APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 6 No. 1 (2025) 486-504
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

The Development of System and Content of Capture the Flag (CTF) Platform

Muhammad Atif Mohd Fadzil[1], Zubaile Abdullah[1*]

[1] *Fakulti Sains Komputer dan Teknologi Maklumat,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: zubaile@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.01.027

Article Info

Received: 20 July 2024
Accepted: 19 June 2025
Available online: 30 June 2025

Keywords

Capture the flag, cyber security training, Agile approach, hand-ons skills, SQL injection

Abstract

New tools and methods have led to a continuous increase in cyber-crime, causing more harm through a rise in attacks. The demand for cybersecurity professionals is exceptionally high due to the increasing frequency and sophistication of cyber-attacks, prompting many universities to offer courses in this field. While the course curriculum is suitable, there's room for improvement by focusing on hands-on skills through assessments. Hence, a Capture The Flag (CTF) platform has been developed for Bachelor's in Computer Science (Information Security) with Honours (BIS) students. This platform provides practical challenges related to cybersecurity. BIS students can become familiar with a CTF environment featuring real-life challenges. The Agile methodology was used to develop this platform on the Ubuntu platform, utilizing the CTFd framework for a smooth development process. The development process also leveraged Docker containers to ensure a consistent and isolated environment for deployment, further facilitating the smooth operation and scalability of the platform. The platform aims to expose BIS students to CTF scenarios, enhancing their hands-on assessment skills in cybersecurity.

1. Introduction

Cyber threats like viruses and hacking can be dangerous. It can have very damaging consequences for individuals, stealing personal information, and disrupt critical infrastructure and vital services of government or an organization. With the development of new tools and techniques, cyber-crime is consistently increasing in terms of the number of attacks and the level of damage caused to its victims. Based on the statistics from Cyber Security Malaysia (CSM), Malaysia reported 4741 cases of cyber threats on 2023[1]. This shows how important cyber security knowledge is to overcome these cyber threats.

Because of the high demand for cybersecurity, many universities offer cybersecurity or information security courses including Universiti Tun Hussien Onn Malaysia (UTHM) in Computer Science and Information Technology (FSKTM). According to Dr Muhaini, as Deputy Dean of FSKTM (2024), 94.17% graduate from FSKTM successfully get a job after their graduate [16]. Based on this statistic, it is shown that higher employability contributes to the cybersecurity industries.

Although the curriculum and syllabus for courses in FSKTM is suitable, it can be enhanced further by doing assessment that focuses on increasing hands-on skill. Furthermore, it can improve practical experience, especially skill in handling situations during cyber threat and can learn more cybersecurity in practical ways. In addition, one of the best approaches to increase understanding on hands on skills and understanding of cybersecurity is Capture the Flag (CTF).

Capture the Flag (CTF) is a type of game specifically designed for the field of information and network security [2]. Teams compete against each other, trying to solve security or vulnerability problems in a limited period. These flags can be anything from a string of letters to an image or data file [3]. Furthermore, CTFs are also crucial training grounds for cybersecurity education because they replicate real-world scenarios where users must overcome a variety of obstacles to find vulnerabilities and secure systems. One of the frameworks that can be used to implement is CTFd. CTFd is an open source capture the flag web service scoreboard framework written by Kevin Chung. It is very easy, a generic framework for "jeopardy" -style computer security competitions. The frameworks support team management, puzzle or challenge organization, real-time tracking, and many others features supportive of normative CTF competitions [4].

2. Literature Review

This section explains about the literature review that has been done related to the CTF platform system, security features and existing online booking system.

2.1 Cybersecurity training

In recent years, large-scale cyberattacks have occurred worldwide more and more frequently, and with ever greater consequences. One of the cases is The WannaCry ransomware campaign in May 2017 infected over 400,000 computers in 150 countries that make this case one of the largest ransomware attacks to date [1]. This accident makes hands-on cybersecurity education and training are becoming more and more relevant in these circumstances, as the only way such security incidents can be prevented and handled adequately [2]. Most current cybersecurity education and training programs employ hands-on activities aimed at improving the functional skills and abilities of the participants. One of the programs that are used for cybersecurity training is the use of Capture the Flag (CTF) platform that allows students or users to learn cybersecurity skills in a fun and engaging way [3].

2.2 Capture the Flag (CTF)

Capture the Flag (CTF) is a competition where participants search for flags in an environment, typically with a focus on computer security or education. The goal is to find flags that provide evidence of achieving certain objectives, such as accessing a file, interacting with a service, or reading from a database table [4]. CTF challenges are created to intimate real situations that security experts face. For instance, some CTF challenges focus on reverse engineering, where members are given a piece of malware or other programming to examine and uncover weaknesses. One of the most well-known kinds of CTF is the jeopardy-style competition. In this configuration, groups are given a progression of challenges or questions, each challenge has been appointed with suitable points. The teams aim to finish these challenges as fast and possible to get a point. The group with the highest score at the end of the competition is declared as the winner [5].

2.2.1 CTFd Framework

CTFd (Capture the Flag framework) is a powerful, open-source platform developed mainly with Python and the Flask web framework to support the organization and management of Capture the Flag (CTF) cybersecurity competitions. It offers a wide range of features such as challenge creation, real-time scoring, team management, and detailed analytics, all accessible via a user-friendly web interface. CTFd can be easily installed on various operating systems, including Ubuntu, through simple commands to set up its dependencies and environment. Once deployed, the platform's modular architecture and plugin support enables organizers to customize and extend it to meet specific competition needs [18].

2.3 Challenge / Module

In the context of Capture the Flag (CTF) competitions, a challenge module refers to a specific problem or task that participants must solve in order to obtain a flag. Each module in the scenario corresponds to a sole CTF problem, and participants can have a unique experience by combining different problems together [6]. According to Kevin Chung, creator of CTFd says the success of a CTF event, in terms of learning and evaluation, is directly related to the design of the competition's challenges. It's unlikely that an overly simplistic challenge will provide much educational value, but it will likely be solved quickly while difficult challenges have the chance to teach more to a competitor, but there's a risk of many competitors feeling left out [7]. There are a few categories that include CTF such as cryptography, web, forensic, OSINT, general knowledge, and steganography.

2.3.1 Cryptography

Cryptography is a challenge that involves the application of cryptographic techniques to solve a puzzle or uncover hidden information in text or file. These challenges require students to decode text messages that are

encrypted with both classical and modern authentication methods [4]. The purpose of this challenge is to test understanding students to decode incomprehensible data into meaningful information [3].

2.3.2 Web Challenge

Web challenge or web exploitation is the act of finding and exploiting vulnerabilities in web applications. These vulnerabilities often show up in CTFs as web security challenges where the user needs to exploit a bug to gain some kind of higher-level privileges. Some of the common vulnerabilities that user can find in CTF challenges such as SQL injection, command injection and cross site scripting [4], [8].

2.3.3 Forensic

In a CTF context, "Forensics" challenges can include file format analysis, steganography, memory dump analysis, or network packet capture analysis. Furthermore, examining and extracting hidden information from static data files, rather than executable programs or remote servers, can be regarded as a forensic challenge [3]. One of the tools that can be used to solve this challenge Wireshark for capture and analyse the data traveling back and forth on a network in real time. The purpose of this challenge is to test student understanding on evidence recovery from various sources using appropriate tools.

2.3.4 General Knowledge

General questions are any kind of knowledge question; answers are usually general knowledge in the security field or can be found by using search engines. The goal of this type of task is to challenge the user's knowledge, but also to provide an easy way to get points in a CTF competition. In a CTF event, challenges may additionally provide hints and/or restrictions for accepted answers [9].

2.3.5 Steganography

Steganography is the practice of sending data in a concealed format so the very fact of sending the data is disguised. Unlike cryptography, which conceals the contents of a secret message, steganography conceals the very fact that a message is communicated. These challenges used to test understanding students on how to use to analyses image or data to uncover hidden information [3].

2.3.6 OSINT

OSINT, or Open-Source Intelligence, is the process of collecting and analyzing information that is publicly available from sources such as websites, social media, and public records. It is widely used in fields like cybersecurity, law enforcement, and business to gather insights and make informed decisions based on legally accessible data. This practice has evolved significantly with advancements in technology and the increasing availability of online information [17].

2.4 Security Features

Security features are crucial elements designed to protect systems and information from unauthorized access and potential threats. They play a vital role in ensuring the safety and confidentiality of data. These features act as safeguards, preventing unauthorized individuals or malicious entities from exploiting vulnerabilities. By incorporating security measures, like encryption, access controls, and authentication protocols, a system can defend against various risks. The need of security features creating a secure environment that mitigates the potential impact of cyber threats. Basically, security features act as silent guardians, working in the background to keep information safe and systems resilient.

