BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN COMPUTER SYSTEM SECURITY 2022

E-LEARNING: SECURING WEB APPLICATION HACKING AND IMPLEMENTATION ON THE VULNERABILITIES

ANNIS EZZA ELLYANA BINTI SHAHARIN
(52215220025)

UNIVERSITY KUALA LUMPUR

JANUARY 2022

E-LEARNING: SECURING WEB APPLICATION HACKING & IMPLEMENTATION HARDENING ON THE VULNERABIILITIES

ANNIS EZZA ELLYANA BINTI SHAHARIN

(52215220025)

Report submitted in fulfilment of requirement for the Bachelor of Information Technology (Hons.) in Computer System Security
University Kuala Lumpur

JANUARY 2022

DECLARATION

I declare that this report is my original work and all references have been cited adequately as required by the Universiti Kuala Lumpur. Unless otherwise indicated or acknowledged ad reference work. This topic has not been submitted to any academic institution.

In the event that my thesis, be found to violate the conditions mentioned above. I voluntarily waive the right of conferment of my degree and be subjected to disciplinary rules and regulations of Universiti Kuala Lumpur.

Date: 10.06.2022

Signature:

Full Name: Annis Ezza Ellyana Binti Shaharin

ID Number: 52215220025

APPROVAL PAGE

We have supervised and examined this report and verify that it meets the programmed and University and University's requirement for the Bachelor/ Diplomain (2022).

Date:

Signature:

Supervisor's Name: Mardiana Binti Mahari

Date:

Signature:

Assessor Name: Ts. Norsuhaili Binti Seid

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious, the Most Merciful, and all praise to Allah for giving us strength, patience, guidance, and beneficial knowledge along our journeyin completing the final year report project.

I sincerely would like to express my deepest gratitude towards my supervisor Madam Mardiana Binti Mahari who are very keen and energetic in supporting and giving valuable advice, guidance, and feedback regarding the error that I had made along the process in completing the Final Year Project (FYP) research paper. She motivates me to work hard and believe that I can achieve on what I was doing. Her advice was beneficial and helpful in so many ways and her encouragement help mein keeping me on track along my journey in the completion of the Final Year Project (FYP) research paper. I'd also like to express my appreciation towards my campus which is the Universiti Kuala Lumpur - Malaysian Institute of Information Technology (UniKL MIIT) for providing me with a conducive learning atmosphere or laboratory formy experimental observation as well as all of the necessary resources for me to complete this research project.

I also would like to show my appreciation towards my family and friend who are very supportive from the start until the completion of my research paper. Their support was meaningful since they had helped me in going through a phase where I’m mentally and physically exhausted. Lastly, I would like to thanks to all my respondents and participant who is very correspondingly cooperating with me through all the process of my research project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLE

ABSTRACT

Over the past few years, there has been a worrying trend of increment in number of web application intrusions. Based on reports released by reliable sources, these incidents are due to the lack of experts in performing accurate risk assessment to mitigate the risk while performing web security testing. Risk assessment is the core process in providing appropriate recommendations when dealing with vulnerabilities discovered in a web application. To overcome this problem by developed E-learning platform to give awareness to new learner and student on how to hardens the vulnerabilities. Therefore this research paper will be highlighting the problem of insufficient experts to guide the less experienced information security analyst in conducting effective risk mitigation and countermeasure on the vulnerabilities. The objective of this research will be to develop secured E-learning platform for beginner to learn secured web application based on selected OWASP ranking. The E-learning platform system will cover lab and how to hardens the vulnerabilities based on OWASP Top 10 ,such as crossite scripting, open redirection, SQL injection, Unrestricted file upload and broken access. The target user will only be the less experienced, student and new learner. The methodology used in the research would be based on the rapid application development . The main activity conducted is the construction of knowledge based of e-learning platform system by develop the case study, quiz and video countermeasure .The results, user will gain knowledge and information in cybersecurity using e-learning system.

LIST OF ABBREVIATIONS

UNIKL MIIT - University Kuala Lumpur Institute of Information Technology

CSS – Crossite scripting

PenTesting - Penetration Testing

SQL Injection – Structer Query Langguage

CVE - Common Vulnerabilities and Exposures

URL - Uniform Resource Locator

PHP – Hypertext Preprocessor

CSS – Casscading Style Sheet

CHAPTER 1: INTRODUCTION

1.1 Background

In this era, technology areas human job. Everything has been done systematically which save humans energy and consume less time to accomplish a task. Besides that, technology has given numerous benefits to this society, but it has many disadvantages as well which will be encountered by the user if not using it securely. The goal of the project is to give a knowledge and benefit for student and new learner about a web application to identify the vulnerabilities in their product/system and provide a list of countermeasures to resolves the bugs. E-learning Securing Web Hacking Security and Implementation Hardening On The Vulnerabilities is application that is purposefully insecure. Web security enthusiasts, developers, and students can use it to identify and avoid web vulnerabilities. This e-learning web application training curriculum prepares individuals to carry out successful penetration testing and ethical hacking initiatives. This project is a E-learning web application is a software project that incorporates security vulnerabilities on purpose for educational reasons for students and newcomer on cybersecurity industries. Moreover, this project focused on 5 vulnerabilities from the OWASP Top 10 security, such as:

I. **Injection, find for SQL Injection, SQL injection, or SQLI,** is a common attack vector in which malicious SQL code is used to change backend databases and get access to information that was not intended to be revealed. This information could range from sensitive corporation information to user lists to private customer information.

II. **Cross-site scripting, discover for POP-UP XSS** Injection attacks, often known as cross-site scripting (XSS), are attacks in which malicious scripts are injected into otherwise trustworthy and harmless websites.XSS attacks When an attacker uses an online application to send malicious code to a separate end user, usually in the form of a browser side script, this is known as a cross-site scripting attack. In addition, this platform features

III. **Unrestricted file upload vulnerabilities,** An attacker can use the programme to upload or send damaging data that is automatically processed within the product's environment. The term "unrestricted file upload" is used in vulnerability databases and other places, but it isn't precise enough. When an application allows a user to directly submit a malicious file to be run, this is known as a local file upload vulnerability. When a programme uses user input to download a remote file from an Internet site and save it locally, this is known as a remote file upload vulnerability.

IV. **Open Redirection Vulnerabilities,** Open redirection vulnerabilities arise when an application includes user-controllable data into the target of a redirection in an unsafe manner. An attacker can establish a URL within the programme that leads to any external domain**.**

V. **Broken Access Control,** If authentication and access limitations aren't adequately enforced, it's simple for attackers to take anything they want. Due to access control vulnerabilities, unauthenticated or unauthorised users may get access to sensitive data and systems, as well as user privilege settings. It is difficult to uncover configuration flaws and unsafe access control measures since automated processes cannot always test for them. While penetration testing may detect a lack of authentication, other techniques are necessary to find configuration flaws. Using secure coding approaches and preventive measures such as administrative lockout, it is possible to avoid weak access limits and credential management issues**.**

1.2 Problem Statement

There is no platform E-learning suitable on securing web hacking for student and beginner. Based on the evaluation, Users need a very friendly interface E-learning platform. There are several users are not from IT security courses, it can help people to learn and to increase their knowledge. This E-learning provide a practical exercises task to develop higher order learning and critical thinking.

People nowadays lack of knowledge to secure web application.Due the current situation the risk of web application attack are very high. Current attack on web application can impact business risk. For the example, latest news it’s from company FireEye on web application. The impact of the company from the attack is decrease the investor and also lack of the trust issue from the end user. From the journal of Computer and Science System, The exponential growth of Internet interconnection has led to a significant rise in cyber-attack incidents, many of which have disastrous and deadly consequences. Malware is the most prevalent weapon used to carry out malicious activities in cyberspace, either by exploiting existing weaknesses or by utilising the unique qualities of emerging technologies.

There are various platforms to analyse cyberattacks with no countermeasures. Therefore, this project concept is E-learning that gives an idea to the user on how and which security countermeasures can solve the bugs. The E-learning platform is different from the other web application. For the example, BWAPP it does not contain features to solve all the vulnerabilities. The BWAPP target for the user is for professional security researcher but for this E-learning platform is for students and new learner.

1.3 Objective of Study

1) To study on how to create a platform to educate student and new learner on how to secure the web application by implement the OWASP top 10 vulnerabilities
2) To develop secured E-learning platform for beginner to learn secured web application based on selected OWASP ranking.
3) To test E-learning platform

1.4 Scope

The target system for this project is student and the beginners, who wants to gain knowledge in security platform. E-learning can be used in two ways: to display educational content and to facilitate educational processes. This project is to increase information retention, and to create platform with interesting and engaging teaching methods is essential.

1.4.1 The function of the system

- From the code (source code of a website) the system will scan the entire code and produce a result to analyzing/discovering the vulnerabilities or bugs. From that, the user able to solve the bugs by refers the countermeasures as given in the output/result.
- E-learning Web Application Hacking Security & Implementation Hardening on The Vulnerabilities is crucial for keeping hackers and cybercriminals from obtaining access to sensitive data
- The goal of E-learning website security is to Avoid these (and other) attack kinds. Website security is more formally defined as the act or practise of protecting websites against unauthorised access, use, modification, destruction, or disruption.
- Features for this education web application is provide testing and review the solution of **SQL injection, Cross-site scripting discover for POP-UP XSS, Unrestricted file upload vulnerabilities, Open redirection Vulnerabilities and Broken Access Control.** The primary main is to assist security new learner and students in testing their abilities and technologies in a legal setting. This education platform is a simple environment as possible by developing a feature add-on that can be readily implemented.
- Features for this education platform is penetration testing vulnerabilities Top 10 OWASP. A penetration test is a hands-on inspection conducted by a real person to discover and exploit flaws in your system.
- Hardening vulnerability’s part is using video and give the explanation on PDF file to explain the solution. These websites, especially currently,

serve to make the learning process more enjoyable and appealing to students.

1.5 Significant of Project

This project gives a new learner on security field a confidence to boost in their finding vulnerabilities. The Beginners who want to gain knowledge in the security field by providing tutorials, exercises, and many more to improve the level of security skills my using concept E-learning on the system. This project building an amazing GUI interface that the user can access easily and understand the steps on what to do next and give the solution on how to hardens the vulnerabilities.

Automation makes it easy for the user in this platform, The automated has made it easier for user to do security assessments on websites and web applications with minimal setup and integration. The task that used to necessitate a thorough understanding of the online application can now be completed automatically by the web application scanner.

