Secure Web Application for Clinic

Nurshahira Binti Othman
Bachelor Of Information Technology (Hons) In Computer System Security
Universiti Kuala Lumpur
Malaysian Institute of Information Technology
nurshahira.othman@s.unikl.edu.my

Amna Binti Saad
Universiti Kuala Lumpur
Malaysian Institute of Information Technology (MIIT)
1016, Jalan Sultan Ismail, 20250 Kuala Lumpur
amna@unikl.edu.my

***Abstract*— In the era of globalization, technological advancements influence how people live their lives. For example, the online scheduling is an amazing technology add-on for outpatients looking for convenience during their treatment phase. However, the web application must be patched with security to develop a secure system. Rapid Application Development Model (RAD) is the methodology in this project since it is a prototype. This research presents a study of Secure Web Application for Clinic which is a web-based application system developed for allowing the outpatient to make an online booking appointment using the system, and the admin can add a session for the doctor or add a new doctor to the clinic. In addition, the doctor can be remotely updated on the latest session or appointments that have been made. Furthermore, this research paper will study the web's security implementation, which is OWASP's Top 10 2021 guideline for developing a secure web application and protecting the patient's sensitive data, such as their password for authentication, by using a cryptography method, MD5. Finally, this research paper tests the security as it results that the OWASP guideline is significant for assuring the system's reliability and may be implemented as an example by other web developers, particularly when developing web applications for the healthcare industry.**

Keywords—Web Application, OWASP Top 10, Appointment

I. INTRODUCTION

The government has created a small public health institution called the clinic to offer outpatient care. Clinics often only treat minor illnesses like fever, cough, asthma, etc. Since then, the clinic has grown to be a top priority for the sick person's healthcare. The number of patients will rise daily, making the clinic unable to handle the volume of patients at once. These issues gave rise to the concept of creating a system that would assist the general public in reducing queue congestion and clinic wait times. A Secure Web Application for the Clinic was developed to make it easier for the outpatients to register and make an early online booking before receiving treatment there.

The individuals whose health information was inappropriately accessed face several potential harms. First, disclosing personal information may cause intrinsic harm simply because others know that private information. The data collected from the database must be protected because it contains sensitive information such as patient profiles [1]. So, trust should be set up at every step between each participant. Security can be provided by using a general cryptograph for this project for protecting the outpatients' private data and OWASP Top 10 2021 as guidelines for developing a secure web application which is significant for assuring the reliability of the system for the user.

The system's user interface must also be friendly, comfortable, and simple, considering the outpatients will be using the system and the healthcare service providers are comfortable with the system flow. The application uses PHP and HTML as the front end and SQL database as the back end.

The rest of this paper is organized as follows: Section II reviews existing literature on related works by other researchers, Section III gives detail of the methodology, the result is provided in Section IV. Section V contains the conclusion.

II. RELATED WORK

A. *Secure Web Application for Clinic*

Secure Web Application for Clinic is a web-based application that offers a website health-related service. This is to facilitate the patient to make an online booking via the website and choose their respective doctor to attend them during the treatment phase. In addition, this web-based application will allow them to book or cancel an appointment before their routine visit to an outpatient center or clinic. This also will assist the doctor and admin side to have easier access to the patient's data and information before the appointment.

The web application is secured based on OWASP Top 10 2021 [2], specifically 01:2021-Broken Access Control (Directory Traversal and Information Disclosure), A04:2021-Insecure Design (Big Redirect Detected), and A05:2021-Security Misconfiguration (Content Security Policy (CSP) Header Not Set). Furthermore, in order to gain the user's trustworthiness of the system, OWASP Top 10 2021 remediation guidance has been implemented as a basis for security risk assessment and protect sensitive outpatient data such as their password for authentication by using a cryptography method which is the MD5 hash function.

B. *Appointment And Booking System For Clinics*

The Appointment and Booking System for the clinic is a web-based developed to enable the patient to register online using this system. Patients can choose the available dates displayed for booking to get follow-up care. Another function is that patients can see their previous history of treatment records added by a doctor [4].