2.4.1 Two-factor Authentication

Two-factor authentication (2FA) adds an extra layer of security by requiring two steps to confirm your identity when accessing online accounts. It typically involves combining two out of three verification factors: "what you have," "who you are," and "what you know." For example, a common practice is entering a password (what you know) and then receiving a code on your phone (what you have). This dual verification process enhances security by necessitating multiple forms of identification [10]. With 2FA, in addition to entering a password, users are also required to provide a second factor, such as a code from a text message or an app, to log in. This makes it much harder for hackers to gain access to accounts, even if they have stolen the password. Two-factor authentication is a very effective way to protect online accounts from hacking. It is recommended that all users enable 2FA on their accounts, especially those that contain sensitive information, such as bank accounts and email accounts [11].

2.4.2 Session time-out

To reduce the risk of attackers launching and taking overactive sessions, it's necessary to set expiration timeouts for each session. These timeouts determine how long a session stays active. If a web application doesn't have sufficient session expiration, it increases the chances of various attacks. For an attacker to reuse a valid session ID and take control of the session, the session must still be active. Setting expiration timeouts helps to prevent this kind of unauthorized access. To lower the risk of attackers taking control of active sessions, it's important to establish expiration timeouts for each session. These timeouts determine how long a session can stay active. If a web application lacks adequate session expiration, it raises the likelihood of different types of attacks. For an attacker to take charge of a session by reusing a valid session ID, the session needs to remain active. Setting expiration timeouts is crucial for preventing this unauthorized access. When a session expires, the web application must actively take steps to invalidate the session on both sides, the client and server sides [12].

2.4.3 Captcha

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is a type of challenge-response test used to determine whether the user is a human or a bot. Originally, CAPTCHA is designed to safeguard webpages and online accounts from automated spam and bots. The test serves as a method to ensure security. It is commonly used on websites that require user input, like online forms, registration pages, and login portals [13]. With the CAPTCHA that is used to ensure that genuine user interactions are prioritized, it is suitable for authentication page for CTFd platform.

2.5 Comparison Between Existing System and Proposed System

The existing system's review is necessary to compare the systems. The goal of this review is to identify the existing application's weaknesses and flaws and to enhance the proposed platform construction.

2.5.1 Hack the Box (HTB)

Hack the Box (HTB) is an online CTF platform that provides a hands-on challenge and practical approach to learn and improve cybersecurity knowledge and skills. HTB was created by Haris Pylarinos, commonly known as “ch4p”. Haris Pylarinos founded HTB to provide a platform for cybersecurity enthusiasts and professionals to enhance their skills through hands-on challenges and simulations. HTB is valued for its interactive approach to learn, allowing individuals to build and refine their skills in a dynamic and engaging manner.

2.5.2 Pico CTF

PicoCTF is an online cybersecurity competition designed for middle and high school students, created by Carnegie Mellon University. It challenges participants with a series of puzzles and hacking tasks that teach computer science and cybersecurity concepts in a fun and engaging way. The competition aims to inspire and educate the next generation of cybersecurity experts by providing hands-on learning experience. Table 1 shows the comparison between existing CTF platforms which are Hack the Box (HTB), PicoCTF and the proposed system (FSKTM CTF platform). The features include type of integration, password requirement, login, session timeout, type of publication, captcha implementation, user mode, email verification, and challenge module.

Table 1 *Comparison between existing system and proposed system*

Platform	HTB	PicoCTF	Proposed CTF platform
Type of integration	Web based	Web based	Web based
Password requirement	3 characters	8 characters	8-character, Special character, Upper and lower case
Login	Yes	Yes	Yes
Session time out	Yes	Yes	Yes
Type of publication	Public	Public	Private for FSKTM student
Captcha implementation	No	Yes	Yes
User mode	Individual mode	Individual / team mode	Individual / team mode
Email verification	Yes	Yes	Yes
Challenge module	Pwn, Crypto, Web, Mobile, Forensic, Osint, Blockchain	Web challenge, Reverse engineering, Forensic, General skills, Binary	Web challenge, Forensic, Cryptography, Steganography, General challenge, OSINT

exploitation

3. Methodology

This section discussed the methodology that was used in this project. Object-Oriented Methodology (OOM) implemented by using an agile model. Using Agile methodology [14] for developing a Capture the Flag (CTF) platform like CTFd framework is beneficial because it allows flexibility, quick adjustments, and continuous improvement. Agile helps create a better, more user-friendly CTF platform by being adaptable and responsive to changes and user needs. The Agile model consists of four phases which are planning, design, develop, test, deploy and review phase as shown in Fig. 1.

Fig. 1 *Agile methodology*

3.1 Planning Phase

Several tasks are included in the planning phase with the goal of fully comprehending the context of the project. First, the scope, objective, and problem statements are determined. Studying CTF environment is conducted to obtain a variety of viewpoints from user perspective. The functional and non-functional user requirements are described in detail, together with the intended project outcomes and importance. Additionally, software and hardware requirements for CTF platform for BIS students are also studied in this phase.

3.2 Design Phase

Essential parts are quickly developed during the Design phase, which is a fast iteration step based on requirements received. This includes building the system's navigation flow, developing the database structure for users, and designing the user interface, which includes key features like creating the challenge. This phase also covers security components like strong password enforcement and Captcha.

3.3 Develop Phase

During development phase involves design requirements into workable prototype. At this point in the development process, the main goal is to create a working prototype of CTF platform. Implementing challenge modules and authentication functionality, two essential components of the suggested CTF platform receives particular attention.

3.4 Testing Phase

Throughout the testing phase stage of agile methodology for CTF platform, engaging potential users is essential. In this stage, the demo version is shown to target end users, which include admin for the CTF platform and BIS student from FSKTM. Users must interact with the demo version at this phase in order to assess its functioning, offer suggestions, and communicate their preferences through interactive sessions.

3.5 Deploy Phase

The development phase of the CTF platform system involves the actual implementation based on the design specifications. The system is deployed using the CTFd framework on the Ubuntu Operating system, and system functionalities are implemented using the Python programming language. The database structure is established using MariaDB to ensure efficient data storage and retrieval through the CTFd framework. The system will deploy through the docker and establish in local host and establish during system deployment through VM ware.

3.6 Review Phase

In the review phase of Agile development for the CTF platform utilizing the CTFd framework, an assessment is carried out on the implemented features and functionalities. In this phase also, user acceptance test and system design feedback will be conducts to get the data for future update to the platform. Users must interact with the proposed system at this phase in order to assess its functioning, offer suggestions, and communicate their preferences through interactive sessions.

4. System Analysis and Design

System analysis and design show the system functional and non-functional requirements, use-case diagram, sequence diagram, activity diagram, class diagram, entity relationship diagram (ERD), and user interface design,

4.1 Functional and Non-Functional Requirements

Functional requirements are used to describe the functions that must be performed by a system, subsystem, device, software program, or other types of products while Non-functional requirements are used to describe a product, its construction, or limitations on its design or behavior. Table 2 and 3 are a list of functional requirements and a list of non-functional requirements for CTF platform for BIS students.

Table 2 *Functional requirements for CTF platform*

Module	Functionality
Login - Admin, User	• The user and admin login into the CTF platform system
Registration - User	• The user registers their account by adding username, email and password to the system.
Scoreboard - Admin, User	• User able to view the scoreboard page. • Admin manages the scoreboard page.
Statistic - Admin	• Admin able to view the statistic scoring board from user.
Challenge - Admin, User	• User submits the flag for challenge module. • Admin manages the challenge module by adding, delete or hide the challenge.
Notification - Admin, User	• The user able to view the notification and admin manage the notification

Table 3 Non-*Functional requirements for CTF platform*

Module	Functionality
Operational	• The system can generate a scoreboard from challenge score
Performance	• The performance of the system should be fast without uninterrupted
Security	• The system enforces to set the password with at least 8 characters during registration • The user and admin may access the system with the correct username and password • Utilize hcaptcha in authentication • Implementation of time session management • Implementation of encryption for password using bcrypt encryption
Integrity	• This system will available only until the system is on which is the system is running
Availability	• This system will available only until the system is on which is the system is running

4.2 Use Case Diagram

A use case diagram is a visual representation showing how users (actors) interact with a system, highlighting what the system can do from the user's perspective. It identifies the main functions or tasks (use

cases) the system performs and explains how different users or systems interact with these tasks. The diagram typically includes actors (users or other systems), use cases (system functions), and their relationships. This helps in understanding the system's requirements and planning its structure, ensuring all user interactions are covered. Fig. 2 presents the use case diagram for CTF platform for BIS students.