This E-learning web application will provide guideline on how to use this platform. The module has the guideline video and PDF file on how to solve the solution on each vulnerability. The second advantage is that users may take the course anywhere, since the courses are kept on web applications and are available 24 hours a day, seven days a week. They may access this platform via devices such as laptops, desktop PCs, etc. In addition, the user may read the rules, obtain online case study materials, enrol in courses, and rapidly develop their cybersecurity expertise.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

In this chapter will involved with the study, design, development, implementation, and assessment of an e-learning management system to create a user-friendly environment for potential students to gain information at any educational level.. From the research (Berners-Lee, 2020) Trinidad and Tobago's education system has a real chance to advance in terms of digital infrastructure and digital education, as smaller countries have the best chance of achieving system-wide transformations. E-learning is a relatively new concept in education system, but with proper design and implementation based on existing e-learning applications, a world-class digital education programme can be established and implemented

Nowadays, there are various web applications for security scanning especially for beginners who want to gain knowledge in the security field by providing tutorials, exercises, and many more to improve the level of security skills. Besides that, this project E-learning Securing Web Hacking Security and Implementation Hardening on The Vulnerabilities focused on e-learning for beginners which the user can discover the vulnerabilities of a system. Moreover, this project building an amazing GUI interface that the user can access easily and understand the steps on what to do next.

The existing security scanning web application, BWAPP, DVWA and GRABBER have few similar techniques compared to this project which is E-learning Web Application Hacking Security and Implementation Hardening on The Vulnerabilities. Besides that, the data collected from the existed s concluded to give an advanced security scanning web application to users who can access it effortlessly.

This web application security is an exercise method of protecting websites and web applications from being hacked or gaining unauthorised access. This E-learning Web Security is provided challenging module task, and to secure websites and applications, there are many factors that go into web security and web protection, such as staying up to date on new threats and how to mitigate them in the real world in industries cyber security.

2.2 E-Learning Technology

E-learning is a phrase used to describe a new kind of user training. Compared to conventional instructional approaches, it boosts users' knowledge not only in schools but also in businesses. In educational environments such as continuing education, business training, and academic courses, e-learning happens.

E-learning is a relatively new method of acquiring knowledge mostly via the Internet. Web apps and online education Platforms are essential, since billions of people depend on them to do mundane jobs. The accessibility, user-friendliness, and pervasiveness of Web apps have rendered them susceptible.

Initially, all papers and resources (eBooks, videos, articles, photographs, etc.) are stored on a website to make it simpler for consumers to connect directly and use them fast. Users may use multi-media devices such as laptops, PCs, and mobile phones, for instance. With a high-speed internet connection, users may effortlessly connect to websites and access online course materials.

The e-learning environment helps organisations, schools, and enterprises reduce the upfront expenditures associated with adopting software and training people. They do not need to spend a substantial amount of money on data storage memory.

2.3 E-LEARNING MANAGEMENT SYSTEMS ASSESSMENT

E-learning is fundamentally characterised in a variety of ways due to the diversity of its users, each of whom has their own idiosyncrasies and area of applicability. In terms of its inception and evolution as a training instrument, e-learning systems exhibit a pedagogical and technical duality.

The whole teaching-learning procedure is technological in the sense that it relies on web-based software tools. From the perspective of its application, one can identify the vision of its end users, namely that, regardless of their age and level of education, they would see the e-learning system as a source of services that will assist them in meeting their educational obligations. The scope of e-learning may be restricted if it is defined as "the use of Internet technology to offer a variety of knowledge- and performance-enhancing solutions" (Rosenberg, 2010). The fundamental requirements are:

- The e-learning network allows instruction or information to be immediately updated, saved, retrieved, disseminated, and shared.
- It is sent to the end user via computers and normal Internet infrastructure.
- It is concerned with a broader vision of learning that extends beyond traditional training paradigms.

Based on the research there are three of these websites, Khan Academy (https://www.khanacademy.org/), Moodle (https://moodle.org/), and Memrise (https://www.memrise.com/), had design elements and features that can incorporate into the project. According to (Patel, 2019), I would want to incorporate the following elements of educational websites based on Khan Academy, Moodle, and Memrise:

1) **Evaluation:** Utilize exams and quizzes incorporated within a course for continual student assessment. According to (Hattie & Timperley, 2007), feedback should address three questions: (What are the objectives?), (How is progress being made toward the goal?), and (What actions must be performed to achieve greater progress?).High Quality Content– Limiting the size of modules for courses will increase learner

engagement because smaller modules have a better sense of progress, will ensure hands-on learning by incorporating interactions and activities, and will make the website more engaging by using images and graphics visuals.

2) **Online Enrollment**– A sign up or login page for students and users is required on an e learning website.
3) **Reports and Analytics**– By analyzing data from online reports of user online behavior and activities, an assessment can be made to determine whether the site is providing the desired environment and content to the users.
4) **Social Community**– The majority of people spend a significant amount of time on social media. Including a discussion forum for all users will improve their social interactions.
5) **Support for Learners in a timely manner**– Details of technical support and email contacts must be included so that all users can receive assistance (Wang, 2019).

2.4 Introduction Element Of E-Learning Platform.

2.4.1 Graphic User Interface in E-Learning

The interface design for e-learning is crucial because learning efficacy and interface design are intricately related. The design of an e-learning interface should be influenced by how users learn and the activities they are required to do inside the programme. Some components of the user interface continue to be inefficient. The graphical user interface (GUI) allows users to engage with e-learning courses via the use of graphical components.The primary function of a Graphical User Interface (GUI) in an eLearning course is to assist learners in navigating the course without difficulty.

The essential guidelines for creating graphic users on an E-learning platform are much simpler for novices to follow. It allows you to effortlessly transfer data across applications using cut-and-paste or drag-and-drop. It requires considerable memory and processing power. Expert users may find it slower to use than a command-line interface.

2.4.2 WordPress

WordPress is an open-source content management system (CMS) that simplifies website creation and administration. It is the world's most used content management system. Every day, millions of company owners, bloggers, and publishers use WordPress to manage their online presence. The greatest benefit of utilising the WordPress platform is that no technical skills are required to publish content online. WordPress stores and organises all data in a database, from the text of your posts and pages to your user accounts and site URLs. This is what makes WordPress such a quick and efficient web publishing platform.

The WordPress platform is entirely free for both business and personal usage, with no catches. This programme is free because it is totally maintained by volunteers contributing to an open-source initiative. Open-source software differs from other physical items since nobody owns WordPress. It is thus totally dependent on volunteers for its maintenance, support, and development.

2.4.3 Bootstrap

Bootstrap is an HTML, CSS, and JS package that aims to facilitate the creation of informative web pages (as opposed to web apps). Include it in a web project primarily to apply Bootstrap's colour, size, font, and layout choices to the project. Bootstrap is a framework that makes it easier and quicker to develop websites. It includes HTML and CSS design templates for, among other things, typography, forms, buttons, tables, navigation, modals, and image carousels. Additionally, JavaScript plugins are supported.

2.4.4 Wix

Wix provides customizable website templates and an HTML5 website builder with capabilities like applications, graphics, picture galleries, fonts, vectors, and animations. Moreover, individuals may construct their own websites from scratch. Wix is a website builder, a simple tool that allows you to develop an online presence quickly using a drag-and-drop interface without the need for coding or FTP knowledge. To begin using Wix's site hosting, you just need an email address. Indeed, if you don't mind the advertisements, you may start a free website.

2.4.5 PHP Language

PHP (Hypertext Preprocessor) is a programming language designed for constructing dynamic and interactive webpages. It was one of the first server-side languages to be integrated in HTML, making it possible to add functionality to web sites without accessing other files.

This web-based e-learning system is developed using PHP, JavaScript, Bootstrap templates, jQuery, and MySQL as the database. This method is quite useful, particularly for the creation of online classes, exercises, and quizzes.

It is straightforward to understand and implement; one of the key reasons PHP has grown so popular is because it is simple to get started with. Most individuals can rapidly construct a web page with a single PHP file, even without considerable expertise or experience in web programming. PHP has fewer entry barriers than many other programming languages due to its simple syntax and the ease with which command functions may be taught.

PHP language's versatility PHP is platform neutral, meaning that it operates on Mac OS, Windows, and Linux and is compatible with the majority of web browsers. Additionally, it supports all major web servers, making deployment on a range of systems and platforms simple and inexpensive.

2.5 Analysis and Design of a Learning Management System Database

To construct a database for the educational platform, there must be a rule-compliant structure including several items. Additionally, there must be linkages between the tables and the right data type must be selected for the mentioned fields. Objects consist of two kinds of tables and stored procedures that will be utilised to build the database for the electronic learning platform. There have been constructed tables, Because the educational platform is largely centred on courses, a table is required to handle the construction of courses, which will consist of video and text files. Therefore, a separate table must be created for text files and another for video files.

Due of the instructional aspect of this platform, several new assignments will be introduced. When there are too many courses without regulation, a multitude of issues arise. In order to organise and structure the educational platform, we have built a dedicated table for (searching for a certain) course. In addition, it is necessary to design and develop supplementary tables, such as a help table, an articles table, etc. A stored procedure is a function of SQL Server. The following are the benefits of adopting stored procedures: On the side of database maintenance, the test side and its speed are substantially quicker than ordinary commands, and the database is also extremely secure. Below is an example of a database built on the platform of an E-learning system.

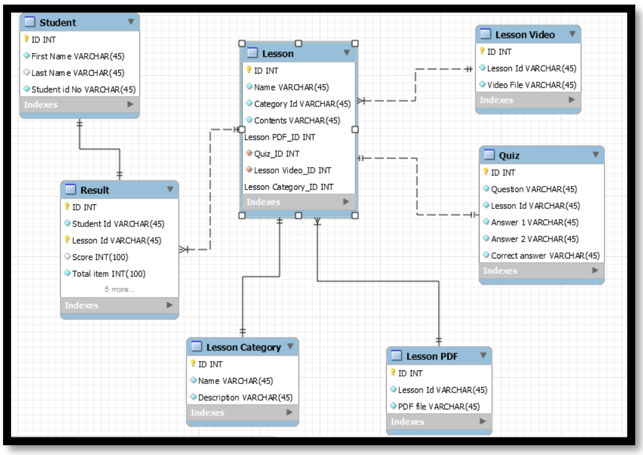


Figure 2: Management System Design Database

2.6 Multimedia for E-learning.

Multimedia material adds to the development and diversification of the learning process, resulting in greater retention of information. Educational video may boost the likelihood that students and users will interact with the subject. Video-based course material may assist students from all around the globe.The advancement of multimedia and information technologies has also influenced the manner in which education is imparted. This development has resulted in increased adoption of e-learning systems and the integration of multimedia content into e-learning systems. This article discusses a model for developing e-learning systems that incorporate multimedia content.

