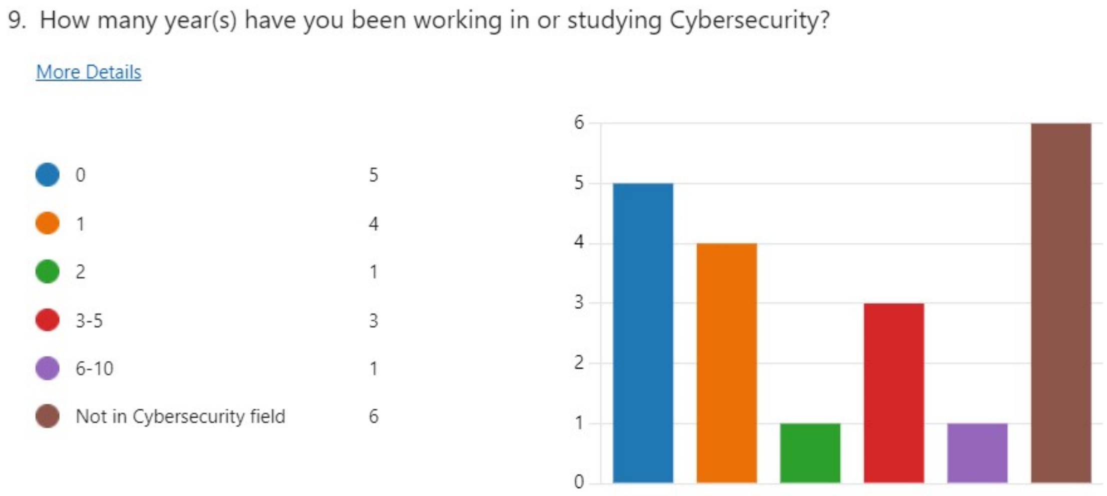
● Very familiar	2
● Moderately Familiar	1
● Slightly Familiar	4
● Not Familiar at All	9

Figure 13: Distribution of familiarity with OWASP Top 10 of Control Group

6.2 Participants year(s) of work or study in Cybersecurity

Experimental group

The number of years a participant has been in Cybersecurity is also likely to influence the performance. In this group, 55% of the participants are not in the Cybersecurity field while 45% are in the Cybersecurity field and fall between 1 to 10 years of experience.

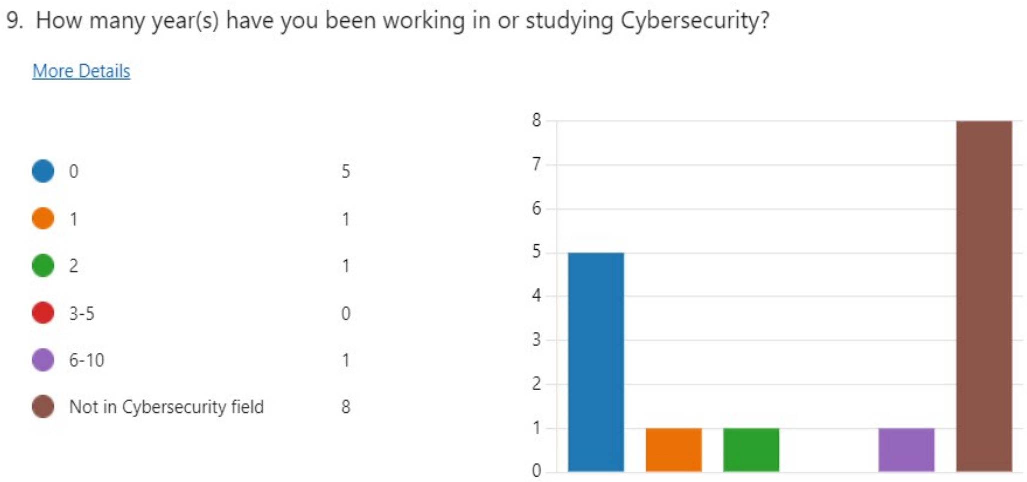

9. How many year(s) have you been working in or studying Cybersecurity?

● 0	5
● 1	4
● 2	1
● 3-5	3
● 6-10	1
● Not in Cybersecurity field	6

Figure 14: Distribution of years of experience of the Experimental Group

Control Group

In comparison to the experimental group, about 81% of participants are not in the Cybersecurity field while about 19% of participants are in the Cybersecurity field with 1-2 years of experience and 1 participant with 6-10 years' experience.