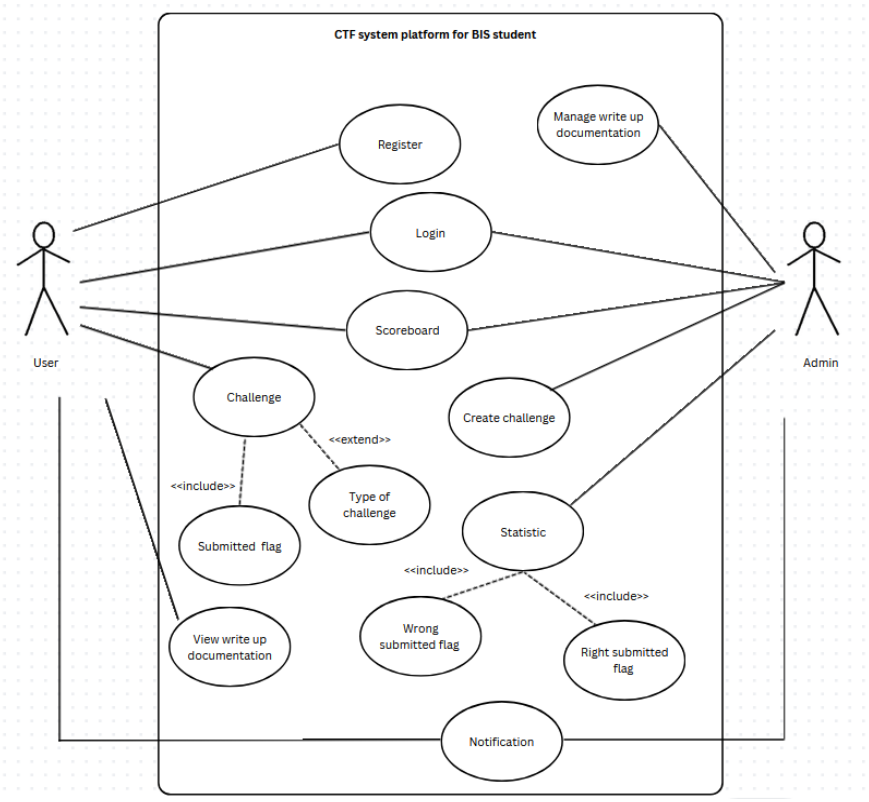

Fig. 2 *Use Case diagram for CTF platform*

4.3 Sequence Diagram

The sequence diagrams illustrate the interactions within the CTF platform system for three user types: Admin, Superior, and Staff. Each diagram (Fig. 3 to Fig. 7) outlines the login process, access to the dashboard, and interaction with the challenge module. Admins log in, create a challenge, view statistic, scoreboard and edit new user while user can register, login, solve the challenge and view personal scoreboard with different breakdown category.