Graphic

A graphic is a digital representation of non-textual information, such as a sketch, chart, or image. Graphics serve a number of functions, from enhancing the visual appeal of Web sites to serving as the presentation and user interaction layer for fully-fledged Web applications.

Examples of graphics include maps, pictures, designs and patterns, family trees, diagrams, architectural or engineering plans, bar charts and pie charts, typography, schematics, line art, and flowcharts, among many more.

Diverse visual use cases need unique solutions; hence, a range of technologies are accessible. While PNG is the optimum format for images, SVG and the Canvas API are required for interactive line art, data visualisation, and even user interfaces. CSS was developed to augment formats like HTML and SVG. Webcams meet the technical illustration and documentation needs of several sectors.

Audio Sound

Incorporating audio into a multimedia application may offer the user with information unavailable via any other way of communication. Certain sorts of information cannot be presented successfully without sound. It is virtually hard to correctly convey in writing a bear's heart or the ocean's roar.

In addition, audio may facilitate the user's understanding of information delivered in another medium. A narrative might, for instance, be used to narrate what is observed in an animated clip. This may aid the user in comprehending the application's objective and lead to enhanced comprehension. Experts in the field of learning have determined that providing information to several senses enhances subsequent recall. Moreover, it might boost the user's interest in the content.

There are several audio formats available. Today, red book audio is arguably the most popular audio format. This is the industry-standard word for audio compact discs for consumers. It is an internationally recognised standard, formally designated IEC 908. Due to the colour of the booklet explaining its forms, this standard is known to as the red book audio. In addition, red book audio sound may be used in multimedia applications, where it serves as the basis for the highest-quality sound accessible.

Windows wave files are another sort of audio file that can only be played on machines running the Windows operating system. A wave file includes both the digital data necessary to play the sound as well as a header that specifies the resolution and playback rate. Wave files may include any sound that a microphone is capable of recording.

Musical Instrument Digital Interface, or MIDI, is the last sort of audio sound that may be used. The MIDI format is a standard produced by musical instrument manufacturers. Rather than a digital representation of the sound, the MIDI standard is a set of signals that signify the played musical note. The MIDI standard only allows the storage of musical notes. Sequencers are used to make MIDI music.

Animation

The word "animation" refers to moving visual pictures. The movement of a person practising cardiopulmonary resuscitation is considerably more instructive than a static picture. Similarly to how a static visual picture is an effective means of communication, so too is animation. Movement-related topics are especially well-suited for animation.

Concepts like as playing the guitar or golfing are difficult to convey with a single image or even a sequence of photos, and are considerably more challenging to describe in language. The presentation of various aspects of your multimedia application is simplified by animation.

Video

A video may deliver a substantial amount of information in a short amount of time. Video helps you to express more information in less time compared to writing. Because video is more appealing to the senses, it may simultaneously present and communicate more information.

Videos improve student motivation, which leads to academic achievement. Students will absorb and recall the subject more successfully if they are interested in it. They allow you to stop, rewind, or skip the movie to facilitate class discussions or study certain areas.

2.7 Quiz

Quizzes in e-learning are used to monitor, report on, and assess student progress and outcomes. A quiz at the conclusion of a course serves as a graded assessment. Meanwhile, a mini quiz at the end of each course seeks to reinforce essential topics before moving on to new material. In other words, mini quizzes are utilized to determine whether or not learners have successfully assimilated the material before proceeding to the following segment.

Writing appropriate eLearning quiz questions is crucial to success in both evaluation and knowledge retention. Interim quiz results equip students for reaching their course goals and offer them an indication where they have to make a push. Quizzes also enable Instructional Designers take performance snapshots, adjust their techniques on the fly and, eventually, lead to improved eLearning

The benefit of quiz in e-learning platform can enhance the retention and transfer of knowledge. The quizzes ask you to recall previously acquired material to mind. By recovering information, you organize it and establish cues and connections. Repeated over time, knowledge that is often retrieved becomes more retrievable in the future. It also can motivate learner by learners to stay focused and keep going forward. It can challenge student perceptions to stir up their attention by posing a question that they are likely to be inaccurate.

2.8 Create Quiz In E-learning Platform

2.8.1 Kahoot

Due to the plethora of new tools and apps accessible in the virtual world, contemporary education has become more pleasant. Among them is Kahoot. It is a learning programme that aids learning through engaging games, quizzes, and a variety of other activities. Within minutes, it is possible to design and distribute quizzes. With this software, organising quizzes and games is straightforward.

Kahoot! is a game-based learning platform that may be used to test students' knowledge, as a formative assessment instrument, or as a classroom distraction. Fifty percent of K-12 students in the United States utilise one of the most popular game-based learning systems, which has 70 million monthly active unique users.

2.8.2 Quizlet

Quizlet is a web-based application designed to help students learn via the use of interactive tools and activities. The objective of Quizlet is to help students practise and master their coursework. Quizlet platforms aid students in exam preparation. With the offered interactive study tools and differentiation possibilities, Quizlet allows students to learn knowledge in a number of ways. Instead of reading over notes, doing worksheets, and generating flashcards on paper, students may just log in and begin learning. In addition, students using mobile devices may download the Quizlet app to study content at any time and from anywhere.

2.8.3 Evaluation

Evaluation is a crucial element of any e-Learning course or programme that aims to foster continual progress. Evaluation permits the determination of e-quality, Learning's effectiveness, and continuous advancement, as well as the comprehension of the benefits and drawbacks of e-Learning courses or programmes, so that they may be enhanced.

By having an assessment, the E-learning will have clear context communication, user-friendliness, and simple navigation. Users will be able to quickly browse to each portion and have obvious navigation pathways to key areas.

2.9 Top 10 OWASP Vulnerabilities

The OWASP Top 10 is an online publication on the OWASP website that rates and examines the ten most severe web application security concerns. International security experts have reached an agreement on this study. Risks are graded based on the frequency with which security issues are identified, their severity, and their potential effect. The goal is to educate developers and web application security experts about the most prominent security concerns, so that they may implement the report's findings and suggestions into their security processes, therefore lowering the existence of these recognised hazards in their applications.

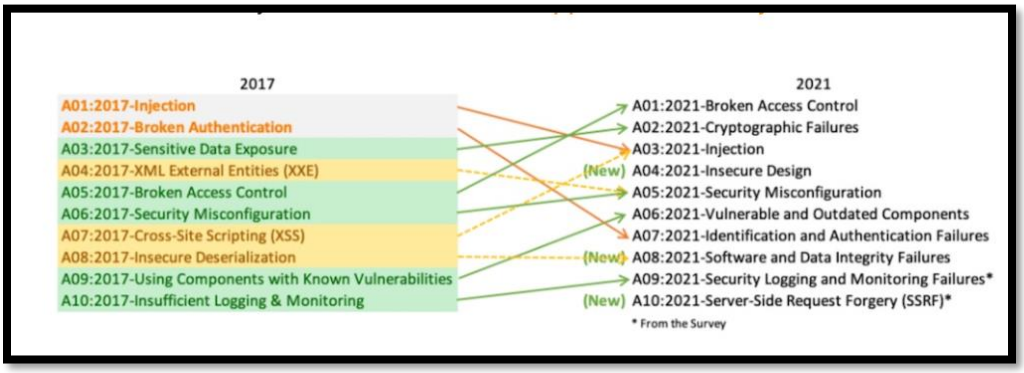

2017
A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring
2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*
* From the Survey

Figure 1.0 Top 10 OWASP

2.9.1 Injection, find for SQL Injection

SQL injection, often known as SQLI, is a common attack vector wherein malicious SQL code is used to change backend databases and get access to data that was not meant to be exposed. This information may include sensitive corporate data, user lists, and private consumer information.

2.9.2 Cross-site scripting, discover for POP-UP XSS

Cross-Site Scripting (XSS) attacks are injection attacks in which malicious scripts are injected into otherwise reputable and harmless websites. An XSS attack occurs when an attacker uses an online application to communicate malicious code to a different end user, often through a browser-side script.

2.9.3 Unrestricted file upload vulnerabilities

The programme enables an adversary to upload or transport malicious data that can be automatically processed inside the product's environment. The term "unrestricted file upload" is used in vulnerability databases and other contexts, although it is inaccurate. A local file upload vulnerability exists when an application allows a user to submit a malicious file directly for execution. When a software utilises user input to download a remote file from an Internet site and store it locally, a remote file upload vulnerability exists.

2.9.4 Open Redirection Vulnerabilities

Open redirection vulnerabilities occur when an application mixes user-controllable data into the destination of a redirection in an unsafe manner. An attacker may establish a URL inside the programme that leads to any external domain.

2.10 Issues and Challenge in Implementing E-Learning

E-learning may enhance training techniques in several contexts, such as long-distance learning, part-time training, academic courses, etc. Students and staff may actually study courses, take examinations, and provide comments or homework assignments through the internet. This innovative approach has the potential to give high-quality education to a vast number of individuals while saving students money, time, and effort.

Examining the sector as a whole indicates a great deal of optimism, with figures for the E-Learning market in 2020 predicting tremendous expansion. However, educators throughout the globe are aware of the industry's most pressing problems. The consumer faces several hazards and disadvantages while using an E-learning platform. To increase the efficiency of e-learning, it is necessary to overcome several difficulties. The obstacles and difficulties associated with adopting E-learning are:Lack of graphic user interface, The Daily Mail is an example of a news website that is packed with advertisements, automatically playing videos, and clickbait articles vying for your attention. The homepage is a jumble of articles, self-playing videos, a popup asking for permission to receive alerts, links to social media profiles, additional clickbait headlines, and clickbait photographs of attractive women. It's a jumbled mass that's difficult to traverse. Initial content creation necessitates substantial investment. The result is a site that is hard to navigate and use.

