SIMULATION SYSTEM TO EDUCATE PEOPLE ON PHIVISP ATTACK

SALMAN BIN KHAIRUL ANUAR

Bachelor of Computer Science
(Computer System & Networking)
with Honours

UNIVERSITI MALAYSIA PAHANG

UNIVERSITI MALAYSIA PAHANG

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : SALMAN BIN KHAIRUL ANUAR

Date of Birth

Title : SIMULATION SYSTEM TO EDUCATE PEOPLE ON PHIVISP ATTACKS

Academic Session : SEMESTER II 2022/2023

I declare that this thesis is classified as:

□	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
□	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☑	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

_______________________	_______________________
(Student's Signature)	(Supervisor's Signature)
	DR. AHMAD FIRDAUS
New IC/Passport Number	Name of Supervisor
Date: 30/06/2023	Date: 30/06/2023

NOTE : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I/We* hereby declare that I/We* have checked this thesis/project* and in my/our* opinion, this thesis/project* is adequate in terms of scope and quality for the award of the degree of *Doctor of Philosophy/ Master of Engineering/ Master of Science in ……………………………..

(Supervisor's Signature)

Full Name : Ts. Dr. Ahmad Firdaus Zainal Abidin
Position : Senior Lecturer
Date : 30/06/2023

(Co-supervisor's Signature)

Full Name :
Position :
Date :

Universiti
Malaysia
PAHANG
Engineering • Technology • Creativity

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

____

(Student's Signature)

Full Name : SALMAN BIN KHAIRUL ANUAR

ID Number : CA20147

Date : 30/06/2023

SIMULATION SYSTEM TO EDUCATE PEOPLE ON PHIVISP ATTACK

SALMAN BIN KHAIRUL ANUAR

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Bachelor Of Computer Science
(Computer System & Networking) With Honours

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

JUNE 2023

ACKNOWLEDGEMENTS

To begin with, I would like to express my heartfelt gratitude to my supervisor, Dr. Ahmad Firdaus, for his constant support, guidance, and assistance during the entire process of writing my thesis. He always provided me with valuable insights and helped me navigate through the various stages of my project. I also want to extend my appreciation to my family and friend, who provided me with much-needed encouragement and support throughout this journey. Their thoughtful comments and recommendations were invaluable in making this process enjoyable.

Finally, I want to praise and thank to الله سبحانه و تعالى for guiding me through all the challenges I faced while writing my thesis. It is through His grace and guidance that I was able to successfully complete this journey.

ABSTRAK

Tesis ini mencadangkan simulasi sistem untuk mendidik individu dan organisasi tentang serangan PhiViSp, atau dikenali sebagai phishing, vishing dan spear phishing. Serangan ini adalah taktik biasa yang digunakan oleh penyerang untuk mendapatkan akses tanpa kebenaran kepada maklumat dan sistem sensitif dan sangat sukar untuk dikesan dan dipertahankan. Sistem simulasi termasuk penerangan, contoh, senario, kajian kes, latihan interaktif dan cabaran yang membolehkan pengguna berlatih mengenal pasti dan mempertahankan daripada jenis serangan ini dalam persekitaran yang selamat dan terkawal. Selain itu, ia menyediakan petua dan amalan terbaik untuk mengenali dan mengelakkan serangan PhiViSp, termasuk panduan untuk mengenal pasti e-mel palsu, laman web dan permintaan untuk maklumat sensitif yang mencurigakan. Sistem ini direka bentuk untuk digunakan oleh individu dan organisasi dari semua saiz dan sektor dan akan dinilai melalui ujian dan maklum balas pengguna. Ia berpotensi untuk mengurangkan dengan ketara risiko menjadi mangsa serangan ini dan mengalami akibat yang berkaitan dengan meningkatkan kesedaran dan pemahaman tentang serangan ini dan menyediakan latihan interaktif untuk mempraktikkan strategi pertahanan.

ABSTRACT

The thesis proposes a simulation system for educating individuals and organisations about PhiViSp attacks, or known as phishing, vishing, and spear phishing. These attacks are a common tactic used by attackers to gain unauthorised access to sensitive information and systems and can be difficult to detect and defend against. The simulation system includes descriptions, examples, scenarios, case studies, interactive exercises, and challenges that allow users to practice identifying and defending against these types of attacks in a safe and controlled environment. Additionally, it provides tips and best practices for recognising and avoiding PhiViSp attacks, including guidance on identifying suspicious emails, websites, and requests for sensitive information. The system is designed to be used by individuals and organisations of all sizes and sectors and will be evaluated through user testing and feedback. It has the potential to significantly reduce the risk of falling victim to these attacks and suffering associated consequences by raising awareness and understanding of these attacks and providing interactive exercises for practicing defense strategies.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

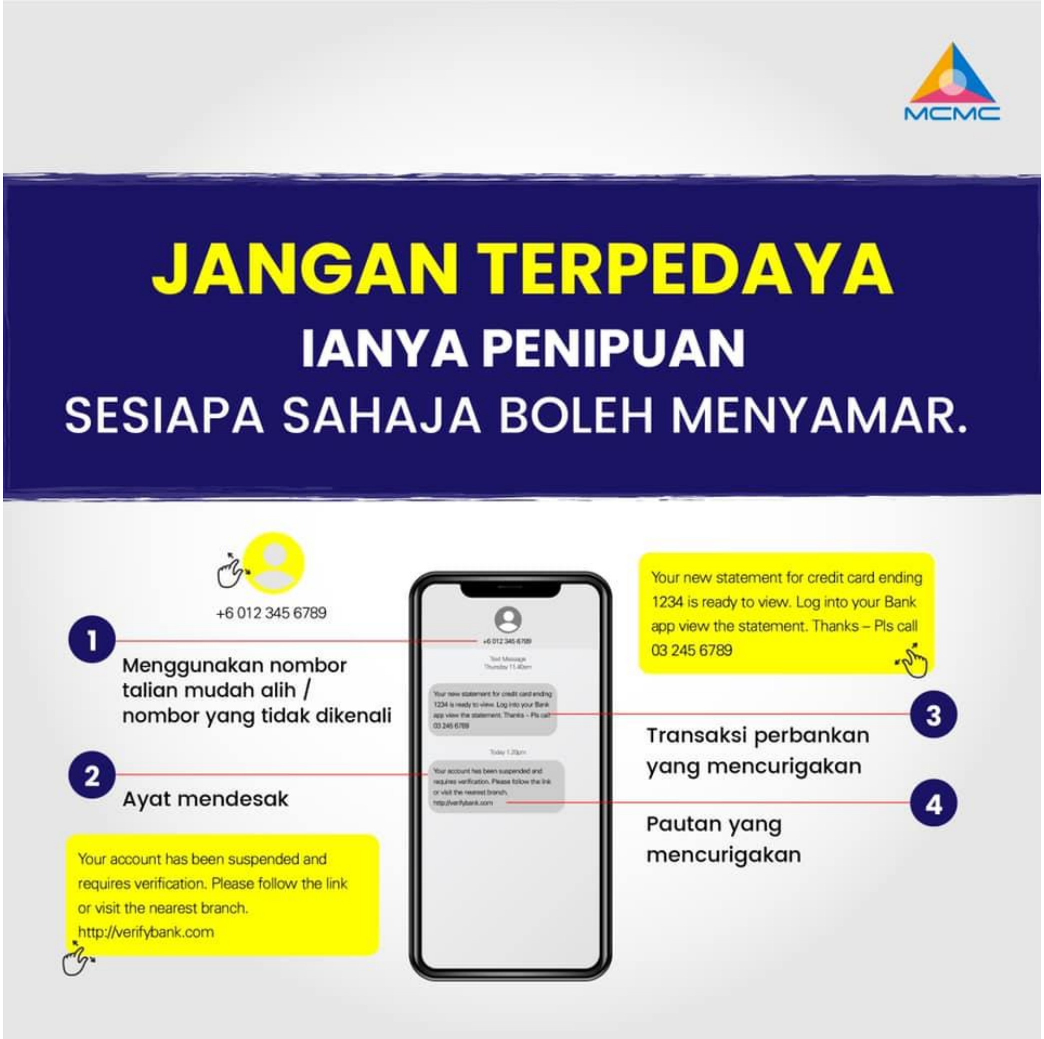
INTRODUCTION

1.1 Introduction

Social engineering is a psychological manipulation that seeks to influence individuals or groups to take actions that may not be in their best interest. It involves using various tactics, such as manipulation, deception, and persuasion, to convince people to divulge sensitive information, perform specific actions, or make decisions that may harm them or their organisation. Social engineering attacks can take many forms, including phishing scams, pretexting, baiting, and scareware. These tactics often rely on individuals' inherent trust and goodwill and their natural desire to help others or comply with authority.

The proposed simulation system aims to educate people about social engineering attacks: phishing, vishing, and spear phishing and encourage caution when interacting with unfamiliar individuals or requests for sensitive information. For example, the system will allow users to simulate a scenario miming a real-life phishing email, including the sender, subject, and content. The email will contain elements commonly found in phishing emails, such as a sense of urgency, a request for personal information, or a suspicious link. The email can be sent to those participating in the simulation, such as employees, students, customers, or friends. The system will evaluate the simulation results, including the number of participants who responded to the phishing email and their actions. The system will also provide feedback to the participants on their actions, including what they did correctly and incorrectly. Lastly, the system also will demonstrate phishing, vishing, and spear phishing attacks in a question format. So, they can be extra cautious when dealing with these situations and improve their cybersecurity awareness.

1.2 Problem Statement



JANGAN TERPEDAYA

IANYA PENIPUAN

SESIAPA SAHAJA BOLEH MENYAMAR.

+6 012 345 6789

1 Menggunakan nombor talian mudah alih / nombor yang tidak dikenali

2 Ayat mendesak

Your account has been suspended and requires verification. Please follow the link or visit the nearest branch. http://verifybank.com

Your new statement for credit card ending 1234 is ready to view. Log into your Bank app view the statement. Thanks – Pls call 03 245 6789

3 Transaksi perbankan yang mencurigakan

4 Pautan yang mencurigakan

Figure 1.1 MCMC Announcement

The first problem statement is that social engineering attacks: phishing, vishing, and spear phishing, can happen to anyone, anywhere, anytime, and the attacker also can be anyone. Unfortunately, it can sometimes come from people we trust, such as friends, family members, or even trusted organisations or businesses (*MCMC Pertingkatkan Kempen Kesedaran Atasi Kegiatan Scammer Di Malaysia | DagangNews.Com*, n.d.). So, it is essential to be cautious and protect yourself from being one of the victims.

In Malaysia, as in any country, it is crucial to be aware of these attacks and how to avoid them. Phishing is a scam in which an attacker attempts to trick you into giving away personal information, such as passwords, credit card numbers, or other sensitive information. Some common scams in Malaysia include online shopping, investment, and phone scams (*Rakyat Malaysia Memang Mudah Tertipu - Sinar Harian*, n.d.). From Figure 1 above, the Malaysian Communications and Multimedia Commission (MCMC) explains that anyone can be a scammer, and scams can happen anywhere.

Furthermore, Malaysians still lack knowledge about phishing, vishing, and spear phishing attacks and can be vulnerable to those attacks. It is often used to obtain sensitive information or access victims' accounts. One of the most known attacks in Malaysia is the Macau Scam. This phone scam originated in Macau but has spread to other countries, including Malaysia (*MCMC Pertingkatkan Kempen Kesedaran Atasi Kegiatan Scammer Di Malaysia | DagangNews.Com*, n.d.). In this scam, victims receive a phone call from someone claiming to be from a government agency or a legitimate organisation, such as a bank or a utility company. The caller may claim a problem with the victim's account or that they are eligible for a prize or compensation. The victim is then asked to provide personal information or to transfer money to resolve the alleged issue. These attacks can be challenging to detect and prevent without the proper knowledge of social engineering.

As a solution, an effective Web-based Simulation System to Educate People on PhiViSp Attacks will be developed to educate people about phishing, vishing, and spear phishing. The system will allow users to simulate a scenario miming a real-life phishing email that can be sent to those participating in the simulation, such as employees, students, customers, or friends. The system also simulates the typical attack situation or tactic as a question and answer. All the User's answers for each question will be stored in the database to track their progress and understanding of these attacks. In addition, the system will give feedback to the user on their answers, including what they did correctly and what they did incorrectly. So, the users can learn about these attacks in different situations and the same time, offer education and training on how to identify and respond to these attack types.

In summary, the proposed simulation system is highly needed to educate people about phishing, vishing, and spear phishing and protect them from these attacks.

1.3 Objective

i. To study the requirement for a Simulation System to Educate People on PhiViSp Attacks.

ii. To develop a prototype system in the Simulation System to Educate People on PhiViSp Attacks.

iii. To validate the proposed prototype system in web-based.

1.4 Scope

i. User

The target users for this web-based Simulation System are all Malaysian people.

ii. Functions

Table 1.1 Functions of Web-based Simulation System

Module	Description
User	i. Users should be able to create accounts and log in to the system using Google accounts. ii. Users should be able to send phishing emails to the intended participants and track their responses. iii. Users should be able to evaluate the simulation results, including the number of participants who responded to the phishing email and their actions. iv. Users should be able to take the simulation quiz and track their progress. v. Users should be able to view reports on their performance, including overall scores. This can allow them to track their progress in understanding social engineering attacks.

Admin	i. Admin should be able to manage user accounts and permissions. ii. Admin should be able to create a scenario that mimics a real-life phishing email. iii. Admin should be able to manage phishing email scenarios. iv. Admin should be able to create and manage the topics. v. Admin should be able to create and customise simulation questions, including adding questions and setting time limits. vi. Admin should be able to manage questions they have created.

iii. Development Platform

The web-based system is chosen because it offers flexibility and can be accessed on any device with an internet connection.

1.5 Thesis Organization

The report will be divided into five chapters: Introduction, Literature Review, Methodology, Result and Discussion, and Conclusion.

The Introduction chapter will provide an overview of the project, including a description of the current issues and problems being addressed. It will also outline the project's problem statement, objectives, and scope.

The Literature Review chapter will examine the existing systems in the field, including SANS Institute, PhishMe, and KnowBe4. In addition, this chapter will compare the advantages and disadvantages of each system.

The Methodology chapter will outline the approach taken to develop the project, including the methodology used, project requirements, a proposed design, proof of initial concept, and testing.

The Result and Discussion chapter discuss the implementation done during the project's development. This chapter also contains the testing that has been done.

The Conclusion chapter concludes the entire project and discusses the constraint and limitations regarding the project and future work for the system.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

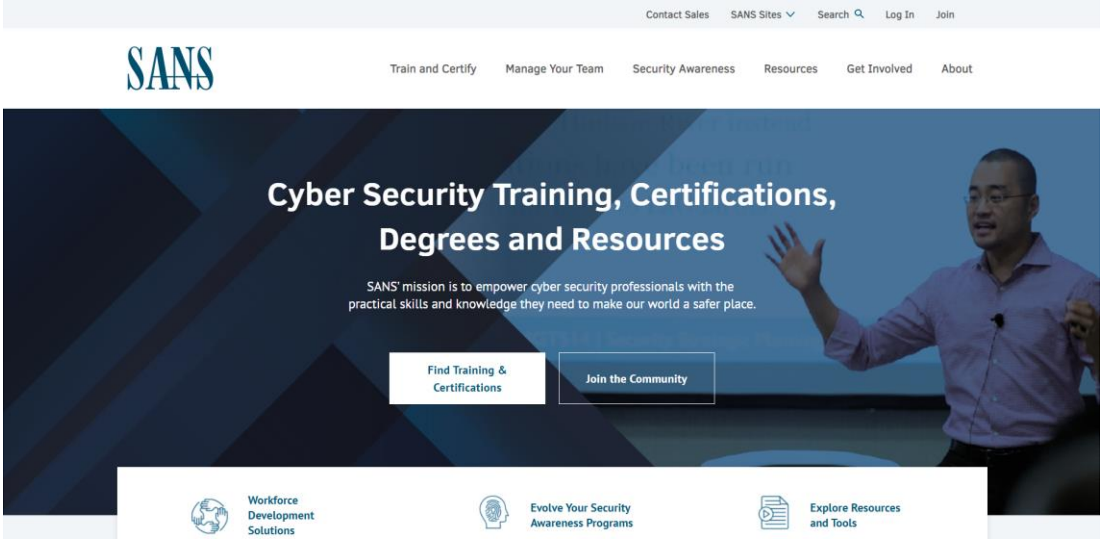
The literature review chapter aims to summarise and compare the current systems with the Simulation System to Educate People on Phivisp Attacks and an in-depth analysis of similar, contemporary systems. In addition, this review will allow us to analyse the field's current state and identify potential areas for improvement or advancement in the proposed simulation system. It also presents a brief overview of the existing approaches. Understanding how to effectively utilise the system and define the software and hardware approach used to build the systems is essential.

This chapter will provide an overview of the systems similar to the proposed one, including the design, intended use, and target audience. It will also evaluate the pros and cons of each system and compare them in terms of their effectiveness in teaching about social engineering, especially phishing, vishing, and spear phishing. Finally, based on this analysis, we will consider how our findings may inform the development and implementation of the proposed simulation system.

2.2 Existing Systems/Works

This chapter will compare three current systems, SANS Institute, PhishMe, and KnowBe4, with our proposed Phivisp simulation system.

2.2.1 SANS Institute



Cyber Security Training, Certifications, Degrees and Resources

SANS' mission is to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.

Figure 2.1 SANS Institute website

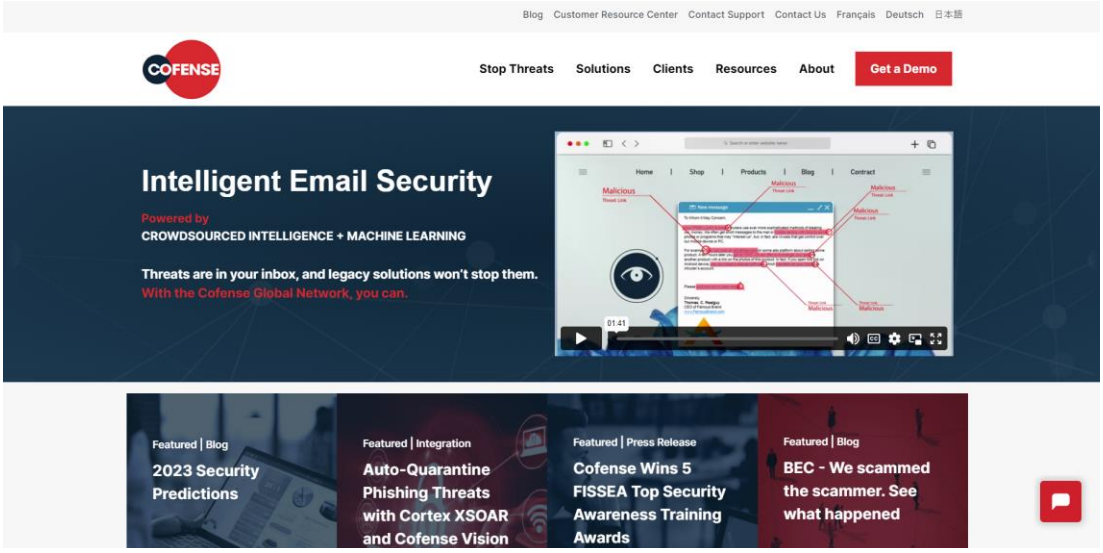
The SANS Institute is a well-respected organisation that provides cybersecurity training and certification programs to professionals worldwide. Founded in 1989, SANS (SysAdmin, Audit, Network, Security) is a cooperative research and education organisation that provides practical, actionable guidance on computer security and related topics (*Corporate Mission | SANS Institute*, n.d.).

One of the key offerings of the SANS Institute is its training courses, which cover a wide range of topics, including ethical hacking, forensics, and secure coding. These courses are typically delivered in a classroom setting, but SANS also offers a range of online courses and virtual training options. In addition to its training programs, SANS hosts several high-profile conferences and events throughout the year, bringing together cybersecurity experts to share knowledge and best practices.

In addition to its training and education programs, the SANS Institute is involved in several other cyber-related activities. For example, the organisation maintains some "Internet Storm Centers" that track and report on the latest cyber threats. In addition, it conducts research and development on various security-related topics. Finally, SANS also offers a range of certification programs that allow professionals to demonstrate their expertise across multiple cybersecurity domains.

Overall, the SANS Institute is a well-respected organisation known for its high-quality training and education programs and contributions to the broader cybersecurity community. Whether you are an IT professional looking to improve your skills or a business leader seeking to strengthen your organisation's security posture, the SANS Institute is an excellent resource to consider.

2.2.2 PhishMe



Intelligent Email Security

Powered by
CROWDSOURCED INTELLIGENCE + MACHINE LEARNING

Threats are in your inbox, and legacy solutions won't stop them.
With the Cofense Global Network, you can.

Featured | Blog
2023 Security Predictions

Featured | Integration
Auto-Quarantine Phishing Threats with Cortex XSOAR and Cofense Vision

Featured | Press Release
Cofense Wins 5 FISSEA Top Security Awareness Training Awards

Featured | Blog
BEC - We scammed the scammer. See what happened

Figure 2.2 PhishMe website

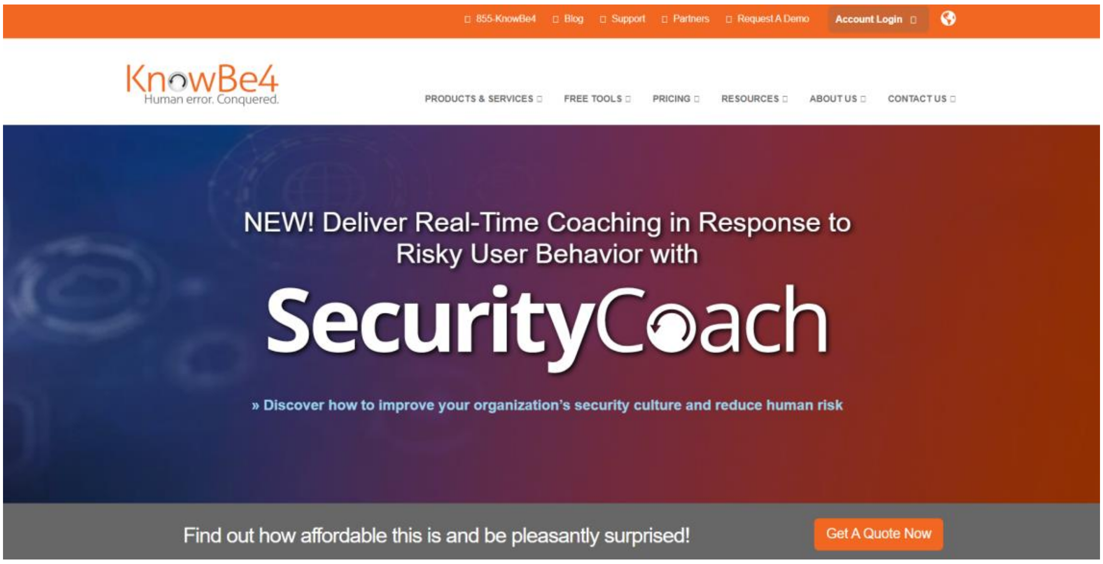
PhishMe is a security awareness training and simulated phishing platform that helps organisations educate employees about cyber threats and test their susceptibility to phishing attacks (*Proactive Security Solutions | Cofense Email Security*, n.d.). The platform includes a range of interactive modules and simulations that cover topics such as phishing, malware, and password security, as well as best practices for protecting sensitive information and avoiding online threats.

PhishMe's simulated phishing attacks allow organisations to send bogus emails to their employees and track their responses. This can help organisations identify employees at risk of falling for a phishing attack and provide them with additional training to improve their cybersecurity awareness.

In addition to its training and simulation capabilities, PhishMe offers a range of tools for managing and analysing phishing attacks, including an incident response platform that helps organisations respond to and mitigate the impact of real-world phishing attacks.

PhishMe is a comprehensive platform that provides organisations with various tools and resources to improve their employees' cybersecurity awareness and defend against phishing attacks. It is designed to be easy to use and customise, with multiple options for adapting the training to fit the specific needs of different organisations.

2.2.3 KnowBe4



NEW! Deliver Real-Time Coaching in Response to Risky User Behavior with SecurityCoach

» Discover how to improve your organization's security culture and reduce human risk

Find out how affordable this is and be pleasantly surprised!

Figure 2.3 KnowBe4 website

KnowBe4 is a security awareness training and simulated phishing platform that helps organisations educate employees about cyber threats and test their susceptibility to phishing attacks (Security Awareness Training | KnowBe4, n.d.). The platform offers a range of interactive modules and simulations that teach employees about phishing, malware, and password security. These modules can be customised to meet an organisation's needs and goals.

In addition to its training capabilities, KnowBe4 offers a simulated phishing platform allowing organisations to send bogus emails to their employees. These emails are designed to mimic real-world phishing attacks and can be customised to reflect the types of attacks that an organisation is most likely to encounter. When employees receive a simulated phishing email, they are allowed to report it as suspicious. If they fail to report the simulated phishing email, they are given additional training to help them recognise and respond to such attacks in the future.

Overall, KnowBe4 is a comprehensive platform that helps organisations educate employees about cyber threats and improve their defences against them. By training employees to recognise and respond to phishing attacks, organisations can reduce their risk of falling victim to them, which can have significant financial and reputational consequences.

2.3 Analysis/ Comparison of Existing System

This subchapter compares several key elements of the existing systems with the proposed Phivisp simulation system.

Table 2.1 Comparison Table of Existing System

	SANS Institute	Phish Me	Know Be4	PhiViSp Simulation System
Type of Product	Training platform	Training platform	Training platform	Educational and training platform
Primary focus	Cybersecurity training	Social engineering threats	Social engineering threats	Phishing, vishing, and spear phishing attacks
Simulation training	Yes	Yes	Yes	Yes
Training module	Yes	Yes	Yes	Yes
Analytics and Reporting	Yes	Yes	Yes	Yes

Other features	Simulated phishing platform (PhishSim).	Simulated phishing attacks, security awareness training, and interactive quizzes.	Security awareness training, simulated phishing attacks, interactive quizzes.	Simulate phishing, vishing, spear phishing attacks, security awareness training, interactive quizzes, and video tutorials.
Customisation options	Yes	Yes	Yes	Yes
Simulated phishing	Yes (PhishSim)	Yes	Yes	Yes
Pricing	Varies	Varies	Varies	No
Target audience	Enterprise	Enterprise	Enterprise	Individual

Based on the table above, SANS Institute, PhishMe, KnowBe4, and PhiViSp Simulation System are all products that provide some form of simulation training and other features related to cybersecurity and social engineering threats. SANS Institute is a cybersecurity training platform offering various features, including a simulated phishing platform (PhishSim) and customisation options. PhishMe and KnowBe4 are also training platforms focusing on social engineering threats, offering simulated phishing attacks, security awareness training, and interactive quizzes. PhiViSp Simulation System is an educational and training platform that simulates phishing, vishing, and spear phishing attacks and also offers security awareness training, interactive quizzes, and video tutorials. All four systems offer analytics and reporting capabilities and have customisation options. SANS Institute, PhishMe, and KnowBe4 have varying pricing models, while PhiViSp Simulation System is free. SANS Institute and the three simulation systems target enterprises, while PhiViSp Simulation System is intended for individual users.

Table 2.2 Comparison table of existing online quiz platforms

Features	Google Forms	Kalam	Kahoot	Quizzes	This study
Cost	Free	Freemium (paid plans available)	Freemium (paid plans available)	Freemium (paid plans available)	Free
Question types	Multiple choice, checkboxes, short answer, dropdown, linear scale, multiple choice grid, checkbox grid	Multiple choice, checkboxes, short answer, long answer, file upload, rating, opinion scale, matrix, ranking, matching, hotspot, drag-and-drop	Multiple choice, true/false, open-ended, puzzle, survey	Multiple choice, true/false, open-ended, essay, fill-in-the-blank, matching, multiple response, poll	Multiple choice, true/false, open-ended, essay, fill-in-the-blank, matching, multiple response, poll
Audience size	Unlimited	Up to 100 participants in free version, up to 500 participants in paid version	Up to 50 participants in free version, up to 2,000 participants in paid version	Unlimited	Unlimited
Time limit for questions	x	√	√	√	√
Analytics results	√	√	√	√	√
Focus on social engineering centred questions	x	x	x	x	√
Monitor the user's progress in similar questions	x	x	x	x	√

Provide video tutorial and explanation in each question when the question is wrong	x	x	x	x	√

In summary, comparing different online quiz platforms shows that while some similarities exist, each platform has unique features. This study offers multiple-choice and open-ended questions for Google Forms, Kalam, Kahoot, and Quizzes. Still, there are differences in the types of the questions provided, such as linear scale and checkbox grid questions in Google Forms, file upload and hotspot questions in Kalam, and puzzle and survey questions in Kahoot. Additionally, while Google Forms and this study are free, Kalam, Kahoot, and Quizzes have freemium models with paid plans available. Finally, all platforms offer analytics results, and most allow unlimited audience size and have a time limit for questions. This study focuses on social engineering-centred questions, monitoring the user's progress in similar questions, and providing video tutorials and explanations for incorrect answers.

2.4 Summary

To wrap up this literature review, the systems being reviewed include the SANS Institute, PhishMe, and KnowBe4. The SANS Institute is a well-respected organisation that provides cybersecurity training and certification programs. PhishMe is a security awareness training and simulated phishing platform. KnowBe4 is a security awareness training platform that helps organisations educate employees about cyber threats and test their susceptibility to social engineering attacks.

The proposed simulation system will be compared to these similar, contemporary systems to identify potential areas for improvement or advancement. In addition, the review will evaluate the effectiveness of the systems in teaching about social engineering, specific phishing, vishing, and spear phishing. It also will consider the existing systems' design, intended use, and target audience. The finding from these existing systems is essential to understand the various options for improving protection against social engineering threats through the proposed simulation system. The comparison also can help make informed decisions about the tools and resources that best fit their needs and identify each platform's strengths and weaknesses. Finally, the key findings will be used in developing and implementing the proposed simulation system.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter discusses the overall approach or framework of system development methodology, which refers to the process and approach followed when creating and developing a system. It involves various stages, from planning and design to testing and deployment, and ensures that the final product of "Simulation System to Educate People on Phivisp Attacks" meets the needs and requirements. During the development phase, the system will be turned into a prototype. The prototype development process for the system is split into two stages: requirements and design. Additionally, a Gantt chart will be presented to illustrate the estimated timeline and phases of the system development from the start to the completion of the study.

3.2 Waterfall Model

The Waterfall model is a process that follows a linear sequence in syste development that involves completing each stage of the process sequentially. It is a well-established software engineering approach that has been used for many years (SDLC - Waterfall Model, n.d.).

The Waterfall model consists of stages, including requirements gathering and analysis, design, implementation, testing, deployment, and maintenance. The process begins with gathering and documenting requirements, which outline what the system should do and how it should be used. From there, the system is designed based on these requirements and then implemented according to the design. Once the system has been developed, it undergoes thorough testing to ensure it meets the needs and is fit for use. Next, the plan is deployed and made available to users if it passes testing. Finally, the system is maintained and updated to support functionality and meet user needs.

One of the main advantages of the Waterfall model for this project is that it allows for a high level of predictability and control, as each stage of the process is completed in a specific order (How to Use the Waterfall Method in Any Project: ActiTIME Guide, n.d.). However, it can also be inflexible and may not be well-suited to situations where requirements are likely to change during development.

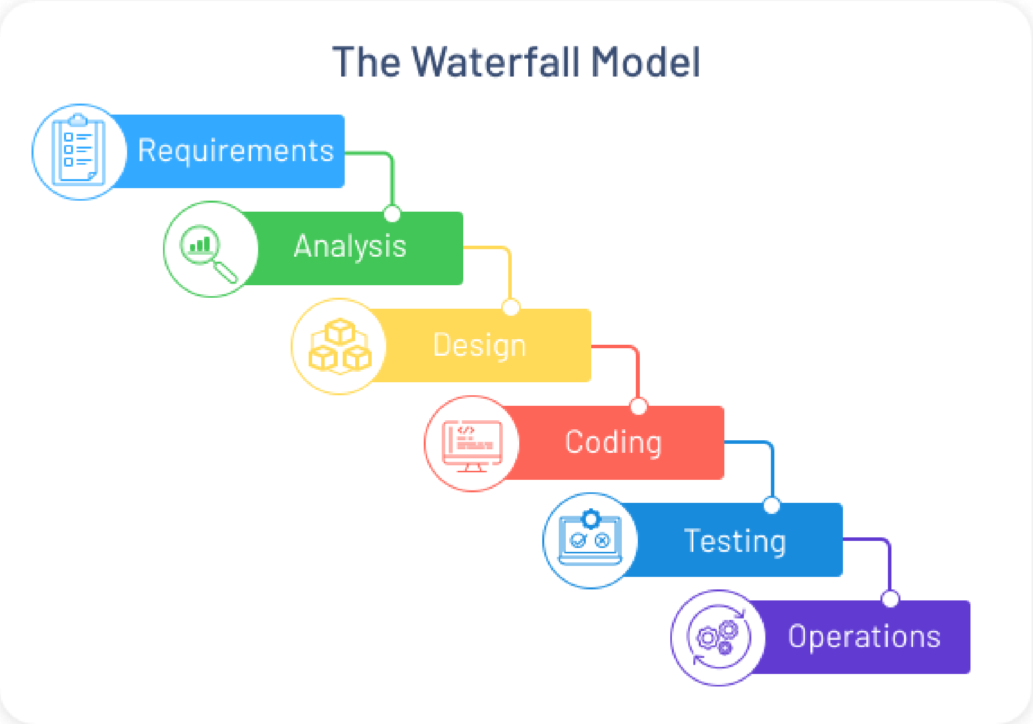


Figure 3.1 Waterfall model

3.2.1 Requirement Phase

The requirements phase is the first stage of the system development process. It involves gathering and analysing the requirements for the system, which includes identifying what the system should do and how it should be used (McGovern et al., 2003). It is also essential to understand the needs and goals of the end users and stakeholders, as well as any constraints or limitations that may impact the development of the system by conducting research, gathering input from end users, and conducting interviews or surveys.