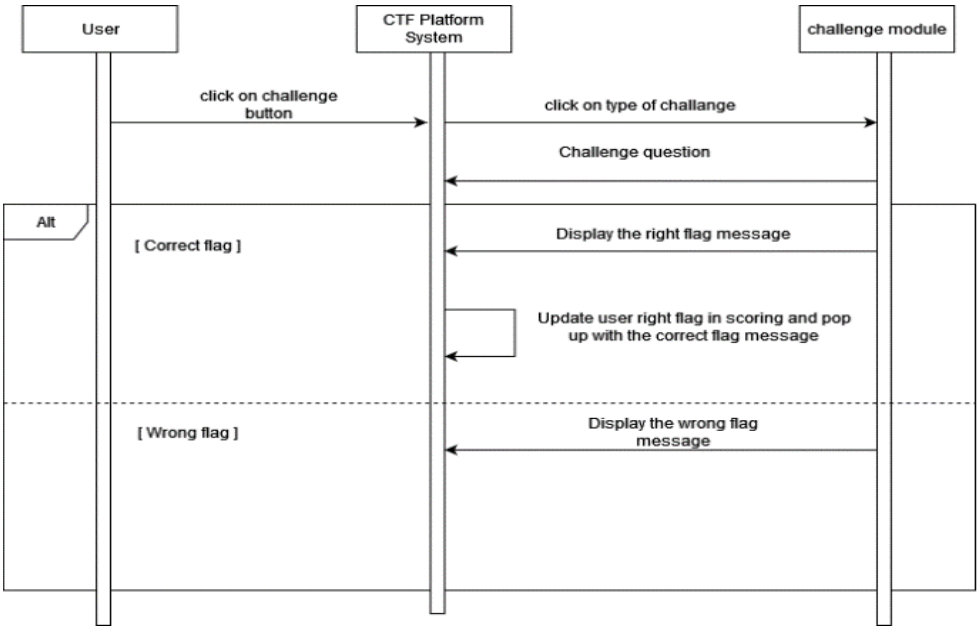

Fig. 3 *Sequence diagram for submitted flag process*

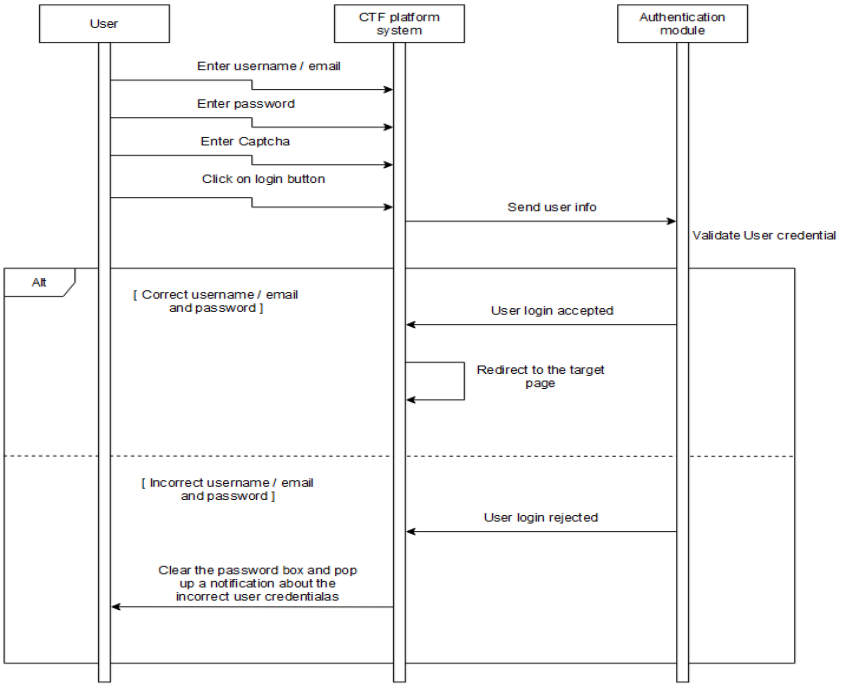

Fig. 4 *Sequence diagram for user login process*

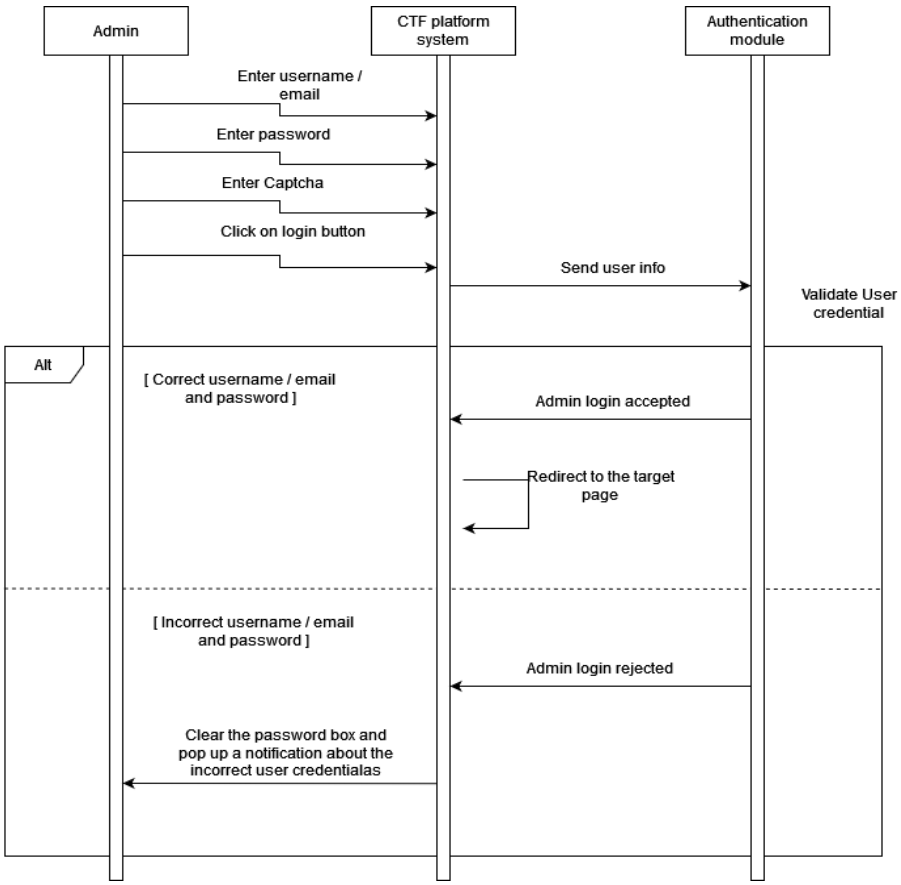

Fig. 5 *Sequence diagram for admin login process*

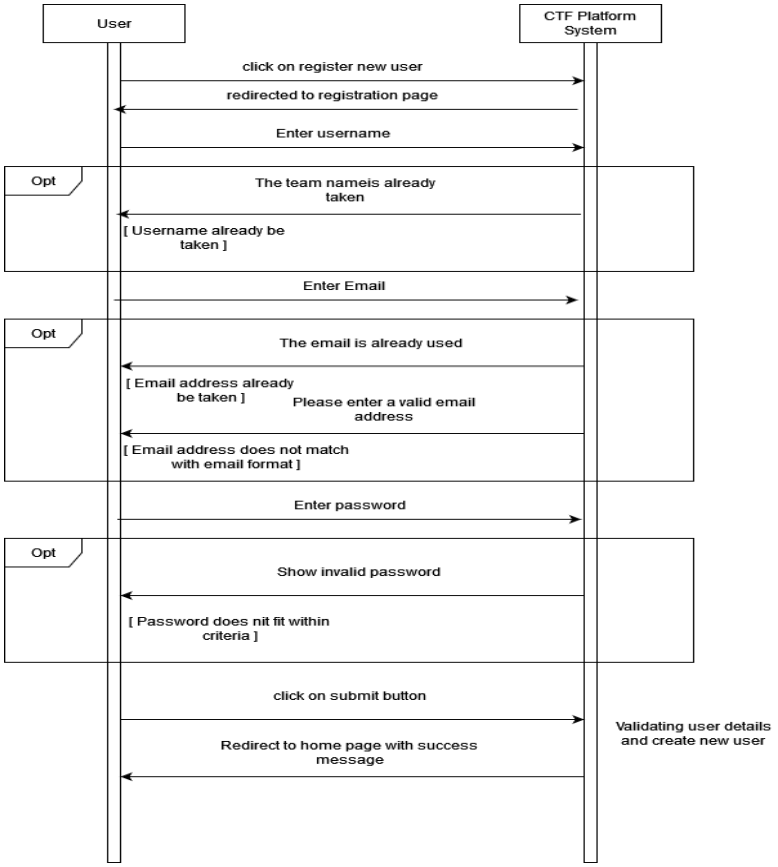

Fig. 6 *Sequence diagram for new users register*

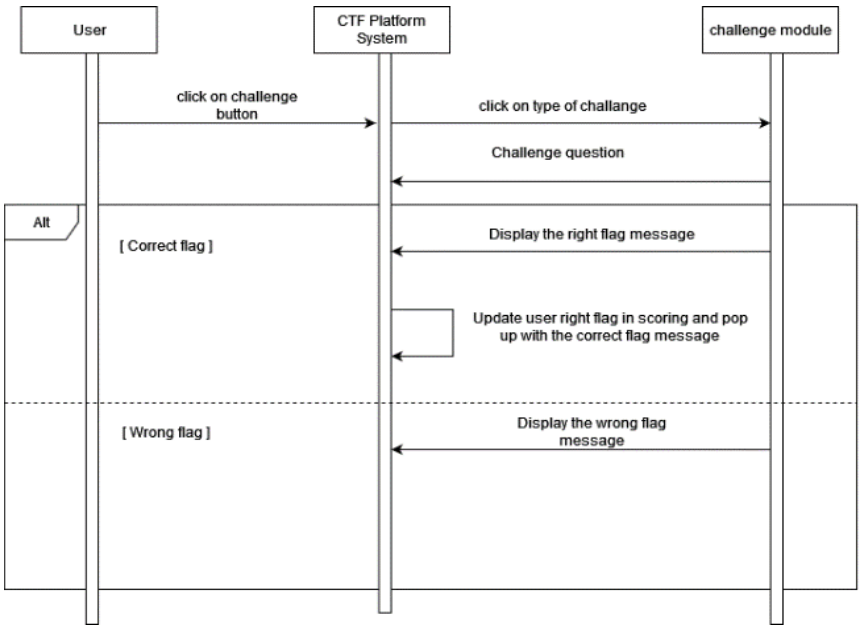

Fig. 7 *Sequence diagram for submitted flag process*

4.4 Activity Diagram

Activity diagrams in Fig 8 and Fig. 9 play a crucial role in developing the "CTF platform system for BIS student". They offer a visual depiction of the system's workflow, providing a clear and intuitive understanding of its logical flow.

Applied Information Technology and Computer Science Vol. 6 No. 1 (2025) p. 486-504

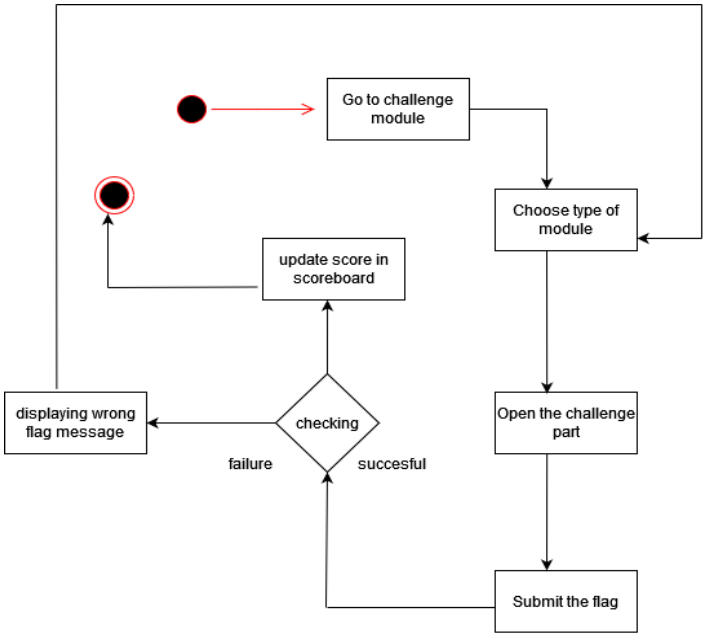

Fig. 8 *Activity diagram for CTF platform system*

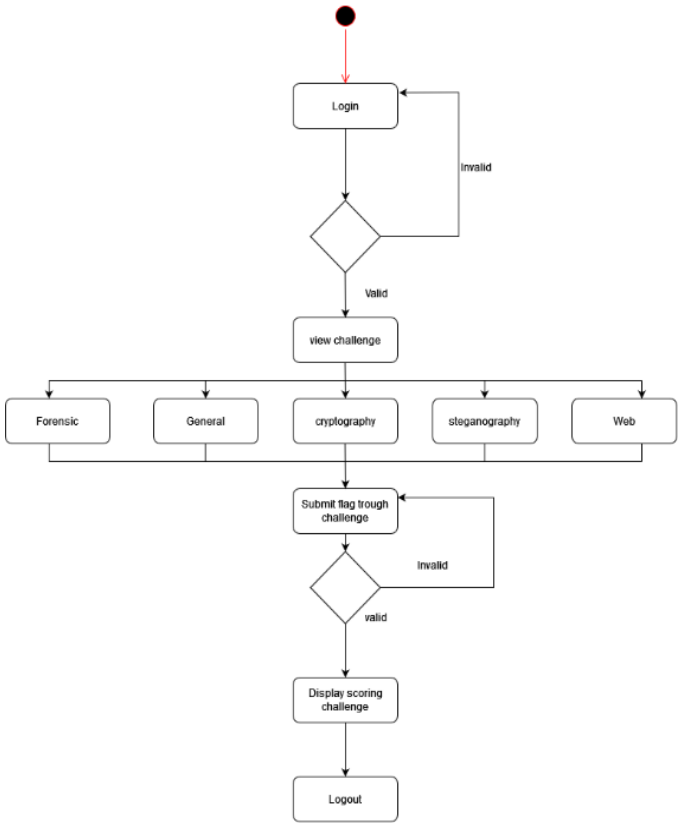

Fig. 9 *User activity diagram*

4.5 ER Diagram

The entity relationship diagram (ERD) is a system diagram that shows the connection between the entity and its data. It's a modeling method used to visually represent the information structure of an organization's entity and the interactions among entities more precisely. Fig. 10 displays the entity relationship diagram for CTF platform system.