9. How many year(s) have you been working in or studying Cybersecurity?

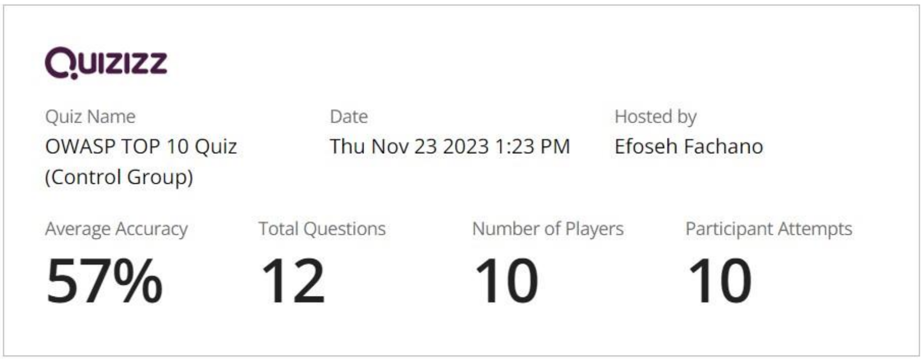
More Details

● 0	5
● 1	1
● 2	1
● 3-5	0
● 6-10	1
● Not in Cybersecurity field	8

Figure 15: Distribution of years of experience of Control Group

6.3 Participants Quiz Performance

The metric used in Quizziz report to measure the overall performance is the accuracy.
It was calculated as Accuracy = Total points gained by group for correct & partial correct answers / (Total points for the quiz * number of students).
The control group got an accuracy of 57% while the experimental group got an accuracy of 63%.

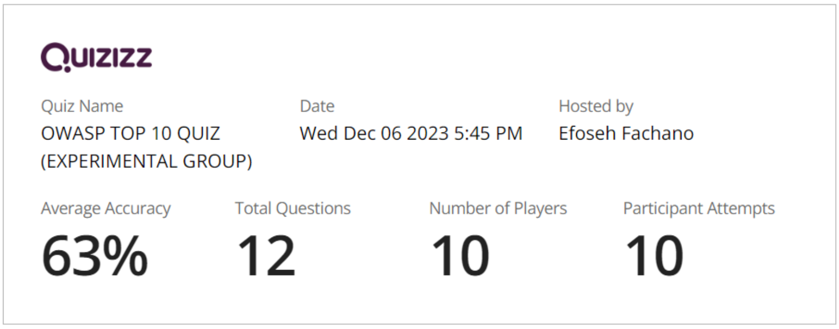


QUIZIZZ

Quiz Name	Date	Hosted by
OWASP TOP 10 Quiz (Control Group)	Thu Nov 23 2023 1:23 PM	Efoseh Fachano

Average Accuracy	Total Questions	Number of Players	Participant Attempts
57%	12	10	10

Figure 16: Overall Quiz accuracy of the Control Group



QUIZIZZ

Quiz Name	Date	Hosted by
OWASP TOP 10 QUIZ (EXPERIMENTAL GROUP)	Wed Dec 06 2023 5:45 PM	Efoseh Fachano