For example, the proposed simulation system tracks users' progress in understanding social engineering attacks. Then, the project requirements are gathered and analysed. Once the project's needs have been determined, the strategy for the subsequent stages can be designed accordingly. The Software Requirement Specification (SRS) document typically documents all system requirements.

3.2.2 Design Phase

In the design phase, the system is designed based on the requirements gathered and analysed in the previous stage. It involves creating detailed technical specifications and design documents outlining how the system will be built and function (*What Is WaterFall Model in Software Developement Life Cycle | SDLC*, n.d.).

During the design phase, developing prototypes or mockups of the system is essential to help visualise and test different design concepts. This can help identify potential issues or challenges early on in the process and make necessary adjustments. Once the design phase is complete, the system can be implemented and developed according to the specifications created.

3.2.3 Implementation Phase

The implementation phase is the stage in which the system is developed according to the design created in the previous phase. It involves converting the design specifications into working code and any necessary integration with existing systems or components. The implementation phase is typically the longest and most complex stage of the Waterfall model, as it involves building the system. Therefore, it is essential to carefully plan and manage the implementation process to ensure the system is developed efficiently and effectively. Once the implementation phase is complete, the system will be ready for testing to ensure it meets the requirements and is fit for use.

3.2.4 Testing Phase

The testing phase is when the system is thoroughly tested to ensure it meets the requirements and is fit for use. It is important to thoroughly test the system at this stage to identify and fix any issues before deployment (*Agile Testing vs. Waterfall Testing*, n.d.). Then, the system is ready to be deployed and made available to users if it passes testing. However, issues discovered during testing may need to be addressed before the system's development can move on to the next phase.

3.2.5 Deployment Phase

The deployment phase is when the developed system is made available to users. This phase typically follows the testing phase, in which the system is thoroughly tested to ensure it meets the requirements and is fit for use.

Proper planning and execution of the deployment process are crucial to ensure the system is successfully deployed and made available to users without issues. In addition, after the system has been deployed, it is vital to continue monitoring and maintaining it to ensure that it remains functional and meets the users' needs.

3.2.6 Maintenance Phase

The maintenance phase is the final stage of the development process. It involves ongoing updates and improvements to the system to ensure it remains functional and meets the users' needs. In addition to addressing issues and adding new features, the maintenance phase may involve performance monitoring, user support, and documentation. Overall, the maintenance phase is an essential part of the Waterfall model, as it helps ensure that the system continues to function effectively and meet the users' needs over time.

3.3 Project Requirement

3.3.1 Functional Requirement

i. Users should be able to create accounts and log in to the system using Google accounts.

ii. Users should be able to send phishing emails to the intended participants and track their responses.

iii. Users should be able to evaluate the simulation results, including the number of participants who responded to the phishing email and their actions.

iv. Users should be able to take the simulation quiz and track their progress.

v. Users should be able to take the question and track their progress.

vi. Users should be able to view reports on their performance, including overall scores. This can allow them to track their progress in understanding social engineering attacks.

vii. Admin should be able to manage user accounts and permissions.

viii. Admin should be able to create a scenario that mimics a real-life phishing email.

ix. Admin should be able to manage phishing email scenarios.

x. Admin should be able to create and manage the topics.

xi. Admin should be able to create and customise simulation questions, including adding questions and setting time limits.

xii. Admin should be able to manage questions they have created.

xiii. The system should be able to generate the user's performance report in pdf format.

xiv. The system should be secure and protect user data.

3.3.2 Non-Functional Requirement

i. **Performance:** The system should be able to handle a high volume of traffic and transactions without experiencing delays or downtime.

ii. **Security:** The system should protect sensitive user data from unauthorised access or tampering.

iii. **Scalability:** The system should handle increasing users and workload without experiencing performance issues.

iv. **Compatibility:** The system should be compatible with various devices and browsers regardless of its operating system.

3.3.3 Constraint and Limitation

i. **Time:** The project may not be able to be completed within the allocated time due to the tight deadline.

ii. **Resources:** Due to lacking resources, the project must be completed sequentially rather than in parallel, consuming more time.

3.4 Propose Design

3.4.1 Context Diagram

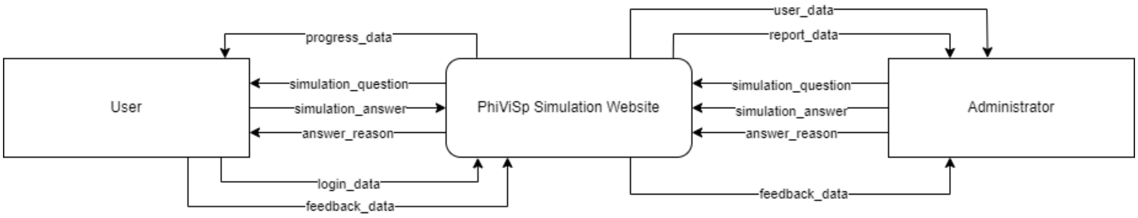


Figure 3.2 Context Diagram

The figure above shows the context diagram for the PhiViSp simulation website. The User and the administrator are the two actor types comprising the system. When using the PhiViSp simulation website, each entity serves various purposes, some shared with other entities and some entirely their own. There is also a significant amount of data flow that occurs between the system and the end users. In most cases, the User can log in to the website to gain access to the simulation question. They are also able to access the answers to the question that are presented in each scenario. When the User has completed all the questions, they can view their progress in understanding phishing, vishing, and spear phishing.

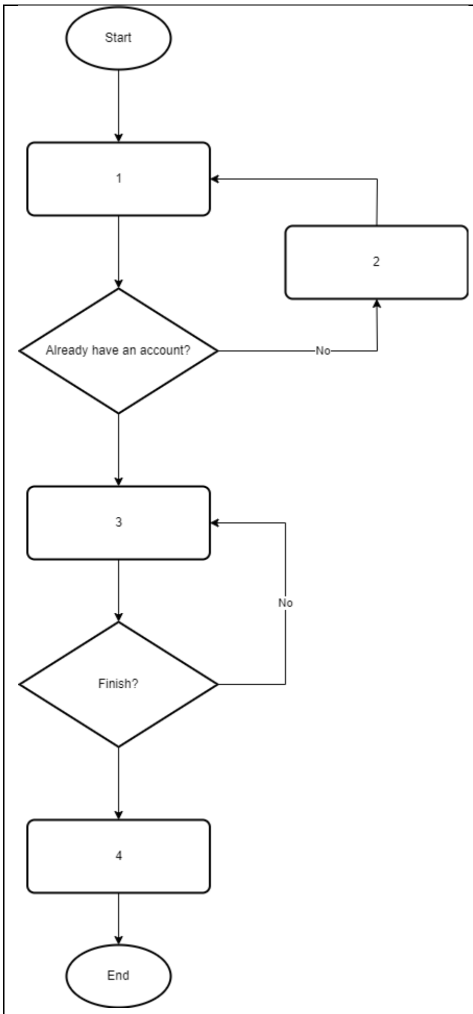
On the other hand, the administrator can view the data and progress the User has made. They can also revise the simulation question and responses to PhiViSp circumstances. Last but not least, the administrator can view the comments left by the users.

3.4.2 Flowchart Design

3.4.2.1 Flowchart for User

Table 3.1 Flowchart for User

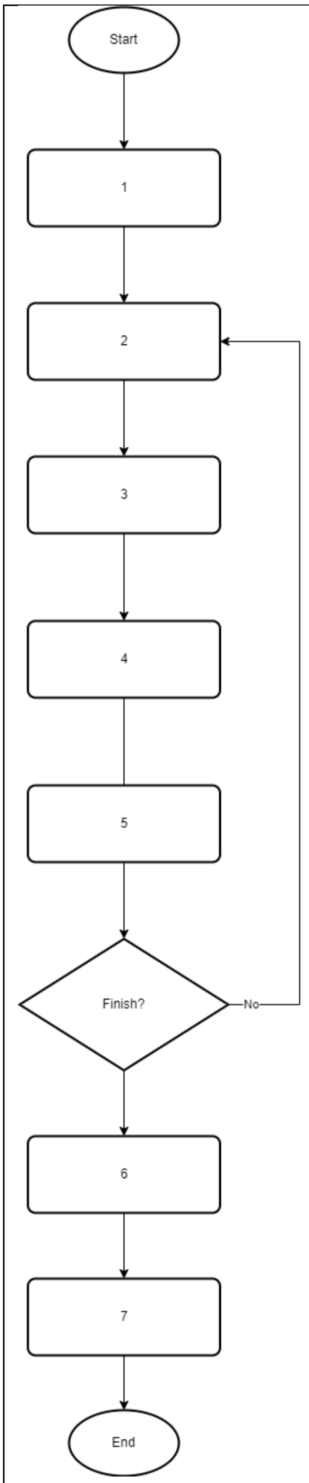
Process	Action	Responsibility

 Start 1 2 Already have an account? No 3 No Finish? 4 End	1. Sign in to the system. Does the User have an account? 2. Sign up for the system. 3. Access the simulation question. Proceed to the next question. 4. Generate result.	1. User 2. User 3. User 4. User

3.4.2.2 Flowchart for Administrator

Table 3.2 Flowchart for Administrator

Process	**Action**	**Responsibility**

 Start 1 2 3 4 5 Finish? No 6 7 End	1. Sign in to the system. 2. Select topic. 3. Create question. 4. Create answer 5. Add reason/solution Finish? 6. Publish question. 7. View question.	1. Administrator 2. Administrator 3. Administrator 4. Administrator 5. Administrator

3.4.3 Use Case Diagram

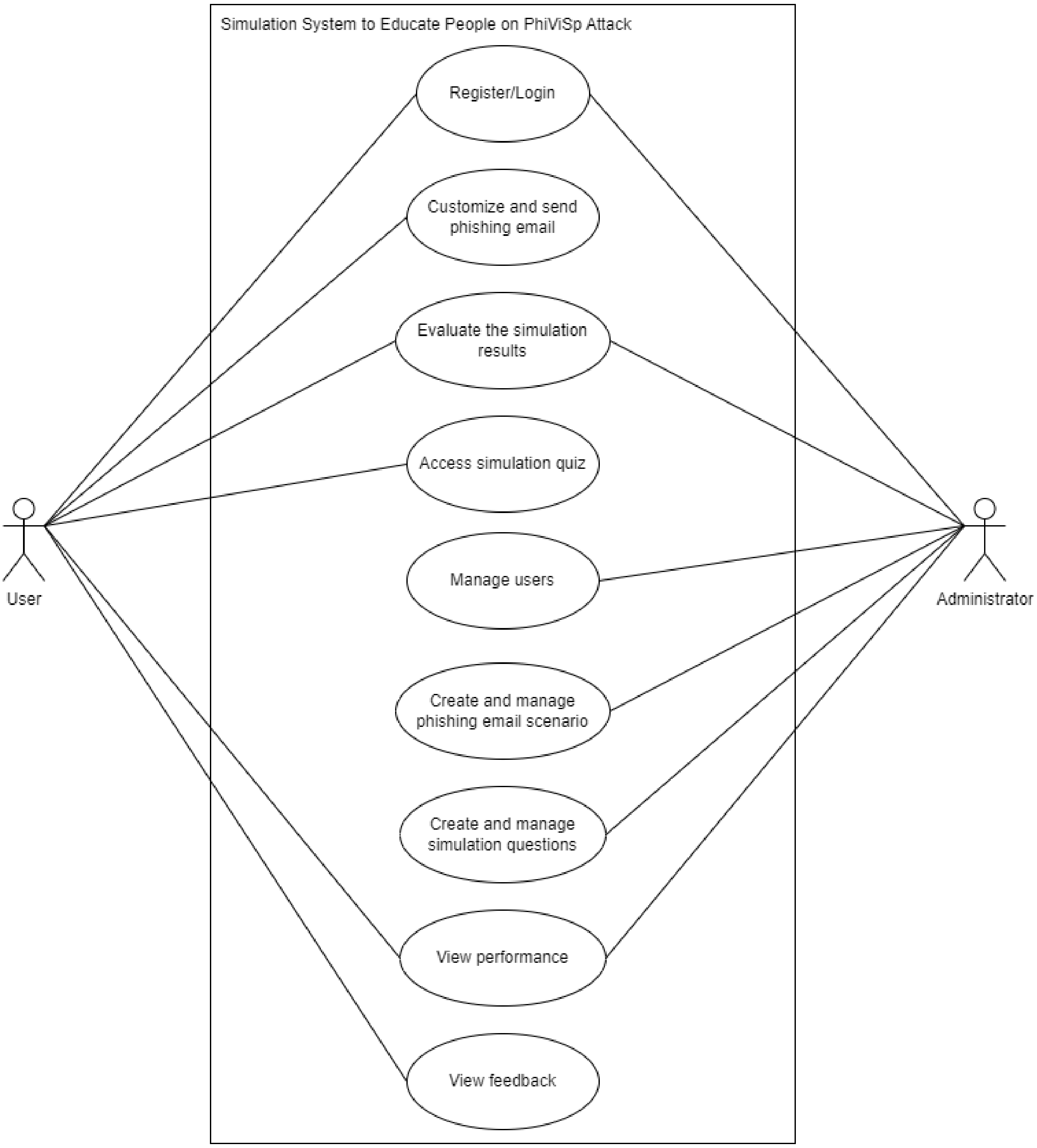

Simulation System to Educate People on PhiViSp Attack
Register/Login
Customize and send phishing email
Evaluate the simulation results
Access simulation quiz
Manage users
Create and manage phishing email scenario
Create and manage simulation questions
View performance
View feedback
User
Administrator

Figure 3.3 Use Case Diagram

Table 3.3 Use case description

Title	Simulation System to Educate People on PhiViSp Attacks
Description	The Simulation System to Educate People on PhiViSp Attacks educates individuals and organisations on the dangers of phishing attacks and how to identify and respond to them.
Actors	The actors in this use case include the administrator, who sets up and manages the simulation, and the user, who can customise and send the phishing email to the participants.
Preconditions	The preconditions for this use case include a valid account for the administrator, access to an email client or mockup tool, and a set of participants who have agreed to participate in the simulation.

Flow of Events	i. The administrator sets up the simulation by creating a phishing email scenario, including the sender, subject, and content. ii. The user sends the phishing email to the intended participants. iii. The participants receive the phishing email and respond according to their knowledge and understanding. iv. The administrator tracks the responses and evaluates the results, including the number of participants who responded to the phishing email and their actions. v. The administrator provides feedback to the participants on their actions, including what they did correctly and incorrectly. vi. The administrator offers education and training on identifying and responding to phishing emails.
Postconditions	The postconditions for this use case include increased awareness and understanding of phishing emails among the participants and reduced likelihood of falling victim to a phishing attack.

3.4.4 Activity Diagram

3.4.4.1 Activity Diagram for User

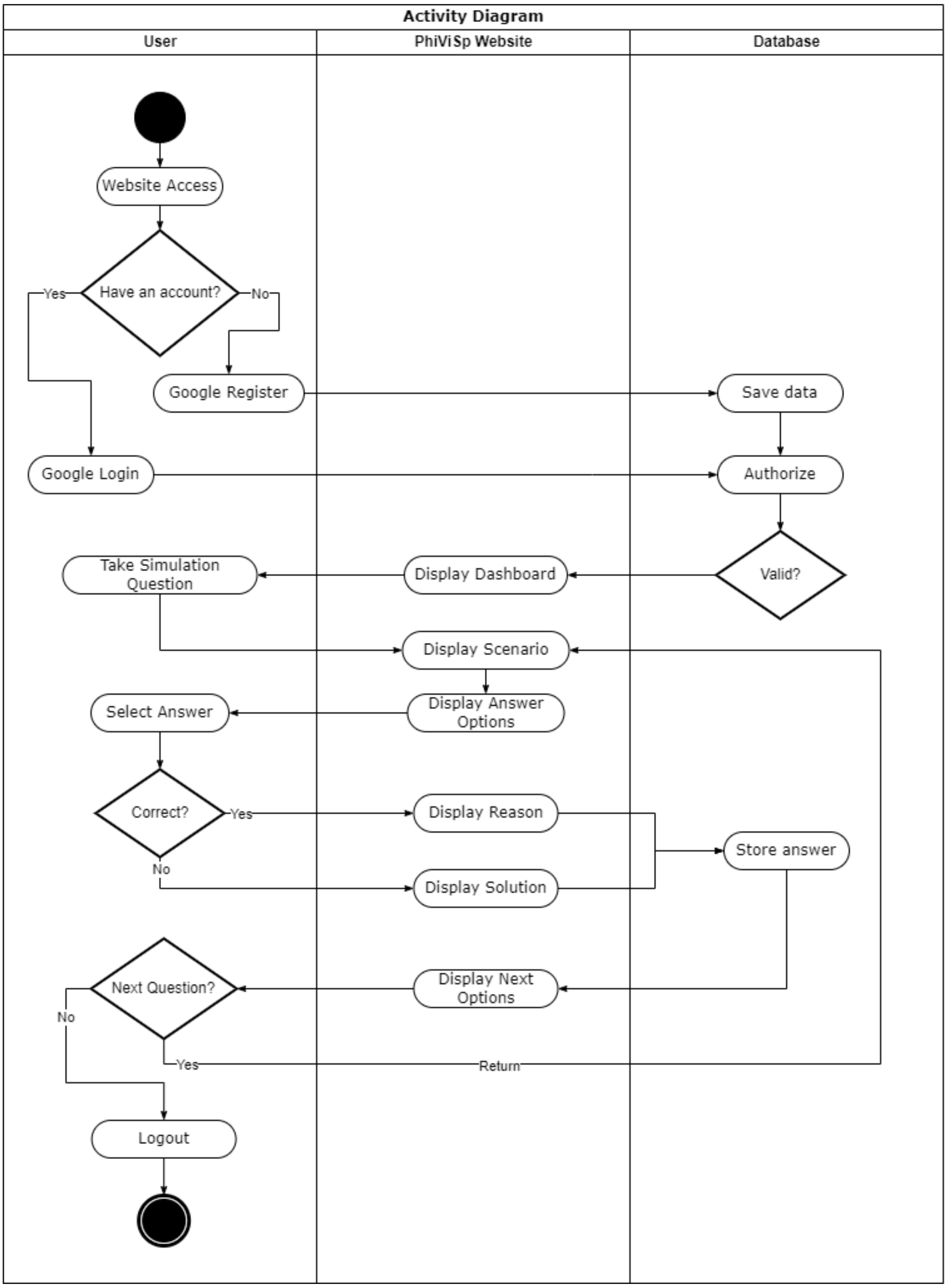


Figure 3.4 Activity Diagram for User

3.4.4.2 Activity Diagram for Administrator

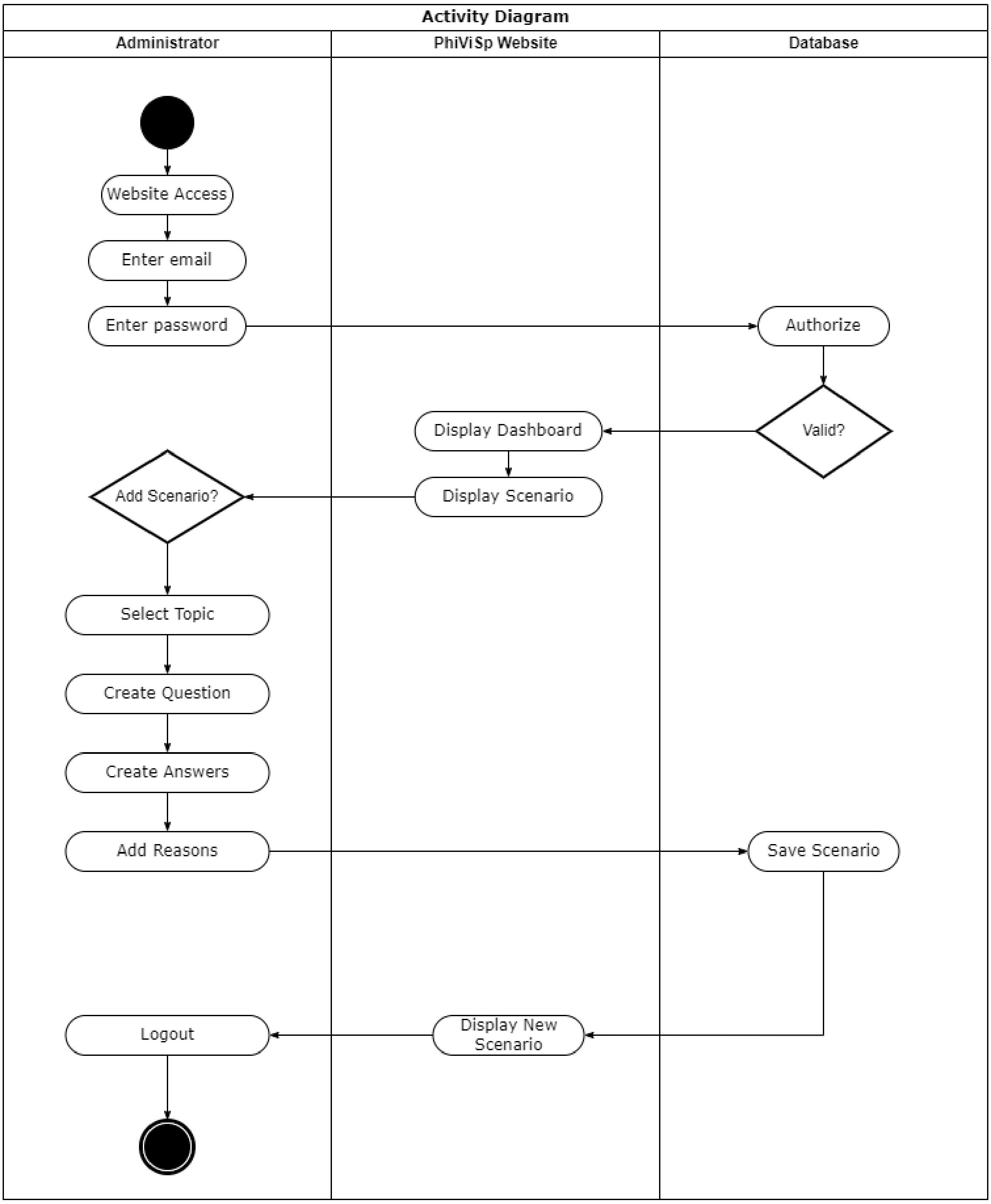


Figure 3.5 Activity Diagram for Administrator

3.4.5 Entity Relationship Diagram

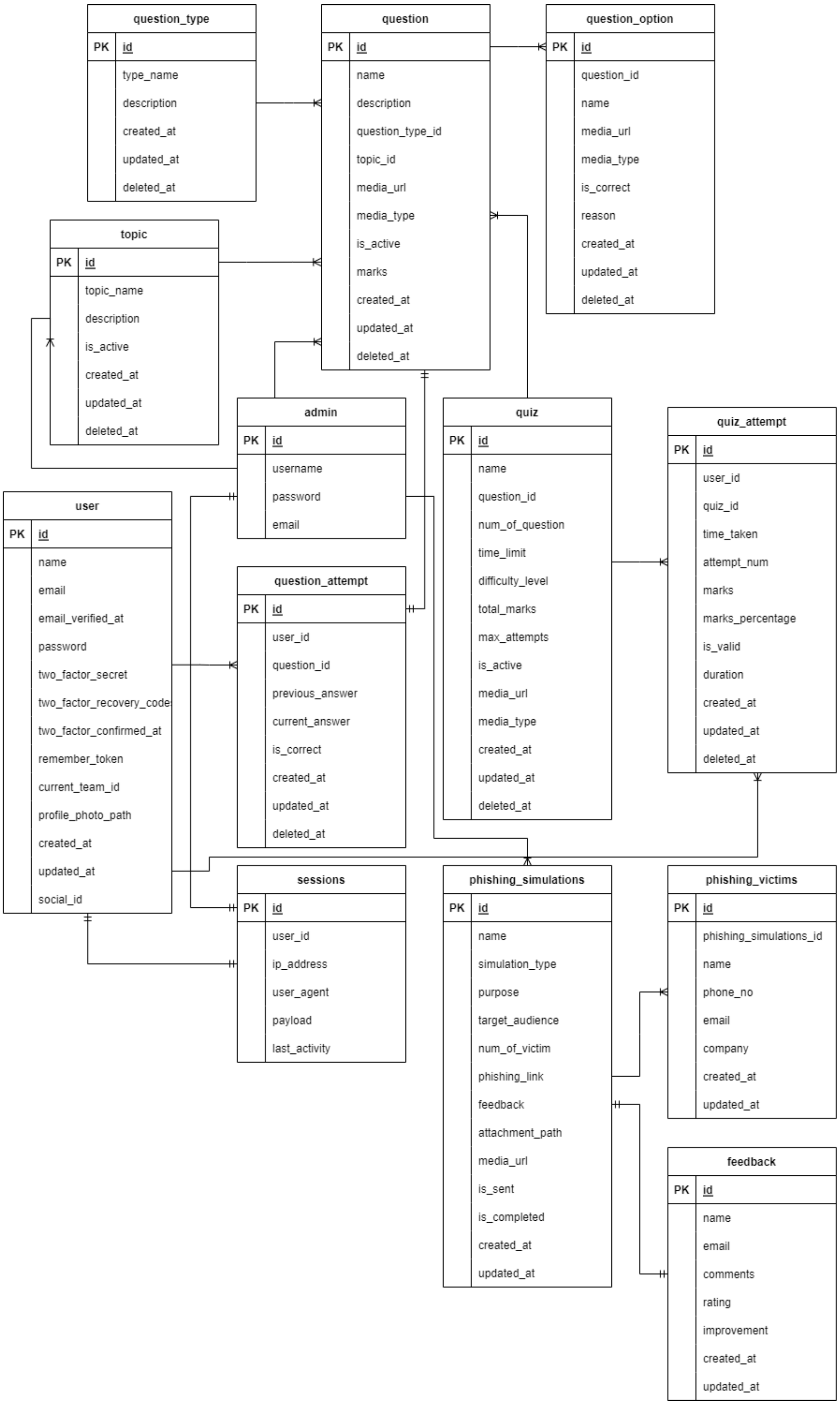


Figure 3.6 Entity Relationship Diagram

3.5 Data Design

3.5.1 Data Dictionary

questions

Table 3.4 Data Dictionary for questions

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key	
Name	Text			
Description	Text			
Question_type_id	Bigint(20)	Unsigned	Foreign key, null	
Topic_id	Bigint(20)	Unsigned	Foreign key, null	
Media_url	Text		Null	
Media_type	Varchar(255)		Null	
Is_active	Tinyint(1)		Default = 1	
Created_at	Timestamp		Null	
Updated_at	Timestamp		Null	
Deleted_at	Timestamp		null	

question_types

Table 3.5 Data Dictionary for question_types

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key, auto increment	
Name	Varchar(255)			
Created_at	timestamp		null	
Updated_at	timestamp		null	
Deleted_at	timestamp		null	

question_options

Table 3.6 Data Dictionary for question_options

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key, auto increment	
Question_id	Bigint(20)	Unsigned	Foreign key, null	
Name	Varchar(255)		null	
Media_url	Text		Null	
Media_type	Varchar(255)		Null	
Is_correct	Tinyint(1)		Default = 0	
Created_at	Timestamp		Null	
Updated_at	Timestamp		Null	
Deleted_at	Timestamp		null	

quiz

Table 3.7 Data Dictionary for quiz

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key, auto increment	
Name	Varchar(255)			
Slug	Varchar(255)			
Description	text		null	
Total_marks	Double(8,2)		0.00	
Pass_marks	Double(8,2)		0.00	
Negative_marking_settings	longtext		Null	
Max_attempts	Int(10)	Unsigned	0	

Is_published	Tinyint(4)		0	
Media_url	Varchar(255)		null	
Media_type	Varchar(255)		null	
Duration	Int(10)	Unsigned	0	
Valid_from	timestamp			
Valid_upto	timestamp		null	
Time_between_attempts	Int(10)	Unsigned	0	
Created_at	timestamp		null	
Updated_at	timestamp		null	
Deleted_at	timestamp		null	

quiz_attempts

Table 3.8 Data Dictionary for quiz_attempts

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key, auto increment	
Quiz_id	Bigint(20)	Unsigned	Foreign key, null	
Participant_id	Int(10)	Unsigned	Foreign key	
Participant_type	Varchar(255)			
Created_at	timestamp		null	

Updated_at	timestamp		null	
Deleted_at	timestamp		null	

quiz_attempt_answers

Table 3.9 Data Dictionary for quiz_attempts_answers

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key, auto increment	
Quiz_attempt_id	Bigint(20)	Unsigned	Foreign key, null	
Quiz_question_id	Bigint(20)	Unsigned	Foreign key, null	
Quiz_option_id	Bigint(20)	Unsigned	Foreign key, null	
Answer	Varchar(255)		null	
Created_at	timestamp		null	
Updated_at	timestamp		null	
Deleted_at	timestamp		null	

quiz_questions

Table 3.10 Data Dictionary for quiz_questions

Column	Type	Attributes	Constraint	Description
Id	Bigint(20)	Unsigned	Primary key, auto increment	
quiz_id	Bigint(20)	Unsigned	Foreign key, null	
question_id	Bigint(20)	Unsigned	Foreign key, null	
Marks	Double(8, 2)	Unsigned	Default = 0.00	
Negative_marks	Double(8, 2)	Unsigned	Default = 0.00	
Is_optional	Tinyint(1)		Default = 0	

order	Int(10)	Unsigned	Default = 0	
Created_at	timestamp		null	
Updated_at	timestamp		null	
Deleted_at	timestamp		null	

topic

Table 3.11 Data Dictionary for topic

Column	Type	Attributes	Constraint	Description
id	Bigint(20)	Unsigned	Primary key, auto increment	
name	Varchar(255)			
slug	Varchar(255)			
Parent_id	Bigint(20)	Unsigned		
Is_active	Tinyint(1)		Default = 1	
Created_at	timestamp		null	
Updated_at	timestamp		null	

users

Table 3.12 Data Dictionary for users

Column	Type	Attributes	Constraint	Description
id	Bigint(20)	Unsigned	Primary key, auto increment	
name	Varchar(255)			
email	Varchar(255)			
Email_verified_at	Timestamp		null	
password	Varchar(255)			
Two_factor_secret	Text		Null	

Two_factor_recovery_codes	Text		Null	
Two_factor_confirmed_at	Timestamp		Null	
Remember_token	Varchar(100)		null	
Current_team_id	Bigint(20)	Unsigned	Null	
Profile_photo_path	Varchar(2048)		Null	
Created_at	timestamp		Null	
Updated_at	timestamp		Null	
Google_id	Varchar(255)		Null	

sessions

Table 3.13 Data Dictionary for sessions

Column	Type	Attributes	Constraint	Description
id	Bigint(20)	Unsigned	Primary key	
User_id	Bigint(20)	Unsigned	null	
Ip_address	Varchar(45)		null	
User_agent	text		null	
Payload	longtext			
Last_activity	Int(11)			

3.6 Proof of Initial Concept

3.6.1 Initial Design for Administrator

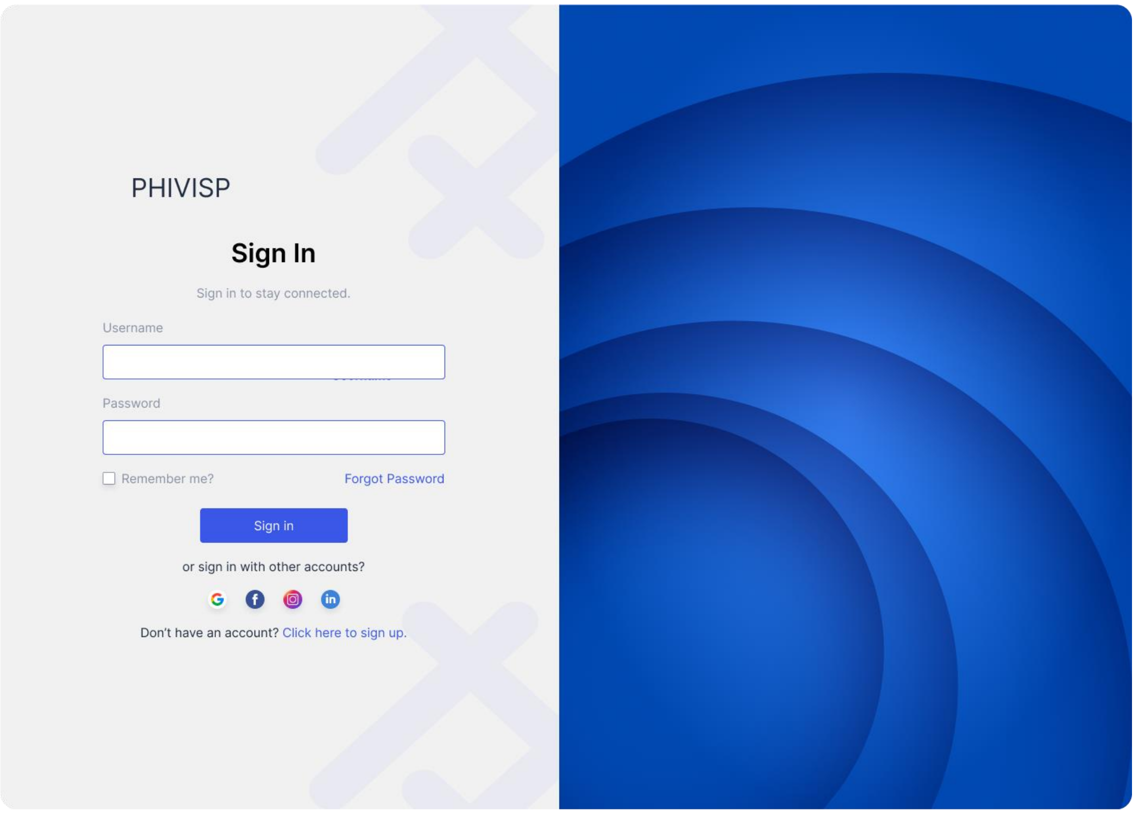

PHIVISP
Sign In
Sign in to stay connected.
Username
Password
□ Remember me?
Forgot Password
Sign in
or sign in with other accounts?
Don't have an account? Click here to sign up.