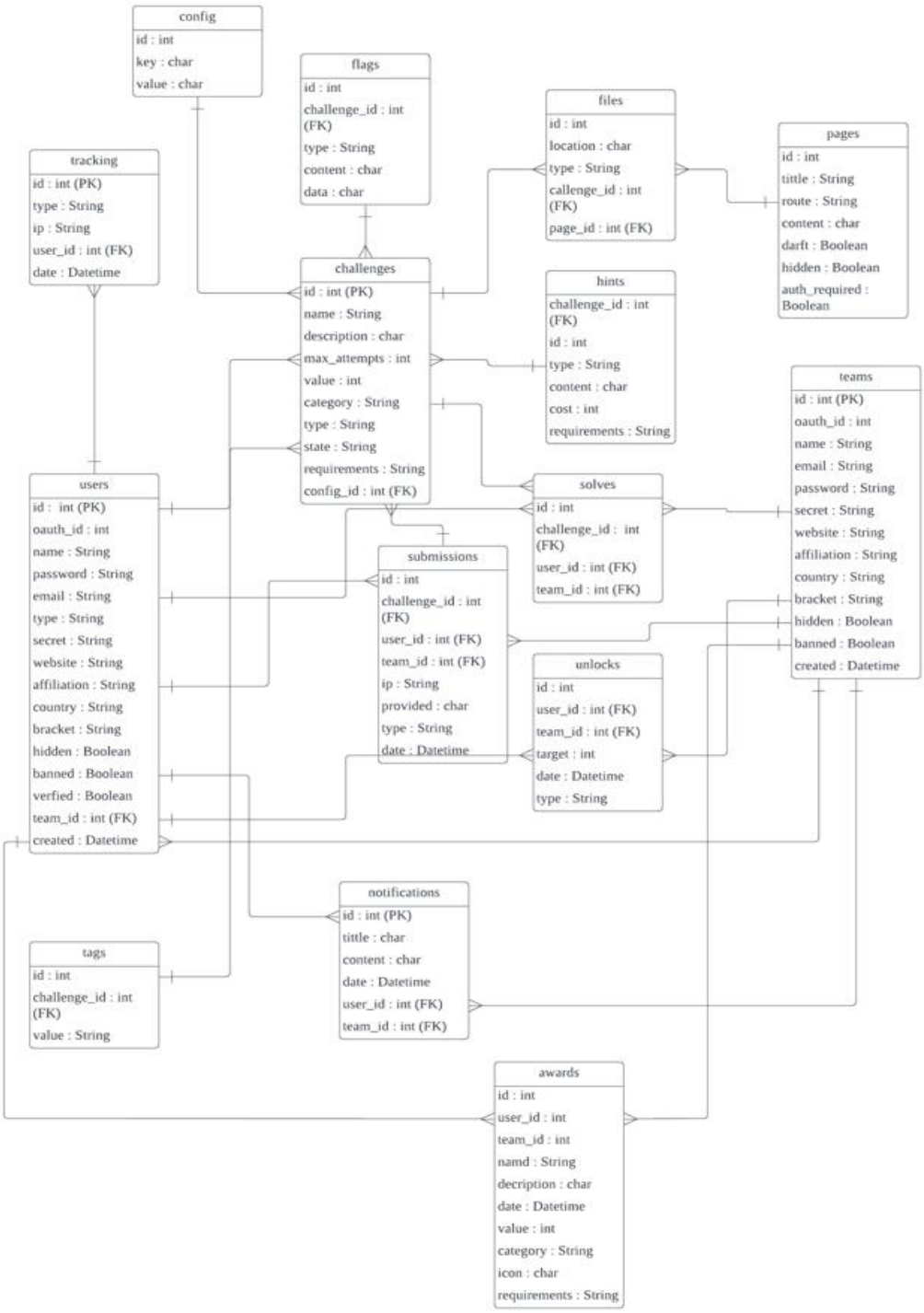

Fig. 10 *ER diagram for CTF platform system*

5. Implementation and Testing

Implementation is the process of creating and building the software system based on the design, while testing is the process of checking if the system works correctly and is reliable.

5.1 Implementation

The following section will cover the modules that were utilized in this system. The modules for registration, login, statistics, scoreboard, and view challenge will be covered. The several sections will each contain a description of the program's partial code for a particular module.

5.1.1 Login

Fig. 11 displays the login page. Users will have to login first, after login process the system will check whether the user submit the right username and password, if the system detects the user insert the wrong username or password, the system will prompt the message "Your username or password is incorrect". If the user submits the right username and password, it will redirect user to challenges page as shown in Fig. 12.

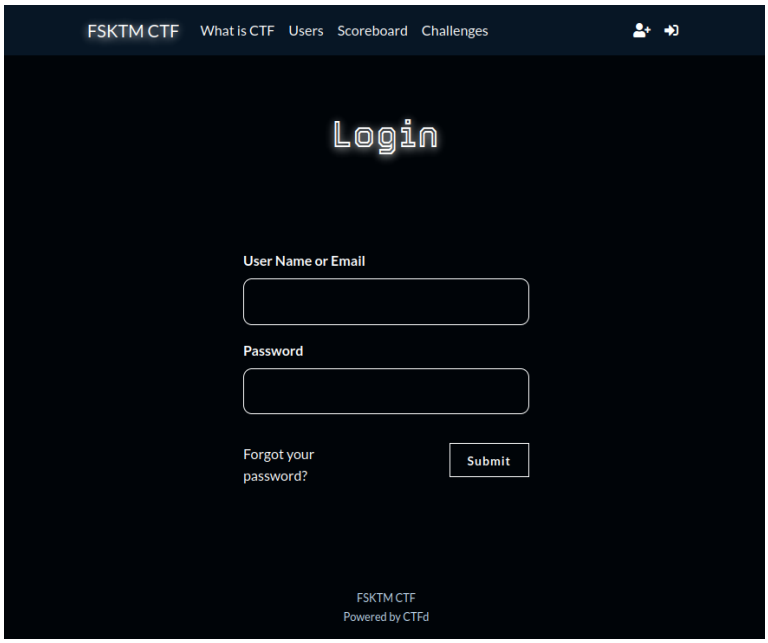

Fig. 11 *Login page for CTF platform*

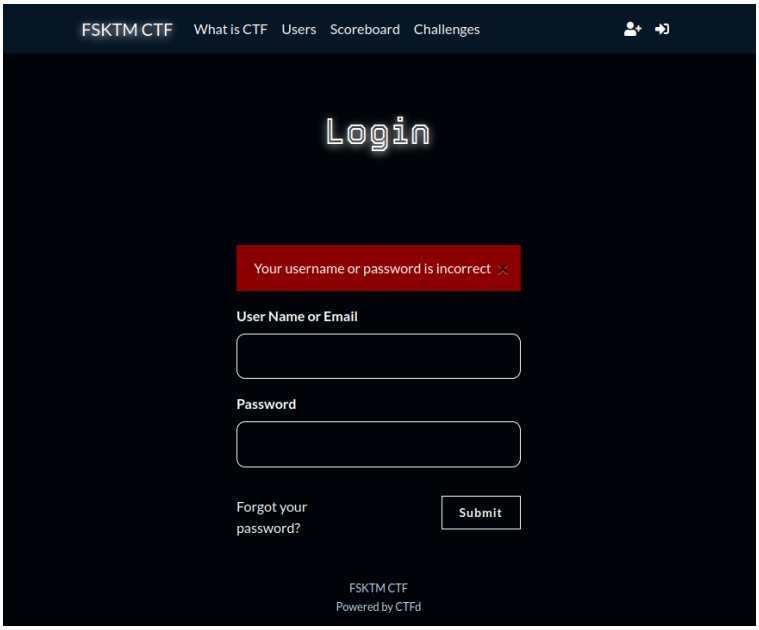

Fig. 12 *Error message when fill in the wrong password* or username

5.1.2 Registration

Fig. 13 shows registration forms for users. For new users, it requires usernames, email, password that enforce with strong password policy, code that has been given by admin, and verification with hcaptcha. Meanwhile for new admin registration, it requires for admin to add in admin panel as shown in Fig. 14.