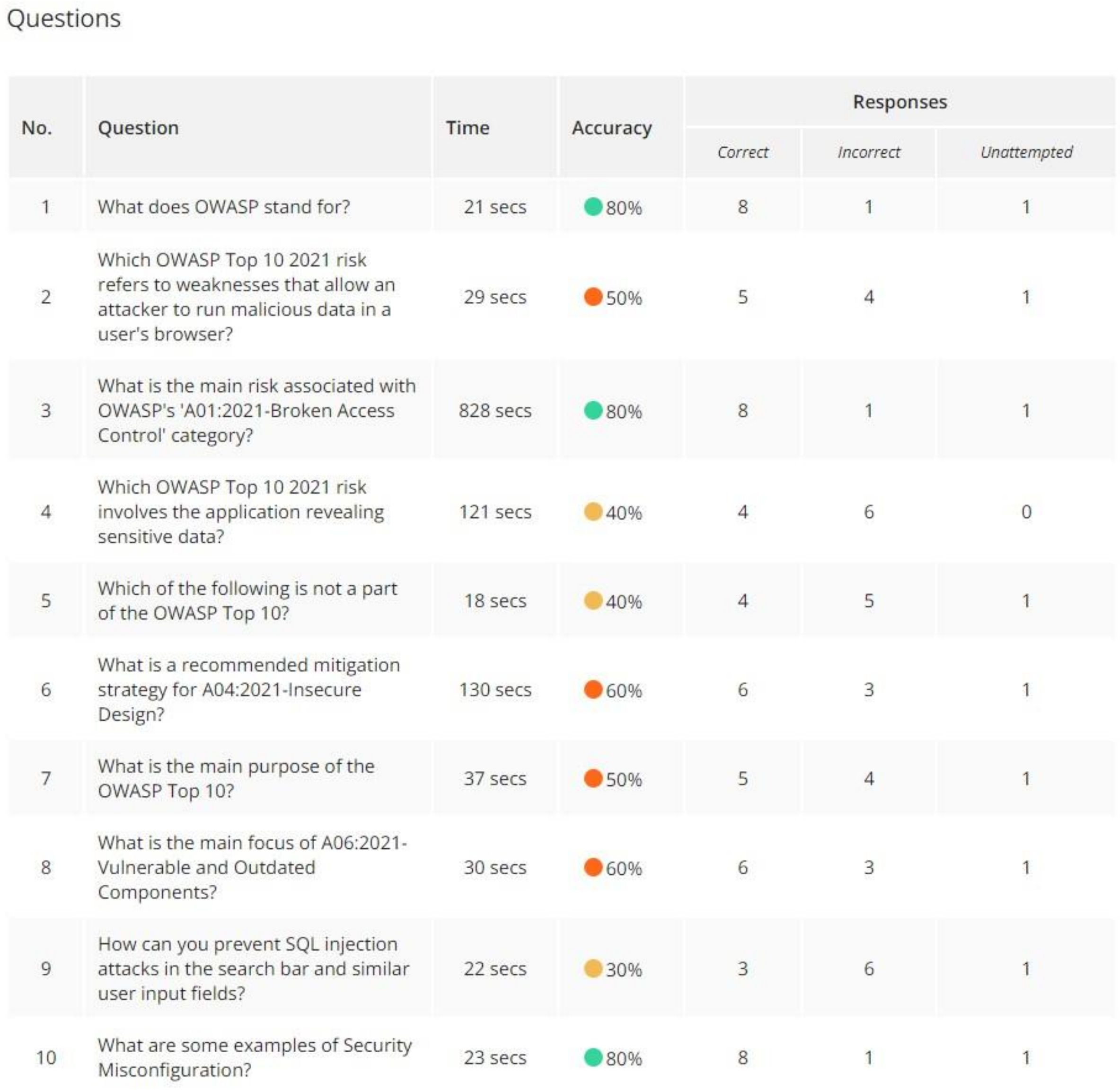
Average Accuracy	Total Questions	Number of Players	Participant Attempts
63%	12	10	10

Figure 17: Overall Quiz accuracy of the Experimental Group

6.4 Discussion

Figure 16 and 17 shows the results from the quiz and it indicates that there is some benefit in conducting gamified cybersecurity training as opposed to the standard training with slides. Gamified training can help to improve the accuracy of participants, in turn this can improve knowledge retention and thereby increase compliance with cybersecurity standards.