Figure 3.7 Administrator Login

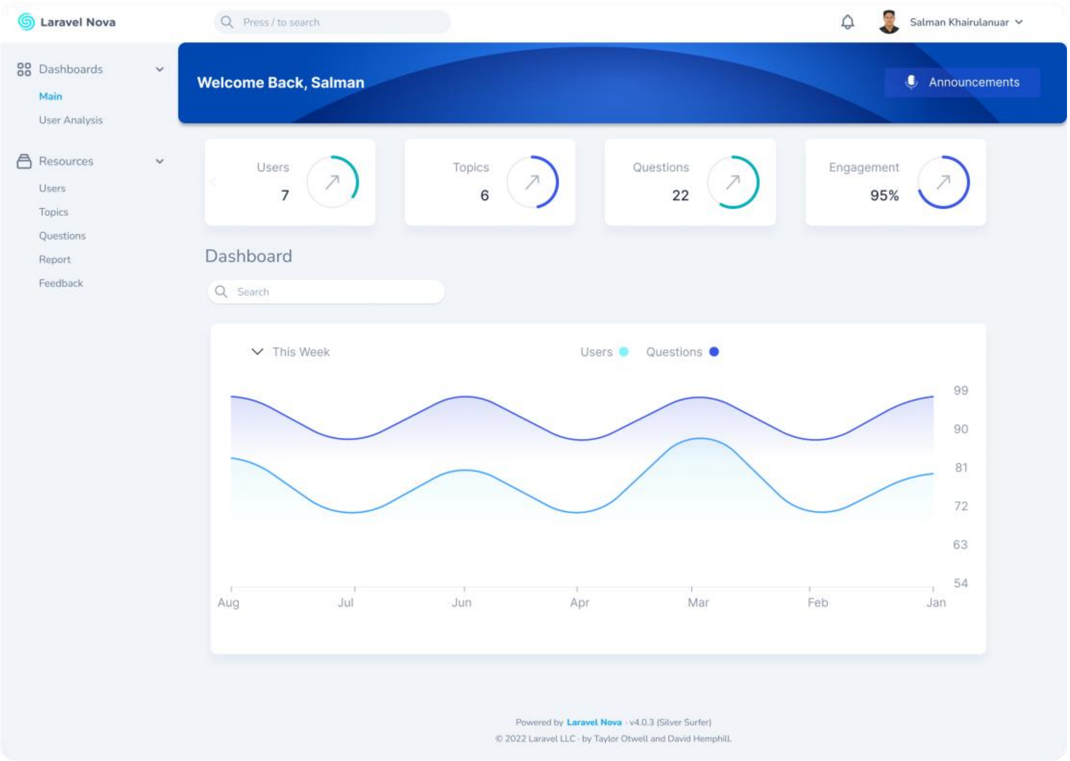
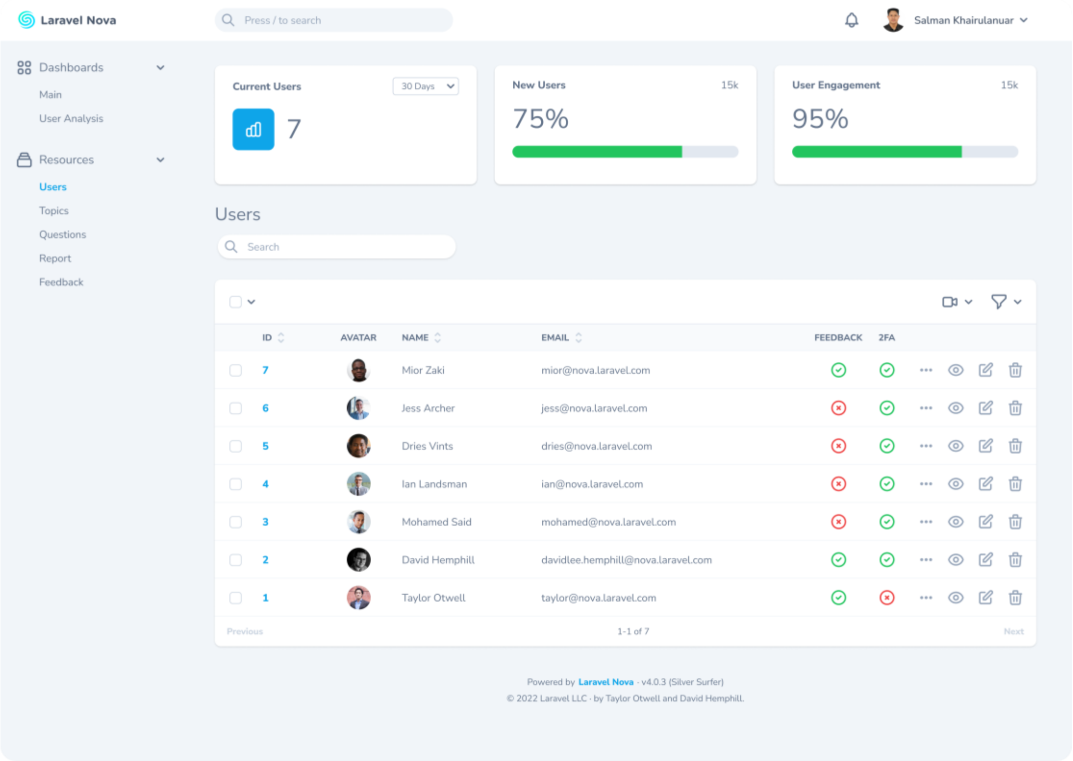


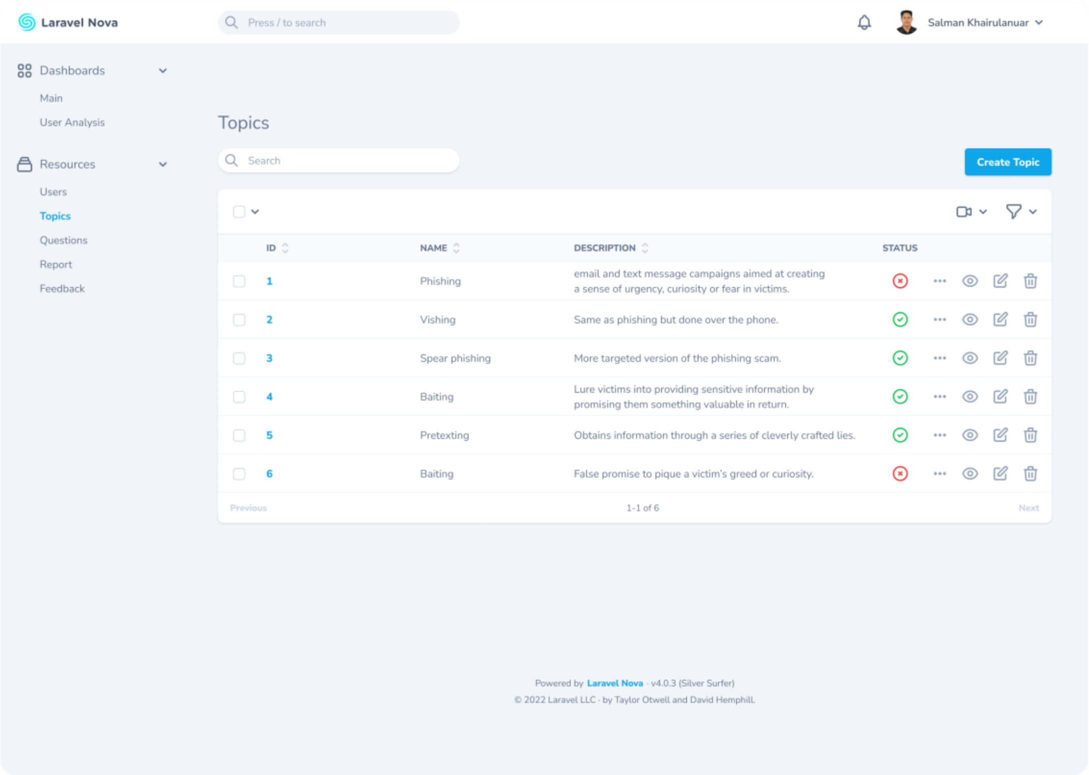
Figure 3.8 Administrator Dashboard



ID	AVATAR	NAME	EMAIL	FEEDBACK	2FA
7		Mior Zaki	mior@nova.laravel.com	✓	✓
6		Jess Archer	jess@nova.laravel.com	✗	✓
5		Dries Vints	dries@nova.laravel.com	✗	✓
4		Ian Landsman	ian@nova.laravel.com	✗	✓
3		Mohamed Said	mohamed@nova.laravel.com	✗	✓
2		David Hemphill	davidlee.hemphill@nova.laravel.com	✓	✓
1		Taylor Otwell	taylor@nova.laravel.com	✓	✗

Previous
1-1 of 7
Next
Powered by Laravel Nova · v4.0.3 (Silver Surfer)
© 2022 Laravel LLC · by Taylor Otwell and David Hemphill.

Figure 3.9 Administrator Manage Users

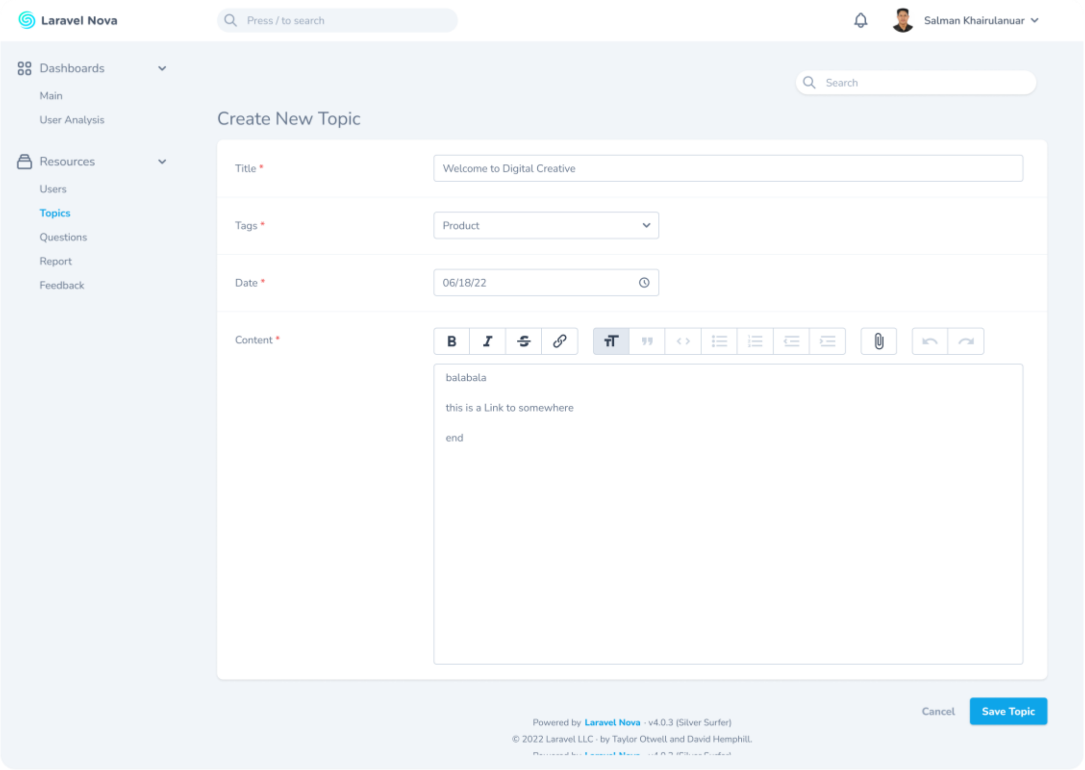


Topics

ID	NAME	DESCRIPTION	STATUS
1	Phishing	email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims.	✗
2	Vishing	Same as phishing but done over the phone.	✓
3	Spear phishing	More targeted version of the phishing scam.	✓
4	Baiting	Lure victims into providing sensitive information by promising them something valuable in return.	✓
5	Pretexting	Obtains information through a series of cleverly crafted lies.	✓
6	Baiting	False promise to pique a victim's greed or curiosity.	✗

Powered by Laravel Nova · v4.0.3 (Silver Surfer)
© 2022 Laravel LLC · by Taylor Otwell and David Hemphill.

Figure 3.10 Administrator Manage Topics



Create New Topic

Title * Welcome to Digital Creative

Tags * Product

Date * 06/18/22

Content *

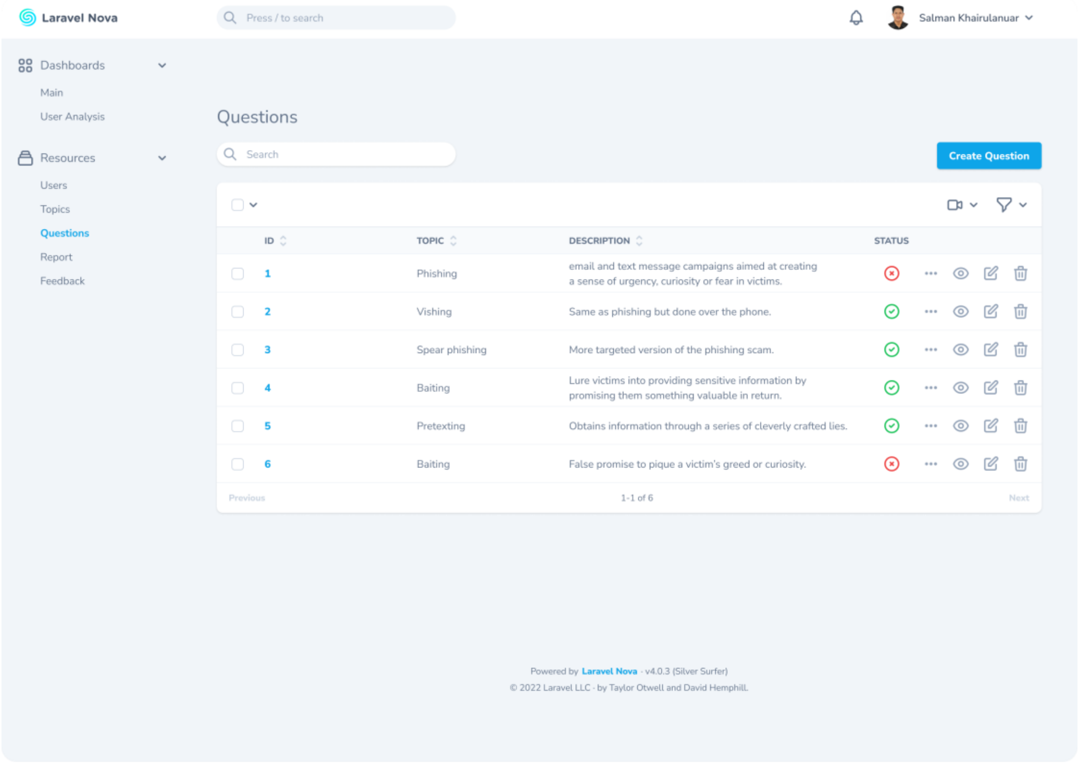
balabala

this is a Link to somewhere

end

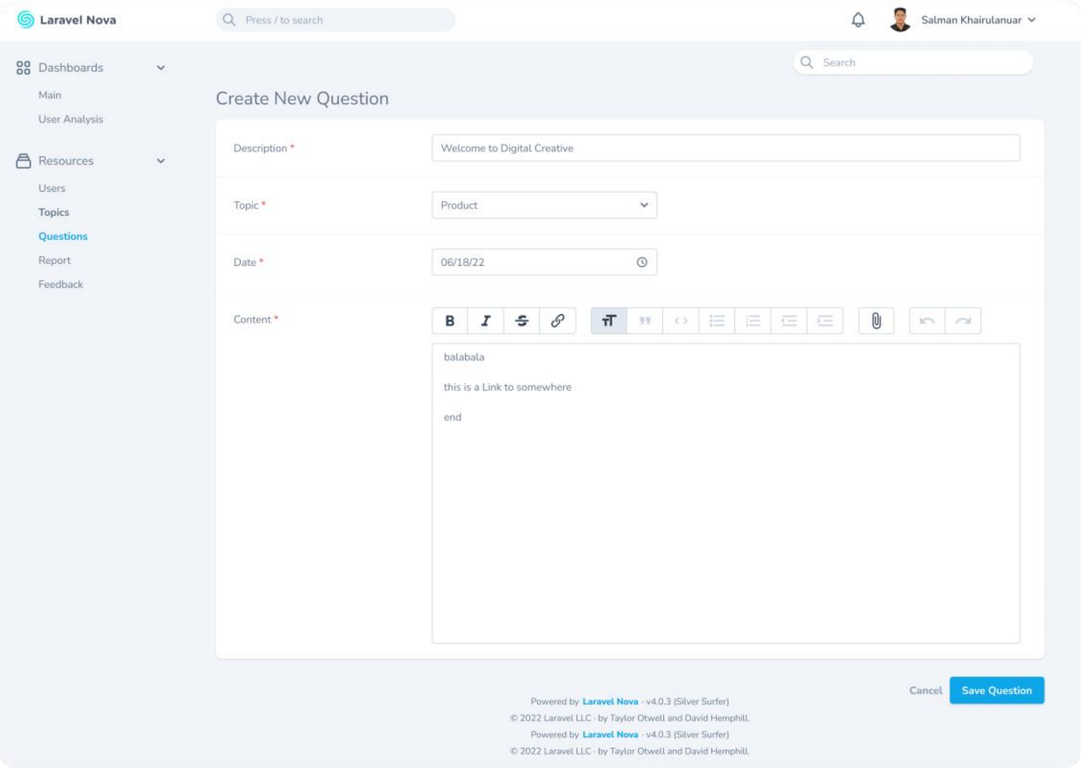
Powered by Laravel Nova · v4.0.3 (Silver Surfer)
© 2022 Laravel LLC · by Taylor Otwell and David Hemphill.

Figure 3.11 Administrator Create Topic



ID	TOPIC	DESCRIPTION	STATUS
1	Phishing	email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims.	☒
2	Vishing	Same as phishing but done over the phone.	✓
3	Spear phishing	More targeted version of the phishing scam.	✓
4	Baiting	Lure victims into providing sensitive information by promising them something valuable in return.	✓
5	Pretexting	Obtains information through a series of cleverly crafted lies.	✓
6	Baiting	False promise to pique a victim's greed or curiosity.	☒

Figure 3.12 Administrator Manage Questions


Laravel Nova
Press / to search
Salman Khairulanuar
Dashboards
Main
User Analysis
Resources
Users
Topics
Questions
Report
Feedback
Search
Create New Question
Cancel
Save Question
Powered by Laravel Nova · v4.0.3 (Silver Surfer)
© 2022 Laravel LLC · by Taylor Otwell and David Hemphill.
Powered by Laravel Nova · v4.0.3 (Silver Surfer)
© 2022 Laravel LLC · by Taylor Otwell and David Hemphill.

Description * Welcome to Digital Creative

Topic * Product

Date * 06/18/22

Content *

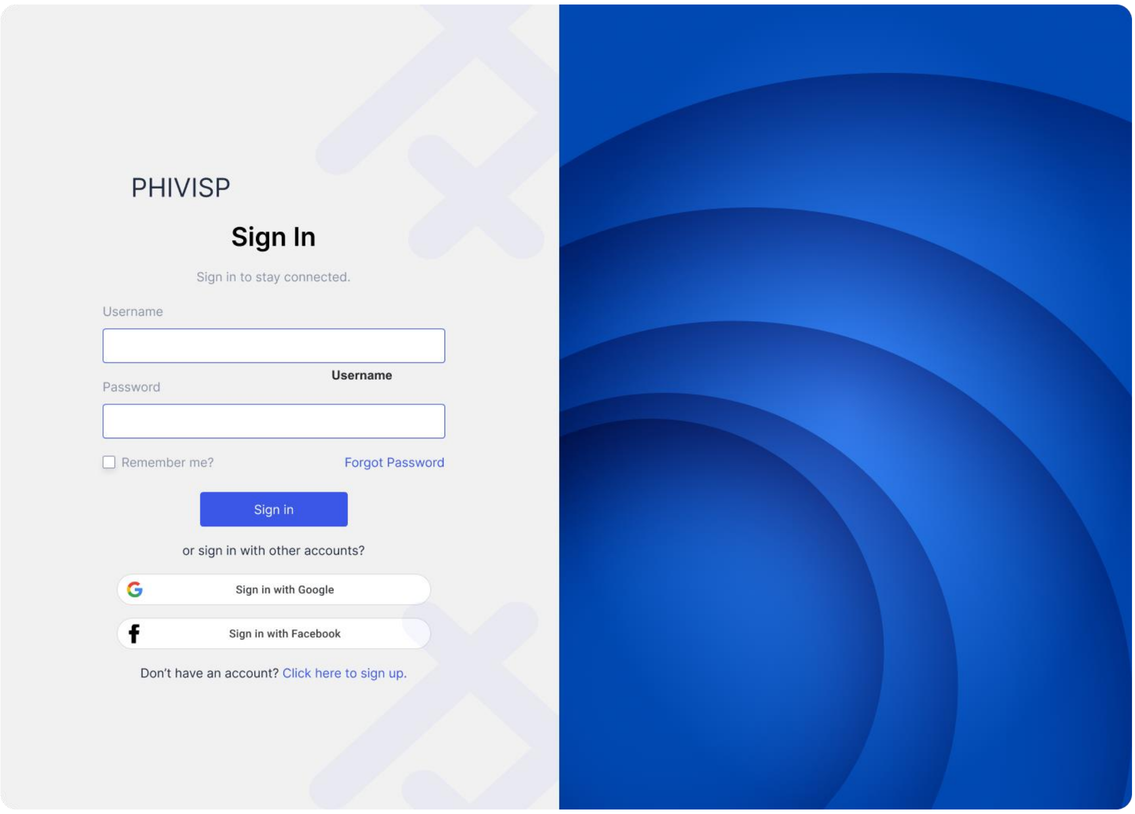
balabala

this is a Link to somewhere

end

Figure 3.13 Administrator Create Question

3.6.2 Initial Design for User



PHIVISP

Sign In

Sign in to stay connected.

Username

Username

Password

□ Remember me?

Forgot Password

Don't have an account? Click here to sign up.

Figure 3.14 User Login

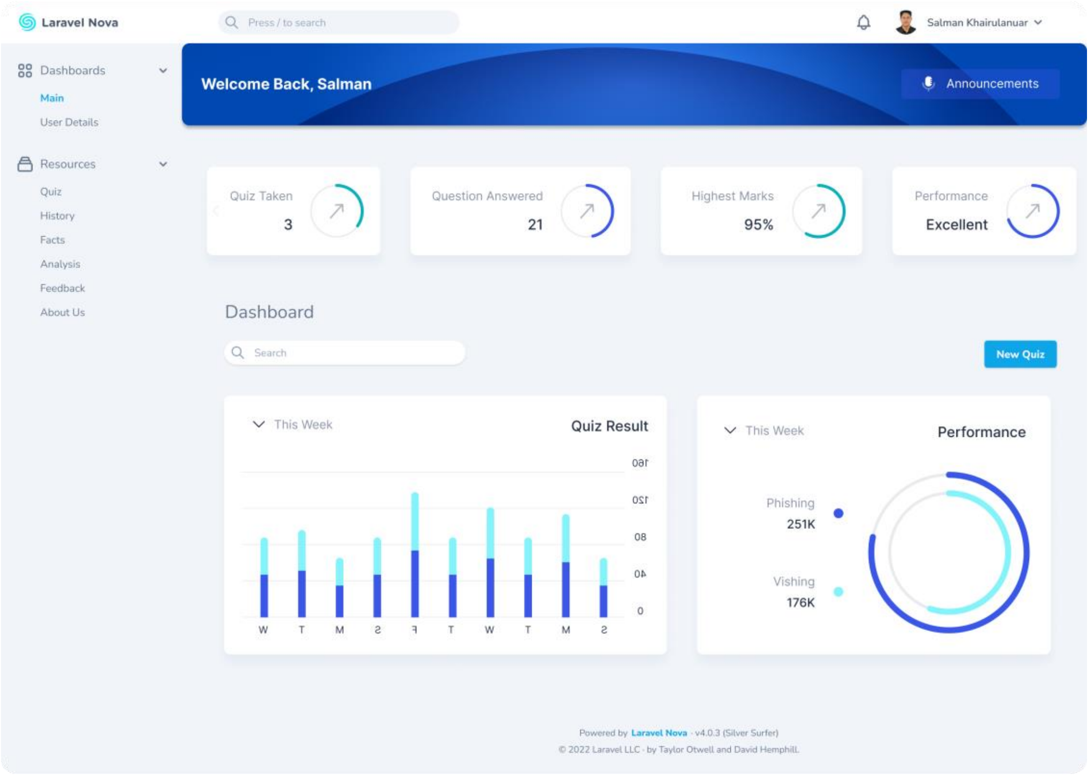
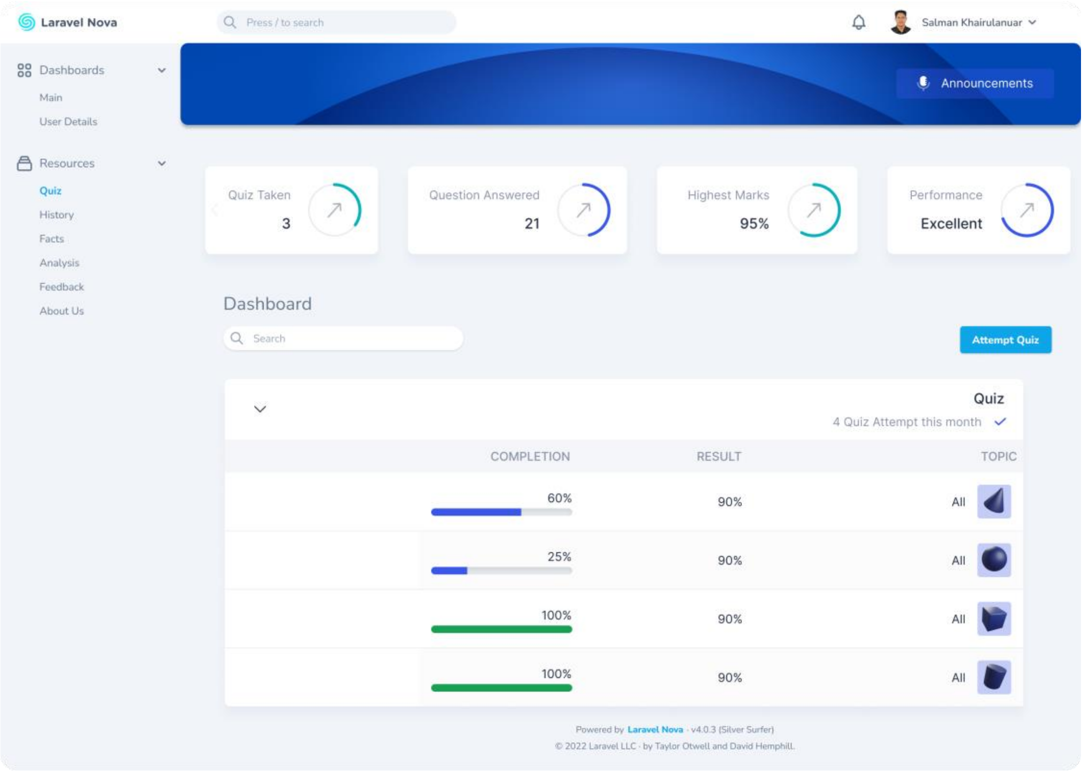
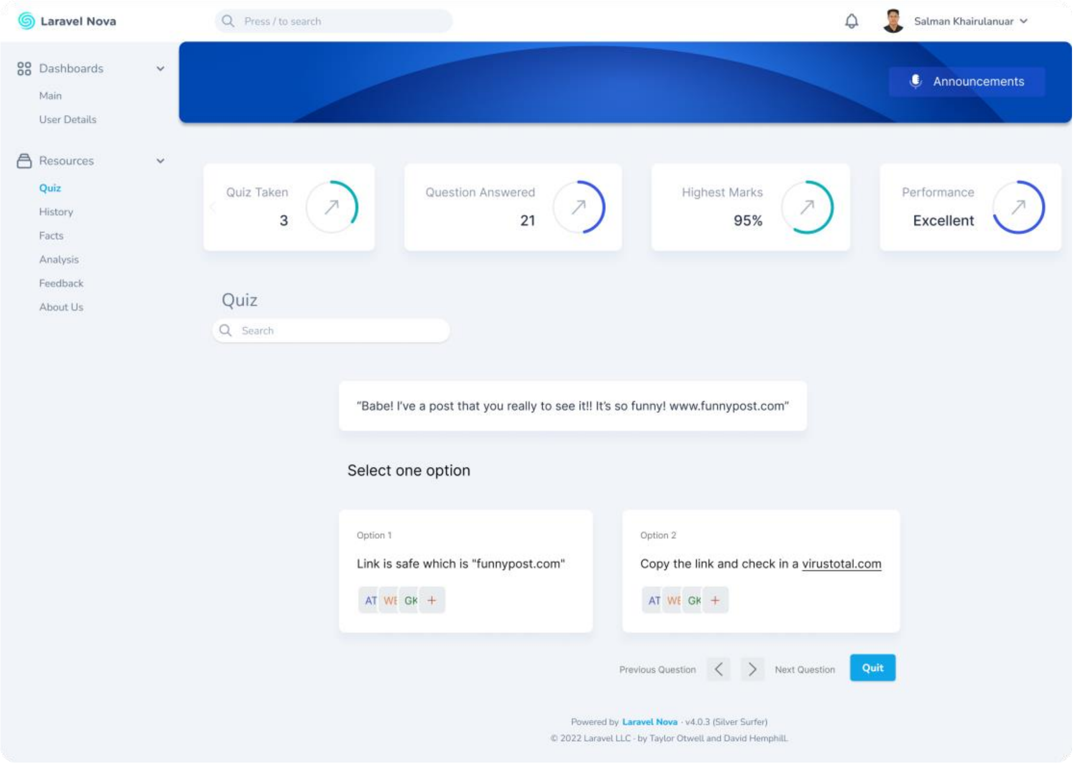


Figure 3.15 User Dashboard



COMPLETION	RESULT	TOPIC
60%	90%	All
25%	90%	All
100%	90%	All
100%	90%	All

Figure 3.16 User Quiz



"Babe! I've a post that you really to see it!! It's so funny! www.funnypost.com"

Select one option

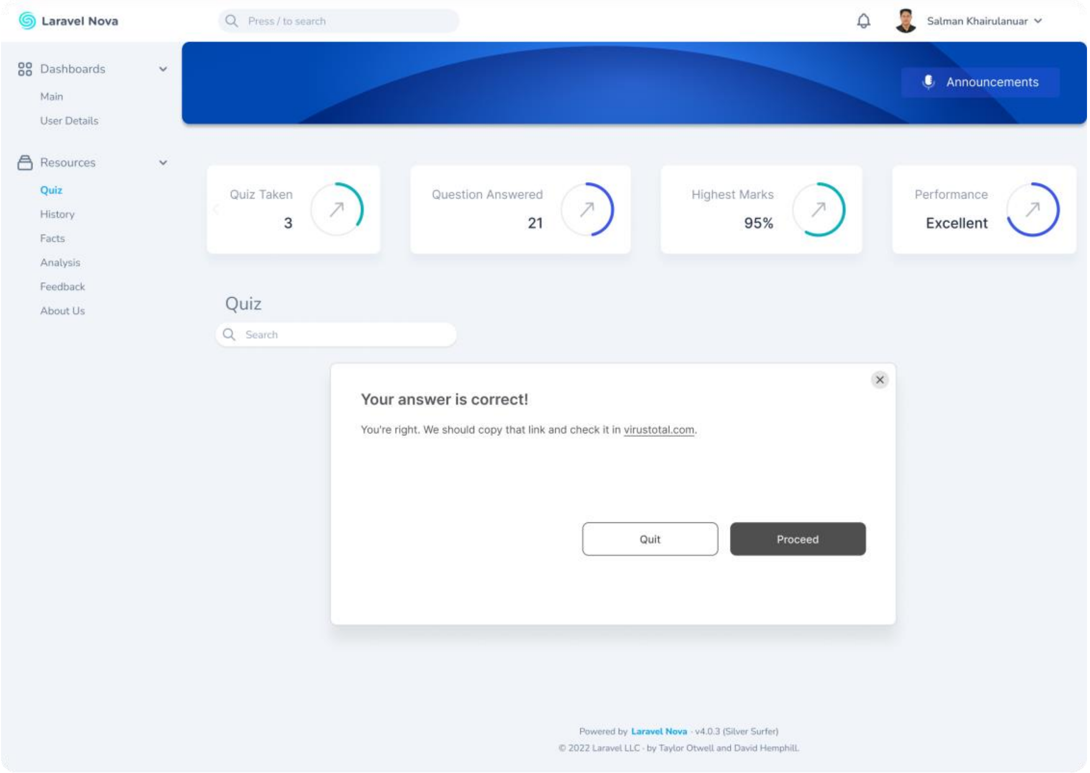
Option 1

Link is safe which is "funnypost.com"

Option 2

Copy the link and check in a virustotal.com

Figure 3.17 User Quiz Question



Your answer is correct!