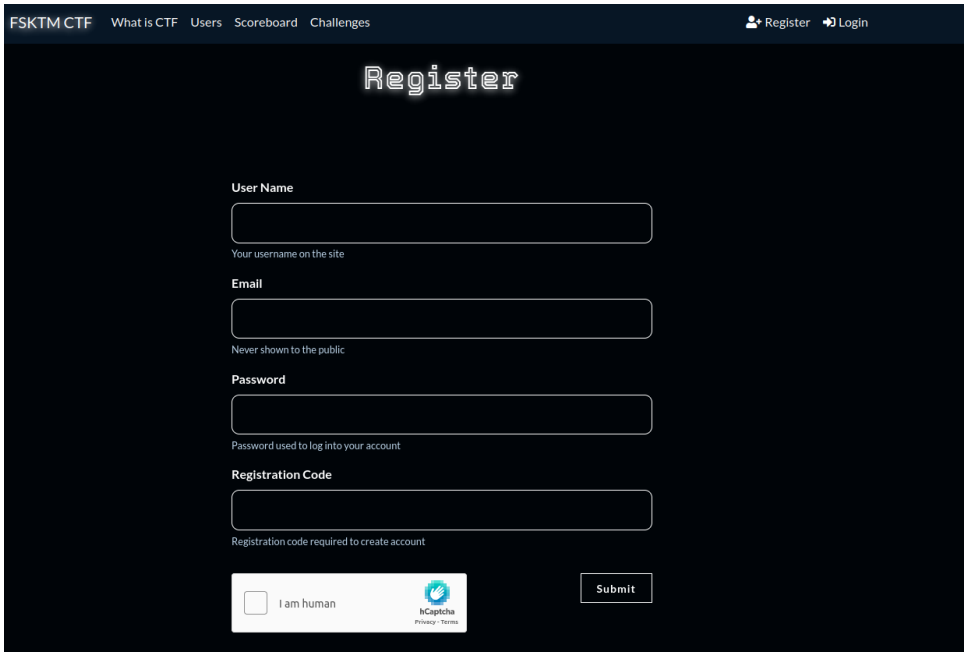

Fig. 13 *Registration of new users for CTF platform system*

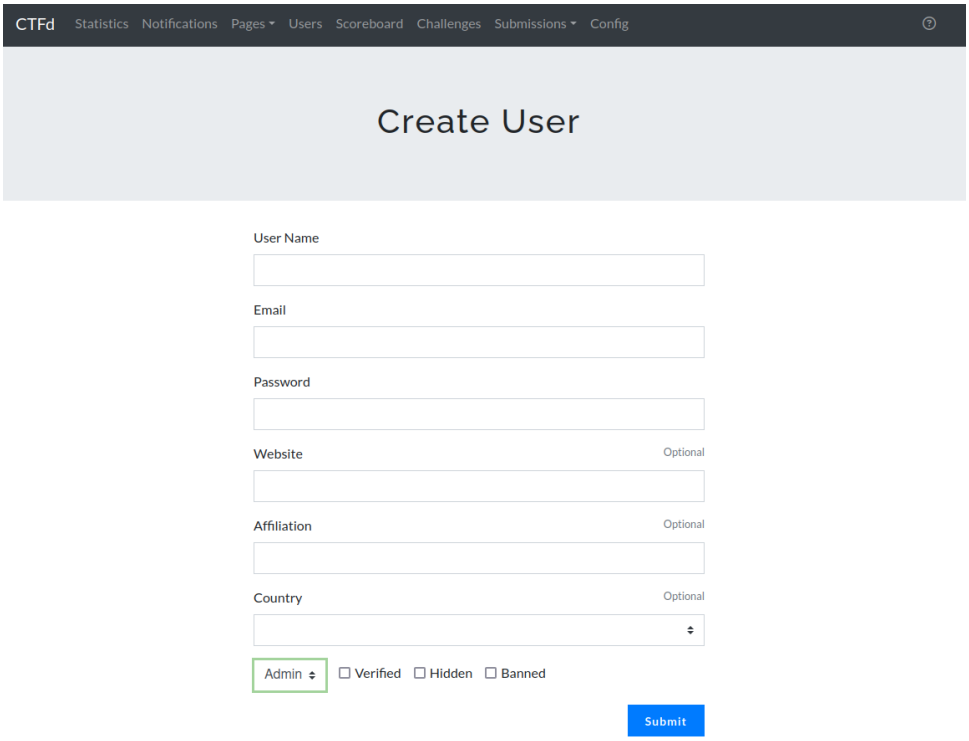

Fig. 14 *Registration new admin for CTF platform system*

5.1.3 Challenge

Challenge modules have two separate functions for administrators and user. For users, the only privilege that they have is view and solve the challenge as shown in Fig. 15. This challenge comprehends the aspects in information security such as cryptography, steganography, web, forensic, Open-source intelligence (OSINT), and general knowledge.

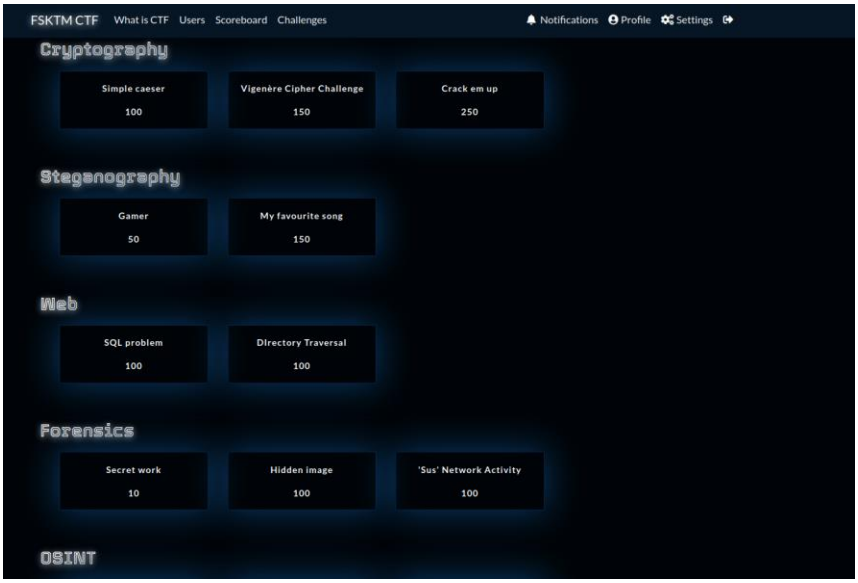

Fig. 15 *Challenge Page in CTF platform*

To solve this challenge, users need to understand the description that has been displayed from the challenge. Some of the challenges include hints to solve the challenge as shown on Fig. 16. After user insert the flag, it will prompt a message that say "Correct" show that the flag that is submit is right. If wrong, incorrect messages will be displayed as show in Fig. 17. Fig. 18 shows admin privilege to create the challenge.