C. Online Doctor Appointment System

A web-based doctor appointment system has been developed. Both doctors and patients can register themselves, which is monitored by the receptionist(admin). The doctors can login using their username and password and check for patient appointment requests. If the appointment is available, a notification is sent to the patient about the same [5].

D. Developing a Secure Web Application Using OWASP Guidelines

This study evaluates how good OWASP guidelines are in helping developers build a secure Web application. The developed system is then tested using code auditing and penetration testing to identify the achievement of system security for the application [3].

III. RESEARCH METHODOLOGY

In this project, we use the Rapid Application Development Model (RAD) [6] since we will be focusing on prototypes. We might not have to start again every time a new feature was added, or the client rejected a version if we used this process. RAD was designed as an efficient way to establish an application from concept through deployment. Although RAD allows for maximum flexibility and adaptation, the development process is guided by five phases.

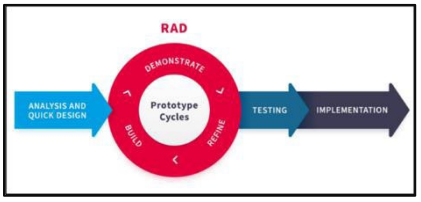

Figure 1: Rapid Application Development (RAD) Model

A. Use case diagram

A use case diagram is a tool for condensing information about a system and the users inside it. It is often displayed as a visual representation of how various system components interact with one another. Use case diagrams will detail the system's activities and the order in which they occur, but they need to go into detail on how those events are carried out.

B. A use case diagram for a patient.

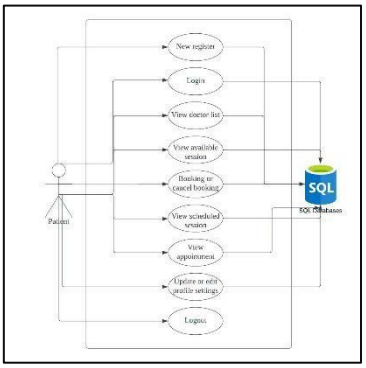

Figure 2: Use a case diagram for patient

C. A use case diagram for a doctor

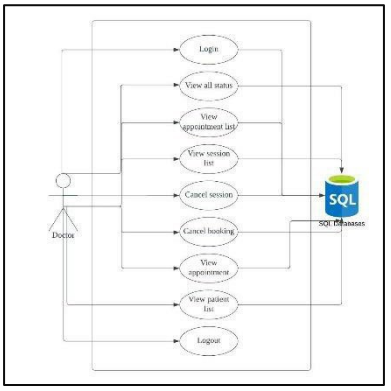

Figure 3: Use case diagram for doctor

D. A use case diagram for admin.

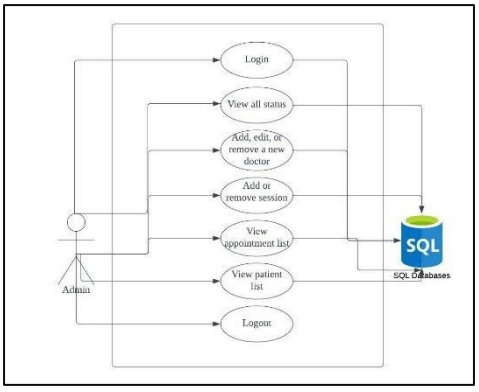

Figure 4: Use case diagram for admin

IV. TESTING AND RESULT

A. Functionality Testing

A functionality test evaluates a software's compatibility with a functionality requirement or specification. Functional tests ensure that the output meets the functional requirements of the software application by delivering the relevant input.

Table 1: Valid Registration

Valid Registration	
Test Case	A patient enters a valid name, address, IC number, date of birth, e-mail address, mobile number, new password, and password confirmation by following the requirements.
Expected Result	The system successfully stores all the patient's data in the database MySQL.
Output Result	Pass

Table 2: Valid Login

Valid Login	
Test Case	The users (patient/doctor/admin) enter their valid registered e-mail addresses and password.
Expected Result	The users (patient/doctor/admin) can access the system.
Output Result	Pass

Table 3: Booking Process

Booking Process	
Test Case	The patient can click Book Now button to book a session.
Expected Result	Booking completed and added in My Bookings History.
Output Result	Pass

B. Security Testing

Security testing is to evaluate the security of a computer system or network by identifying vulnerabilities and assessing the effectiveness of security solutions. It can involve actions like penetration testing, vulnerability scanning, and risk assessments and involves a variety of tools and techniques for finding, assessing, and mitigating security issues. Security testing identifies and assesses risks and vulnerabilities so that the appropriate precautions can be taken to secure the system or network against intrusion or exploitation.