You're right. We should copy that link and check it in virustotal.com.

Figure 3.18 User Quiz Solution

This page will display the solution or the reasons for the selected option and whether the user answered the questions correctly. This will directly improve the User's knowledge about social engineering, especially phishing, vishing, and spear phishing. Furthermore, the answer will be stored in the database to ensure any improvement when the users answer the same question next time.

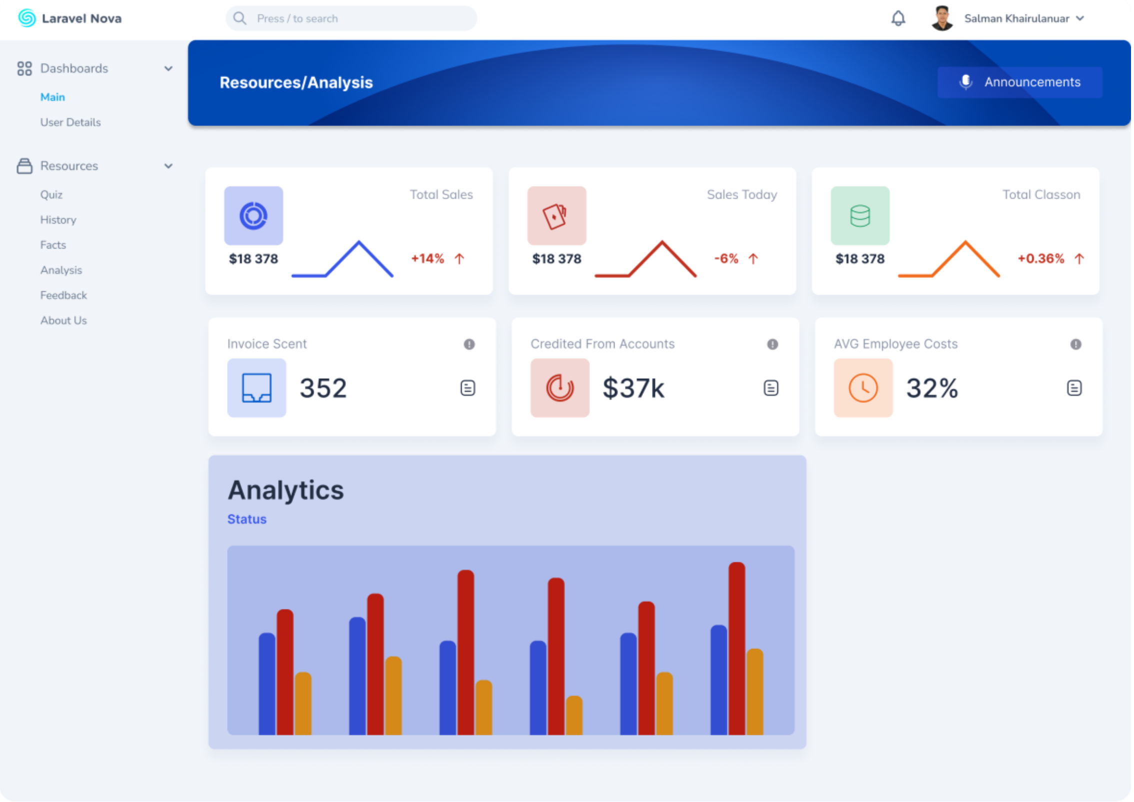


Figure 3.19 User Analysis

The user Analysis page offers users a detailed analysis of which topics of social engineering the users will most likely be exploited by the attackers. Users also can view which questions they answered wrong repeatedly. The other features are average time consumed for each question, highest and lowest marks, how much their social engineering knowledge improves, and more.

3.7 Testing/Validation Plan

3.7.1 User Acceptance Test (UAT) form for Administrator

Table 3.14 UAT Form for Administrator

No.	Module	Status		Comment
1.	Login to the PhiViSp system	Pass	Fail	
2.	Create, view, edit and delete questions.	Pass	Fail	
3.	Add an answer option and explanation for the question.	Pass	Fail	
4.	Create, view, edit and delete topics.	Pass	Fail	
5.	Attach questions to the topic.	Pass	Fail	
6.	Create, view, edit and delete quizzes.	Pass	Fail	
7.	Attach the topic to the quiz.	Pass	Fail	
8.	Create, view, edit and delete phishing simulation.	Pass	Fail	
9.	Add victims to the phishing simulation.	Pass	Fail	

10.	Send phishing and feedback emails to the victims.	Pass	Fail	
11.	View and delete simulation feedback.	Pass	Fail	
12.	Create page hints	Pass	Fail	
13.	Create and manage users.	Pass	Fail	

This test performed by:

Name: ____

Signature: ____

Date: ____

3.7.2 User Acceptance Test (UAT) form for User

Table 3.15 UAT Form for User

No.	Module	Status		Comment
1.	Login using a Google account.	Pass	Fail	Good
2.	Attempt and continue the quiz.	Pass	Fail	Good
3.	Select the question option and submit the answer.	Pass	Fail	Good
4.	Display explanation for the question.	Pass	Fail	Good
5.	View details about phishing simulation.	Pass	Fail	Good
6.	Display simulation feedback.	Pass	Fail	Good
7.	Display page hint	Pass	Fail	Good

This test performed by:

Name: ____

Signature: ____

Date: ____

3.8 Potential Use of Proposed Solution

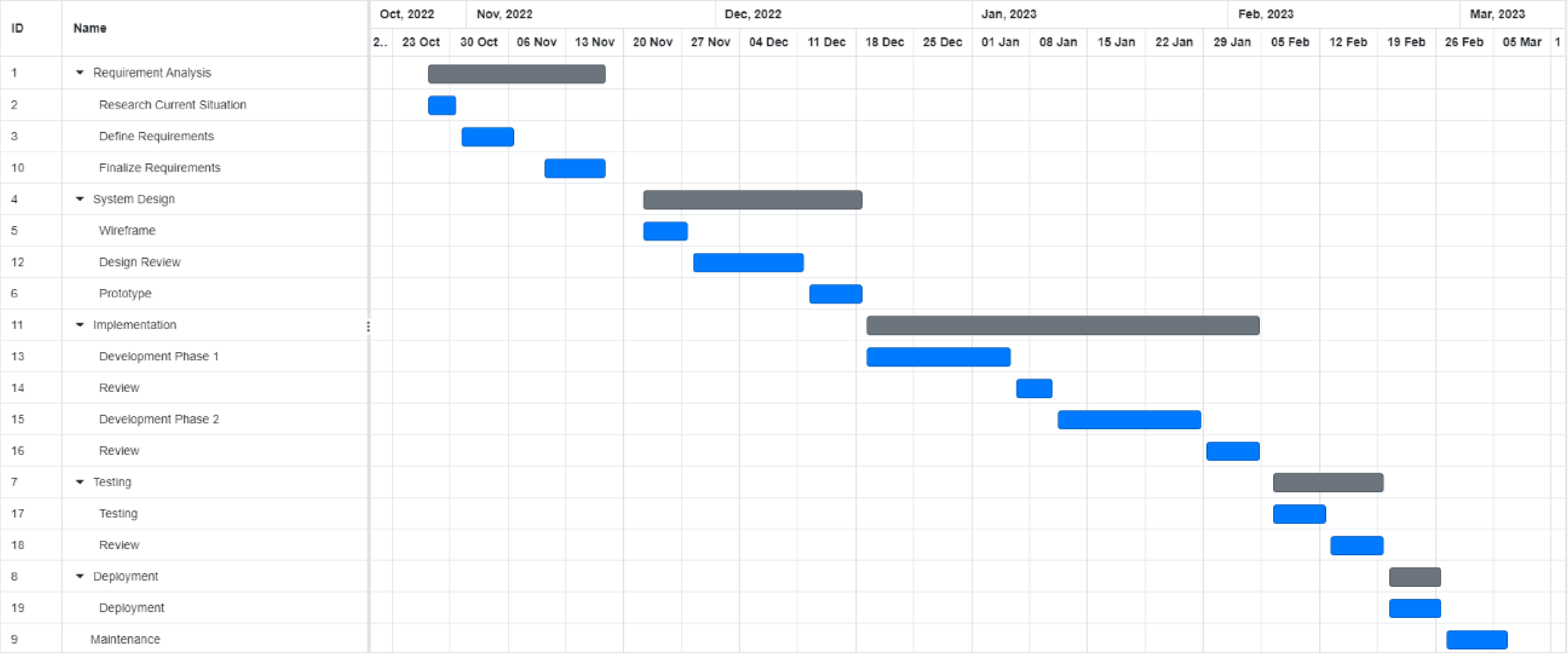
The PhiViSp simulation website can be a valuable tool for individuals to improve their cybersecurity awareness and protect themselves from threats. For example, phishing simulations can teach users how to identify and avoid suspicious emails, while vishing simulations can help them recognise and respond to potential phone scams. Spear phishing simulations, on the other hand, can help the user understand how attackers target specific individuals or groups and how to protect themselves from these attacks. In these simulations' websites, users can learn how to identify and avoid common tactics used by cybercriminals, such as using urgent language, mimicking official logos, or creating fake websites.

On the other hand, this simulation website also can be used to test employees' ability to identify and respond to suspicious emails. In contrast, vishing simulations test employees' ability to identify and respond to questionable phone calls. Finally, spear phishing simulations test employees' ability to identify and respond to targeted attacks tailored to specific individuals or groups within an organisation. By regularly conducting these simulations, organisations can identify vulnerabilities in their employees' cybersecurity knowledge and provide targeted training to address them.

Overall, the proposed simulation website can provide individuals and organisations with the knowledge and skills to protect themselves from potential cyber threats and help organisations proactively protect themselves against cyber-attacks.

A phishing, vishing, and spear phishing simulation system can provide individuals with the knowledge and skills to protect themselves from potential cyber threats. A phishing, vishing, and spear phishing simulation system can provide individuals with the knowledge and skills to protect themselves from potential cyber threats.

3.9 Gantt chart



ID	Name
1	Requirement Analysis
2	Research Current Situation
3	Define Requirements
10	Finalize Requirements
4	System Design
5	Wireframe
12	Design Review
6	Prototype
11	Implementation
13	Development Phase 1
14	Review
15	Development Phase 2
16	Review
7	Testing
17	Testing
18	Review
8	Deployment
19	Deployment
9	Maintenance

Figure 3.20 Gantt Chart

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This chapter will discuss the requirements gathering, system design, implementation, and testing of PhiViSp. PhiViSp is a web-based system developed for all Malaysians. The system is implemented using Laravel Framework, Visual Studio Code, MySQL, and Figma. During testing, the team identified errors and bugs, which were fixed immediately.

4.2 Implementation Process

The initial stage of developing PhiViSp involved creating an Entity Relationship Diagram (ERD) to define the database structure of the system. The ERD was used to identify the relevant entities, their attributes, and the relationships between them. This information was then used to create the necessary tables and database for the PhiViSp system in phpMyAdmin.

Regular testing will be conducted throughout development to ensure the system works as expected. The testing was done in various stages, including unit, integration, and system. PhiViSp will allow users to simulate a scenario miming a real-life phishing email, including the sender, subject, and content. In addition, the email will contain elements commonly found in phishing emails, such as a sense of urgency, a request for personal information, or a suspicious link. The system also will demonstrate phishing, vishing, and spear phishing attacks in a question format. The system is designed to be secure, with user authentication and data encryption features.

The development, implementation, and testing of PhiViSp, resulting in a reliable and user-friendly system. The system's design and features were designated to fulfil the user's needs, and regular testing was carried out to ensure the system was free of errors and bugs. In conclusion, the proposed simulation system is an effective tool to educate people about social engineering attacks and encourage caution when dealing with unfamiliar individuals or requests for sensitive information. Ultimately, the simulation system is vital in promoting a safer digital environment for everyone.

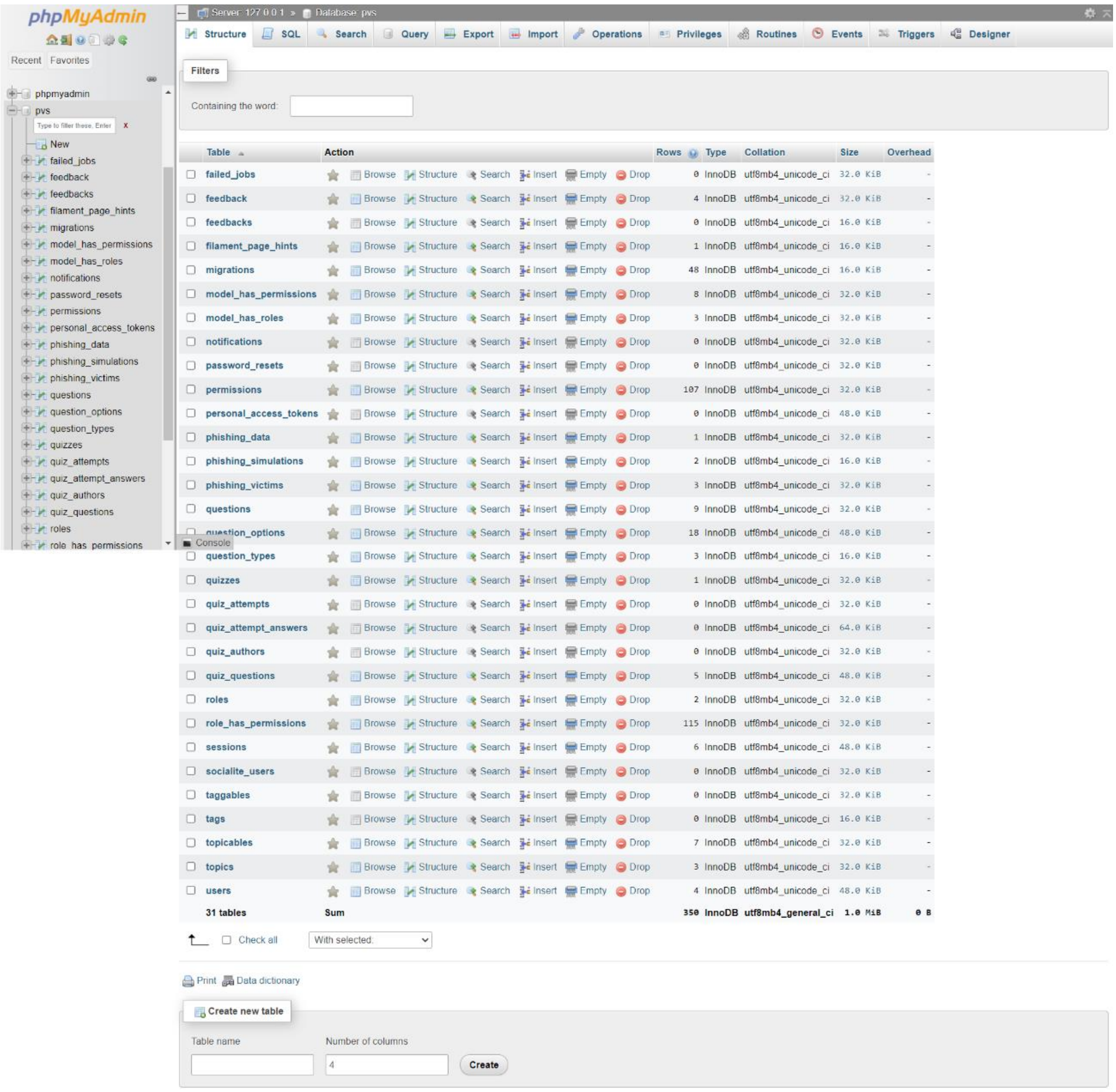
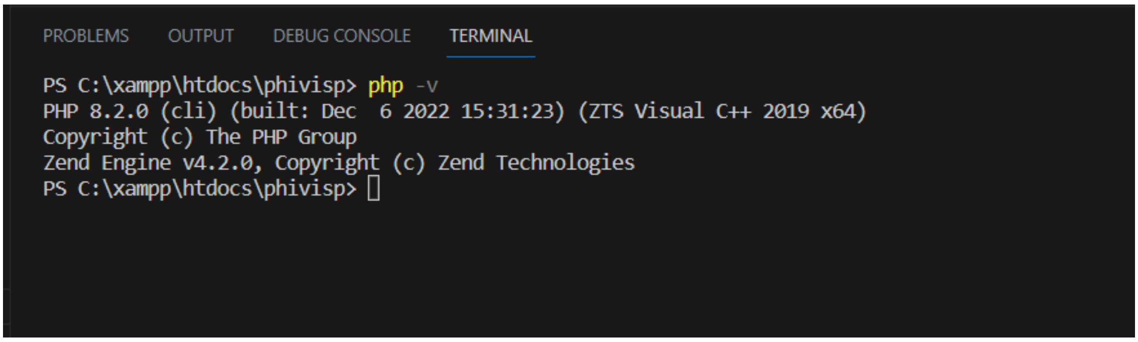


Table	Action	Rows	Type	Collation	Size	Overhead
□ failed_jobs	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ feedback	Browse Structure Search Insert Empty Drop	4	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ feedbacks	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
□ filament_page_hints	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
□ migrations	Browse Structure Search Insert Empty Drop	48	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
□ model_has_permissions	Browse Structure Search Insert Empty Drop	8	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ model_has_roles	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ notifications	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ password_resets	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ permissions	Browse Structure Search Insert Empty Drop	107	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ personal_access_tokens	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
□ phishing_data	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ phishing_simulations	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
□ phishing_victims	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ questions	Browse Structure Search Insert Empty Drop	9	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ question_options	Browse Structure Search Insert Empty Drop	18	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
□ question_types	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
□ quizzes	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ quiz_attempts	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ quiz_attempt_answers	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	64.0 KiB	-
□ quiz_authors	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ quiz_questions	Browse Structure Search Insert Empty Drop	5	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
□ roles	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ role_has_permissions	Browse Structure Search Insert Empty Drop	115	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ sessions	Browse Structure Search Insert Empty Drop	6	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
□ socialite_users	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ taggables	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ tags	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
□ topicables	Browse Structure Search Insert Empty Drop	7	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ topics	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
□ users	Browse Structure Search Insert Empty Drop	4	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
31 tables	Sum	350	InnoDB	utf8mb4_general_ci	1.0 MiB	0 B

Figure 4.1 Tables in the PhiViSp database

PhiViSp is developed using the Laravel framework in combination with Filament. Laravel is a renowned open-source web application framework for PHP. It was introduced by Taylor Otwell in 2011 to simplify and enhance web development through its elegant syntax and comprehensive set of tools and features. Laravel follows the Model-View-Controller (MVC) architectural pattern and incorporates functionalities such as routing, middleware, ORM (Object-Relational Mapping), and templating engine by utilising Laravel and Filament, PhiViSp benefits from the robustness of Laravel and the powerful data management capabilities provided by Filament. This combination enables efficient development and empowers the creation of web applications, APIs, and content management systems (CMS).

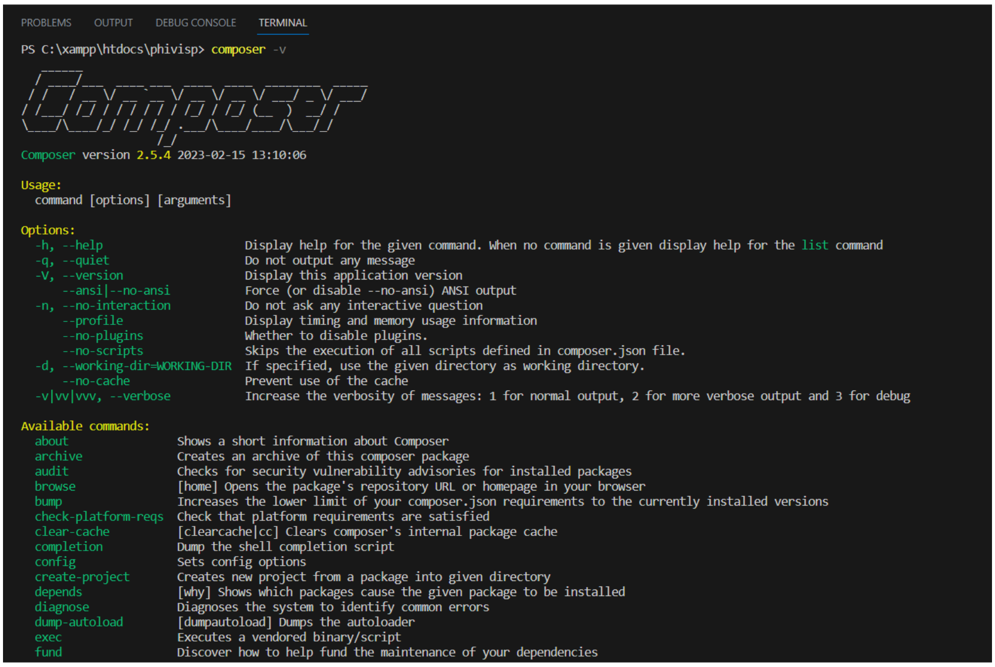


```
PS C:\xampp\htdocs\phivisp> php -v
PHP 8.2.0 (cli) (built: Dec  6 2022 15:31:23) (ZTS Visual C++ 2019 x64)
Copyright (c) The PHP Group
Zend Engine v4.2.0, Copyright (c) Zend Technologies
PS C:\xampp\htdocs\phivisp> 
```

Figure 4.2 Installed PHP version

Figure 4.2 shows that PHP version 8.2.0 is installed on the environment.

The Composer is installed on the environment.

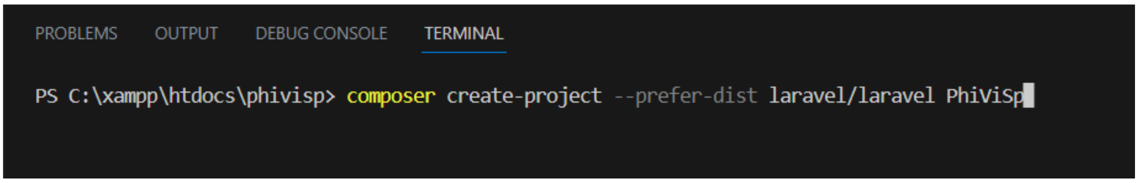


```
PS C:\xampp\htdocs\phivisp> composer -v
   ______
  / ____/___  ____ ___  ____  ____  ________  _____
 / /   / __ \/ __ `__ \/ __ \/ __ \/ ___/ _ \/ ___/
/ /___/ /_/ / / / / / / /_/ / /_/ (__  )  __/ /
\____/\____/_/ /_/ /_/ .___/\____/____/\___/_/
                    /_/
Composer version 2.5.4 2023-02-15 13:10:06

Usage:
  command [options] [arguments]

Options:
  -h, --help                     Display help for the given command. When no command is given display help for the list command
  -q, --quiet                    Do not output any message
  -V, --version                  Display this application version
      --ansi|--no-ansi           Force (or disable --no-ansi) ANSI output
  -n, --no-interaction           Do not ask any interactive question
      --profile                  Display timing and memory usage information
      --no-plugins               Whether to disable plugins.
      --no-scripts               Skips the execution of all scripts defined in composer.json file.
  -d, --working-dir=WORKING-DIR  If specified, use the given directory as working directory.
      --no-cache                 Prevent use of the cache
  -v|vv|vvv, --verbose           Increase the verbosity of messages: 1 for normal output, 2 for more verbose output and 3 for debug

Available commands:
  about                Shows a short information about Composer
  archive              Creates an archive of this composer package
  audit                Checks for security vulnerability advisories for installed packages
  browse               [home] Opens the package's repository URL or homepage in your browser
  bump                 Increases the lower limit of your composer.json requirements to the currently installed versions
  check-platform-reqs  Check that platform requirements are satisfied
  clear-cache          [clearcache|cc] Clears composer's internal package cache
  completion           Dump the shell completion script
  config               Sets config options
  create-project       Creates new project from a package into given directory
  depends              [why] Shows which packages cause the given package to be installed
  diagnose             Diagnoses the system to identify common errors
  dump-autoload        [dumpautoload] Dumps the autoloader
  exec                 Executes a vendored binary/script
  fund                 Discover how to help fund the maintenance of your dependencies
```

Figure 4.3 Installed composer version

The "composer -v" command will display the installed composer version if the Composer is installed. For example, figure 4.3 confirms that composer version 2.5.4 is installed on the environment.

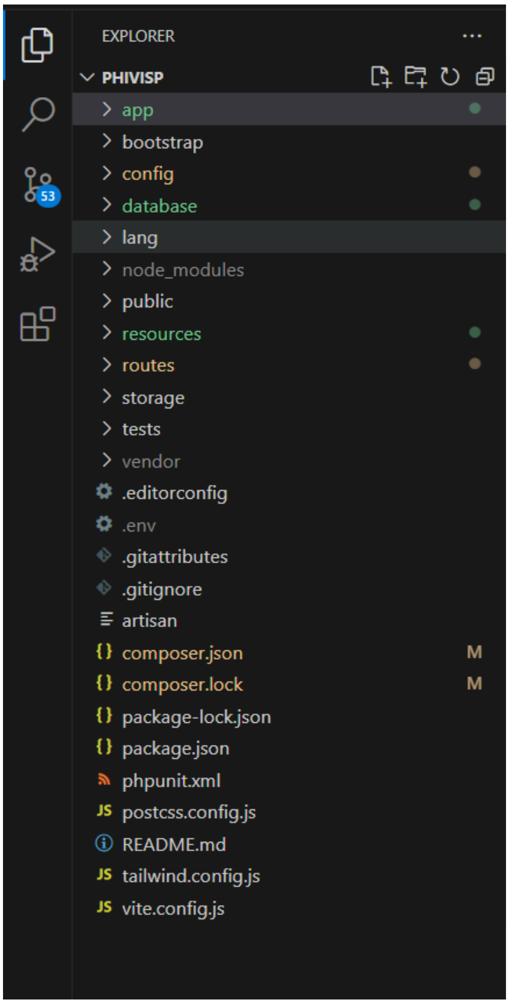
Create Laravel project



```
PS C:\xampp\htdocs\phivisp> composer create-project --prefer-dist laravel/laravel PhiViSp
```

Figure 4.4 Create PhiViSp Laravel project

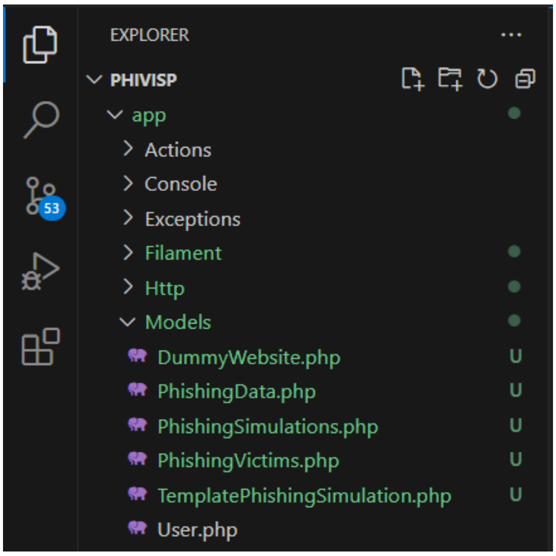
Figure 4.4 shows the command that needs to be run in the terminal or command prompt of the development environment, such as Visual Studio Code, to create the PhiViSp project using the Laravel Framework.



```
PHIVISP
> app
> bootstrap
> config
> database
> lang
> node_modules
> public
> resources
> routes
> storage
> tests
> vendor
.editorconfig
.env
.gitattributes
.gitignore
artisan
composer.json                M
composer.lock                M
package-lock.json
package.json
phpunit.xml
postcss.config.js
README.md
tailwind.config.js
vite.config.js
```

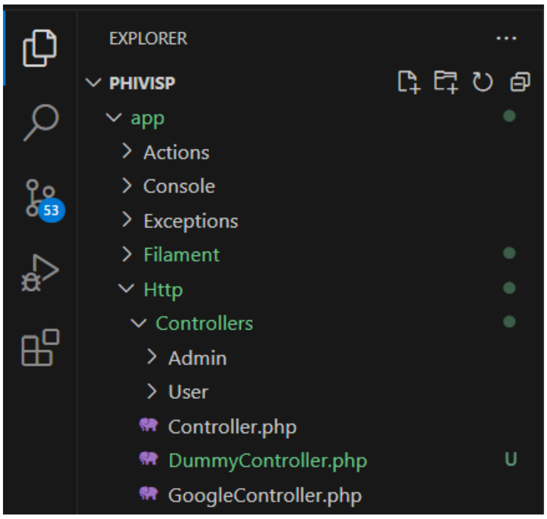
Figure 4.5 File structure for the Laravel project

Figure 4.5 shows the files created in the PhiViSp project. The PhiViSp project uses the Laravel framework and Filament Laravel package, which follows the Model-View-Controller (MVC).



```
EXPLORER                                   ...
∨ PHIVISP
  ∨ app
    > Actions
    > Console
    > Exceptions
    > Filament
    > Http
    ∨ Models
       DummyWebsite.php                    U
       PhishingData.php                    U
       PhishingSimulations.php             U
       PhishingVictims.php                 U
       TemplatePhishingSimulation.php      U
       User.php
```

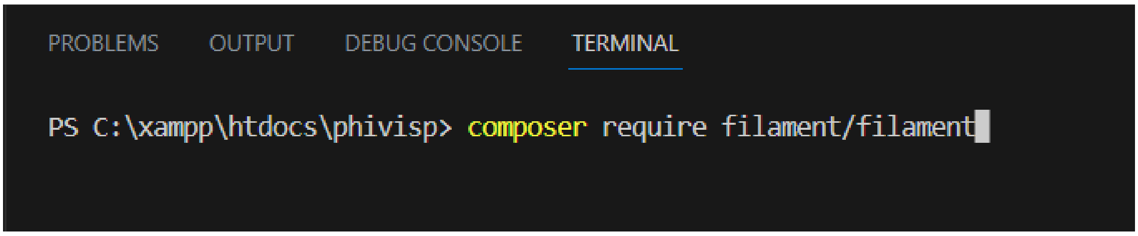
Figure 4.6 Models



```
EXPLORER                                   ...
∨ PHIVISP
  ∨ app
    > Actions
    > Console
    > Exceptions
    > Filament
    ∨ Http
      ∨ Controllers
        > Admin
        > User
         Controller.php
         DummyController.php               U
         GoogleController.php
```

Figure 4.7 Controllers

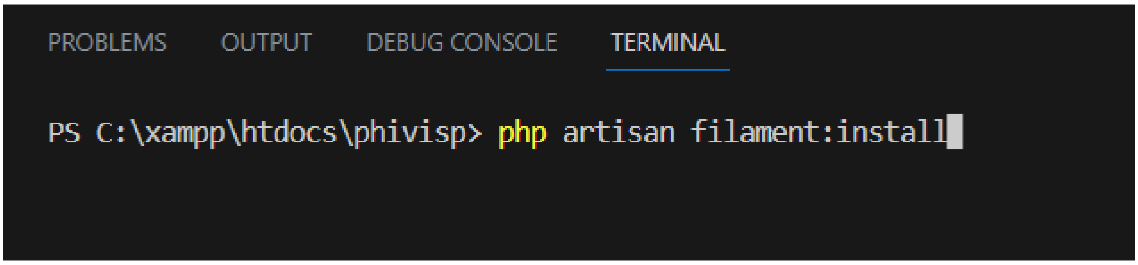
Create a Filament package in the Laravel project



```
PS C:\xampp\htdocs\phivisp> composer require filament/filament
```

Figure 4.8 Fetch the Filament package

This command tells Composer to fetch the Filament package from the Packagist repository and install it in the Laravel project. Then, the Composer will download and install the Filament package into the Laravel project.



```
PS C:\xampp\htdocs\phivisp> php artisan filament:install
```

Figure 4.9 Install the Filament

The command shown in Figure 4.9 performs the necessary setup and configuration steps to install Filament in the Laravel project.