Aside from that, the website loads slowly due to heavy traffic: A web server can only handle requests from a certain number of users at any given level. Once that threshold is exceeded, the website will load more slowly. The slower a website is, the more visitors it has. As website traffic increases, server providers may need to devote more resources to the site. Too many HTTP Requests may cause a website to load slowly: The number of HTTP requests will grow if a website has a large number of JavaScript, CSS, and picture files.

Each time a user views the site, the browser makes an excessive number of requests to the server to load an excessive amount of files. Obviously, this would result in a slower website load time.

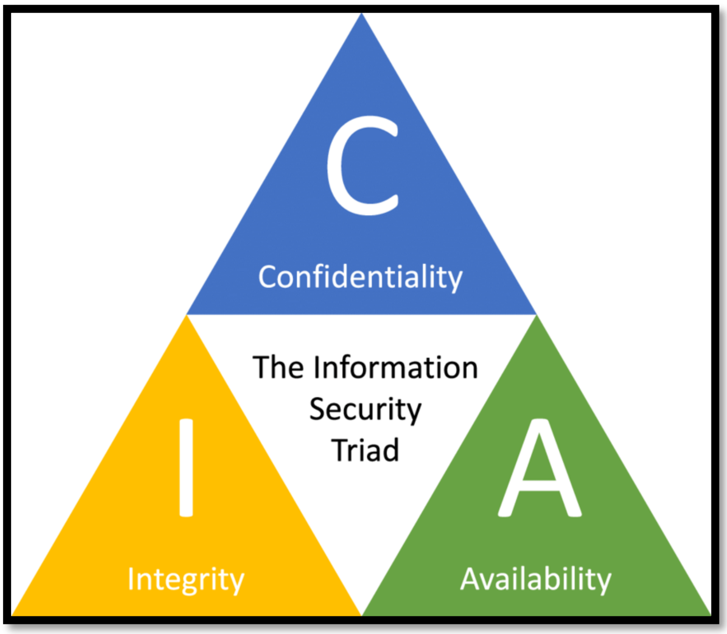
The E-learning content or images are of poor quality. The basic purpose of image formatting is to strike a balance between file size and acceptable quality. Almost all of these optimizations can be performed in more than one method. To avoid poor image quality is choose the right file format by implement PNG can creates images of superior quality, but at the cost of a bigger file size. Was designed as a lossless picture format, but it is also capable of lossy compression. JPEG employs both lossy and lossless compression. You can alter the quality setting to get a fair balance of file size and quality. Other than that, IF - utilizes a maximum of 256 colors. It is the optimal option for animated visuals. It makes no use of lossy compression.

Low standard writer content, from the research, in general low-quality websites, e-learning and pages share these three characteristics. A low-quality page looks unattractive and immediately conveys the message "Low trust." Simply by looking at the design, typography, and overall look and feel, user begin to feel uneasy. Other than that, the content is not succinct or exhaustive. Simply by reading a few sentences, user can determine whether the content was generated by a script or a machine and was not proofread by a human eye. The content appears to have been generated automatically and not by hand. The page contains numerous pop-up windows, third-party scripts, banner advertisements, and other obtrusive elements that detract from the user experience and force you to click on something before you can read anything on the page.

Furthermore, **Security issues and certification problems,** Keeping E-learning Having current safety features is an essential to begin with. For instance, WordPress users should update their plugins to the most recent version at regular intervals. Secure e-learning online The ingenuity of threats never ceases to increase. These dangers, adepts in disguise and deceit, are always evolving to irritate, steal from, and destroy the system. The number of online security threats to e-learning is rising at now.

There are several types of dangers that are directly or indirectly related to an e-learning system. Online Social network sites threats, On occasion, hackers upload harmful code directly into a social networking site, including through adverts and third-party programmes. On Twitter, shortened URLs may be exploited to fool users into accessing malicious websites that, when viewed from a work computer, can harvest sensitive data.

2.11 Security Elements On E-leaning Platform



\

Figure 2.1 Confidentiality, Integrity, And Availability

Three important pillars serve as the cornerstone of information security. Every information technology service must meet the fundamental criteria of confidentiality, integrity, and accessibility (CIA). Confidentiality prevents unauthorised access to information, integrity prevents unauthorised modification of information, and access is accessible to the intended receiver (Stamp, 2006). In order to assure a safe system, Edible et al. (2006) added three extra information security services to the CIA's three basic pillars.

Identification and authentication provide accurate verification during the log-on procedure. Authorization guarantees that a user may only access data for which they have authorization. The non-repudiation principle guarantees that system users are held responsible for their activities.

2.11.1 ReCAPTCHA

In 2013, a Carnegie Mellon University research team produced a ground-breaking article that described a variety of software algorithms that could distinguish humans from machines. This group also came up with the catchy acronym. As CAPTCHAs established the de facto standard for Internet security, Luis von Ahn, a member of the original research team, was more concerned about how much time was being wasted on these tiny puzzles. Von Ahn claimed that humanity as a whole was wasting 500,000 hours per day on CAPTCHAs in a fantastic 2011 TED Talk.

ReCAPTCHA is a free programme that guards against spam and abuse on websites. It distinguishes between humans and bots using advanced risk analysis algorithms. reCAPTCHA works by presenting any of the scanned words that aren't recognised to a human for interpretation alongside a known term. You authenticate yourself as a human by successfully typing the known word, and the reCAPTCHA system gets some confidence that you have correctly digitised the second.

By implementing reCAPTCHA on an E-learning platform, hackers are prevented from abusing internet services by stopping automated software from sending fraudulent or harmful online requests. Protect the integrity of online polls by preventing hackers from utilising robots to submit repeated fraudulent replies.

2.11.2 Add HTTPS and an SSL Certificate

SSL certificates enable websites to convert from the less secure HTTP protocol to the more secure HTTPS protocol. An SSL certificate is a data file held on a website's origin server. SSL certificates allow SSL/TLS encryption by include the website's public key, identity, and other information.HTTPS helps avoid Man in the Middle (MitM) attacks, but they can still happen if someone can impersonate E-learning website SSL/TLS certificate. To avoid E-learning, check certifications issued for websites that aren't recognised. With Certification Authority Authorization (CAA) resource records, it's also possible to limit who can issue certificates for E-learning website domains.

2.12 Add HTTPS and an SSL Certificate

From the research, there are various web applications for security scanning especially for beginners who want to gain knowledge in the security field by providing tutorials, exercises, and many more to improve the level of security skills. Besides that, this project E-learning Securing Web Hacking Security and Implementation Hardening on The Vulnerabilities focused on e-learning for beginners which the user can discover the vulnerabilities of a system. Moreover, this project building an amazing GUI interface that the user can access easily and understand the steps on what to do next. The existing security scanning web application, BWAPP, DVWA and GRABBER have few similar techniques compared to this project which is E-learning Web Application Hacking Security and Implementation Hardening on The Vulnerabilities. Besides that, the data collected from the existed s concluded to give an advanced security scanning web application to users who can access it effortlessly.

2.12 Summarization Comparison Between Web Application and E-learning Web Application Hacking Security and Implementation Hardening On The Vulnerabilities

From the research, there are various web applications for security scanning especially for beginners who want to gain knowledge in the security field by providing tutorials, exercises, and many more to improve the level of security skills. Besides that, this project E-learning Securing Web Hacking Security and Implementation Hardening on The Vulnerabilities focused on e-learning for beginners which the user can discover the vulnerabilities of a system. Moreover, this project building an amazing GUI interface that the user can access easily and understand the steps on what to do next. The existing security scanning web application, BWAPP, DVWA and GRABBER have few similar techniques compared to this project which is E-learning Web Application Hacking Security and Implementation Hardening On The Vulnerabilities. Besides that, the data collected from the existed s concluded to give an advanced security scanning web application to users who can access it effortlessly.

	BWAPP	E-learning Web Application Hacking Security And Implementation Hardening On The Vulnerabilities	Damn Vulnerable Web Application (DVWA)	GRABBER
Source code analyzer	X	X	X	X
SQL injections	X	X	X	X
Cross-site scripting	X	X	X	X
Open Redirection Vulnerabilities	X	X	X	
Unrestricted file upload vulnerabilities.	X	X	X	X
Broken Access Control	X	X	X	
User friendly		X		
PDF report		X		
Provide countermeasures		X		
Provide video on how to solve the vulnerabilities.		X		
CVSS Score		X		

Table 2.1 Comparison between web application

Conclusion

In conclusion. the literature review provides more detailed information regarding the research that is relevant to these studies. As we can make a comparison between previous web application security for new learner, it’s hard to explore and not user friendly. E-learning: Web Application Hacking Security and Implementation Hardening on The Vulnerabilities is to give the benefit for all the users to gain a knowledge to become a good pen tester in the future. The unique of this project is, it has the solution on how to hardens the vulnerabilities based on Top 10 vulnerabilities on OWASP. Lastly, this project will give the good impact on E-learning platform for beginners and students in identifying and preventing web vulnerabilities. This web application training programme equips people to execute successful penetration testing and ethical hacking projects.

Chapter 3: RESEARCH METHODOLOGY

3.1 Introduction

The term "project methodology" refers to a paradigm that has been used to create, plan, implement, and achieve project goals. Planning methodology is effective for this project since it demonstrates how each work will be completed. It also enables the project's complete management process to be controlled through effective decision-making and problem-solving.

Rapid Application Development (RAD) is an iterative software development methodology that prioritises prototype releases and changes. The advantages of Rapid Application Development (RAD) include increased flexibility and adaptability, since developers are able to make changes rapidly throughout the development process. Iterative development may help minimise development time and speed up delivery. Therefore, code reuse is encouraged, resulting in less human coding, less potential for mistake, and quicker testing durations. Additionally, improved adoption of new technology.

Models are widely used in the software development process as a form of description. They are abstractions that help developers cope with the complexity of the issue they are researching or the solution they are constructing by expressing and conveying what is essential while excluding irrelevant information.

The appropriate development approach for the E-learning project: Web Application Intrusion Protection and Execution Rapid Application Development (RAD) is a methodology for hardening vulnerabilities. Since developers are able to make changes swiftly throughout the development process, RAD increases adaptability and flexibility. It is encouraged to reuse code, which results in less human coding, less opportunities for error, and shorter testing durations.