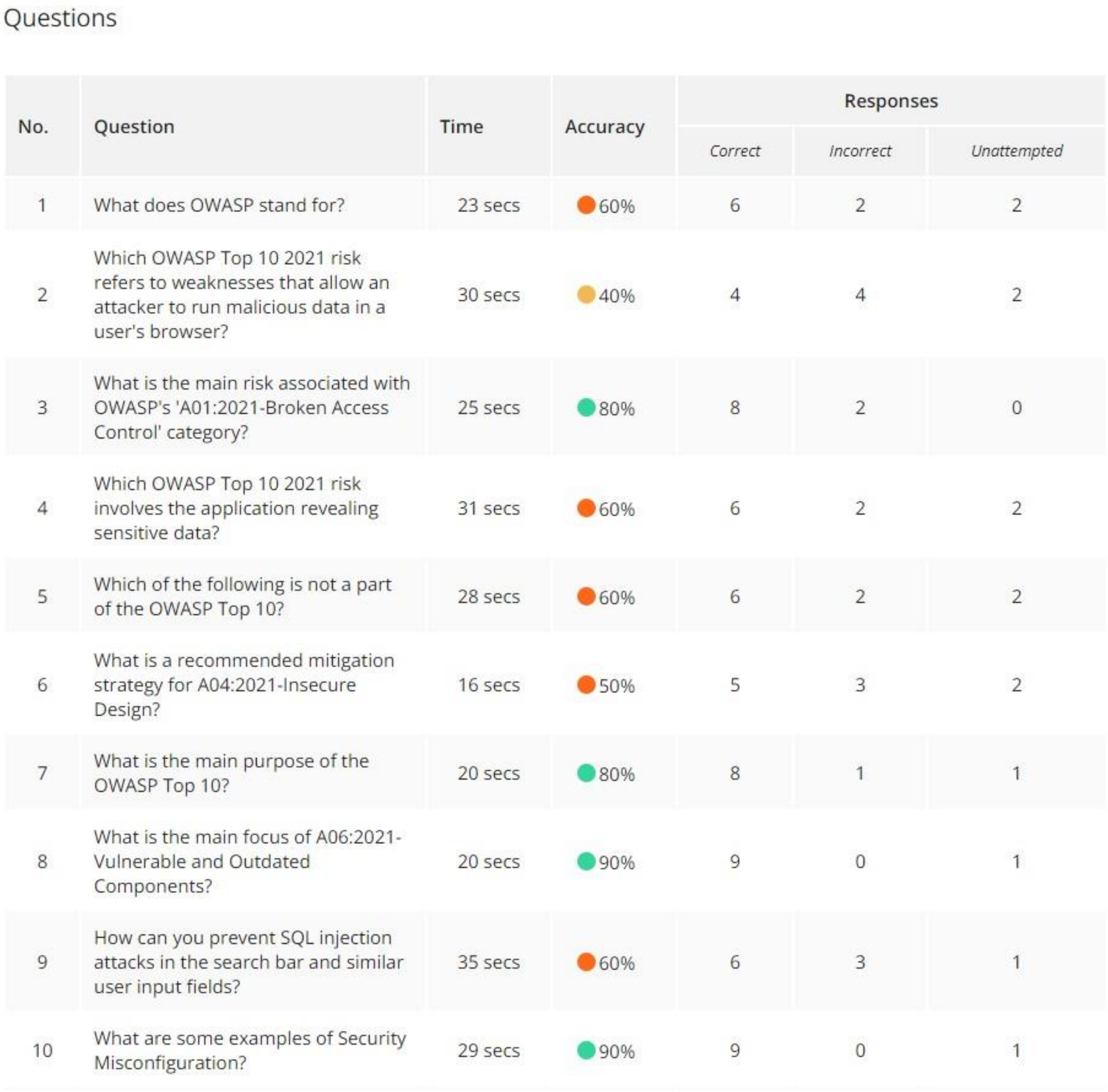
The findings in Figure 18 and 19, indicate that most participants learned to understand the meaning of the acronym OWASP, the participants in the control group scored 80% accuracy for this while the participants in the experimental group scored 60% accuracy. While for the question that asked about the main purpose of OWASP Top 10, the participants in the control group scored 50% accuracy and in the experimental group participants scored 80% accuracy



Questions

No.	Question	Time	Accuracy	Responses		
				Correct	*Incorrect*	*Unattempted*
1	What does OWASP stand for?	21 secs	● 80%	8	1	1
2	Which OWASP Top 10 2021 risk refers to weaknesses that allow an attacker to run malicious data in a user's browser?	29 secs	● 50%	5	4	1
3	What is the main risk associated with OWASP's 'A01:2021-Broken Access Control' category?	828 secs	● 80%	8	1	1
4	Which OWASP Top 10 2021 risk involves the application revealing sensitive data?	121 secs	● 40%	4	6	0
5	Which of the following is not a part of the OWASP Top 10?	18 secs	● 40%	4	5	1
6	What is a recommended mitigation strategy for A04:2021-Insecure Design?	130 secs	● 60%	6	3	1
7	What is the main purpose of the OWASP Top 10?	37 secs	● 50%	5	4	1
8	What is the main focus of A06:2021-Vulnerable and Outdated Components?	30 secs	● 60%	6	3	1
9	How can you prevent SQL injection attacks in the search bar and similar user input fields?	22 secs	● 30%	3	6	1
10	What are some examples of Security Misconfiguration?	23 secs	● 80%	8	1	1