4.2.1 Interfaces

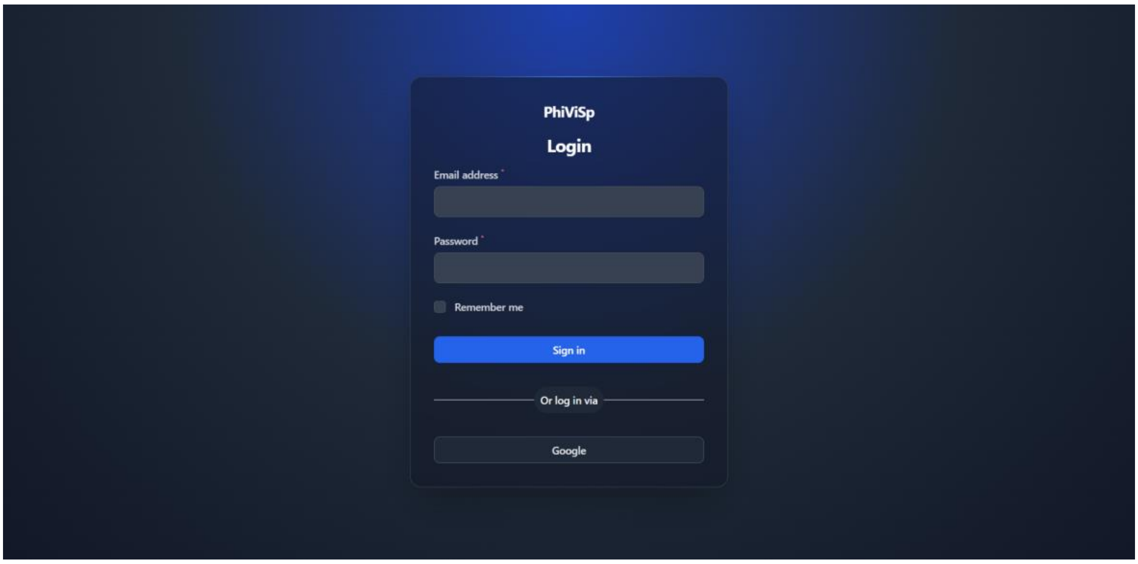


Figure 4.10 Login page

Figure 4.10 shows the login page where users can enter the PhiViSp system by entering their usernames and passwords. Additionally, users have the option to log in using their Google account. If the usernames and passwords match or the Google authentication is successful, the user can access the PhiViSp system.

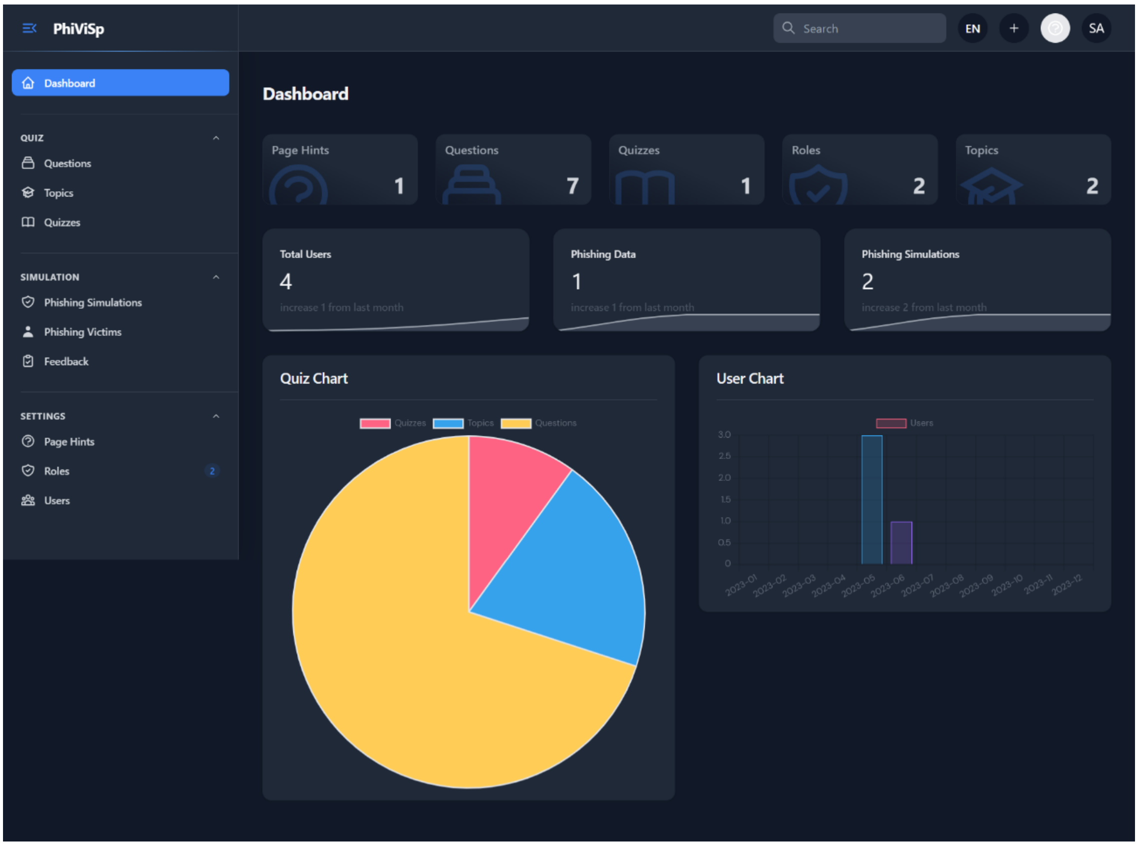
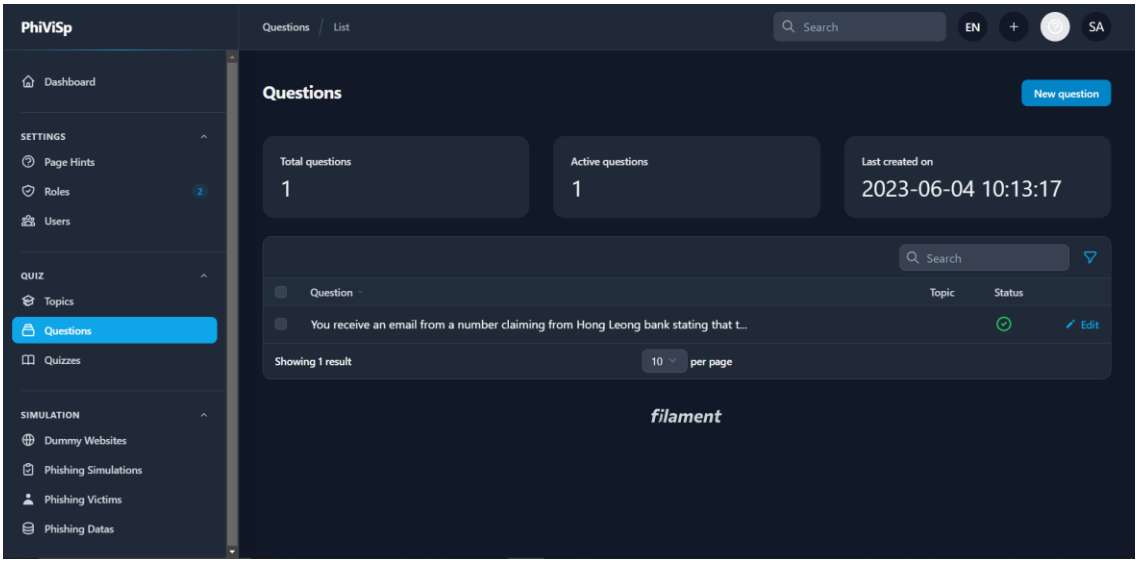


Figure 4.11 Admin dashboard

Figure 4.12 showcases the admin dashboard of the PhiViSp system, presenting essential system information. The dashboard provides an overview of key metrics, such as the number of questions, quizzes, topics, and users. This information gives administrators a glance at the overall usage and activity within the system, allowing them to monitor and manage it effectively.

The dashboard is the initial page administrators encounter upon logging into the PhiViSp system. Next, the admin can navigate to various modules from the dashboard using the left navigation pane. These modules allow administrators to manage and administer different aspects of the system, such as creating and managing topics, questions, quizzes, dummy websites, phishing simulations, phishing victims, and phishing data.



Questions

Total questions 1

Active questions 1

Last created on 2023-06-04 10:13:17

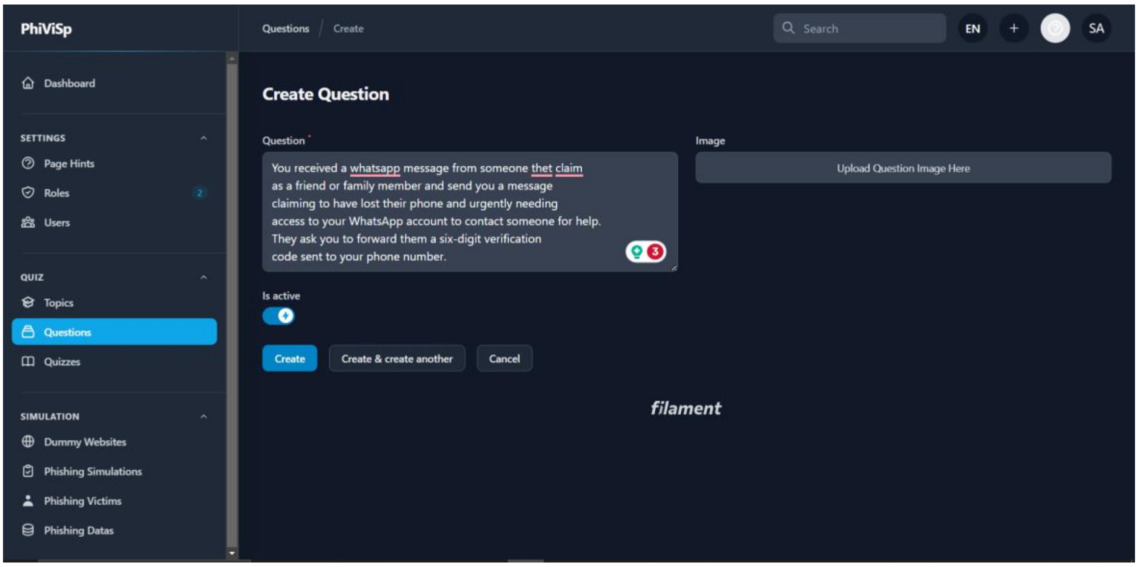
Question	Topic	Status
You receive an email from a number claiming from Hong Leong bank stating that t...		✓

Showing 1 result 10 per page

Figure 4.12 List question

This page displays a list of all the questions created by the admin, along with relevant information such as the number of questions, active questions, and the last time question was made.

The list of questions includes details such as the question itself, the associated topic, and the status of the question. The admin can view the question and its details by clicking the question entry. This will display the question-and-answer options.



Create Question

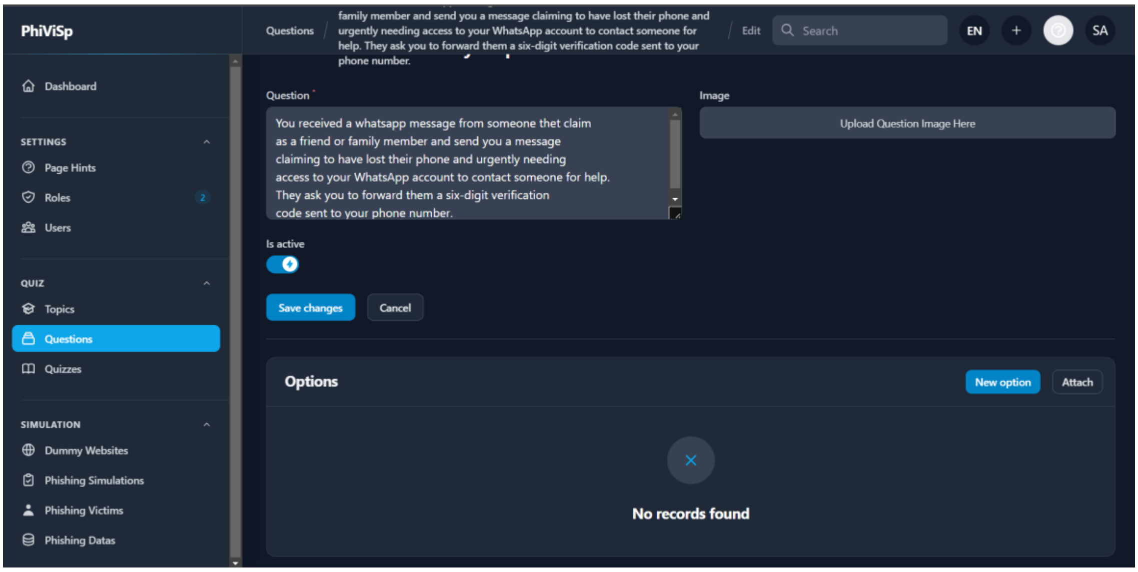
Question*: You received a whatsapp message from someone thet claim as a friend or family member and send you a message claiming to have lost their phone and urgently needing access to your WhatsApp account to contact someone for help. They ask you to forward them a six-digit verification code sent to your phone number.

Image

Is active: ●

Figure 4.13 Create a new question

The "Create Question" page in the PhiViSp system provides an interface for the admin to create a new question. When the admin clicks on the "New Question" button, they will be taken to this page where they can enter the necessary details for the question.



Questions / family member and send you a message claiming to have lost their phone and urgently needing access to your WhatsApp account to contact someone for help. They ask you to forward them a six-digit verification code sent to your phone number.

Question *

You received a whatsapp message from someone thet claim as a friend or family member and send you a message claiming to have lost their phone and urgently needing access to your WhatsApp account to contact someone for help. They ask you to forward them a six-digit verification code sent to your phone number.

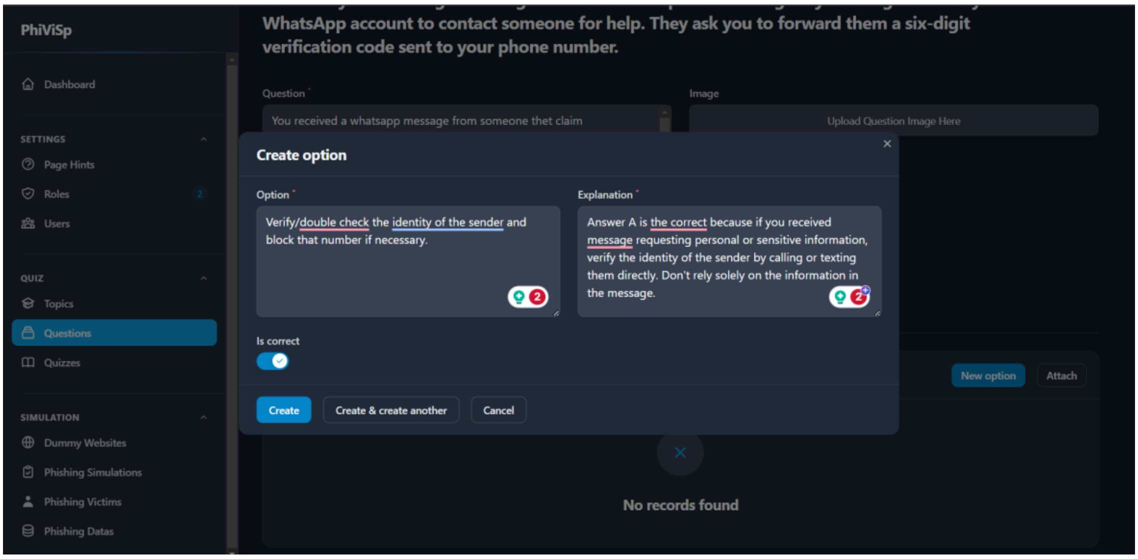
Image: Upload Question Image Here

Is active

Options

No records found

Figure 4.14 Edit question



WhatsApp account to contact someone for help. They ask you to forward them a six-digit verification code sent to your phone number.

Question *

You received a whatsapp message from someone thet claim

Image: Upload Question Image Here

Create option

Option *

Verify/double check the identity of the sender and block that number if necessary.

Explanation *

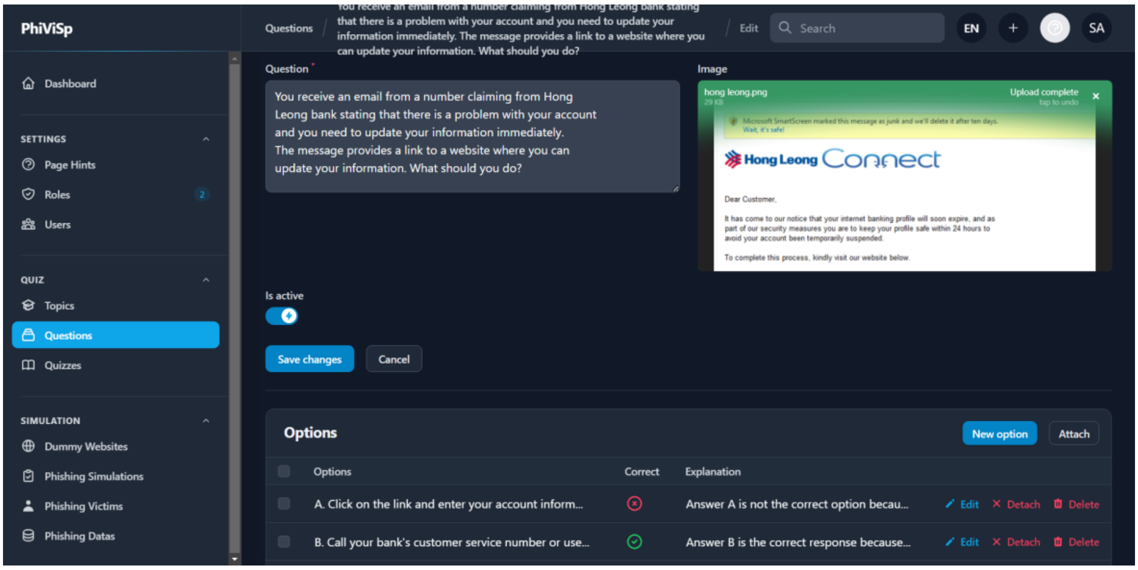
Answer A is the correct because if you received message requesting personal or sensitive information, verify the identity of the sender by calling or texting them directly. Don't rely solely on the information in the message.

Is correct

No records found

Figure 4.15 Create question options

After clicking the "Create" button, the page will redirect the admin to the question edit page. Here, the admin can add answer options and edit the question details further. For each answer option, the admin can specify whether it is the correct option or not. Additionally, the admin can explain all the options, explaining why they are right or wrong. This allows the admin to provide additional information or guidance to users when they answer the question.



PhiViSp
Dashboard
SETTINGS
Page Hints
Roles 2
Users
QUIZ
Topics
Questions
Quizzes
SIMULATION
Dummy Websites
Phishing Simulations
Phishing Victims
Phishing Datas
Questions / You receive an email from a number claiming from Hong Leong bank stating that there is a problem with your account and you need to update your information immediately. The message provides a link to a website where you can update your information. What should you do? / Edit
Search
EN
+
SA

Question *

You receive an email from a number claiming from Hong Leong bank stating that there is a problem with your account and you need to update your information immediately. The message provides a link to a website where you can update your information. What should you do?

Image

hong leong.png
29 KB
Upload complete
tap to undo

Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.
Wait, it's safe!

Hong Leong Connect

Dear Customer,

It has come to our notice that your internet banking profile will soon expire, and as part of our security measures you are to keep your profile safe within 24 hours to avoid your account been temporarily suspended.

To complete this process, kindly visit our website below.

Is active

Save changes | Cancel

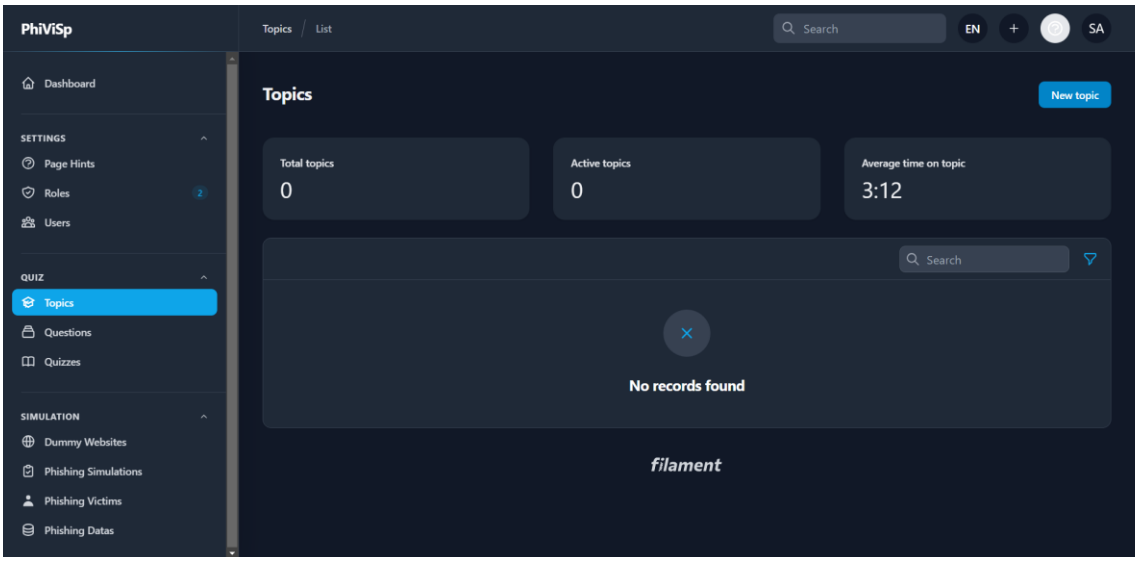
Options

New option | Attach

□	Options	Correct	Explanation			
□	A. Click on the link and enter your account inform...	⊗	Answer A is not the correct option becau...	Edit	Detach	Delete
□	B. Call your bank's customer service number or use...	✓	Answer B is the correct response because...	Edit	Detach	Delete

Figure 4.16 Attached question options

Once the admin has entered all the necessary information, they can save the question. The question will then be added to the system's database.



Total topics 0

Active topics 0

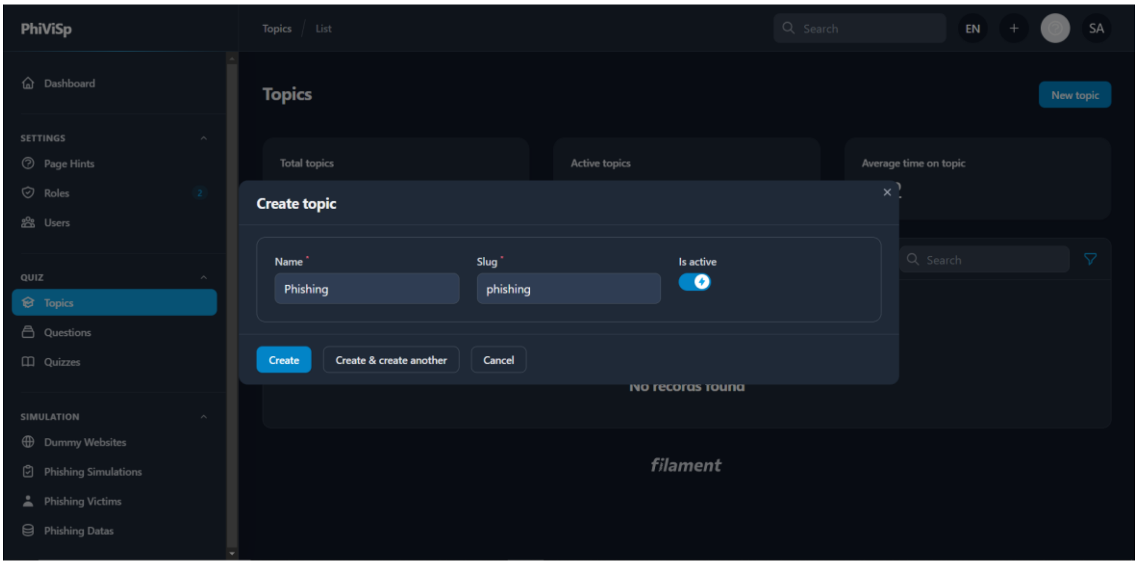
Average time on topic 3:12

No records found

Figure 4.17 List topics

Figure 4.17 shows the list topic page managed by the admin, providing essential information such as the total number of topics, active topics, and the most recent topic created. In addition, it offers a comprehensive overview of the topics within the system, allowing the admin to view and edit topic details and create new topics conveniently.

The list of topics includes key information such as the topic name, associated questions, and the status of each topic. The admin can access the details and related questions by selecting a specific topic, enabling them to review and make any necessary modifications. Additionally, the admin can create a new topic using the "New Topic" button.



Create topic

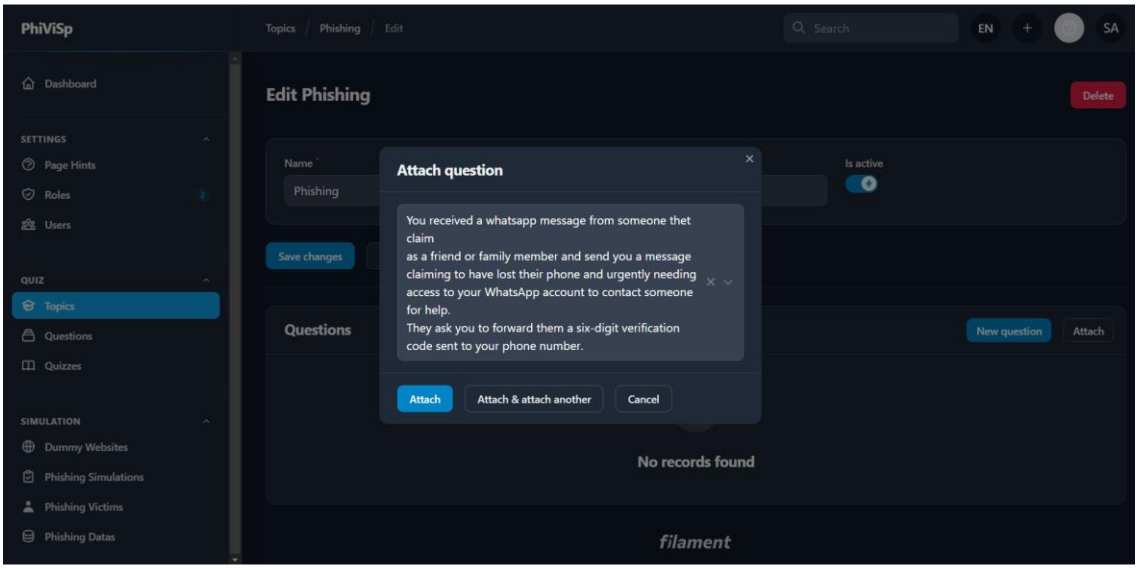
Name*: Phishing

Slug*: phishing

Is active: ●

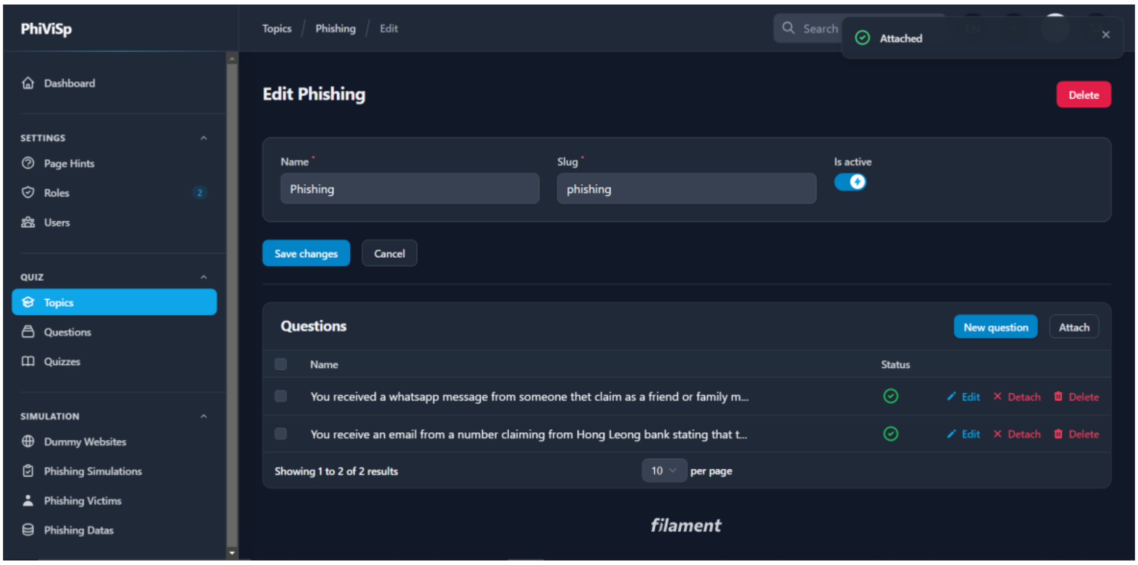
Figure 4.18 Create a new topic

The admin must provide essential information such as the topic name, slug, and activation status to create a new topic. Once the necessary details are filled in, the admin can attach the previously created questions to the respective topic by clicking the "Edit" button.



You received a whatsapp message from someone that claim
as a friend or family member and send you a message claiming to have lost their phone and urgently needing access to your WhatsApp account to contact someone for help.
They ask you to forward them a six-digit verification code sent to your phone number.

Figure 4.19 Attach questions to the topic



Name: Phishing

Slug: phishing

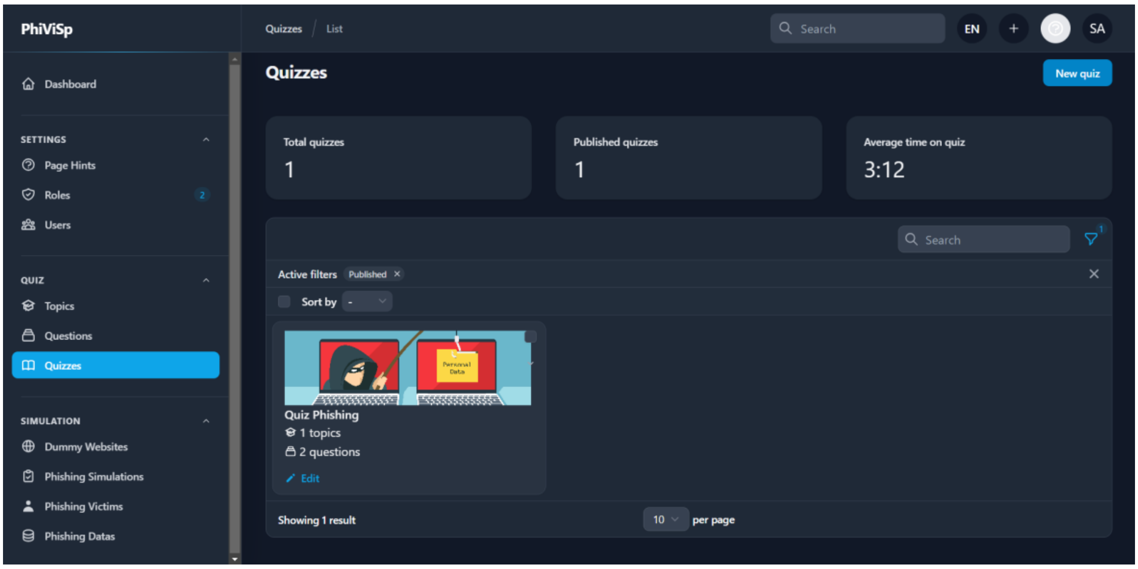
Is active

Name	Status			
You received a whatsapp message from someone thet claim as a friend or family m...	✓	Edit	Detach	Delete
You receive an email from a number claiming from Hong Leong bank stating that t...	✓	Edit	Detach	Delete

Showing 1 to 2 of 2 results 10 per page

Figure 4.20 Edit topic

The admin can associate the questions with the topic within the edit page. This allows for organising and categorising questions under specific topics, making managing and navigating the system easier. The admin also can edit, detach, or delete questions within the topic edit page. They can modify question details, remove questions from the topic, or delete questions if needed.