3.2 Methodology Model

Rapid Application Development

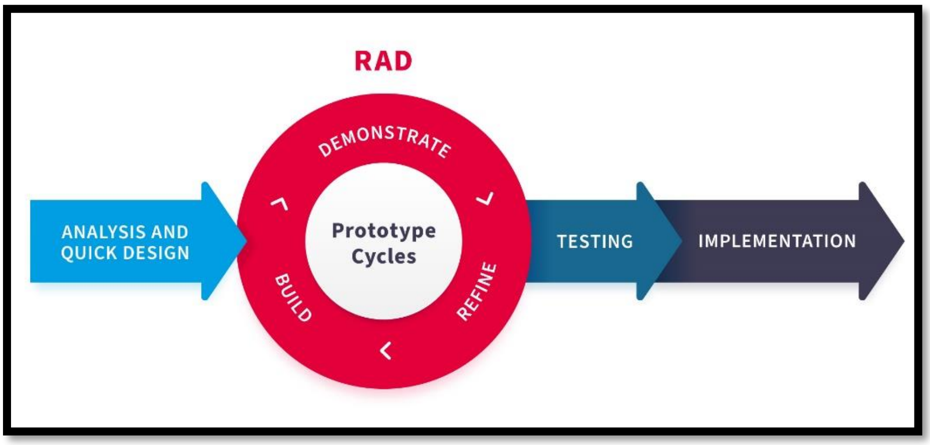


Figure 2.0 Rapid Application Development

3.3 Project methodologies Phases

3.3.1 Step 1: Define and finalize project requirements

Stakeholders meet at this stage to establish and finalise project requirements such as project goals, expectations, timeframes, and budget. To seek management approvals once have properly defined and scoped out each component of the project's needs.

The requirement of the project is to create a great content for students and new learner to explore in security field, this project building an amazing Graphic User Interface (GUI) for user can access easily and understand. The requirement for the projects in this phase is identify the problem, objective, scope of study, significant of project and literature review.

3.3.2 Step 2: Begin Design Prototypes

In this phase, start developing the project to complete the scope. This phase started with create a system design, draw the architecture diagram, use case, and flow chart to develop the E-learning platform. Other than that, A formal meeting with the project supervisor is held to go over the findings of the data gathering, and analysis accomplished thus far in order to construct a full model of the proposed system. After the outline design is complete, interactions between processes or sequences of functions and data are discovered.

The project supervisor will then evaluate the system design and check the detailed system area model and the outline system design to ensure that the project is complete before moving on to developing the overall system design.

3.3.2.1 Architecture Diagram

The architecture diagram for the application is detailed in this section. Understanding the diagram allowed vital details about the applications to be deduced.

E-learning architects create goals and procedures for the use of learning technologies within a company, as well as the infrastructure needed to support these goals and procedures.

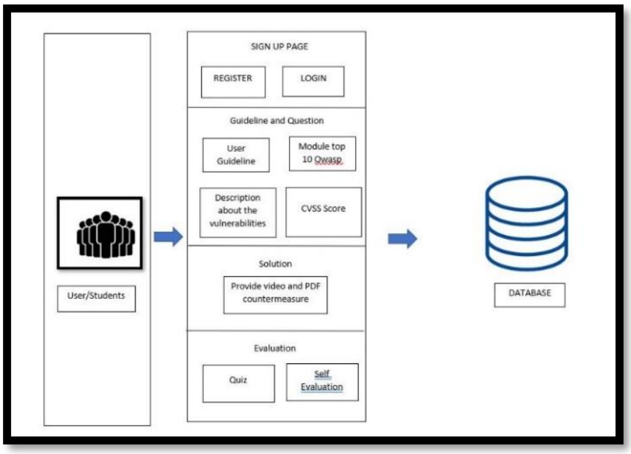


Figure 3.1 Architecture diagram

Flow Diagram

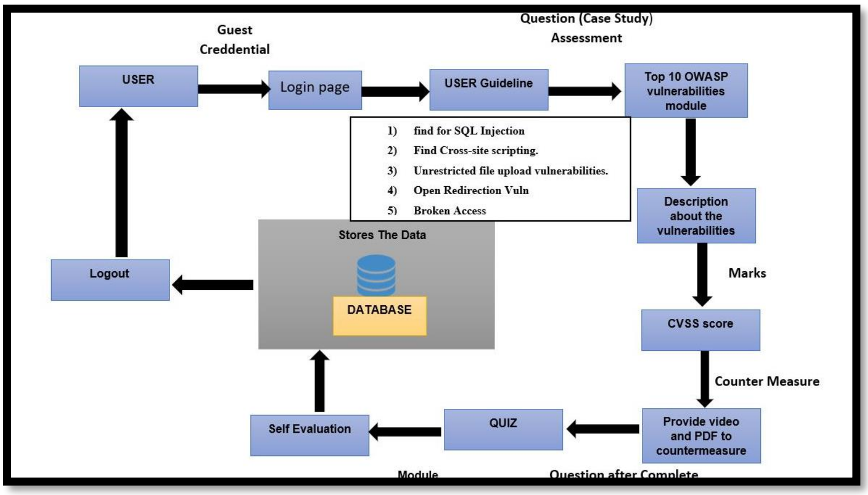


Figure 3.2 Flow diagram

3.3.2.2 Use Cases

A use case diagram aids in comprehending how a user may interact with a system built using the Unified Modelling Language (UML). Lastly, it should assist in defining and organising needs. According to the use case diagram, there are three actors: students, the developer, and the instructor.

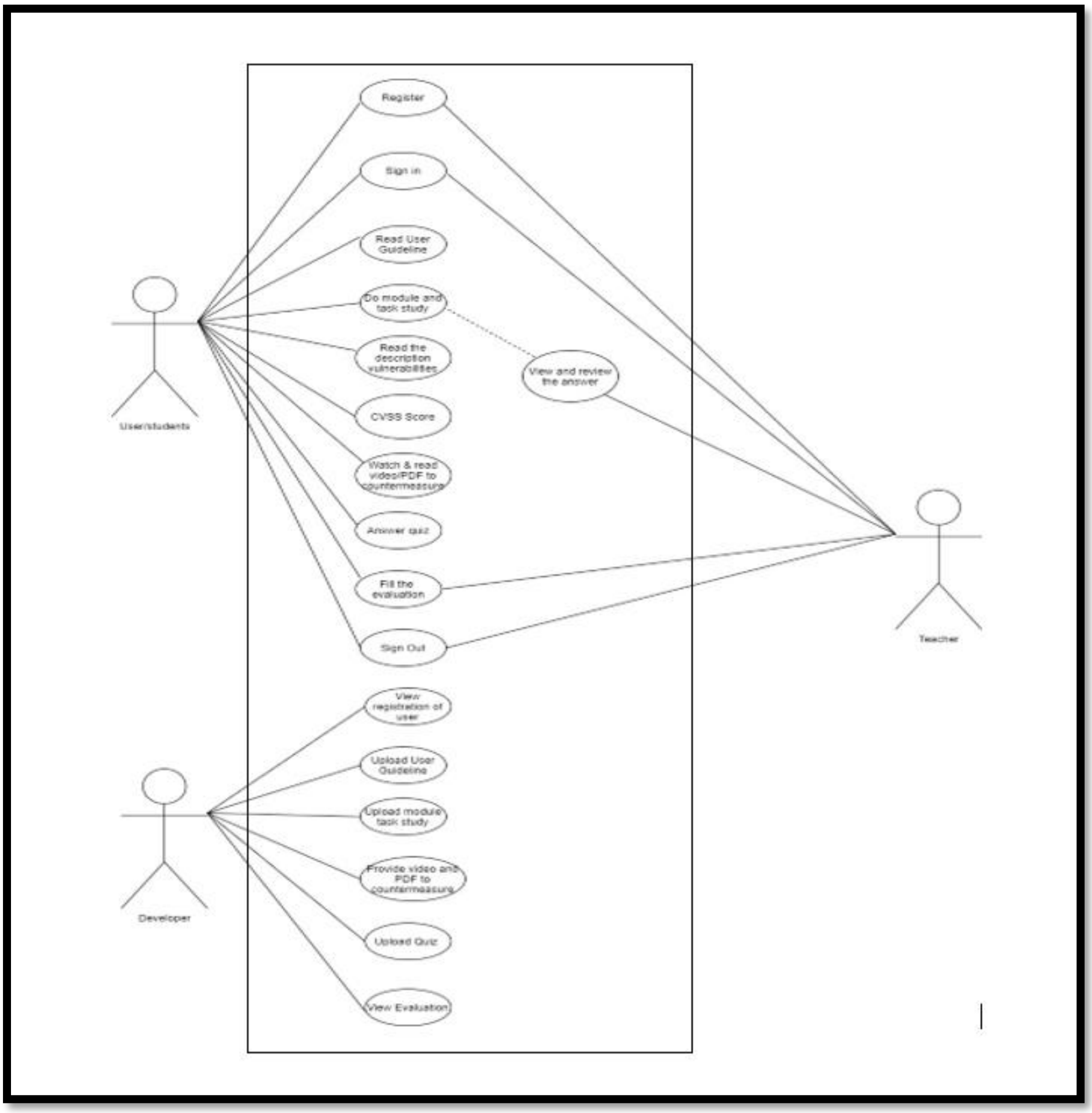


Figure 3.3 Uses Cases

3.3.2.3 Sequence diagram

Analysis sequence diagram provide for a more efficient examination of conditions on the ground, indicating possible cost-cutting and time-allocation options. This is helpful because it enables you to look for procedures that may be merged or adjusted, resulting in less waste and more hourly output. Flowcharts are a great tool for analysing a process and subsequently finding areas for improvement.