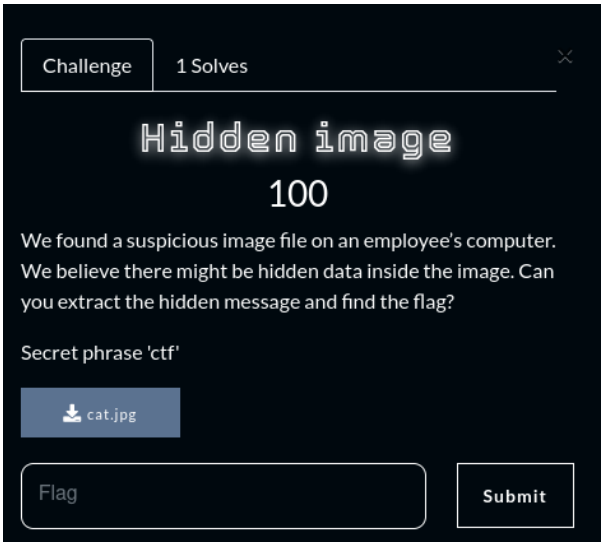

Fig. 16 *one of the challenges is challenge page*

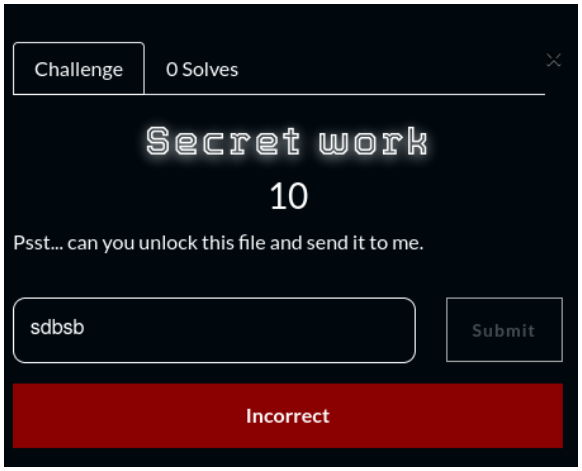

Fig. 17 *"incorrect" message display for wrong flag*

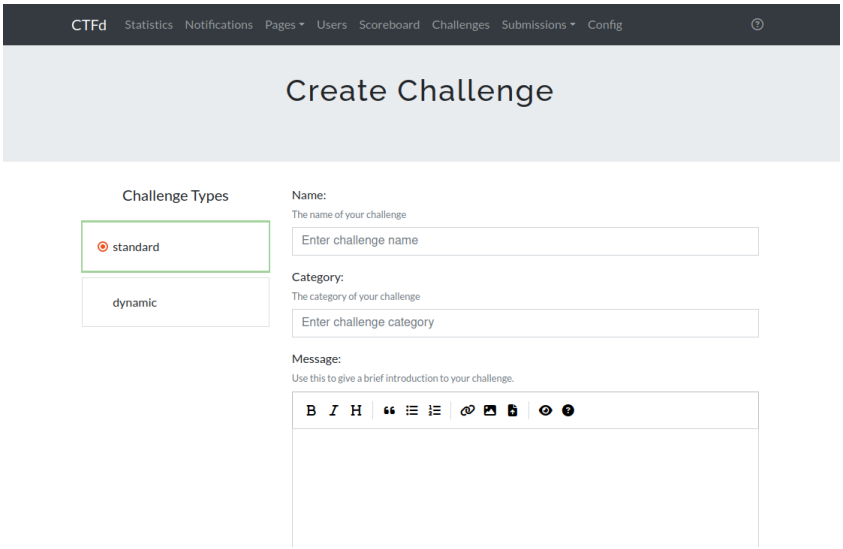

Fig. 18 *Admin privilege to create the challenge*

The partial coding in Fig. 19 defines a named tuple, Challenge for challenge module, with specified fields, and a cached function, get_all_challenges, which retrieves challenges from a database. The function accepts parameters for filtering and querying the challenges. It constructs filters using build_model_filters and applies them to the Challenges query object. If the admin parameter is False, the query excludes hidden and locked challenges. The query is then further refined by additional filters, ordered by challenge value and ID, and executed. Each resulting challenge is converted into a Challenge named tuple, with tags serialized using TagSchema, and added to the results list. Finally, the function returns to the list of challenge objects.

```
Challenge = namedtuple(
    "Challenge", ["id", "type", "name", "value", "category", "tags", "requirements"]
)


@cache.memoize(timeout=60)
def get_all_challenges(admin=False, field=None, q=None, **query_args):
    filters = build_model_filters(model=Challenges, query=q, field=field)
    chal_q = Challenges.query
    # Admins can see hidden and locked challenges in the admin view
    if admin is False:
        chal_q = chal_q.filter(
            and_(Challenges.state != "hidden", Challenges.state != "locked")
        )
    chal_q = (
        chal_q.filter_by(**query_args)
        .filter(*filters)
        .order_by(Challenges.value, Challenges.id)
    )
    tag_schema = TagSchema(view="user", many=True)

    results = []
    for c in chal_q:
        ct = Challenge(
            id=c.id,
            type=c.type,
            name=c.name,
            value=c.value,
            category=c.category,
            requirements=c.requirements,
            tags=tag_schema.dump(c.tags).data,
        )
        results.append(ct)
    return results
```

Fig. 19 *Partial code for challenge module*

5.1.4 Time Session Management

Fig. 20 shows the code for implementation time session. It achieves this by configuring the session lifetime (PERMANENT_SESSION_LIFETIME) to 20 minutes. Additionally, it customizes the session interface using CachingSessionInterface, which helps manage sessions more efficiently with a prefix (your_prefix) and ensures that sessions are securely signed (use_signer=True) and permanent. This means that each user's session will expire 20 minutes after their last activity, enhancing security by automatically logging out inactive users.

```
# Set up the Flask app
app = Flask(__name__)

# Set the permanent session lifetime to 20 minutes
app.config['PERMANENT_SESSION_LIFETIME'] = timedelta(minutes=20)

# Configure the session interface
app.session_interface = CachingSessionInterface(key_prefix='your_prefix', use_signer=True, permanent=True)
```

Fig. 20 *Code segment of time session management*

5.1.5 Captcha

Fig. 21 shows the interface for captcha validation. In this project, hcaptcha has been implemented. The hcaptcha uses image recognition tests that are becoming increasingly difficult to solve as bots get better at solving them through machine learning. Users are required to select the correct image or else an error is prompted.

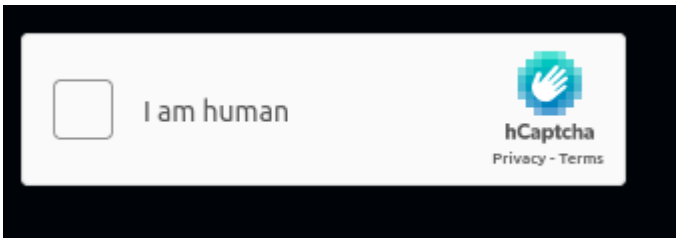

Fig. 21 *hCaptcha*

5.2 Testing

User testing helps identify usability issues, validate design decisions, and ensure that the product or system meets the needs and expectations of its target users. Table 4 and Table 5 show the test plan for Admin and Staff respectively.

Table 4 *User test Result for Admin*

No.	Test case	Pass	Fail
1.	System can be executed from start to end	Pass	
2.	Admin able to login and logout the system	Pass	
3.	Admin able to edit and create the challenge	Pass	
4.	Admin able to view statistic page	Pass	
5.	Admin able to create notification for users	Pass	
6.	Admin able to change password	Pass	
8.	Admin able to view scoreboard of user	Pass	

Table 5 *User test Result for Admin*

No.	Test case	Pass	Fail
1.	System can be executed from start to end	Pass	
2.	User able to login and logout the system	Pass	
3.	User able to view the challenge	Pass	
4.	User able to register in registration page	Pass	
5.	User able to view notifications	Pass	
6.	User able to view scoreboard	Pass	

5.2.1 SQL Injection Testing

Fig. 22 shows an attempt at SQL injection testing on a login page. The tester has entered `' or '1'='1` in the "User Name or Email" field, which is a common SQL injection payload. This payload aims to manipulate the underlying SQL query by making the condition always true (`'1'='1'`), potentially bypassing the login check if the application is vulnerable. However, the application responded with "Your username or password is incorrect," indicating that the input did not succeed in bypassing the authentication, suggesting that the application may be handling user inputs securely, possibly through parameterized queries or proper input validation. Fig. 23 show list of login bypass list.

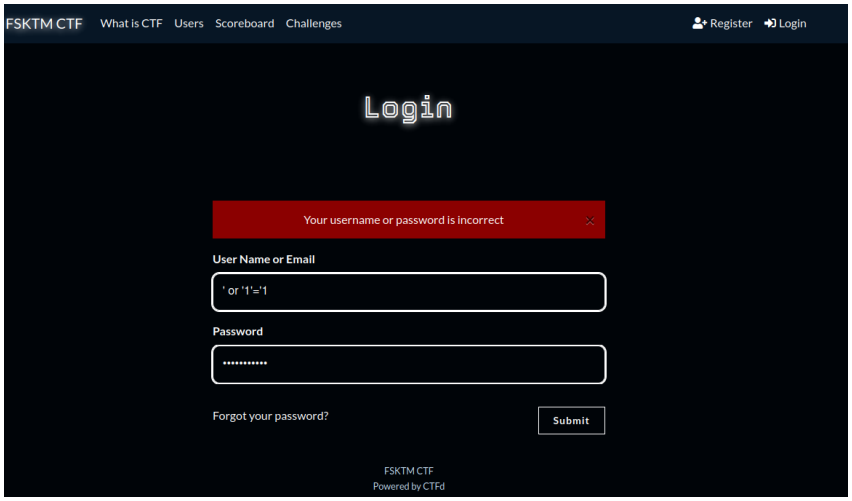

Fig. 22 *SQL injection testing*

- ' or '1'='1
- ' or ''='
- ' or 1]%00
- ' or /* or '
- ' or "a" or '
- ' or 1 or '
- ' or true() or '
- 'or position()=2 or'
- admin' or '
- admin' or '1'='2

Fig. 23 *SQL injection testing*

5.2.2 User Acceptance Test

User Acceptance Testing (UAT) is one of the last phases of the software development life cycle, and this is where UAT comes in. It is carried out after comprehensive testing of the system. The User Acceptance Testing (UAT) participants for this project include the FSKTM student, comprising BIS student and 2 other courses from FSKTM.

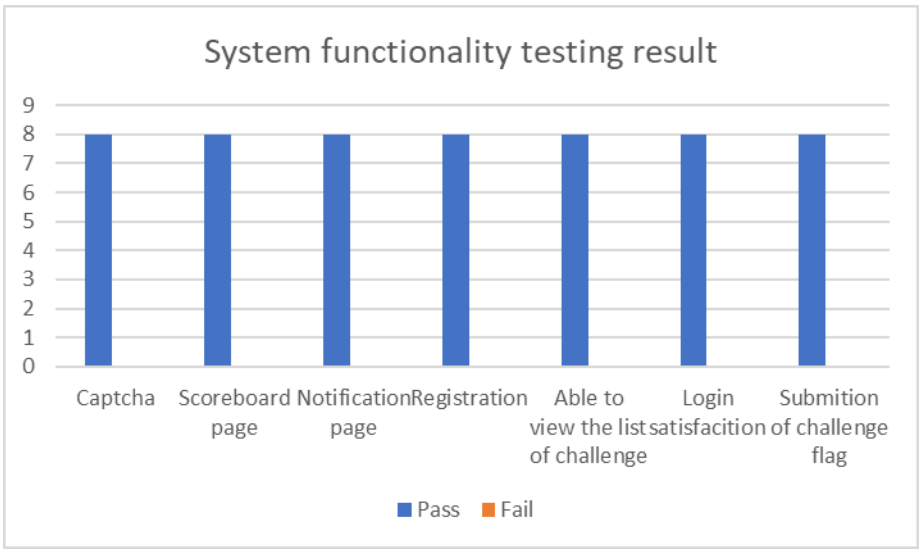

Fig. 24 *System functionality testing result*

Fig 24 shows the pass counts for various features of the system based on user acceptance testing. The features evaluated include login satisfaction, registration, hcaptcha, view of the challenge, notification page, and

submission of challenge flag. Each feature received a pass from the respondents, with pass for each category, indicating strong satisfaction with these features across the board.