Quizzes

Total quizzes 1

Published quizzes 1

Average time on quiz 3:12

Active filters: Published

Sort by -

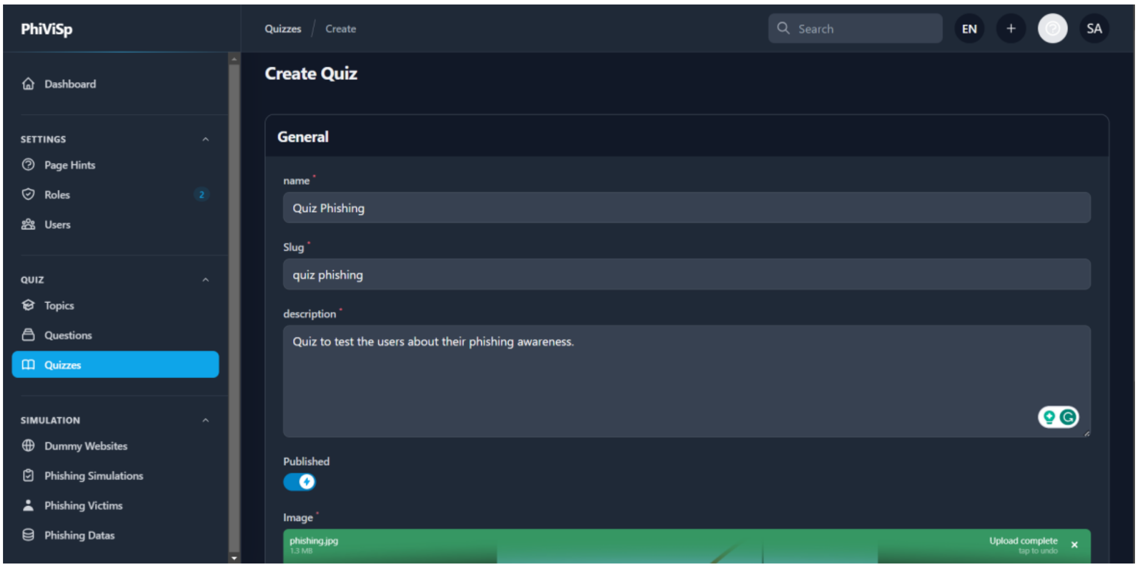
Quiz Phishing
1 topics
2 questions

Showing 1 result

10 per page

Figure 4.21 List quizzes

List quizzes page provides an overview of all the quizzes created by the admin. It shows the total number of quizzes in the system and provides additional information, such as the number of published quizzes and the average time spent on quizzes. The data presented gives the admin a quick snapshot of the quizzes' status and engagement metrics.



Create Quiz

General

name *
Quiz Phishing

Slug *
quiz phishing

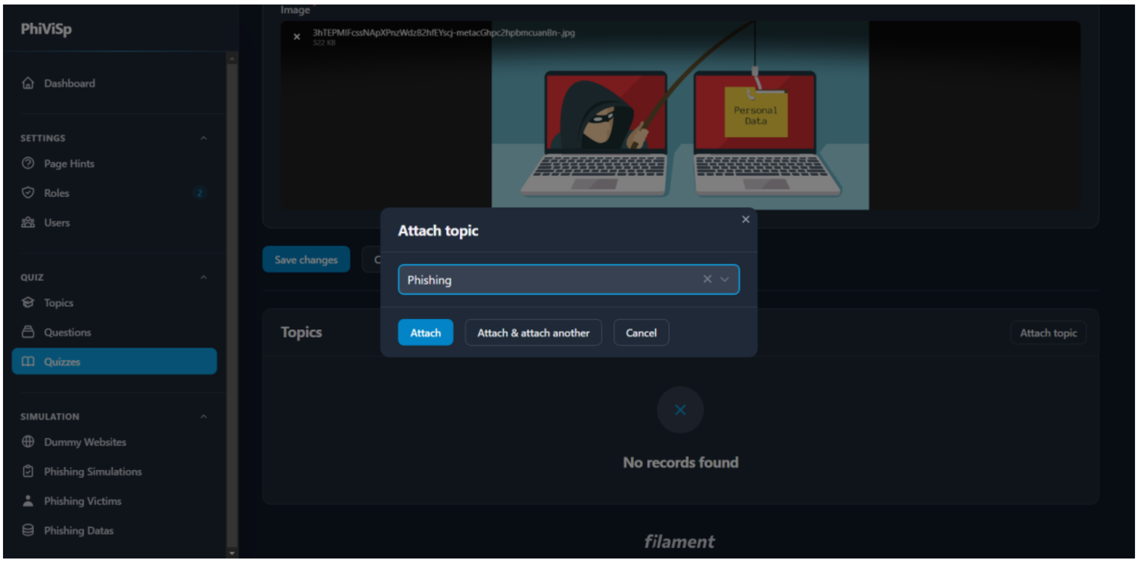
description *
Quiz to test the users about their phishing awareness.

Published
●

Image *
phishing.jpg 1.3 MB
Upload complete tap to undo ×

Figure 4.22 Create a new quiz

The admin can click the "New Quiz" button to create a new quiz. This will open a page where the admin can fill in the necessary information. The required fields include the name of the quiz, a unique slug that serves as its identifier, a description of the quiz, and an option to publish the quiz. Additionally, the admin can upload an image to accompany the quiz, making it visually appealing and easily recognisable. Finally, the admin can save the quiz once all the required information is provided.



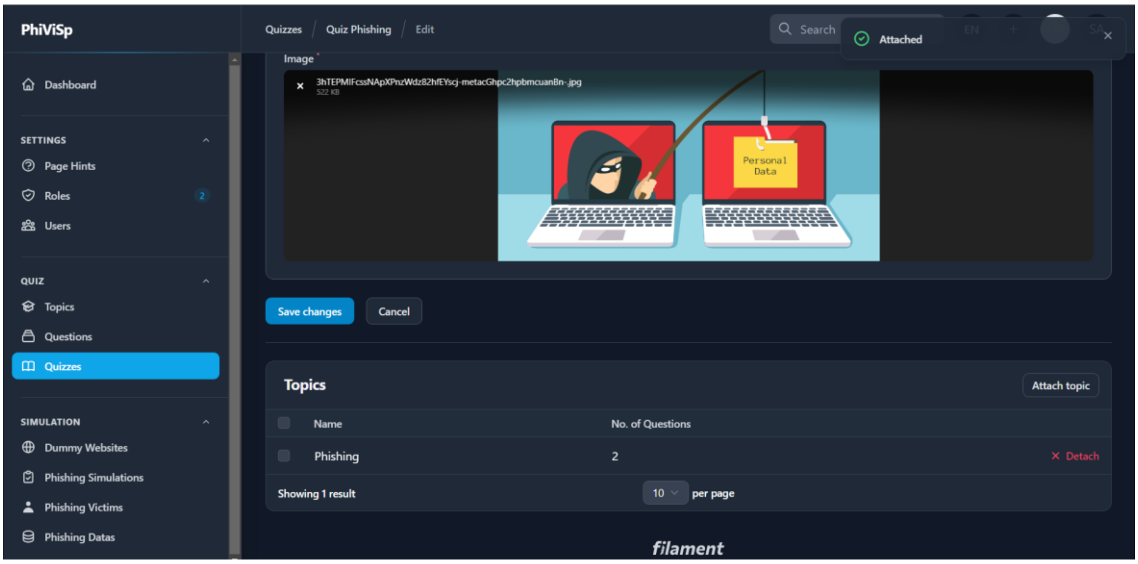
Attach topic

Phishing

No records found

Figure 4.23 Attach topics to the quiz

After creating a quiz, the admin can attach specific topics. This allows the admin to include questions from those topics in the quiz. All associated questions will be automatically added by selecting the desired topics and attaching them to the quiz.



Attached

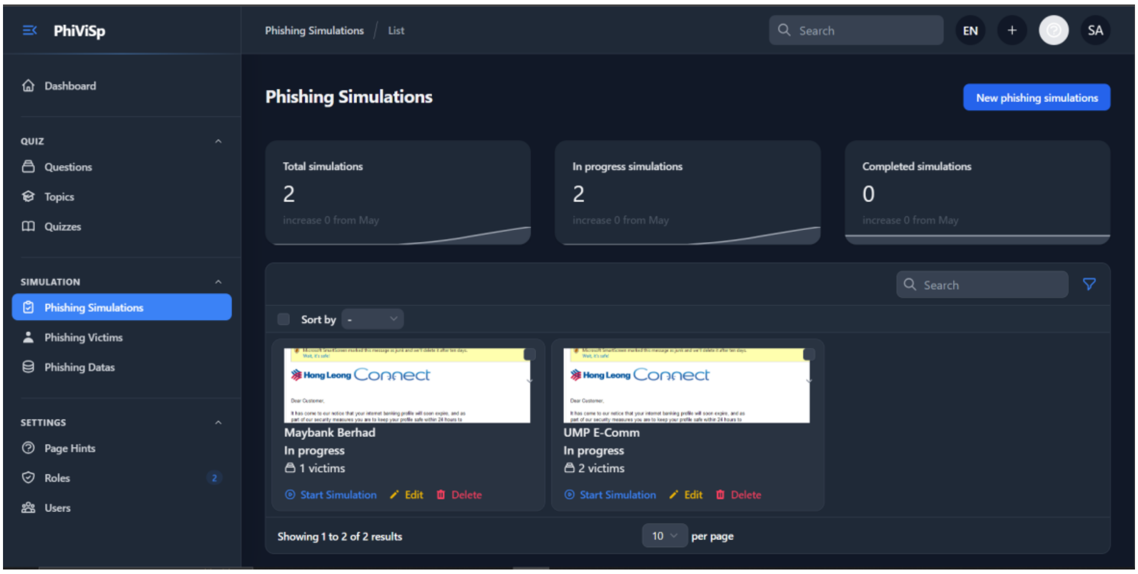
Topics

Name	No. of Questions	
Phishing	2	✕ Detach

Showing 1 result

10 per page

Figure 4.24 Edit quiz



Phishing Simulations

Total simulations
2
increase 0 from May

In progress simulations
2
increase 0 from May

Completed simulations
0
increase 0 from May

Maybank Berhad
In progress
1 victims

UMP E-Comm
In progress
2 victims

Showing 1 to 2 of 2 results

10

Figure 4.25 List phishing simulations page

The page displays a list of created phishing simulations by the admin. The main component of this page is a well-organised table or grid that presents the simulations in a structured manner. Each simulation entry provides essential details such as the image, simulation name, victims, and the simulation status. This overview enables the admin to quickly grasp the key aspects of each simulation at a glance.

The module may also present essential indicators, such as the total number of simulations, active simulations, and the most recently created simulation. These indicators provide a quick snapshot of the overall simulation landscape and help the admin stay informed about the system's current state.

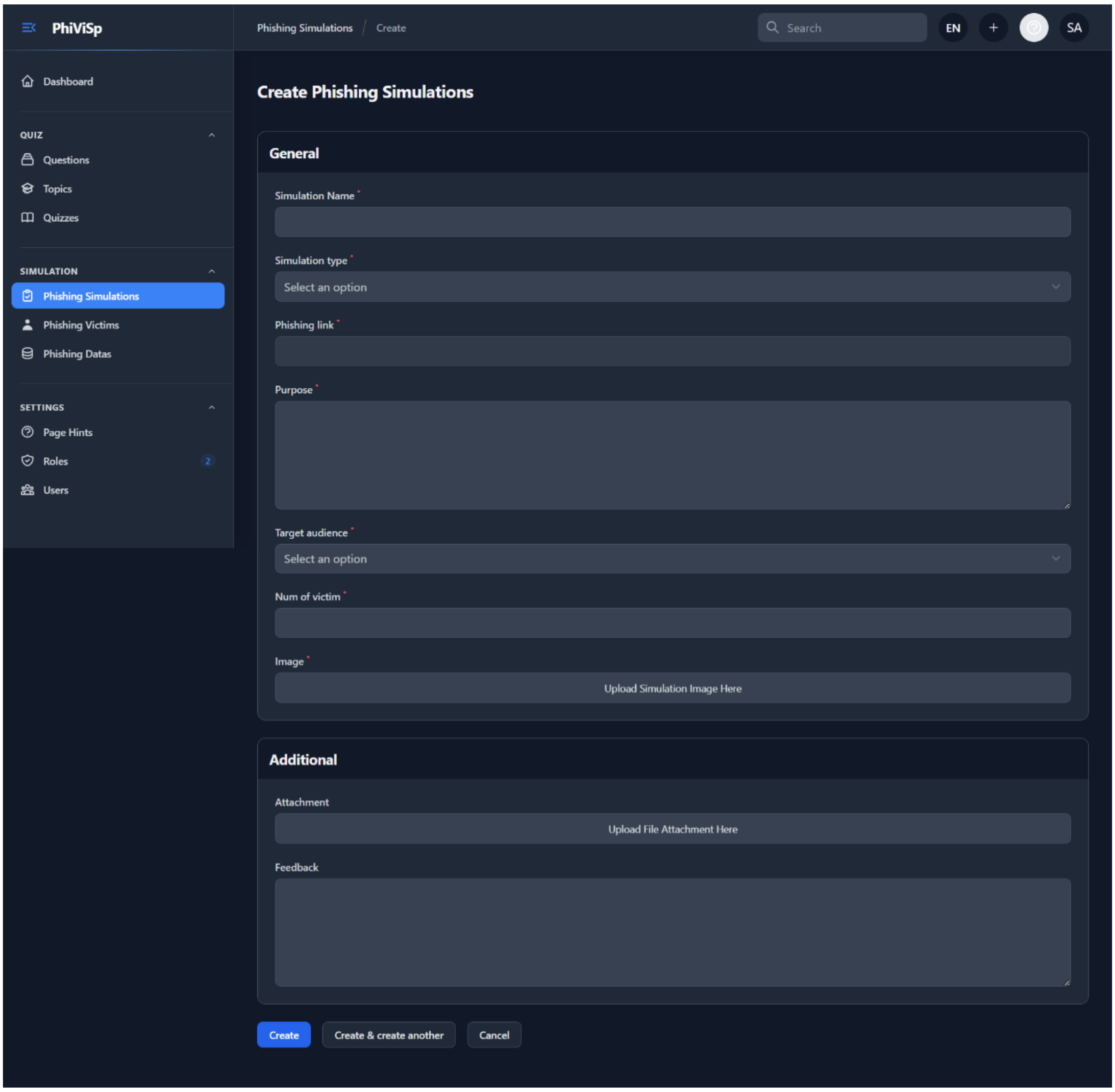
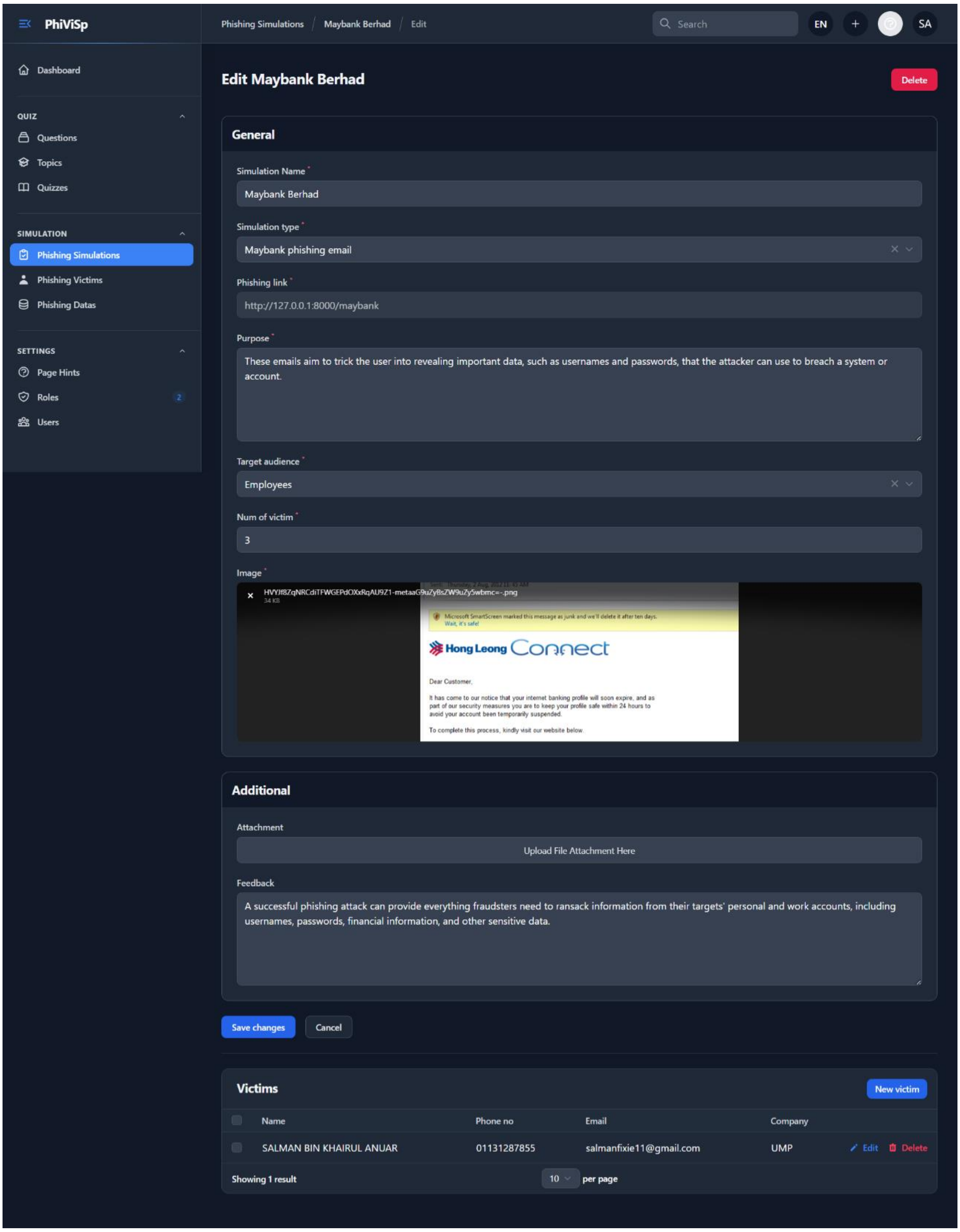


Figure 4.26 Create a phishing simulation page

The admin can create new phishing simulations in the phishing simulation management system. By clicking the "New Phishing Simulation" button at the page's top-right corner, the admin can initiate the process of creating a new simulation.

Once the button is clicked, a form will appear requesting the admin to provide the necessary information for the simulation. This information includes the simulation name, simulation type, purpose, number of victims, target audience, and other attributes.

After providing all the necessary details, the admin can review the entered information and click the "Create" button to create the new phishing simulation. The system will then process the information and generate a unique identifier or reference for the simulation.



Edit Maybank Berhad

Delete

General

Simulation Name *
Maybank Berhad

Simulation type *
Maybank phishing email

Phishing link *
http://127.0.0.1:8000/maybank

Purpose *
These emails aim to trick the user into revealing important data, such as usernames and passwords, that the attacker can use to breach a system or account.

Target audience *
Employees

Num of victim *
3

Image *
HVYJf8ZqNRCdiTFWGEPdOXxRqAU9Z1-metaaG9uZyBsZW9uZy5wbmc=-.png
34 KB

Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.
Wait, it's safe!

Hong Leong Connect

Dear Customer,

It has come to our notice that your internet banking profile will soon expire, and as part of our security measures you are to keep your profile safe within 24 hours to avoid your account been temporarily suspended.

To complete this process, kindly visit our website below.

Additional

Attachment
Upload File Attachment Here

Feedback
A successful phishing attack can provide everything fraudsters need to ransack information from their targets' personal and work accounts, including usernames, passwords, financial information, and other sensitive data.

Save changes Cancel

Victims New victim

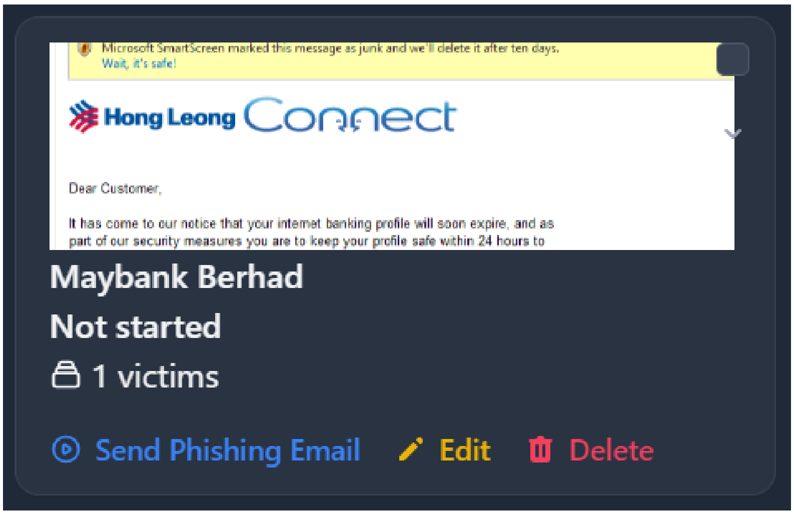
□	Name	Phone no	Email	Company	
□	SALMAN BIN KHAIRUL ANUAR	01131287855	salmanfixie11@gmail.com	UMP	Edit Delete

Showing 1 result 10 per page

Figure 4.27 Edit phishing simulation page

By clicking the edit button on the simulation from the list, the admin gains access to a detailed view or dedicated page for that simulation. This detailed view provides in-depth information about the simulation, including its name, target audience, simulation type, associated emails or messages, and other relevant settings. The admin can review the simulation's details and make any necessary modifications as per requirements.

One important functionality on the edit page is managing simulation victims. The admin can add new victims to the simulation by entering their name, email, phone number, and company details. This feature enables the admin to create a targeted list of individuals receiving the phishing email. The admin can use an input form or a dedicated section on the edit page to add a new victim. The form typically includes fields for entering the victim's name, email address, phone number, and company affiliation. The admin can fill in these details for each victim and submit the form to add them to the simulation.



Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.
Wait, it's safe!

Dear Customer,

It has come to our notice that your internet banking profile will soon expire, and as part of our security measures you are to keep your profile safe within 24 hours to

Maybank Berhad

Not started

1 victims

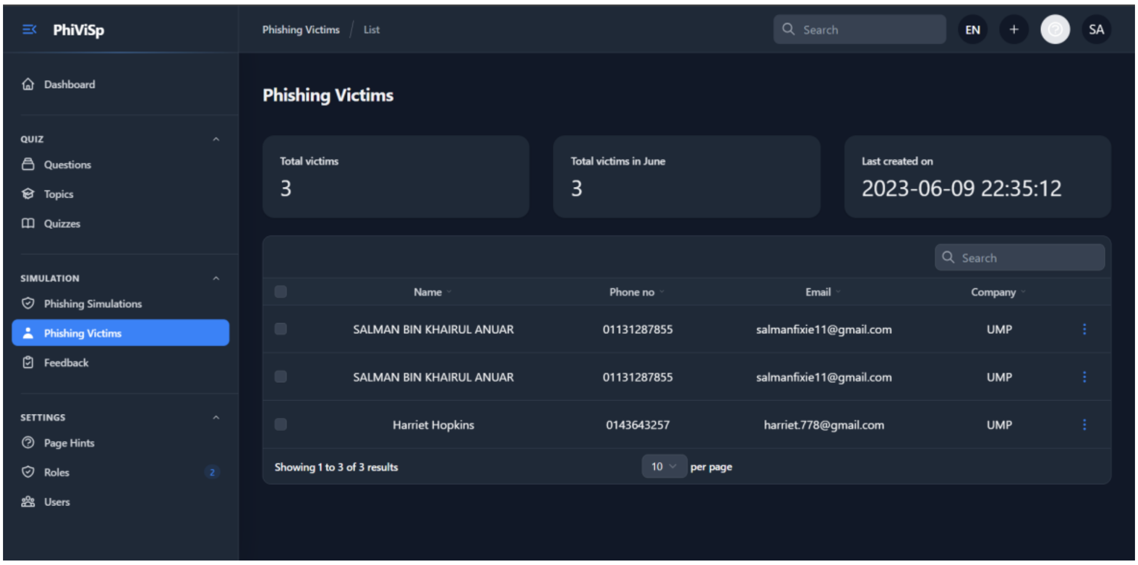
Figure 4.28 Send phishing email button

After completing the setup of the phishing simulation and adding the necessary victims, the admin has the option to start the simulation. To initiate the simulation, the admin can click the "Send Phishing Email" button, which triggers the sending of phishing emails to all the added victims associated with that particular simulation.

Then, the system will begin sending out phishing emails. Each victim's email address will be used to deliver a customised phishing email tailored to the specific simulation. The email content will reflect the chosen simulation type, template, and any other configuration settings defined during the setup phase.

It is crucial to note that phishing simulations should only be conducted for legitimate purposes within an organisation and with proper authorisation. The goal is to simulate real-world phishing scenarios to assess and enhance the security awareness of the organisation's employees or participants.

Once the simulation is initiated, the system will handle the email delivery process, ensuring that each victim receives the phishing email in their respective inboxes. The content of the email will mimic common phishing techniques, aiming to educate and train the recipients on how to identify and respond to such threats effectively.



Phishing Victims

Total victims
3

Total victims in June
3

Last created on
2023-06-09 22:35:12

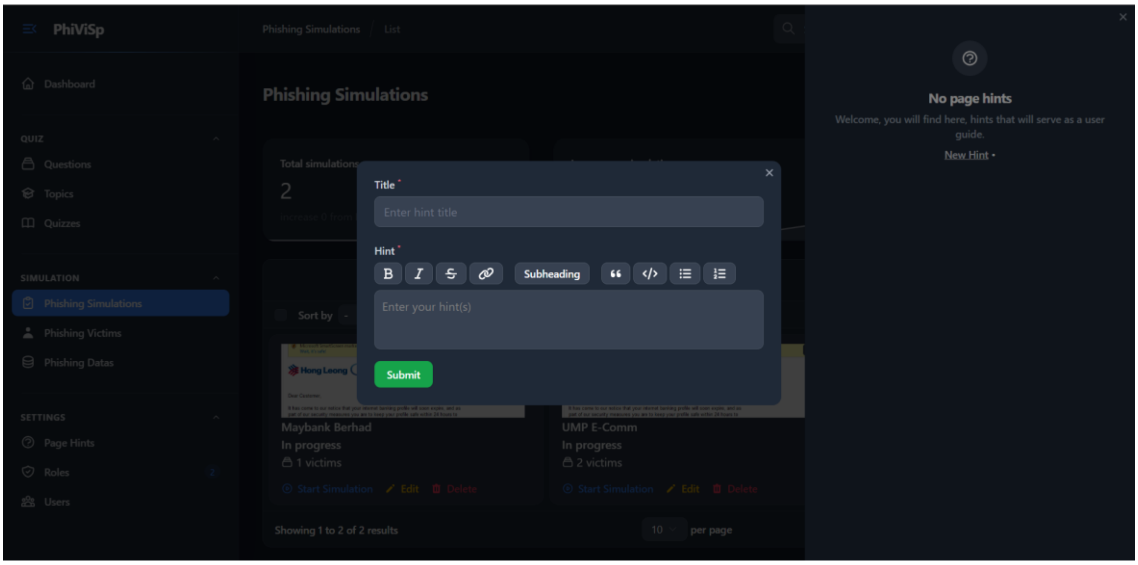
Name	Phone no	Email	Company
SALMAN BIN KHAIRUL ANUAR	01131287855	salmanfixie11@gmail.com	UMP
SALMAN BIN KHAIRUL ANUAR	01131287855	salmanfixie11@gmail.com	UMP
Harriet Hopkins	0143643257	harriet.778@gmail.com	UMP

Showing 1 to 3 of 3 results

10 per page

Figure 4.29 List phishing victim page

The phishing victim page displays a comprehensive list of all the victims created during the phishing simulation. The list includes their name, email address, phone number, company, and status. The admin can perform various actions for each victim, such as editing their details or accessing information about their interactions with the phishing email. This allows the admin to closely monitor the simulation's progress and make informed decisions based on the victims' responses.



Enter hint title

Enter your hint(s)

Maybank Berhad
In progress
1 victims

UMP E-Comm
In progress
2 victims

Showing 1 to 2 of 2 results

10 per page

No page hints

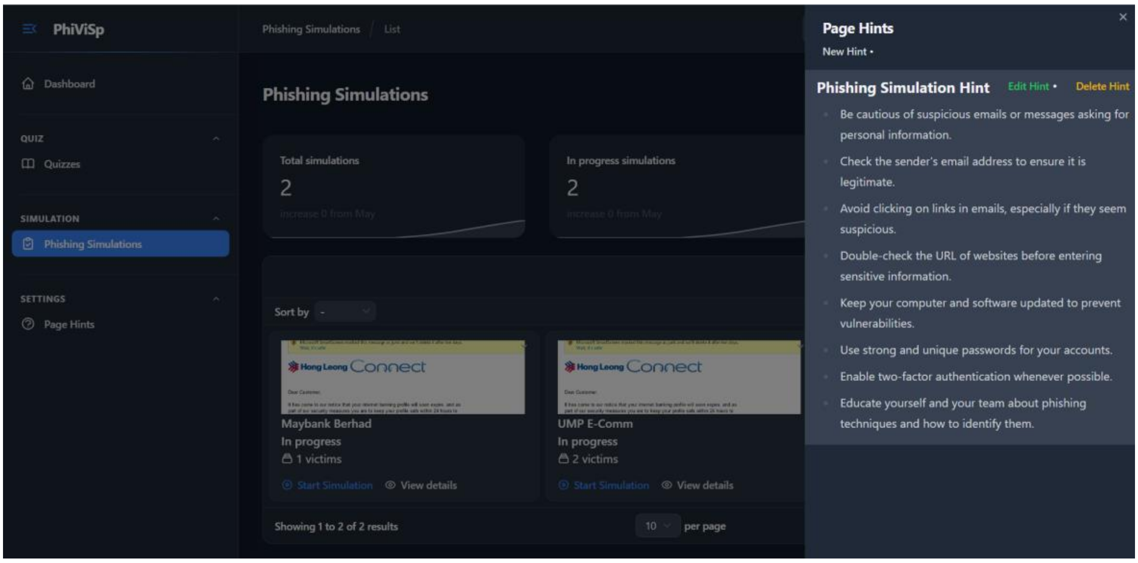
Welcome, you will find here, hints that will serve as a user guide.

Figure 4.30 Create page hint

The page hints that the admin can quickly provide valuable information and guidance to users navigating the application. Admins can enhance the user experience and provide helpful instructions by following a few simple steps.

First, the admin must navigate to the desired page where the hint should be displayed. Once on the page, they can locate the question mark icon in the top-right corner. Clicking on this icon will open a form where the admin can enter the hint's title and a detailed description or instructions in the provided fields.

After filling in the necessary information, the admin can save the hint. Now, whenever users access that particular page, they will notice a hint icon displayed prominently, often represented by a question mark or an information symbol. Users can access the relevant hint associated with the page by clicking on the hint icon.

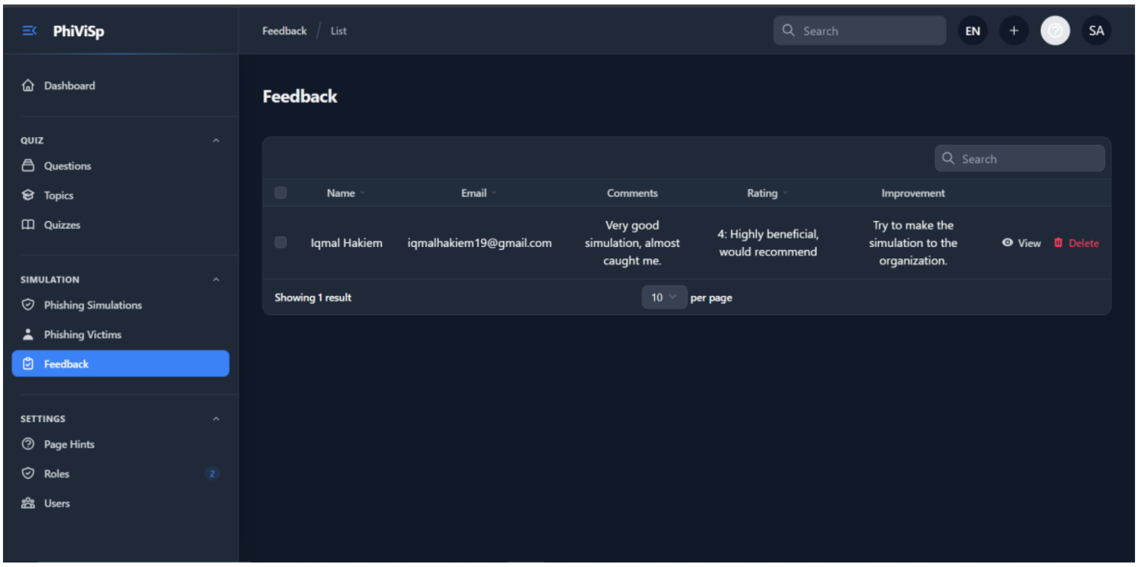


Phishing Simulation Hint

- Be cautious of suspicious emails or messages asking for personal information.
- Check the sender's email address to ensure it is legitimate.
- Avoid clicking on links in emails, especially if they seem suspicious.
- Double-check the URL of websites before entering sensitive information.
- Keep your computer and software updated to prevent vulnerabilities.
- Use strong and unique passwords for your accounts.
- Enable two-factor authentication whenever possible.
- Educate yourself and your team about phishing techniques and how to identify them.