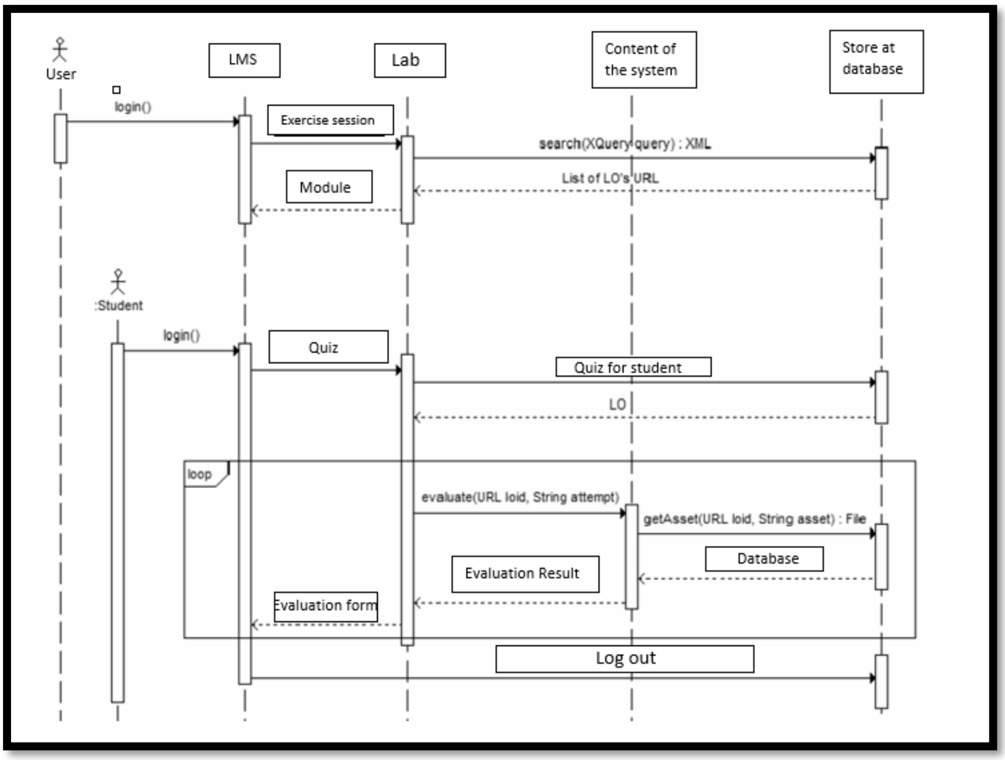


Figure 3.4 Sequence diagram

Model View Controller

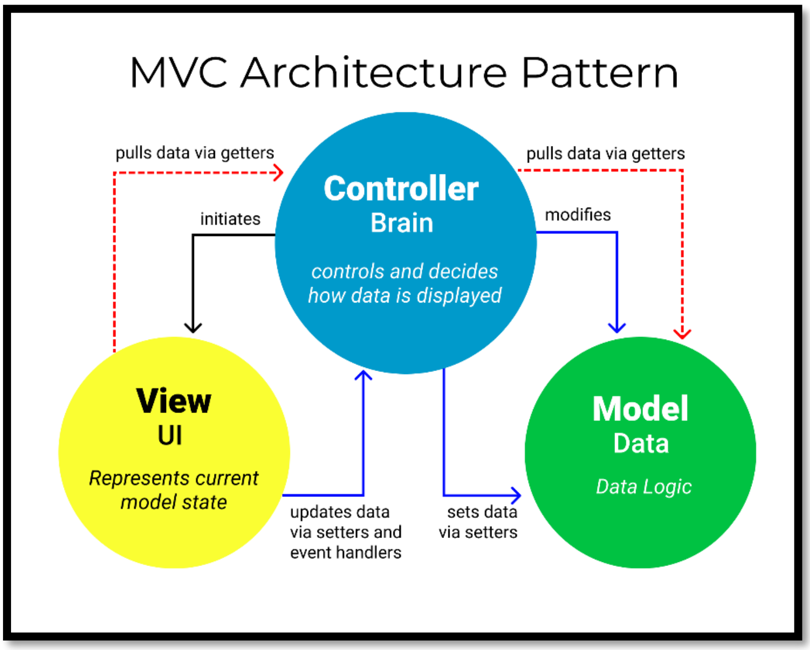


Figure 3.5 MVC Architecture

The data model is a representation of the basic information that your application accesses and manipulates. The model is at the centre of the software, while the viewer and controller help the user interact with the data model in a pleasant way.

Model-View-Controller (MVC) is a common software design pattern used to build user interfaces, data, and control logic. It emphasises the contrast between the business logic and the software's look. This "separation of concerns" enables a more effective division of labour and improved maintenance.

Model View Controller Works

First, the browser sends a request to the Controller. The Controller then exchanges information with the Model to transmit and receive data. The Controller then communicates with the View in order to render the data. The View is concerned only with how the information is presented, not with its final shape. It will be a dynamic HTML file that renders data depending on the Controller's supplied information.

The View will then broadcast its final presentation to the Controller, which will subsequently transfer it to the user output. Important to keep in mind is that the View and the Model never interact. The Controller is the sole means of communication between them.

Important to keep in mind is that the View and the Model never interact. The Controller is the sole means of communication between them. This guarantees that the application's functionality and user interface never interact, making it simpler to develop complex applications.

Model

The model component stores both data and logic. It represents data that is sent between controller components or any associated business logic. For example, a Controller object will fetch client information from the database. It manipulates data before to returning it to the database or presenting it.

It is updated in response to requests from views and controller instructions. It is also the lowest level of the pattern and is responsible for data upkeep.

View

A View is the application component that represents how data is shown. The information gathered from the model data is utilised to create views. A view requests information from the model in order to deliver the output presentation to the user. Charts, diagrams, and tabular data are also shown in the view. For instance, every customer view will have all UI components, such as text fields and drop-down menus.

Controller

The Controller is the software component that regulates user interaction. The controller reads the mouse and keyboard inputs of the user and modifies the model and display appropriately.

To update the state of a model, a Controller delivers it commands (E.g., Saving a specific document). Additionally, the controller sends commands to its associated view to alter the view's presentation (For example scrolling a particular document).

3.3.3 Step 3: Built

This phase start develops the website by using:

PHP and HTML code

This project utilises PHP and HTML. PHP is a programming language, while HTML is a markup language. HTML creates the general structure and content of a web page, whereas PHP supplies dynamic information through scripts. HTML is a client-side language, whereas PHP is a server-side language. The greatest advantage of PHP is that it is open source and free. It may be downloaded from anywhere and is immediately used for internet applications.

Aside from that, it enables the reuse of comparable code and avoids the need to create extensive code and complicated structures while developing web applications. PHP's adaptability enables it to efficiently mix with a number of different programming languages, enabling the software package to use the most effective technology for each function.

Database MySQL

MySQL is the most secure and trustworthy database management system available, and is used by major online applications such as WordPress, Drupal, and Joomla for data storage. The data security and transactional processing capabilities of the most recent version of MySQL may be highly advantageous for any organisation, especially e-commerce businesses with regular money transfers. MySQL's unrivalled scalability on demand enables the management of deeply embedded applications with a smaller footprint, even in massive warehouses containing terabytes of data. MySQL is distinguished by its on-demand adaptability. This open-source solution enables eCommerce businesses with specialised database server needs to fully customise it.

Create vulnerable code TOP 10 OWASP

NO	VULNERABLE TOP 10 OWASP	CODE/DESCRIPTION
1	SQL Injection.	HTML and PHP
2	Reflected Cross-site scripting	HTML and PHP
3	Unrestricted file upload vulnerabilities	HTML and PHP
4	Open Redirection Vulnerabilities	HTML and PHP
5	Command Injection.	HTML and PHP

Table 3.0 Vulnerable Top 10 OWASP

3.3.4 Step 4: Test

This phase must test the software product and ensure that all of its moving parts perform as the customer expects. Continue to include client feedback while the code is tested and retested for functionality. Efforts are made during the test to build an implementation strategy, with a method of implementation selected after an evaluation of the system's design. As part of the system's development and implementation, a list of all required tasks is compiled. Based on the previously mentioned functionalities, an early application prototype will be developed.

Before releasing the E-learning to the public, the project should test and evaluate the test findings produced during functionality testing.

3.3.5 Step 5: Implementation

In this phase, the whole product of E-learning will be released and tested to the end-users. Other than that, they will use the system and give their feedbacks on whether it needs to be improved or altered. Lastly, any updates or changes are being done depending on the feedbacks from the user to make sure the system is entirely fulfilling the needs

Ascertain that the application is functional in its intended context. If a user experiences a problem, document it and fix the issue. If an issue is fixed, the changed code is deployed to the environment. The programme is continuously updated to give new features and maintain an up-to-date environment.

3.4 Method to create E-learning platform

3.4.1 Computer Manage Learning

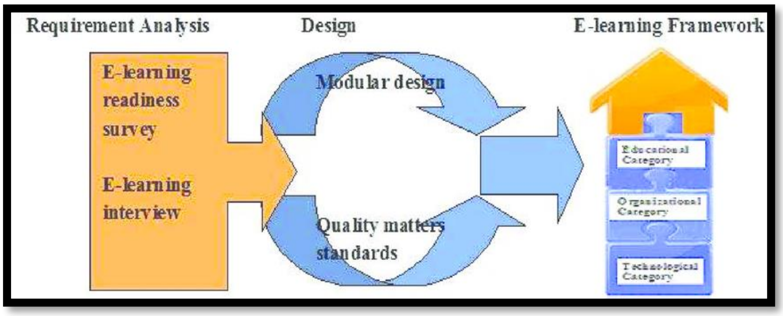


Figure 3.6 Computer Manage Learning (CML)

In computer-managed learning (CML), also known as Computer Managed Instruction, computers are utilised to monitor and analyse learning procedures (CMI). Computer-aided learning systems use information database storage. These databases include pieces of information that the student must learn, as well as a variety of rating features that enable the system to be tailored to the preferences of each individual student.

Due to the two-way link between the student and computer, it is feasible to establish whether or not the learner completed his or her learning goals adequately. If not, the steps may be repeated until the student has achieved his or her learning goals.

Moreover, educational institutions use computer-assisted learning systems to store and retrieve data, which aids educational administration. This may comprise, among other things, lecture notes, training materials, grades, programme data, and enrollment information.

3.4.2 Language

NO	Method	Description
1	php	PHP and HTML are computer languages. PHP is a general-purpose programming language. It is mostly used as a server-side scripting language for the building of websites. PHP frameworks also simplify web development.
2	MySQL®	MySQL: MySQL is a SQL-based relational database management system. The programme serves a broad variety of functions, including data warehousing, e-commerce, and logging. However, the most prevalent use of mySQL is as an online database.

Table 3.1 Language

3.5 Project resources

Each of the hardware and software requirements for this project E-learning technology resources are free since I use my own personal item for the hardware need and the software requirement is open source. The table hardware and software requirements are shown below.