Figure 18: Question accuracy of the Control Group



Questions

No.	Question	Time	Accuracy	Responses		
				Correct	*Incorrect*	*Unattempted*
1	What does OWASP stand for?	23 secs	● 60%	6	2	2
2	Which OWASP Top 10 2021 risk refers to weaknesses that allow an attacker to run malicious data in a user's browser?	30 secs	● 40%	4	4	2
3	What is the main risk associated with OWASP's 'A01:2021-Broken Access Control' category?	25 secs	● 80%	8	2	0
4	Which OWASP Top 10 2021 risk involves the application revealing sensitive data?	31 secs	● 60%	6	2	2
5	Which of the following is not a part of the OWASP Top 10?	28 secs	● 60%	6	2	2
6	What is a recommended mitigation strategy for A04:2021-Insecure Design?	16 secs	● 50%	5	3	2
7	What is the main purpose of the OWASP Top 10?	20 secs	● 80%	8	1	1
8	What is the main focus of A06:2021-Vulnerable and Outdated Components?	20 secs	● 90%	9	0	1
9	How can you prevent SQL injection attacks in the search bar and similar user input fields?	35 secs	● 60%	6	3	1
10	What are some examples of Security Misconfiguration?	29 secs	● 90%	9	0	1

Figure 19: Question accuracy of the Experimental Group

To improve the results more data variables should be included to get statistical analysis. The data collected in this experiment can be used to create frequency statistics of the time taken to answer the question in the quiz and if the participant answered the question correctly or not. Another way to improve the experiment will be to collect qualitative feedback from participants after the study. This feedback could help to get more insights on if participants in the experimental group enjoyed the gamified training and participants in the control group will be given a chance to comment on the slide presentation. Additionally, it would be useful if the participants could share if they enjoyed the competitive nature of the quiz and having badges or being on top of the leaderboard.

7 Conclusion and Future Work

There is some evidence that gamification as a learning approach has some benefits, including increased engagement, improved performance, and enhanced knowledge of the topic. However, the use of gamification in cybersecurity awareness is still not widely used as there are still some cybersecurity trainings using only slide presentations. The aim of this research was to investigate how gamification can be used to bring cybersecurity awareness to employees and students in Ireland. To achieve this goal, a study was conducted using Scratch and Quizziz platform. Two groups were tested, the control group without gaming elements and the experimental group with gaming elements. The experimental group had a higher accuracy compared to the control group.

The research findings suggest that gamification is an effective approach for teaching cybersecurity awareness in institutions as well as in organisations. User-friendly, free and readily available gamification tools such as Quizziz and Scratch are effective in delivering key learning objectives in cybersecurity awareness. The study also found that gaming elements that provide a sense of achievement, such as leaderboards and instant rewards, are more motivating and engaging for participants as opposed to not including those elements.

Although the sample size of 20 for this research is relatively small, some factors such as prior knowledge or lack of and experience in the field influence the result therefore the study cannot be generalized. Future work should aim to design a more robust experiment that addresses the limitations of this current study. To ensure that the future study is more generalized, there should be a plan to increase the sample size. Additionally, conduct a more rigorous statistical analysis to determine the exact impact of each game element on motivation, engagement, and performance. Perhaps also conduct a live gaming quiz session on Quizziz, with 50-100 participants playing all at once could give a different perspective to the research. In addition to that, using platforms such as unity to develop the game can make it more visually appealing and stimulating.

References

Abu-Amara, F., & Tamimi, H. (2021) ‘Cyber Shield Security Awareness Program’, in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom),* New Delhi, India, 2021, pp. 422–425.

Alazmi, S., & De Leon, D. C. (2022) ‘A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners’ *in IEEE Access,* vol. 10, pp. 33200-33219, 2022, doi: 10.1109/ACCESS.2022.3161522

Aljabri, M., Aldossary, M., Al-Homeed, N., Alhetelah, B., Althubiany, M., Alotaibi, O., & Alsaqer, S. (2022) ‘Testing and Exploiting Tools to Improve OWASP Top Ten Security Vulnerabilities Detection’ in *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN),* Al-Khobar, Saudi Arabia, 2022, pp. 797-803, doi: 10.1109/CICN56167.2022.10008360.