Table 4: Directory Traversal Attack

Tested by	Nurshahira
Test Type	Penetration Testing
Test Case	Directory Traversal Attack
Test Case Number	TC-A1-011
Items to be tested	Web Application for Clinic
Test Result	Pass

Table 5: Information Disclosure Attack

Tested by	Nurshahira
Test Type	Penetration Testing
Test Case	Information Disclosure Attack
Test Case Number	TC-A1-012
Items to be tested	Web Application for Clinic
Test Result	Pass

Table 6: Big Redirected Detected Attack

Tested by	Nurshahira
Test Type	Penetration Testing
Test Case	Big Redirected Detected Attack
Test Case Number	TC-A4-013
Items to be tested	Web Application for Clinic
Test Result	Pass

Table 7: Content Security Policy (CSP) Attack

Tested by	Nurshahira
Test Type	Penetration Testing
Test Case	Content Security Policy (CSP) Attack
Test Case Number	TC-A5-014
Items to be tested	Web Application for Clinic
Test Result	Failed

V. CONCLUSION

Overall, this project has been developed and successfully achieved by following the main objectives that have been explained in Section 1.

Mainly this project is developed to make it easier for patients to register and make an early online booking before receiving treatment there. Thus, to gain trustworthiness from all parties, such as patients, doctors, and admin, to have safe access, trust has been set up to protect the system from being penetrated by the cyber-criminal. In this project, we implement a cryptographic method which is MD to encrypt the users'

password and OWASP Top 10 2021 as a guideline for developing a secure web application. During penetration testing, several vulnerabilities have been found in the system, which is (A01:2021-Broken Access Control) – Directory Traversal and Information Disclosure, (A04:2021-Insecure Design) – Big Redirected Detected and (A05:2021-Security Misconfiguration) - Content Security Policy (CSP) Header Not Set.

Thus, a few mitigations have been implemented to secure every part of the system. Based on my reading and research, existing projects or studies are developing a system to make it easy for patients to make an online booking without considering the security implementation. Hence, this project successfully developed a secure web application for the clinic.

ACKNOWLEDGMENT

All praise is due to Allah, the All-Mighty, the All-Compassionate, and the All-Merciful. This study is a component of the undergraduate capstone project for the Universiti Kuala Lumpur. The author would like to extend her gratitude to her parents, siblings, other family members, friends, and anybody else who helped make this tiny endeavour a success.

REFERENCES

[1] Institute of Medicine (US) Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Nass SJ, Levit LA, Gostin LO, editors. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington (DC): National Academies Press (US); 2009. 2, The Value and Importance of Health Information Privacy.

https://www.ncbi.nlm.nih.gov/books/NBK9579/

[2] What is Owasp? What is the owasp top 10? | cloudflare. (n.d.). Retrieved January 23, 2023, from https://www.cloudflare.com/learning/security/threats/owasp-top-10/

[3] Mohd Nizam Osman. (2009). Computer and Information Science. Developing a Secure Web Application Using OWASP Guidelines.

https://www.researchgate.net/publication/42385691_Developing_a_Secure_Web_Application_Using_OWASP_Guidelines

[4] Mohammad Syafiq bin Mohd Razadi. (n.d.). APPOINTMENT AND BOOKING SYSTEM FOR CLINICS. https://myfik.unisza.edu.my/www/fyp/fyp18semkhas/report/041471.pdf

[5] Venkatesh Rallapalli. (2022). Online Doctor Appointment System. International Journal of Engineering Research and Applications.

https://www.ijera.com/papers/vol12no4/Ser-3/I1204034852.pdf

[6] Shah, K. (n.d.). A guide to the rapid application development | Thirdrock Techkno. Third Rock Techkno. https://www.thirdrocktechkno.com/blog/what-is-rapid-application-development/