3.5.1 Hardware Requirement

NO	HRDWARE	DESCRIPTION
1		Laptop will be used in this project to capture the data and all the software will be installed on this hardware. • Laptop model Dell (Inspiron 143000) • The laptop will be used to install Xampp

Table 3.2 Hardware

3.5.2 Software

NO	SOFTWARE	DESCRIPTION
1		XAMPP is a free and open-source web server solution stack bundle developed by Apache Friends that contains the Apache HTTP Server, the MariaDB database, and PHP and Perl scripting language interpreters.
2		SQL is a programming language designed to manage data in a relational database management system or to conduct stream processing in a relational data stream management system.

Table 3.3 Software

3.5.3 Budget/Coasting requirement

Table below shows the important hardware and software needed to support the development process.

Hardware Requirement

NO	Hardware	Price (RM)
1	**Laptop** • Dell (Series DELL Inspiron)	2,500
	TOTAL	**2,500**

Table 3.4 Hardware

3.6 Work Breakdown Structure (WBS)

Setting project milestones has the objective of indicating the specific point in time when a project must be completed in respect to its overall schedule. Every major date in the timetable must be highlighted in order to keep the project on track and prevent running over its permitted timeframes. Getting a project done is a great method to get a lot of deliverables. Figure below represents the work breakdown structure and shows a breakdown of the application development process.

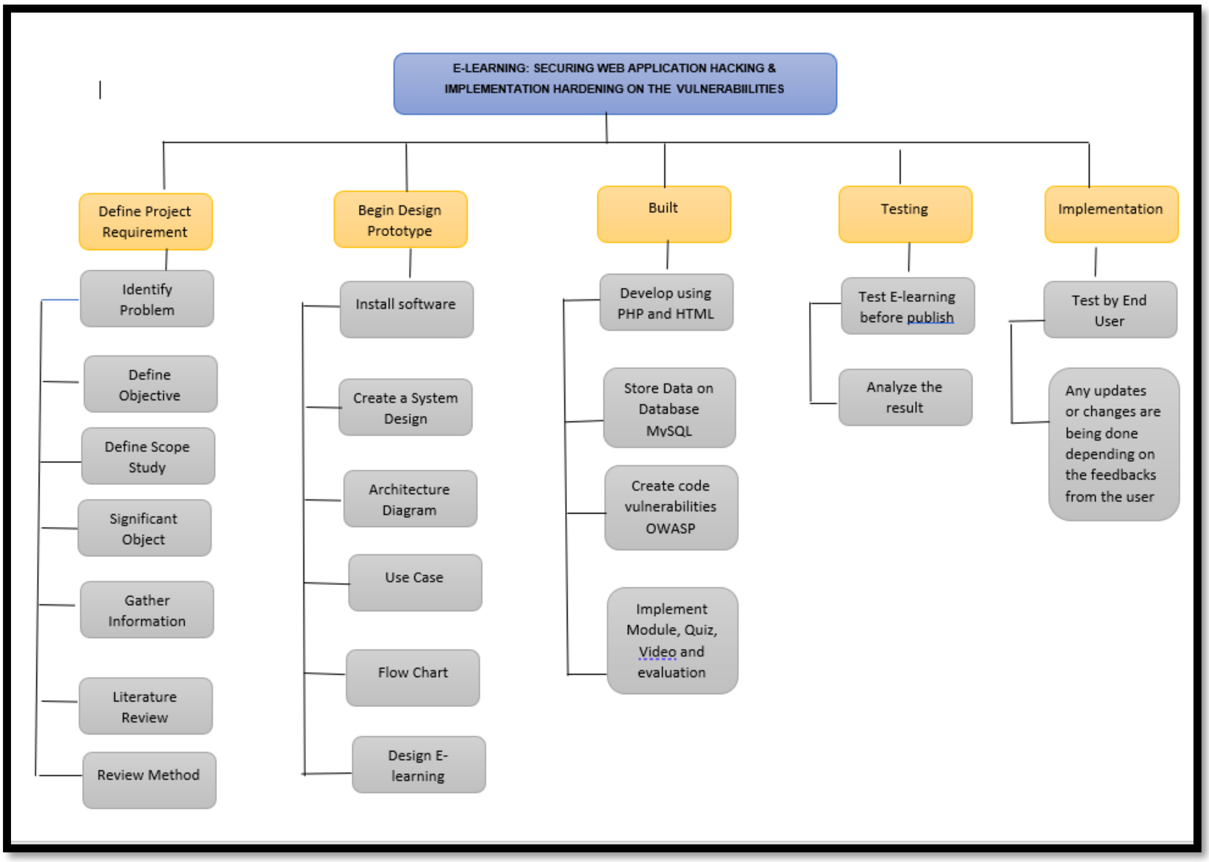

E-LEARNING: SECURING WEB APPLICATION HACKING & IMPLEMENTATION HARDENING ON THE VULNERABIILITIES
Define Project Requirement
Identify Problem
Define Objective
Define Scope Study
Significant Object
Gather Information
Literature Review
Review Method
Begin Design Prototype
Install software
Create a System Design
Architecture Diagram
Use Case
Flow Chart
Design E-learning
Built
Develop using PHP and HTML
Store Data on Database MySQL
Create code vulnerabilities OWASP
Implement Module, Quiz, Video and evaluation
Testing
Test E-learning before publish
Analyze the result
Implementation
Test by End User
Any updates or changes are being done depending on the feedbacks from the user

Figure 3.7 Work Breakdown Structure

Summary

As the internet has become the most important resource in the modern economy, security concerns have never been more common. We must thus protect our resources, data, and user privacy information. As technology progresses and brings new tactics, s, models, and techniques to enhance security levels, hackers will continue to be a part of this never-ending game. Web Application Security and Implementation in E-Learning Hardening on The purpose of Vulnerabilities is to provide all users with the information necessary to become proficient pen testers in the future. Unique to this project is that it provides guidance on how to harden vulnerabilities based on OWASP's top 10 vulnerabilities. This project will have a positive influence on the E-learning platform for novices and students in terms of recognising and avoiding online vulnerabilities. This web application training curriculum prepares individuals to successfully conduct penetration testing and ethical hacking tasks.

CHAPTER 4: PROTOTYPE / PRODUCT DEVELOPMENT

4.0 Introduction

This chapter focuses on the design and execution of the project "E-learning: Securing Web Application Hacking and Implementation Hardening on The Vulnerabilities." The specifications and prototype for this system will be described. This covers the installation of hardware and software, a pen test of the agreed-upon online application, and the implementation of the web application. All processes must be performed to ensure that the programme is correctly installed and functioning.

4.1 Requirements

Requirements are the specifications of the services a software system must deliver and the operating limitations it must adhere to. In other words, the requirements specify what a system must have in order to work. Functional Requirements, Non-Functional Requirements, Hardware Requirements, and Software Requirements will be covered in this chapter.

4.2.1 Functional Requirement

Functional requirements are the services that define the system, as well as how it should respond to inputs and behave. The overview of the functional need is shown in Table 4.1.

Requirement ID	Requirement Statement
SWA01	The system shall require user to enter unique registration key that comes with the product upon purchasing.
SWA02	The system shall allow user to register with unique username and password
SWA03	The system should allow user to log in using username, password, and email
SWA04	The system shall encrypt password before inserting to database.
SWA05	All button in E-learning platform function well.

Table 4.0 Functional Requirement

4.2.2 Non-Functional Requirement

In this section, we will be explaining the functions offered by the system as it is developed or the development process such as timing constraints, process, standards, and others. Table 4.2 shows the summary of non-functional requirement.

Requirement ID	Category	Requirement Statement
SS01	Usability	The system easy to navigate and use for the user.
SS02	Performance	The system able to react fast and load quickly.
SS03	Simplicity	The system design is simple and intuitive.
SS04	Security	The system only authenticates with valid user

Table 4.1 Non-Functional Requirement

4.3 Software requirement

In this section, we will explain the software requirements in building the E-learning: Securing Web Application Hacking and Implementation Hardening On The Vulnerabilities. Table 4.3 on the next page shows specifically the list of software and its functionality for this project.

Software	Description
Apache version 2.4	Running web servers that ability to host one or more HTTP based website.
PHP version 8.1.2	Running PHP language that executed on the server and result is sent to the browser.
phpMyAdmin version 4.7	Manage administration and management of MySQL databases through a graphic user interface (GUI).
MySQL version 5.7	Running SQL database system used on the web that runs on a server.

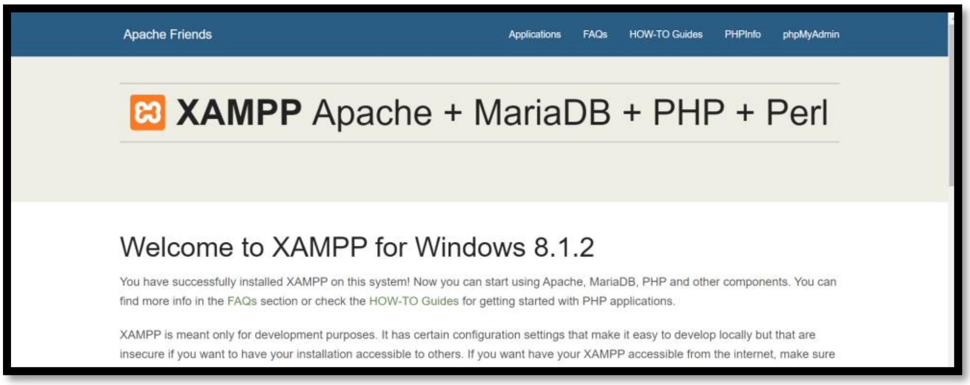
Table 4.2 Software Requirement

4.4 Stage of Development

The development of this project started with the installation of Xampp . The installation of the Xampp is important as it is a platform to write and run the code. After that, we setup the security database for user to access the E-learning platform. Next, we configured Apache, MySQL, PHP, and phpMyAdmin. The details of configuration will be explained in the next section

i. **Install Xampp**

XAMPP enables a local host or server to test a website or client before publishing it to the main server. It offers an appropriate environment for testing and validating the functioning of projects based on Apache, Perl, MySQL, and PHP utilising the host's system.