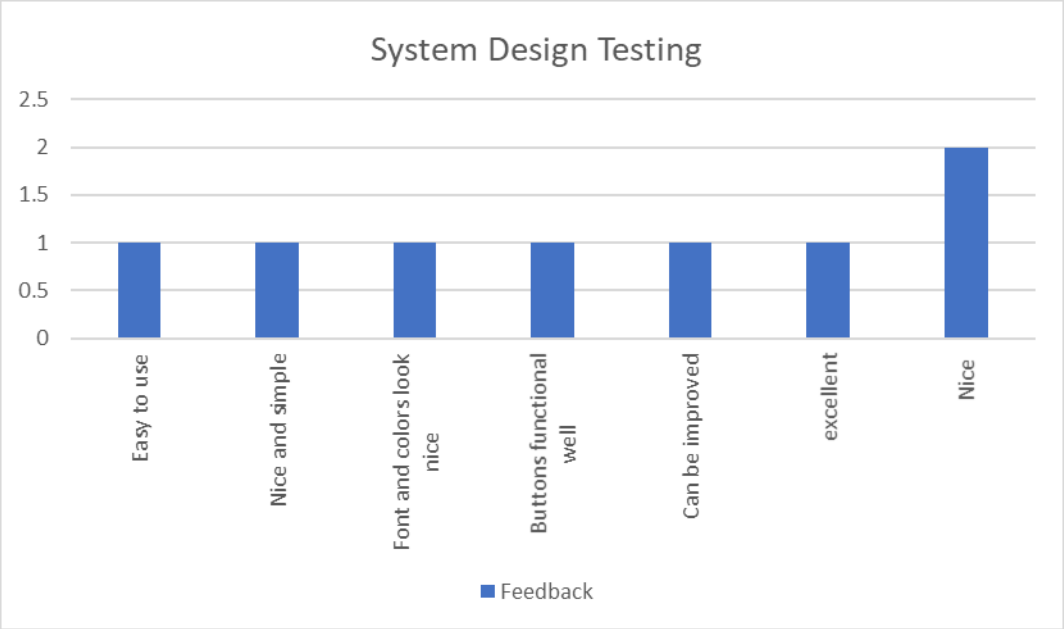

Fig. 25 *System design feedback result*

Figure 25 displays the feedback for the interface of the system, as gathered from a Google Form user acceptance test. The chart shows various comments from the respondents, indicating their opinions on different aspects of the interface. The feedback includes comments in every aspect of design such as "can be improved," "easy to use," "buttons functional well," "nice design," "font and colors look good," "improve design," "excellent," "nice and simple," and "can be improved." The feedback frequency shows that two respondents rated it "nice," while other comments were mentioned once, indicating a generally positive reception with suggestions for further improvement.

6. Conclusion

There are a few benefits related on this proposed project. By developing the content for this project, it can develop technical skills that are related to cybersecurity for FSKTM students, especially for BIS students. With the engagement from BIS students to this project will give an exposure to CTF environment and nature self-efficacy in students [15]. Moreover, by developing the CTF platform, we can track the record progress when students complete the challenge for purpose to test their understanding when doing the challenge

Despite its strengths, the system does face some limitations, such as the need for a dependency on internet connectivity for fully use the function, and potential challenges for non-information security students. Addressing these limitations through future improvements, such as developing a dedicated application, enhancing offline functionality, and making the challenge for every category more suitable for every level, will further enhance the system's effectiveness and user satisfaction.

The implementation of additional features, such as scalability enhancements, advanced security measures, and integration with other management systems, will ensure that the CTF platform for BIS student system continues to meet the evolving needs of its users. To sum up, this platform aims to test the student understanding of cybersecurity through technical assessment and encourage students to learn new knowledge for solving the challenge.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support.

Author Contribution

The authors confirm contribution to the paper as follows: **study conception and design**: M.*A. Mohd Fadzil, Z. Abdullah*; **data collection**: *A. Mohd Fadzil, Z. Abdullah*; **analysis and interpretation of results***: .A. Mohd Fadzil, Z. Abdullah*; **draft manuscript preparation**: *.A. Mohd Fadzil, Z. Abdullah*. All authors reviewed the results and approved the final version of the manuscript.

References

[1] R. Beuran, D. Tang, C. Pham, K. ichi Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: CyTrONE," *Comput Secur*, vol. 78, pp. 43–59, Sep. 2018, doi: 10.1016/j.cose.2018.06.001.

[2] M. Bartnes, N. B. Moe, and P. E. Heegaard, "The future of information security incident management training: A case study of electrical power companies," *Comput Secur*, vol. 61, pp. 32–45, Aug. 2016, doi: 10.1016/j.cose.2016.05.004.

[3] R. E. Santiago Lozada, "Capture the Flag (CTF): Website Tutorial to Boost Cybersecurity Training," *Polytechnic University of Puerto Rico*, 2019, pp. 1,3,4,5,6,7.

[4] H. Hanafi, A. Ahmad, H. Rokman, A. Ibrahim, Z. Ibrahim, M. N. Ahmad Zawawi, and F. Abdul Rahim, "A CTF-Based Approach in Cyber Security Education for Secondary School Students," Electronic Journal of Computer Science and Information Technology, vol. 7, 2021, Art. no. 107, doi: 10.52650/ejcsit.v7i1.107.

[5] S. Wi, J. Choi, and S. K. Cha, "Git-based CTF: A Simple and Effective Approach to Organizing In-Course Attack-and-Defense Security Competition," in 2018 USENIX Workshop on Advances in Security Education (ASE 18), Baltimore, MD, Aug. 2018. [Online]. Available: https://www.usenix.org/conference/ase18/presentation/wi Publisher: USENIX Association.

[6] P. Hulin, A. Davis, R. Sridhar, A. Fasano, C. Gallagher, A. Sedlacek, T. Leek, and B. Dolan-Gavitt, "AutoCTF: Creating Diverse Pwnables via Automated Bug Injection," in 11th USENIX Workshop on Offensive Technologies (WOOT 17), Vancouver, BC, Aug. 2017. [Online]. Available: https://www.usenix.org/conference/woot17/workshop-program/presentation/hulin Publisher: USENIX Association.

[7] K. Chung and J. Cohen, "Learning Obstacles in the Capture The Flag Model," in 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/3gse14/summit-program/presentation/chung Publisher: USENIX Association.

[8] "Overview - CTF 101." Accessed: Nov. 22, 2023. [Online]. Available: https://ctf101.org/web-exploitation/overview/

[9] S. Kucek and M. Leitner, "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments," *Journal of Network and Computer Applications*, vol. 151. Academic Press, Feb. 01, 2020. doi: 10.1016/j.jnca.2019.102470.

[10] A. Nath and S. Xavier, "Issues and Challenges in Two Factor Authentication Algorithms Article in," 2016. [Online]. Available: https://www.researchgate.net/publication/292392168.

[11] "Multi-Factor Authentication | NIST." Accessed: Nov. 19, 2023. [Online]. Available: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication

[12] "Session Management - OWASP Cheat Sheet Series." Accessed: Nov. 20, 2023. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[13] J. Dhanapal, R. Kanimozhi, and D. Jagadeesan, "Authenticating a webpage using CAPTCHA image," International Journal of Advanced Research in Computer Science, vol. 5, no. 7, [Online]. Available: www.ijarcs.info.

[14] Asana. (October 15th, 2022). Agile Methodology. Asana. Available: https://asana.com/resources/agile-methodology.

[15] V. Ford, A. Siraj, A. Haynes, and E. Brown, "Capture the flag unplugged: An offline cyber competition," in Proceedings of the Conference on Integrating Technology into Computer Science Education, ITiCSE, Association for Computing Machinery, Mar. 2017, pp. 225–230. doi: 10.1145/3017680.3017783.

[16] Dr. Muhaini Binti Othman, private communication, October 2024.

[17] H. J. Williams and I. Blum, "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise," RAND Corporation, RR-1964-OSD, 2018. [Online]. Available: https://doi.org/10.7249/RR1964

[18] "CTFd: Open Source CTF Framework," GitHub. [Online]. Available: https://github.com/CTFd/CTFd. [Accessed: 15-Jul-2024].