Figure 4.31 View page hint

This feature ensures that users have access to important contextual information or instructions, improving their overall understanding and usability of the application.



□	Name	Email	Comments	Rating	Improvement	
□	Iqmal Hakiem	iqmalhakiem19@gmail.com	Very good simulation, almost caught me.	4: Highly beneficial, would recommend	Try to make the simulation to the organization.	View Delete

Showing 1 result 10 per page

Figure 4.32 List feedback page

On the feedback page, users can view a comprehensive list of feedback submitted by victims of phishing simulations. This list consists of various attributes that provide valuable insights for the administrators to improve future simulations and enhance their overall effectiveness.

One crucial attribute is the comment section, where victims can explain their experiences during the simulation. This feedback can range from describing the techniques used in the phishing attempt to sharing their emotional response and overall impression. These comments serve as a firsthand account of the victim's perspective, allowing administrators to understand the impact of the simulation on individuals and identify potential areas of improvement.

Additionally, victims are encouraged to provide suggestions for improvement. This attribute allows victims to share their insights and offer constructive feedback on how administrators can enhance the simulation for future participants. These suggestions can cover various aspects, such as the content of the phishing emails, the frequency of simulations, the difficulty level, or the clarity of instructions. By considering these suggestions, administrators can fine-tune their approach and continually refine their phishing simulation program.

4.2.2 Database

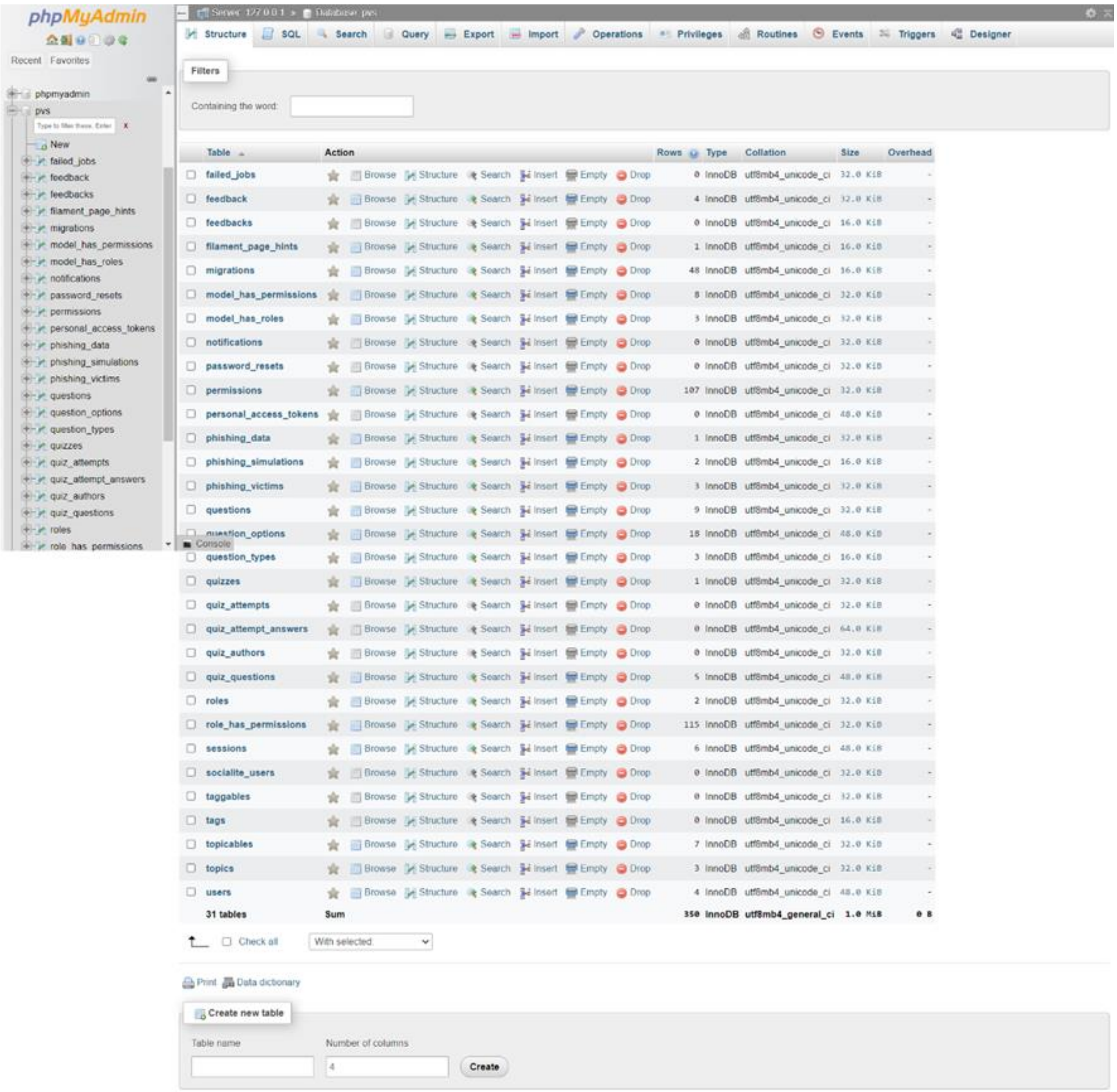
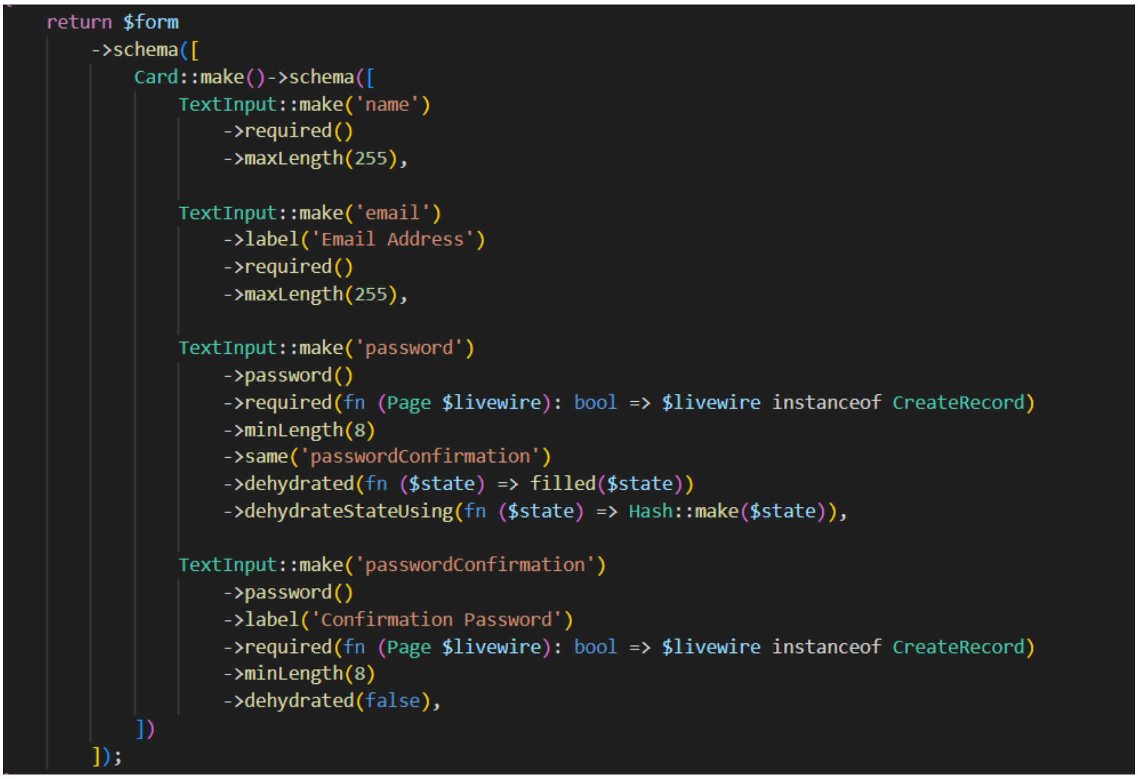


Table	Action	Rows	Type	Collation	Size	Overhead
failed_jobs	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
feedback	Browse Structure Search Insert Empty Drop	4	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
feedbacks	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
filament_page_hints	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
migrations	Browse Structure Search Insert Empty Drop	48	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
model_has_permissions	Browse Structure Search Insert Empty Drop	8	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
model_has_roles	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
notifications	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
password_resets	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
permissions	Browse Structure Search Insert Empty Drop	107	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
personal_access_tokens	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
phishing_data	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
phishing_simulations	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
phishing_victims	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
questions	Browse Structure Search Insert Empty Drop	9	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
question_options	Browse Structure Search Insert Empty Drop	18	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
question_types	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
quizzes	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
quiz_attempts	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
quiz_attempt_answers	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	64.0 KiB	-
quiz_authors	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
quiz_questions	Browse Structure Search Insert Empty Drop	5	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
roles	Browse Structure Search Insert Empty Drop	2	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
role_has_permissions	Browse Structure Search Insert Empty Drop	115	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
sessions	Browse Structure Search Insert Empty Drop	6	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
socialite_users	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
taggables	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
tags	Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_unicode_ci	16.0 KiB	-
topicables	Browse Structure Search Insert Empty Drop	7	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
topics	Browse Structure Search Insert Empty Drop	3	InnoDB	utf8mb4_unicode_ci	32.0 KiB	-
users	Browse Structure Search Insert Empty Drop	4	InnoDB	utf8mb4_unicode_ci	48.0 KiB	-
31 tables	Sum	350	InnoDB	utf8mb4_general_ci	1.0 MiB	0 B

Figure 4.33 Tables in the PhiViSp database

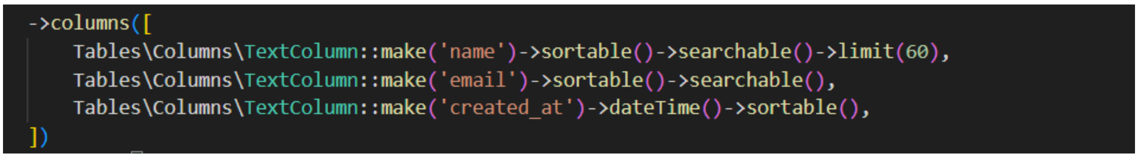
The PhiViSp system utilizes a comprehensive database, as illustrated in Figure 4.33. This diagram represents the various data sources and structures employed within the system to store and manage information related to uses, quiz management and phishing simulations, feedback records, and other relevant details. The database acts as a centralized repository, ensuring efficient data storage and retrieval for the seamless functioning of the PhiViSp system. It allows administrators and users to access and manipulate the necessary information related to the modules offered by this system. By leveraging this database, the system can maintain accurate and up-to-date records, facilitate data analysis, and support decision-making processes about the module's activities within the PhiViSp.

4.2.3 Code



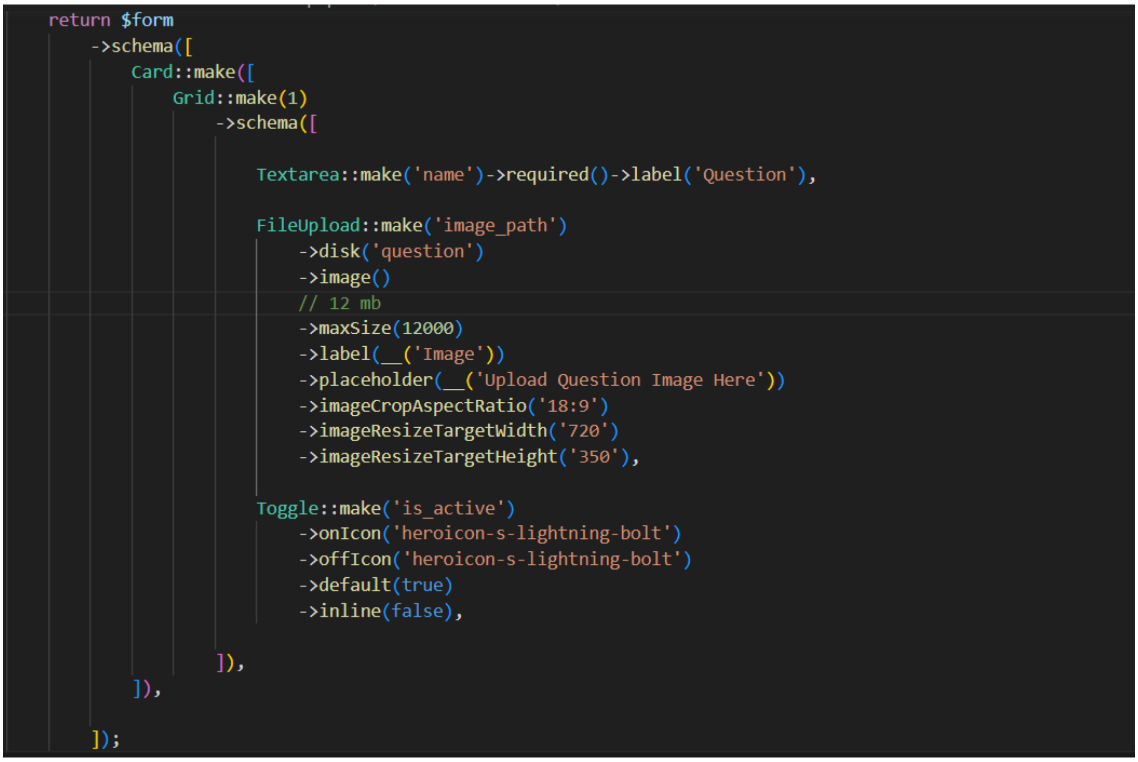
```
return $form
    ->schema([
        Card::make()->schema([
            TextInput::make('name')
                ->required()
                ->maxLength(255),

            TextInput::make('email')
                ->label('Email Address')
                ->required()
                ->maxLength(255),

            TextInput::make('password')
                ->password()
                ->required(fn (Page $livewire): bool => $livewire instanceof CreateRecord)
                ->minLength(8)
                ->same('passwordConfirmation')
                ->dehydrated(fn ($state) => filled($state))
                ->dehydrateStateUsing(fn ($state) => Hash::make($state)),

            TextInput::make('passwordConfirmation')
                ->password()
                ->label('Confirmation Password')
                ->required(fn (Page $livewire): bool => $livewire instanceof CreateRecord)
                ->minLength(8)
                ->dehydrated(false),
        ])
    ]);
```

Figure 4.34 Return form code for User Resource



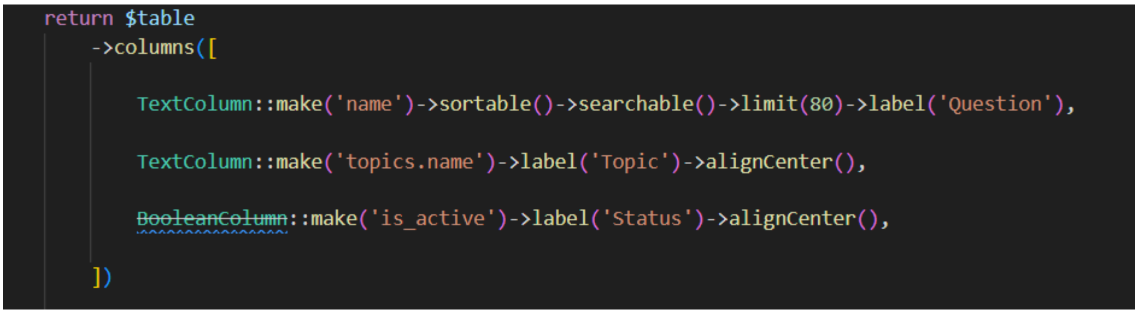
```
->columns([
    Tables\Columns\TextColumn::make('name')->sortable()->searchable()->limit(60),
    Tables\Columns\TextColumn::make('email')->sortable()->searchable(),
    Tables\Columns\TextColumn::make('created_at')->dateTime()->sortable(),
])
```

Figure 4.35 Return table code for User Resource



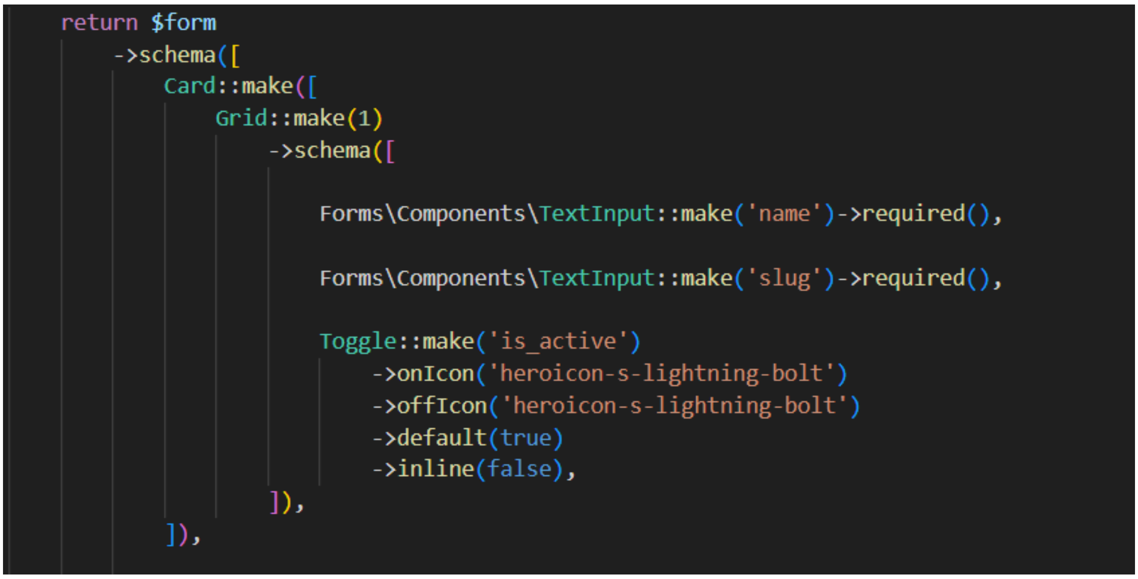
```
return $form
    ->schema([
        Card::make([
            Grid::make(1)
                ->schema([

                    Textarea::make('name')->required()->label('Question'),

                    FileUpload::make('image_path')
                        ->disk('question')
                        ->image()
                        // 12 mb
                        ->maxSize(12000)
                        ->label(__('Image'))
                        ->placeholder(__('Upload Question Image Here'))
                        ->imageCropAspectRatio('18:9')
                        ->imageResizeTargetWidth('720')
                        ->imageResizeTargetHeight('350'),

                    Toggle::make('is_active')
                        ->onIcon('heroicon-s-lightning-bolt')
                        ->offIcon('heroicon-s-lightning-bolt')
                        ->default(true)
                        ->inline(false),

                ]),
        ]),

    ]);
```

Figure 4.36 Return form code for Question Resource



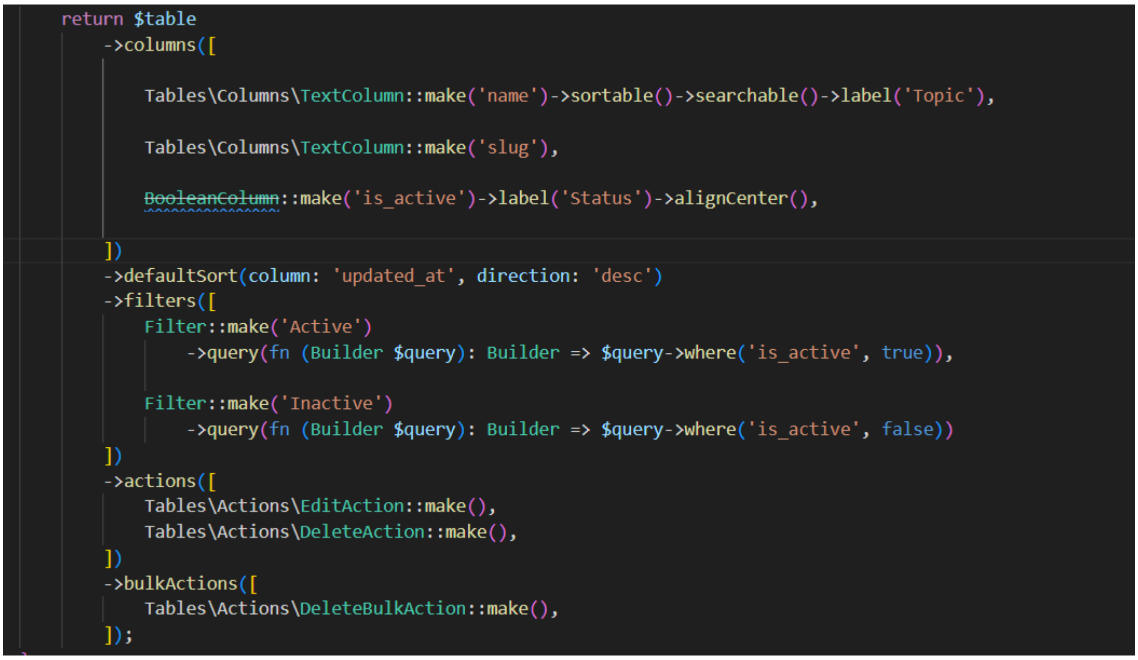
```
return $table
    ->columns([

        TextColumn::make('name')->sortable()->searchable()->limit(80)->label('Question'),

        TextColumn::make('topics.name')->label('Topic')->alignCenter(),

        ~~BooleanColumn~~::make('is_active')->label('Status')->alignCenter(),

    ])
```

Figure 4.37 Return table code for Question Resource



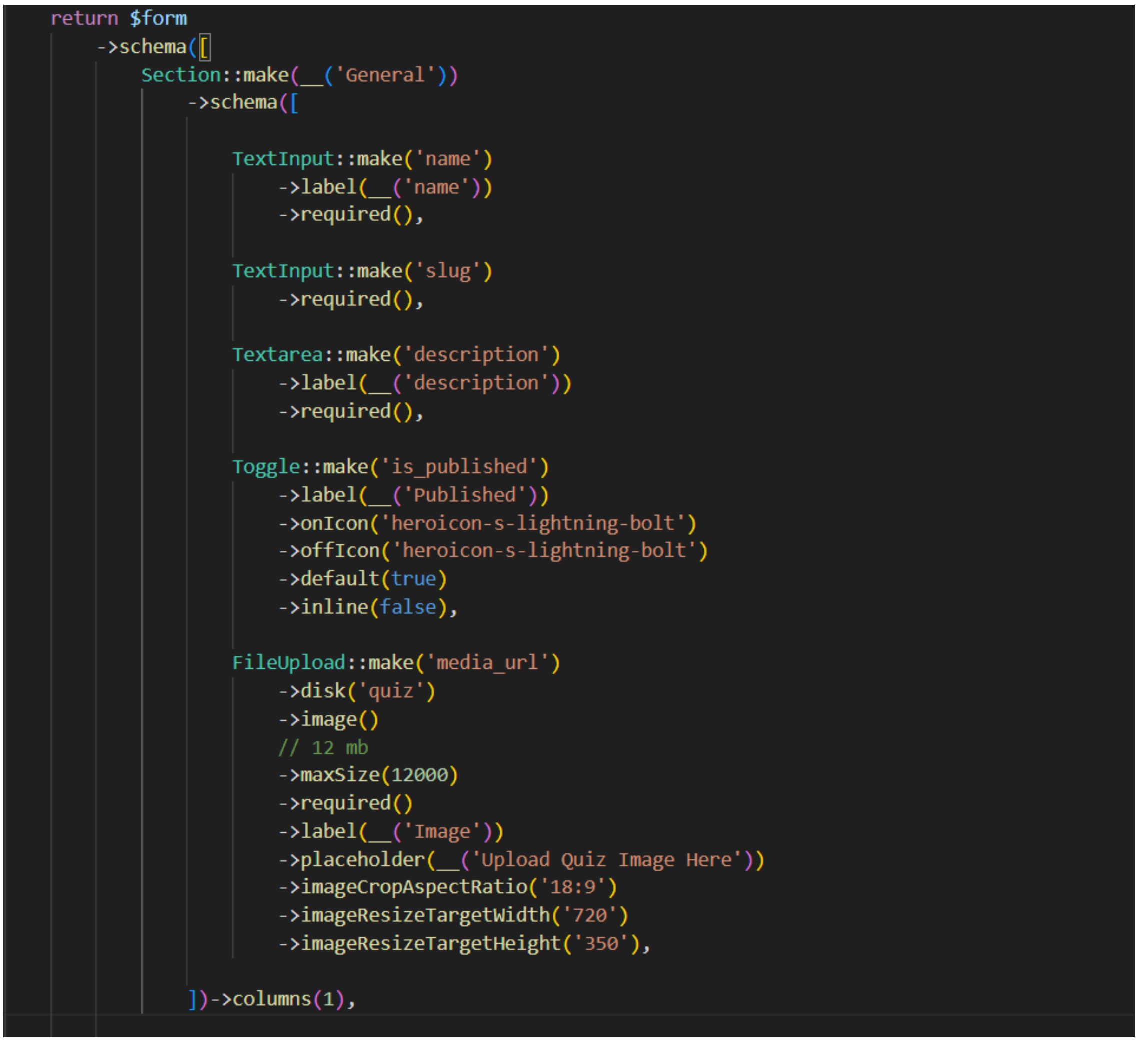
```
return $form
    ->schema([
        Card::make([
            Grid::make(1)
                ->schema([

                    Forms\Components\TextInput::make('name')->required(),

                    Forms\Components\TextInput::make('slug')->required(),

                    Toggle::make('is_active')
                        ->onIcon('heroicon-s-lightning-bolt')
                        ->offIcon('heroicon-s-lightning-bolt')
                        ->default(true)
                        ->inline(false),
                ]),
        ]),
```

Figure 4.38 Return form code for Topic Resource



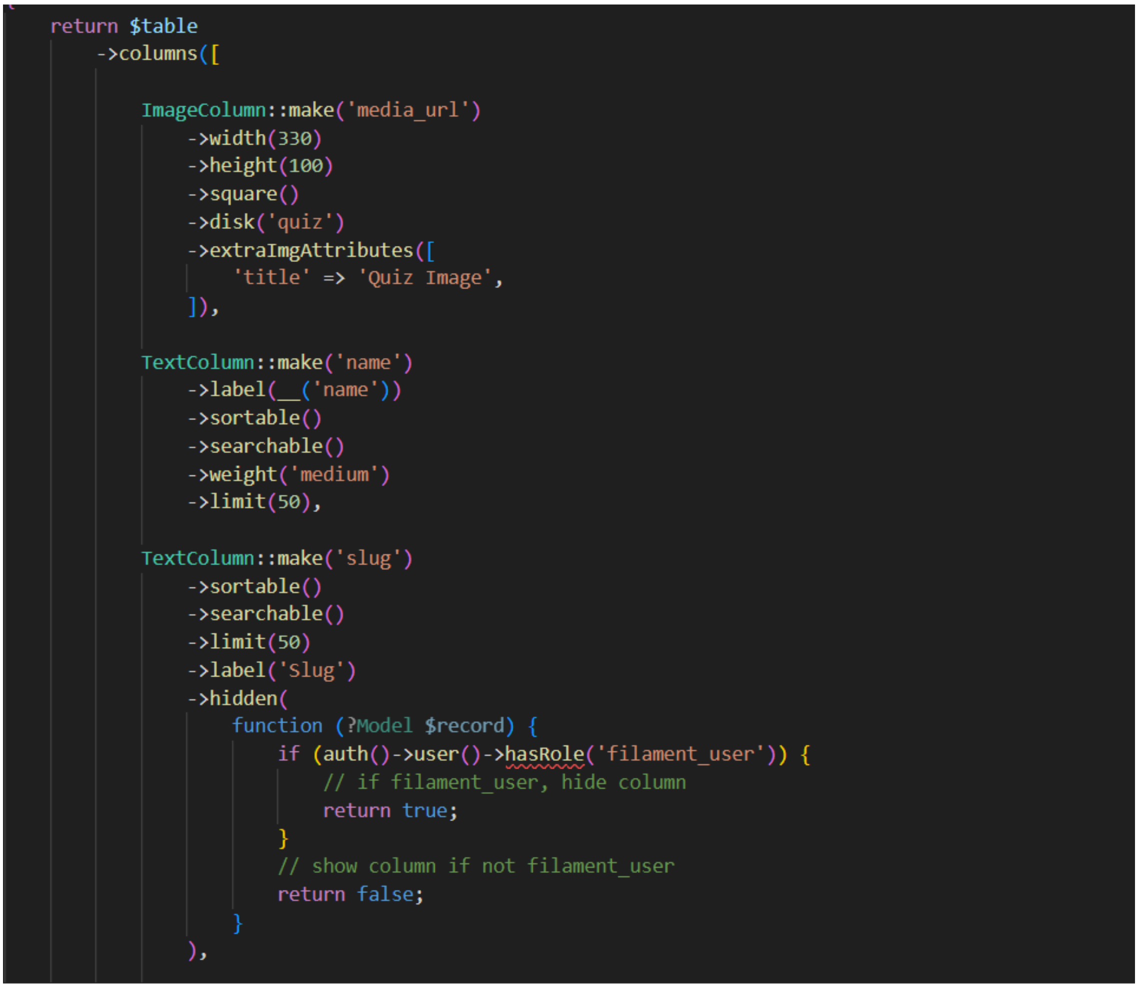
```
return $table
    ->columns([

        Tables\Columns\TextColumn::make('name')->sortable()->searchable()->label('Topic'),

        Tables\Columns\TextColumn::make('slug'),

        BooleanColumn::make('is_active')->label('Status')->alignCenter(),

    ])
    ->defaultSort(column: 'updated_at', direction: 'desc')
    ->filters([
        Filter::make('Active')
            ->query(fn (Builder $query): Builder => $query->where('is_active', true)),

        Filter::make('Inactive')
            ->query(fn (Builder $query): Builder => $query->where('is_active', false))
    ])
    ->actions([
        Tables\Actions\EditAction::make(),
        Tables\Actions\DeleteAction::make(),
    ])
    ->bulkActions([
        Tables\Actions\DeleteBulkAction::make(),
    ]);
```

Figure 4.39 Return table code for Topic Resource



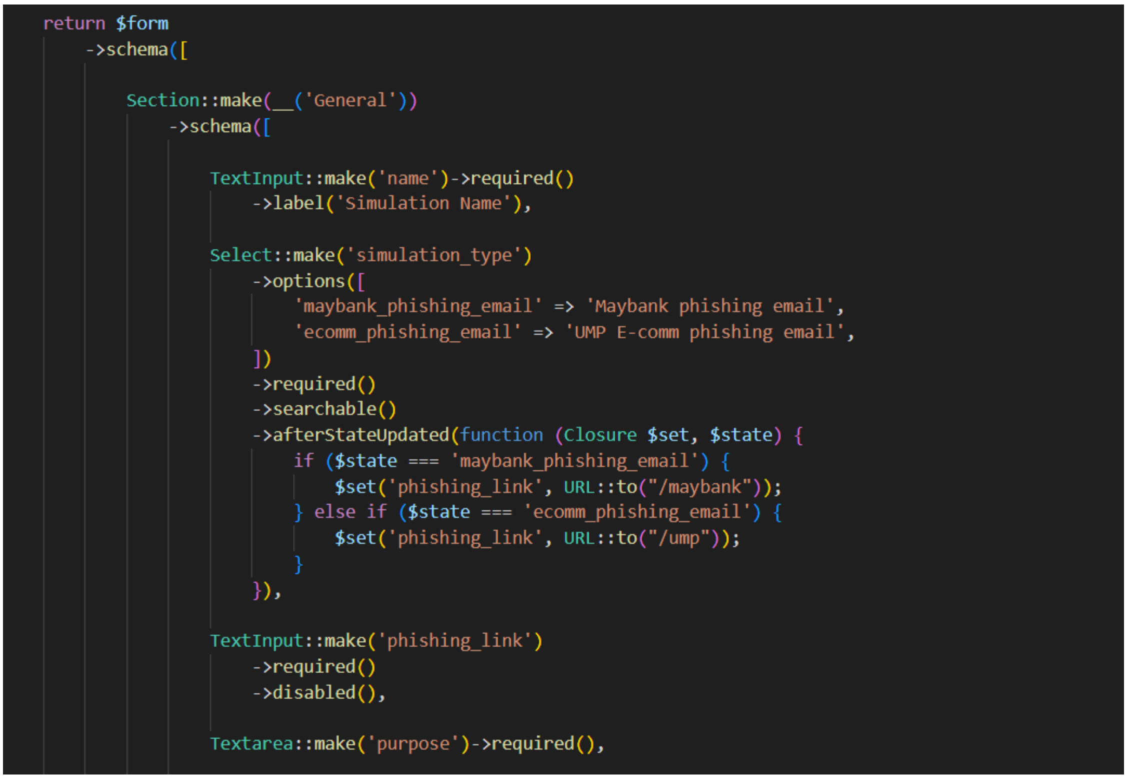
```
return $form
    ->schema([
        Section::make(__('General'))
            ->schema([

                TextInput::make('name')
                    ->label(__('name'))
                    ->required(),

                TextInput::make('slug')
                    ->required(),

                Textarea::make('description')
                    ->label(__('description'))
                    ->required(),

                Toggle::make('is_published')
                    ->label(__('Published'))
                    ->onIcon('heroicon-s-lightning-bolt')
                    ->offIcon('heroicon-s-lightning-bolt')
                    ->default(true)
                    ->inline(false),

                FileUpload::make('media_url')
                    ->disk('quiz')
                    ->image()
                    // 12 mb
                    ->maxSize(12000)
                    ->required()
                    ->label(__('Image'))
                    ->placeholder(__('Upload Quiz Image Here'))
                    ->imageCropAspectRatio('18:9')
                    ->imageResizeTargetWidth('720')
                    ->imageResizeTargetHeight('350'),

            ])->columns(1),
```