Berisford, C. J., Blackburn, L., Ollett, J. M., Tonner, T. B., Yuen, C. S. H., Walton, R., & Olayinka, O. (2022) ‘Can gamification help to teach Cybersecurity?’, in *2022 20th International Conference on Information Technology Based Higher Education and Training (ITHET),* Antalya, Turkey, 2022, pp. 1-9, doi: 10.1109/ITHET56107.2022.10031716.

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022) ‘Developing metrics to assess the effectiveness of cybersecurity awareness program’ in *Journal of Cybersecurity*, Volume 8, Issue 1, 2022, doi: 10.1093/cybsec/tyac006.

Cone, B.D. et al. (2006) ‘Cyber Security Training and Awareness Through Game Play’, in S. Fischer-Hübner et al. (eds) Security and Privacy in Dynamic Environments. Boston, MA: Springer US (IFIP International Federation for Information Processing), pp. 431–436, doi: 10.1007/0-387-33406-8_37.

Davis, N., & Grant, E. S. (2022) ‘Simulated Phishing Training Exercises versus Gamified Phishing Education Games’, in *2022 Fourth International Conference on Emerging Research in Electronics, Computer Science and Technology (ICERECT),* Mandya, India, 2022, pp. 1-8, doi: 10.1109/ICERECT56837.2022.10060595.

DeCusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D., & Mah, B. (2022) ‘A Cybersecurity Awareness Escape Room using Gamification Design Principles’, in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, NV, USA, 2022, pp. 0765-0770, doi: 10.1109/CCWC54503.2022.9720748.

Farah, T., Shojol, M., Hassan, M., & Alam, D. (2016). Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF. *2016 Sixth International Conference on Digital Information and Communication Technology and Its Applications (DICTAP),* Konya, Turkey, 2016, pp. 74-78, doi: 10.1109/DICTAP.2016.7544004.

Hill, W. A., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020) ‘*A Survey of Serious Games for Cybersecurity Education and Training*’, in KSU Proceedings on Cybersecurity Education, Research and Practice. 7.

Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics*, *12*(17):3544, doi: 10.3390/electronics12173544.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', in *International Journal of Information Management*, *45*, pp. 13–24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

Martin, J. and Helebrandt, P. (2022) 'Gamification of cyber ranges in cybersecurity education', in *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Stary Smokovec, Slovakia, 2022, pp. 280-285, doi: 10.1109/ICETA57911.2022.9974714

Matovu, R., Nwokeji, J. C., Holmes, T., & Rahman, T. (2022) 'Teaching and Learning Cybersecurity Awareness with Gamification in Smaller Universities and Colleges', in *2022 IEEE Frontiers in Education Conference (FIE)*, Uppsala, Sweden, 2022, pp. 1-9, doi: 10.1109/FIE56618.2022.9962519

Oroszi, E. D. (2020) '*Using Gamification to Improve the Security Awareness of Users: The Security Awareness Escape Room*', *ISACA Journal*, vol. 4, pp. 1-6.

Sharif, K. H., & Ameen, S. Y. (2020) 'A Review of Security Awareness Approaches With Special Emphasis on Gamification', in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, Iraq, 2020, pp. 151-156, doi: 10.1109/ICOASE51841.2020.9436595.

Tirumala, S. S., Sarrafzadeh, A., & Pang, P. (2016) 'A survey on internet usage and cybersecurity awareness in students', in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Auckland, New Zealand, 2016, pp. 223-228, doi: 10.1109/PST.2016.7906931.

Tirumala, S. S., Valluri, M. R., & Babu, G. (2019) 'A survey on cybersecurity awareness concerns, practices and conceptual measures', in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2019, pp. 1-6, doi: 10.1109/ICCCI.2019.8821951.

Van Steen, T., & Deeleman, J. R. A. (2021) 'Successful Gamification of Cybersecurity Training', *Cyberpsychology, Behavior, and Social Networking, 24*(9), pp. 593–598 doi: 10.1089/cyber.2020.0526.