Figure 4.40 Return form code for Quiz Resource



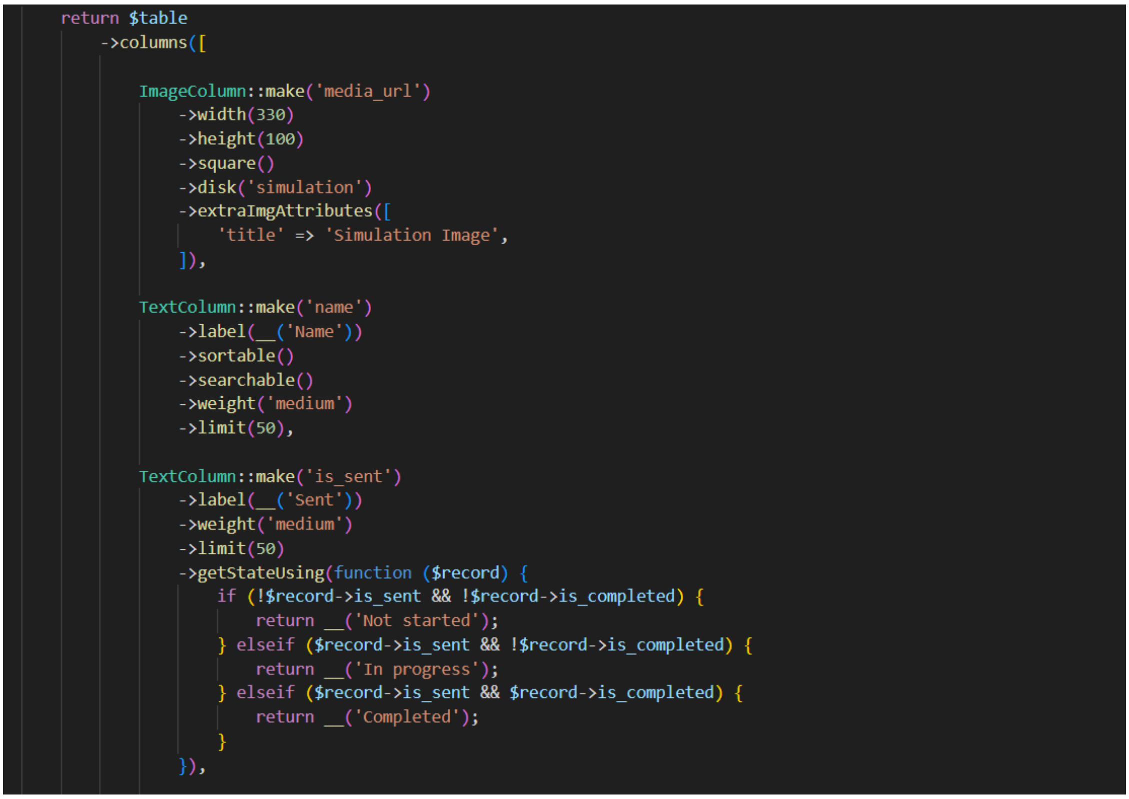
```
return $table
    ->columns([

        ImageColumn::make('media_url')
            ->width(330)
            ->height(100)
            ->square()
            ->disk('quiz')
            ->extraImgAttributes([
                'title' => 'Quiz Image',
            ]),

        TextColumn::make('name')
            ->label(__('name'))
            ->sortable()
            ->searchable()
            ->weight('medium')
            ->limit(50),

        TextColumn::make('slug')
            ->sortable()
            ->searchable()
            ->limit(50)
            ->label('Slug')
            ->hidden(
                function (?Model $record) {
                    if (auth()->user()->hasRole('filament_user')) {
                        // if filament_user, hide column
                        return true;
                    }
                    // show column if not filament_user
                    return false;
                }
            ),
```

Figure 4.41 Return table code for Quiz Resource



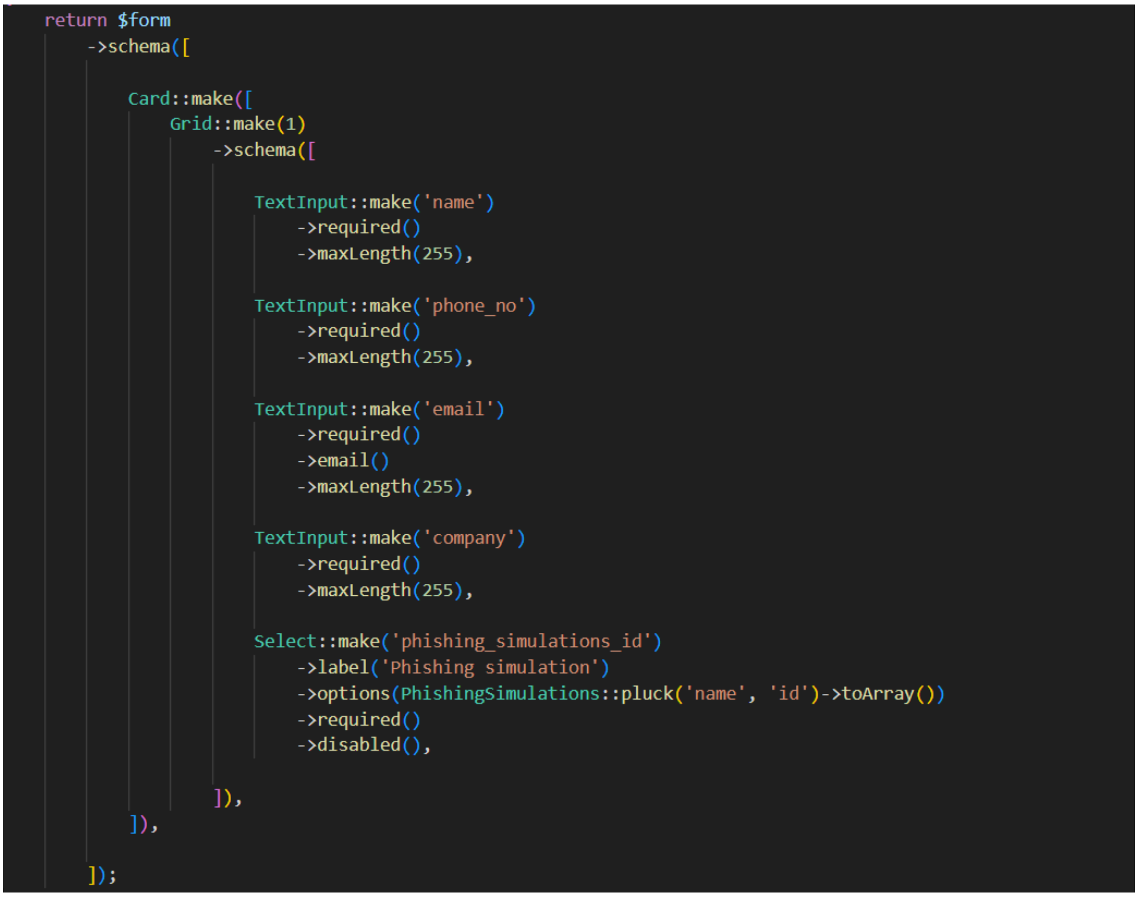
```
return $form
    ->schema([

        Section::make(__('General'))
            ->schema([

                TextInput::make('name')->required()
                    ->label('Simulation Name'),

                Select::make('simulation_type')
                    ->options([
                        'maybank_phishing_email' => 'Maybank phishing email',
                        'ecomm_phishing_email' => 'UMP E-comm phishing email',
                    ])
                    ->required()
                    ->searchable()
                    ->afterStateUpdated(function (Closure $set, $state) {
                        if ($state === 'maybank_phishing_email') {
                            $set('phishing_link', URL::to("/maybank"));
                        } else if ($state === 'ecomm_phishing_email') {
                            $set('phishing_link', URL::to("/ump"));
                        }
                    }),

                TextInput::make('phishing_link')
                    ->required()
                    ->disabled(),

                Textarea::make('purpose')->required(),
```

Figure 4.42 Return form code for Phishing Simulation Resource



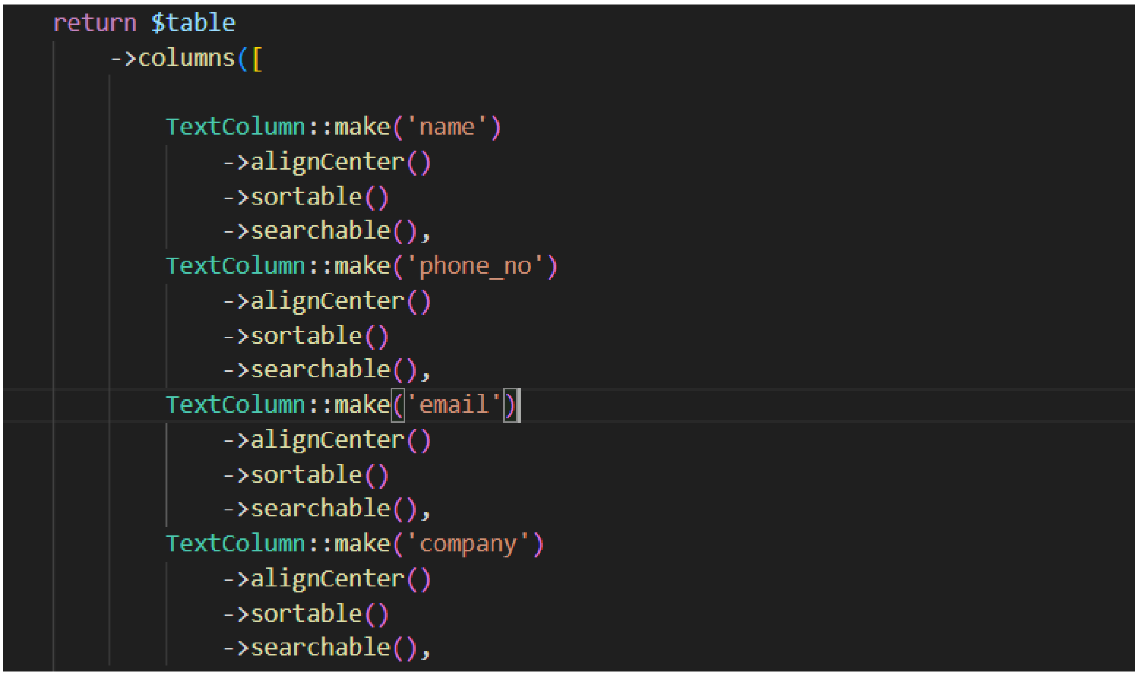
```
return $table
    ->columns([

        ImageColumn::make('media_url')
            ->width(330)
            ->height(100)
            ->square()
            ->disk('simulation')
            ->extraImgAttributes([
                'title' => 'Simulation Image',
            ]),

        TextColumn::make('name')
            ->label(__('Name'))
            ->sortable()
            ->searchable()
            ->weight('medium')
            ->limit(50),

        TextColumn::make('is_sent')
            ->label(__('Sent'))
            ->weight('medium')
            ->limit(50)
            ->getStateUsing(function ($record) {
                if (!$record->is_sent && !$record->is_completed) {
                    return __('Not started');
                } elseif ($record->is_sent && !$record->is_completed) {
                    return __('In progress');
                } elseif ($record->is_sent && $record->is_completed) {
                    return __('Completed');
                }
            }),
```

Figure 4.43 Return table code for Phishing Simulation Resource



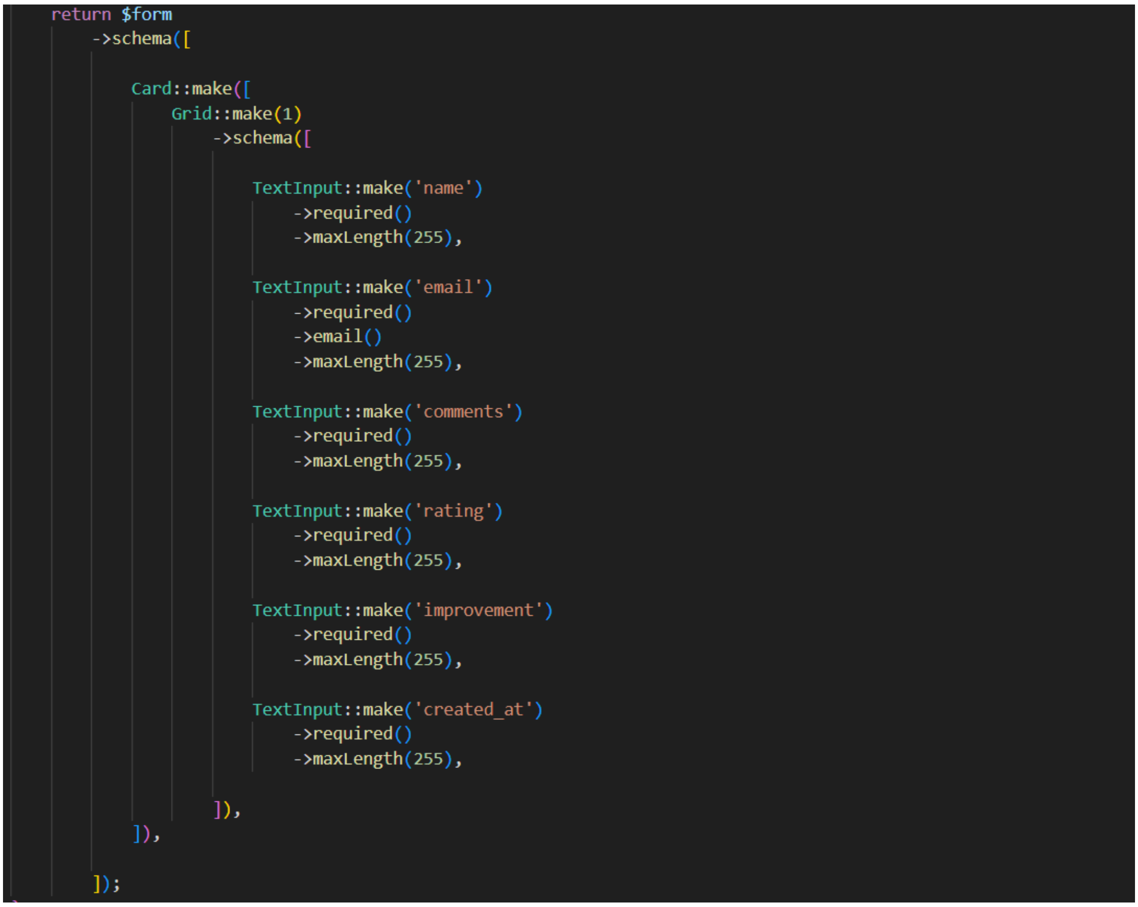
```
return $form
    ->schema([

        Card::make([
            Grid::make(1)
                ->schema([

                    TextInput::make('name')
                        ->required()
                        ->maxLength(255),

                    TextInput::make('phone_no')
                        ->required()
                        ->maxLength(255),

                    TextInput::make('email')
                        ->required()
                        ->email()
                        ->maxLength(255),

                    TextInput::make('company')
                        ->required()
                        ->maxLength(255),

                    Select::make('phishing_simulations_id')
                        ->label('Phishing simulation')
                        ->options(PhishingSimulations::pluck('name', 'id')->toArray())
                        ->required()
                        ->disabled(),

                ]),
        ]),

    ]);
```

Figure 4.44 Return form code for Phishing Victims Resource



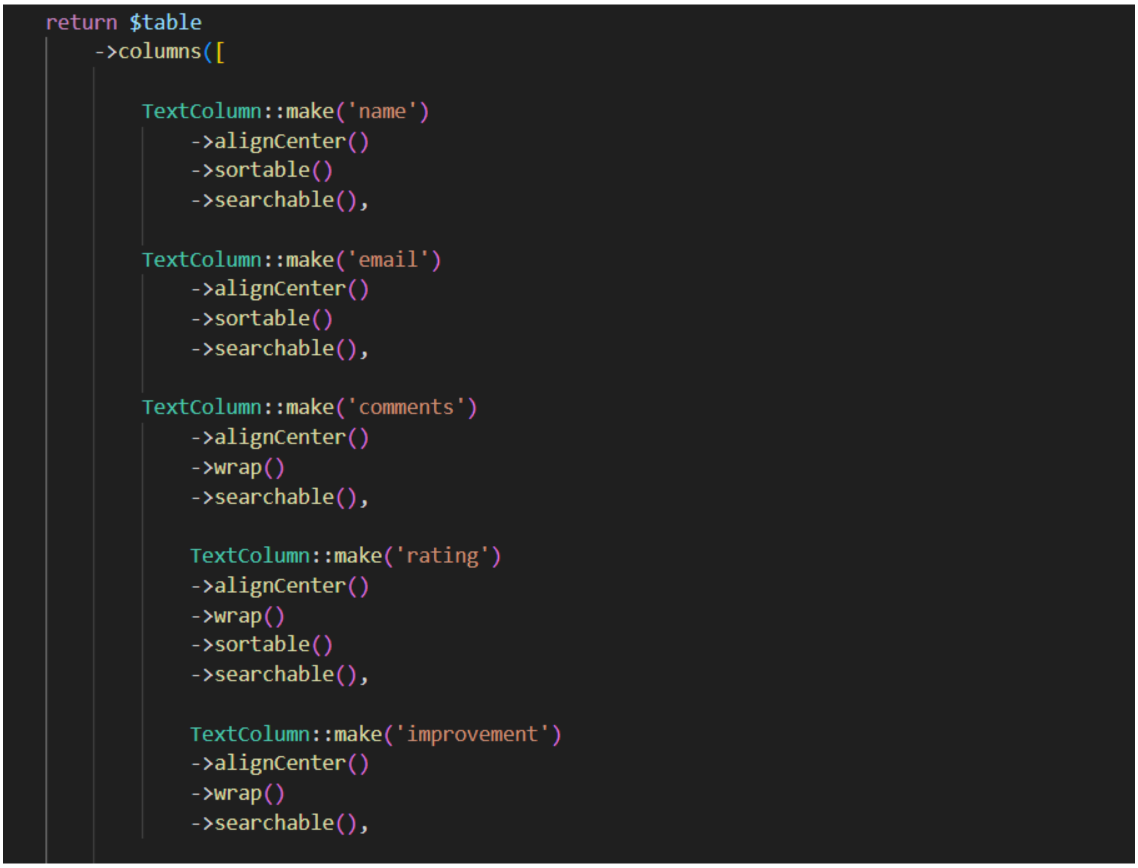
```
return $table
    ->columns([

        TextColumn::make('name')
            ->alignCenter()
            ->sortable()
            ->searchable(),
        TextColumn::make('phone_no')
            ->alignCenter()
            ->sortable()
            ->searchable(),
        TextColumn::make('email')
            ->alignCenter()
            ->sortable()
            ->searchable(),
        TextColumn::make('company')
            ->alignCenter()
            ->sortable()
            ->searchable(),
```

Figure 4.45 Return table code for Phishing Victims Resource



```
return $form
    ->schema([

        Card::make([
            Grid::make(1)
                ->schema([

                    TextInput::make('name')
                        ->required()
                        ->maxLength(255),

                    TextInput::make('email')
                        ->required()
                        ->email()
                        ->maxLength(255),

                    TextInput::make('comments')
                        ->required()
                        ->maxLength(255),

                    TextInput::make('rating')
                        ->required()
                        ->maxLength(255),

                    TextInput::make('improvement')
                        ->required()
                        ->maxLength(255),

                    TextInput::make('created_at')
                        ->required()
                        ->maxLength(255),

                ]),
        ]),

    ]);
```

Figure 4.46 Return form code for Feedback Resource



```
return $table
    ->columns([

        TextColumn::make('name')
            ->alignCenter()
            ->sortable()
            ->searchable(),

        TextColumn::make('email')
            ->alignCenter()
            ->sortable()
            ->searchable(),

        TextColumn::make('comments')
            ->alignCenter()
            ->wrap()
            ->searchable(),

            TextColumn::make('rating')
            ->alignCenter()
            ->wrap()
            ->sortable()
            ->searchable(),

            TextColumn::make('improvement')
            ->alignCenter()
            ->wrap()
            ->searchable(),
```

Figure 4.47 Return table code for Feedback Resource

4.3 Testing and Result Discussion

After the PhiViSp system is developed, a testing process is conducted to evaluate its functionality and usability. First, user Acceptance Testing (UAT) involves users from the target user group. UAT allows users to assess the available features in the system and identify any bugs or errors that need to be addressed.

The UAT plays a vital role in the project development process, as it allows for the identification of any issues or discrepancies that may have been overlooked during development. It ensures that the system meets the needs and expectations of its intended users before it is deployed. However, in addition to UAT, conducting a usability test is equally important to assess the ease of use and user satisfaction of the PhiViSp system.

In terms of usability, a Google Form is created to assess the usability of the PhiViSp system. In addition, the questionnaire collects user feedback regarding their satisfaction and experience when using the web-based system. This feedback helps identify improvement areas and enhance the overall user experience.

CHAPTER 5

CONCLUSION

5.1 Introduction

Chapter 5 provides an overview of the development process of the Phivisp System, and the system is developed using technologies such as the Laravel Framework, Figma, and Visual Studio Code, ensuring scalability, user-friendliness, and effectiveness in achieving the objectives identified in Chapter 1.

To ensure a structured and organised project management approach, the Phivisp System's development process adopts the Waterfall methodology. This methodology emphasises a sequential flow of phases, including requirements gathering, design, implementation, testing, and deployment. By following this methodology, the Phivisp System development team ensures a systematic progression of activities, leading to a well-defined system.

The testing process plays a crucial role in developing the Phivisp System. It involves various testing techniques, such as User Acceptance Testing (UAT) and usability testing. These tests ensure that the system meets the needs and expectations of its intended users, validating its functionality, usability, and performance.

5.2 Limitation and Constraint

i. Simulated Environment

The simulations provided on the PhiViSp website aim to replicate real-world cyber threats to the best extent possible. However, it is important to recognise that these simulations are still within a controlled environment. Real-world attacks may employ more sophisticated techniques, making it challenging to replicate the complexity and nuance of actual cyber threats fully.

ii. Simulation Accuracy

While every effort has been made to ensure the accuracy and realism of the simulations, there may be instances where the simulations do not perfectly mimic real-world scenarios. Cyber threats and attack techniques constantly evolve, and keeping the simulations up to date with the latest trends and tactics employed by cybercriminals may be challenging.

iii. User Experience and Engagement

The effectiveness of the PhiViSp simulations depends on user engagement and active participation. However, individual learning styles and levels of engagement can vary, impacting the overall effectiveness of the training. Some users may require additional guidance or support to benefit from the simulations fully.

5.3 Future Work

i. Expanding Simulation Scenarios

The PhiViSp simulation website can be expanded to include a broader range of cyber threat scenarios. This could involve simulations for emerging attack vectors, such as Internet of Things (IoT) vulnerabilities, ransomware attacks, or social media-based threats. By diversifying the simulation scenarios, users can comprehensively understand different types of cyber threats.

ii. User Feedback and Usability Testing

Continuous user feedback and usability testing are essential for refining and improving Phivisp. Conducting user surveys, interviews, and usability tests can provide valuable insights into users' needs, preferences, and pain points. Incorporating this feedback into the development process ensures that future enhancements address the real-world requirements and challenges faced by Phivisp users, ultimately improving the usability and effectiveness of the tool.

REFERENCES

Agile Testing vs. Waterfall Testing. (n.d.). Retrieved January 1, 2023, from https://solution-soft.com/content/agile-testing-vs-waterfall-testing

Corporate Mission | SANS Institute. (n.d.). Retrieved February 12, 2023, from https://www.sans.org/mission/

How to Use the Waterfall Method in Any Project: actiTIME Guide. (n.d.). Retrieved January 1, 2023, from https://www.actitime.com/project-management/waterfall-model

McGovern, J., Tyagi, S., Stevens, M. E., & Mathew, S. (2003). Component-Based Service Development. *Java Web Services Architecture*, 65–96. https://doi.org/10.1016/B978-155860900-6/50006-3

MCMC pertingkatkan kempen kesedaran atasi kegiatan scammer di Malaysia | DagangNews.com. (n.d.). Retrieved January 5, 2023, from https://www.dagangnews.com/mcmc-pertingkatkan-kempen-kesedaran-atasi-kegiatan-scammer-di-malaysia-18954

Proactive Security Solutions | Cofense Email Security. (n.d.). Retrieved February 12, 2023, from https://cofense.com/product-services/phishme/

Rakyat Malaysia memang mudah tertipu - Sinar Harian. (n.d.). Retrieved January 5, 2023, from https://www.sinarharian.com.my/article/112720/suara-sinar/pojok/rakyat-malaysia-memang-mudah-tertipu

SDLC - Waterfall Model. (n.d.). Retrieved January 1, 2023, from https://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm

Security Awareness Training | KnowBe4. (n.d.). Retrieved February 12, 2023, from https://www.knowbe4.com/

What is WaterFall Model in Software Developement Life Cycle | SDLC. (n.d.). Retrieved January 1, 2023, from https://www.toolsqa.com/software-testing/waterfall-model/

APPENDIX A

Table 5.1 User Acceptance Test (UAT) form for User 1

No.	Module	Status		Comment
1.	Login using Google account.	[✓ Pass]	Fail	Good
2.	Attempt and continue the quiz.	[✓ Pass]	Fail	Good
3.	Select question option and submit the answer.	[✓ Pass]	Fail	Good
4.	Display explanation for question.	[✓ Pass]	Fail	Good
5.	View details about phishing simulation.	[✓ Pass]	Fail	Good
6.	Display simulation feedback.	[✓ Pass]	Fail	Good
7.	Display page hint	[✓ Pass]	Fail	Good

This test performed by:

Name: DR. AHMAD FIRDAUS BIN ZAINAL **Date:** 9 JUNE 2023

Signature:

Table 5.2 User Acceptance Test (UAT) form for User 2

No.	Module	Status		Comment
1.	Login using Google account.	[✓ Pass]	Fail	Good
2.	Attempt and continue the quiz.	[✓ Pass]	Fail	Good
3.	Select question option and submit the answer.	[✓ Pass]	Fail	Good
4.	Display explanation for question.	[✓ Pass]	Fail	Good
5.	View details about phishing simulation.	[✓ Pass]	Fail	Good
6.	Display simulation feedback.	[✓ Pass]	Fail	Good
7.	Display page hint	[✓ Pass]	Fail	Good

This test performed by:

Name: MUHAMMAD IQMAL HAKIM BIN AMERUDDIN **Date:** 9 JUNE 2023

Signature: Iqmal

Table 5.3 User Acceptance Test (UAT) form for User 3

No.	Module	Status		Comment
1.	Login using Google account.	Pass	Fail	Good
2.	Attempt and continue the quiz.	Pass	Fail	Good
3.	Select question option and submit the answer.	Pass	Fail	Good
4.	Display explanation for question.	Pass	Fail	Good
5.	View details about phishing simulation.	Pass	Fail	Good
6.	Display simulation feedback.	Pass	Fail	Good
7.	Display page hint	Pass	Fail	Good

This test performed by:

Name: MUHAMMAD HAZRIQ AKMAL BIN ZAIROL **Date:** 9 JUNE 2023

Signature: Hazriq

Table 5.4 User Acceptance Test (UAT) form for User 4

No.	Module	Status		Comment
1.	Login using Google account.	[✓ Pass]	Fail	Good
2.	Attempt and continue the quiz.	[✓ Pass]	Fail	Good
3.	Select question option and submit the answer.	[✓ Pass]	Fail	Good
4.	Display explanation for question.	[✓ Pass]	Fail	Good
5.	View details about phishing simulation.	[✓ Pass]	Fail	Good
6.	Display simulation feedback.	[✓ Pass]	Fail	Good
7.	Display page hint	[✓ Pass]	Fail	Good

This test performed by:

Name: FIRDHAUS BIN MD SIDEK **Date:** 9 JUNE 2023

Signature: Firdhaus

Table 5.5 User Acceptance Test (UAT) form for User 5

No.	Module	Status		Comment
1.	Login using Google account.	Pass	Fail	Good
2.	Attempt and continue the quiz.	Pass	Fail	Good
3.	Select question option and submit the answer.	Pass	Fail	Good
4.	Display explanation for question.	Pass	Fail	Good
5.	View details about phishing simulation.	Pass	Fail	Good
6.	Display simulation feedback.	Pass	Fail	Good
7.	Display page hint	Pass	Fail	Good

This test performed by:

Name: MUHAMMAD FYRUZ ISMAT BIN 'AZMI **Date:** 9 JUNE 2023

Signature: Fyruz

Table 5.6 User Acceptance Test (UAT) form for User 6

No.	Module	Status		Comment
1.	Login using Google account.	[✓ Pass]	Fail	Good
2.	Attempt and continue the quiz.	[✓ Pass]	Fail	Good
3.	Select question option and submit the answer.	[✓ Pass]	Fail	Good
4.	Display explanation for question.	[✓ Pass]	Fail	Good
5.	View details about phishing simulation.	[✓ Pass]	Fail	Good
6.	Display simulation feedback.	[✓ Pass]	Fail	Good
7.	Display page hint	[✓ Pass]	Fail	Good

This test performed by:

Name: MOHAMAD HARITH AIZAT BIN SUHAILI **Date:** 9 JUNE 2023

Signature: Aizat

Table 5.7 User Acceptance Test (UAT) form for User 7

No.	Module	Status		Comment
1.	Login using Google account.	[✓ Pass]	Fail	Good
2.	Attempt and continue the quiz.	[✓ Pass]	Fail	Good
3.	Select question option and submit the answer.	[✓ Pass]	Fail	Good
4.	Display explanation for question.	[✓ Pass]	Fail	Good
5.	View details about phishing simulation.	[✓ Pass]	Fail	Good
6.	Display simulation feedback.	[✓ Pass]	Fail	Good
7.	Display page hint	[✓ Pass]	Fail	Good

This test performed by:

Name: MOHAMAD MOHSIN BIN ISMAIL **Date:** 9 JUNE 2023

Signature: Mohsin

Table 5.8 User Acceptance Test (UAT) form for User 8

No.	Module	Status		Comment
1.	Login using Google account.	[✓ Pass]	Fail	Good
2.	Attempt and continue the quiz.	[✓ Pass]	Fail	Good
3.	Select question option and submit the answer.	[✓ Pass]	Fail	Good
4.	Display explanation for question.	[✓ Pass]	Fail	Good
5.	View details about phishing simulation.	[✓ Pass]	Fail	Good
6.	Display simulation feedback.	[✓ Pass]	Fail	Good
7.	Display page hint	[✓ Pass]	Fail	Good

This test performed by:

Name: MUHAMMAD IZZAT BIN MOHAMAD RIZAL **Date:** 9 JUNE 2023

Signature: Izzat

Table 5.9 User Acceptance Test (UAT) form for User 9

No.	Module	Status		Comment
1.	Login using Google account.	Pass	Fail	Good
2.	Attempt and continue the quiz.	Pass	Fail	Good
3.	Select question option and submit the answer.	Pass	Fail	Good
4.	Display explanation for question.	Pass	Fail	Good
5.	View details about phishing simulation.	Pass	Fail	Good
6.	Display simulation feedback.	Pass	Fail	Good
7.	Display page hint	Pass	Fail	Good

This test performed by:

Name: MUHAMMAD ASLAM BIN MAT ASRI **Date:** 9 JUNE 2023

Signature: aslam

Table 5.10 User Acceptance Test (UAT) form for User 10

No.	Module	Status		Comment
1.	Login using Google account.	Pass	Fail	Good
2.	Attempt and continue the quiz.	Pass	Fail	Good
3.	Select question option and submit the answer.	Pass	Fail	Good
4.	Display explanation for question.	Pass	Fail	Good
5.	View details about phishing simulation.	Pass	Fail	Good
6.	Display simulation feedback.	Pass	Fail	Good
7.	Display page hint	Pass	Fail	Good

This test performed by:

Name: AHMAD HISYAM BIN SURYANTO SUGIAN **Date:** 9 JUNE 2023

Signature: ahmad hisyam