Welcome to XAMPP for Windows 8.1.2

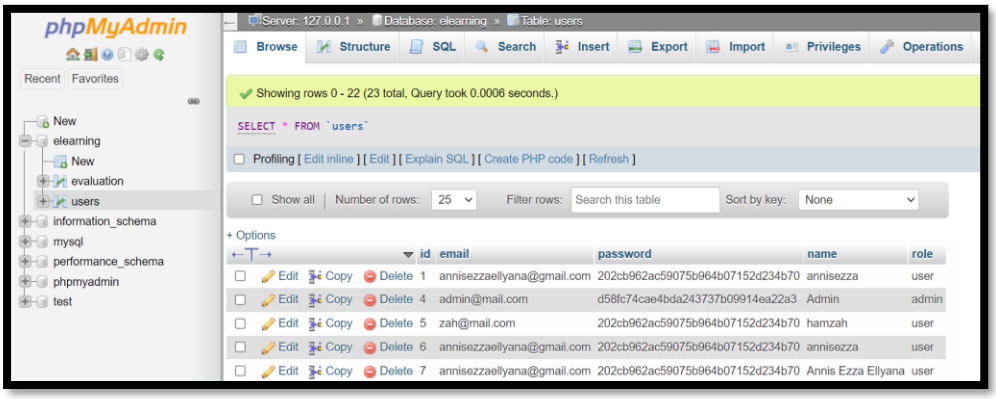
You have successfully installed XAMPP on this system! Now you can start using Apache, MariaDB, PHP and other components. You can find more info in the FAQs section or check the HOW-TO Guides for getting started with PHP applications.

XAMPP is meant only for development purposes. It has certain configuration settings that make it easy to develop locally but that are insecure if you want to have your installation accessible to others. If you want have your XAMPP accessible from the internet, make sure

Figure 4.0 Xampp

ii. **Set up a secure database**

Secure database user access, encrypt the user password and make it unique id.



✓ Showing rows 0 - 22 (23 total, Query took 0.0006 seconds.)

```
SELECT * FROM `users`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

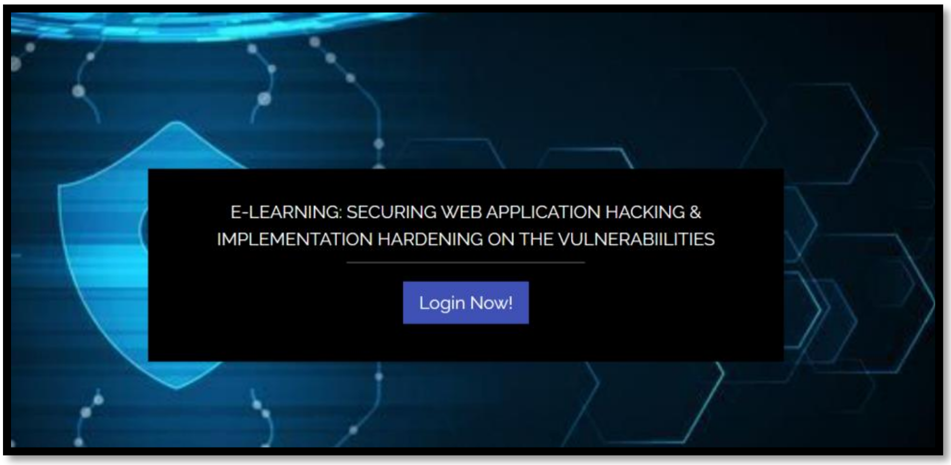
□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

←T→				id	email	password	name	role
□	Edit	Copy	Delete	1	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□	Edit	Copy	Delete	4	admin@mail.com	d58fc74cae4bda243737b09914ea22a3	Admin	admin
□	Edit	Copy	Delete	5	zah@mail.com	202cb962ac59075b964b07152d234b70	hamzah	user
□	Edit	Copy	Delete	6	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□	Edit	Copy	Delete	7	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	Annis Ezza Ellyana	user

Figure 4.2 Encypted password

4.1 E-learning: Securing Web Application Hacking and Implementation Hardening on The Vulnerabilities



E-LEARNING: SECURING WEB APPLICATION HACKING & IMPLEMENTATION HARDENING ON THE VULNERABIILITIES

Figure 4.3 E-learning Web Application

This project gives a new learner on security field a confidence to boost in their finding vulnerabilities. The Beginners who want to gain knowledge in the security field by providing tutorials, exercises, and many more to improve the level of security skills my using concept E-learning on the system. This project building an amazing GUI interface that the user can access easily and understand the steps on what to do next and give the solution on how to hardens the vulnerabilities.

Automation makes it easy for the user in this platform, The automated has made it easier for user to do security assessments on websites and web applications with minimal setup and integration. The task that used to necessitate a thorough understanding of the online application can now be completed automatically by the web application scanner.

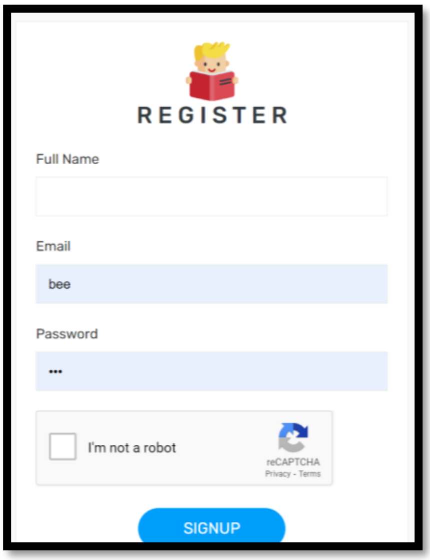
This E-learning website will give instructions on how to use this platform. The module contains a video and PDF file on how to resolve each vulnerability. The second advantage is that users may take the course anywhere, since the courses are kept on web applications and are available 24 hours a day, seven days a week. They may access this platform via devices such as laptops, desktop PCs, etc. In addition, the user may read the rules, obtain online case study materials, enrol in courses, and rapidly develop their cybersecurity expertise.

4.1.1 Coding to develop E-learning: Securing Web Application Hacking and Implementation Hardening on The Vulnerabilities

The E-learning: Securing Web Application Hacking and Implementation Hardening on The Vulnerabilities use PHP Languages, HTML Languages and CSS Languages.

i. Register page

Figure 11 shows Register Page for new user. There is only single authentication for the system. The password required is include complex password. Users need to fill up the email and password before access to the system.



REGISTER

Full Name

Email

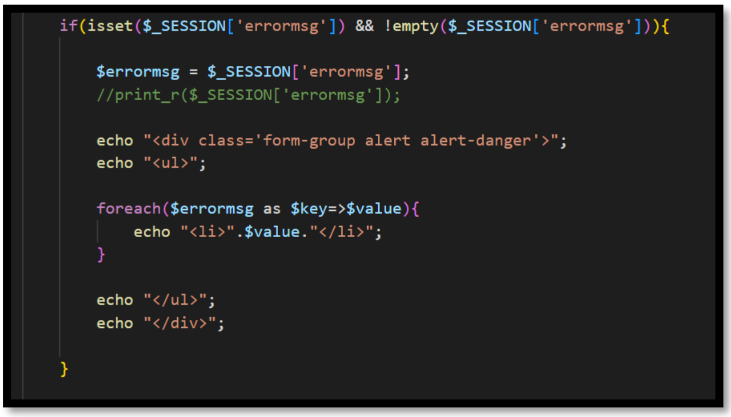
bee

Password

•••

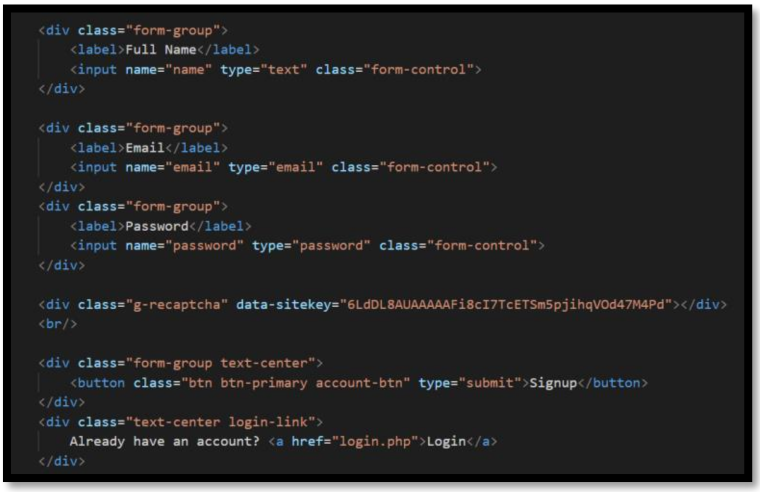
Figure 4.4 Login page

Code to develop the system:



```
if(isset($_SESSION['errormsg']) && !empty($_SESSION['errormsg'])){

    $errormsg = $_SESSION['errormsg'];
    //print_r($_SESSION['errormsg']);

    echo "<div class='form-group alert alert-danger'>";
    echo "<ul>";

    foreach($errormsg as $key=>$value){
        echo "<li>".$value."</li>";
    }

    echo "</ul>";
    echo "</div>";

}
```

Figure 4.5 Code register page



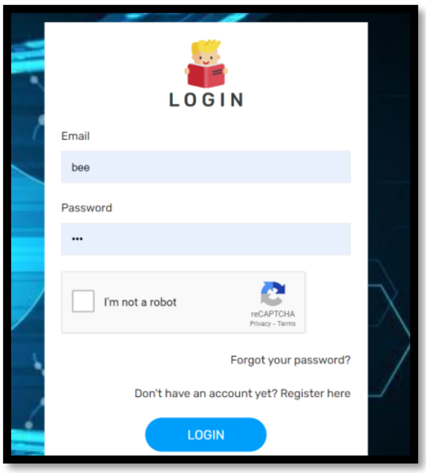
```
<div class="form-group">
    <label>Full Name</label>
    <input name="name" type="text" class="form-control">
</div>

<div class="form-group">
    <label>Email</label>
    <input name="email" type="email" class="form-control">
</div>
<div class="form-group">
    <label>Password</label>
    <input name="password" type="password" class="form-control">
</div>

<div class="g-recaptcha" data-sitekey="6LdDL8AUAAAAAFi8cI7TcETSm5pjihqVOd47M4Pd"></div>
<br/>

<div class="form-group text-center">
    <button class="btn btn-primary account-btn" type="submit">Signup</button>
</div>
<div class="text-center login-link">
    Already have an account? <a href="login.php">Login</a>
</div>
```

Figure 4.6 Code register page

Software development comprises everything that occurs between the idea of a desired piece of software and its eventual realisation, often in a planned and systematic way.

Login User Page

Figure below shows the Login Page of prototype system. The detail information must be provided by user are username, password and recaptcha.



LOGIN

Email

bee

Password

•••

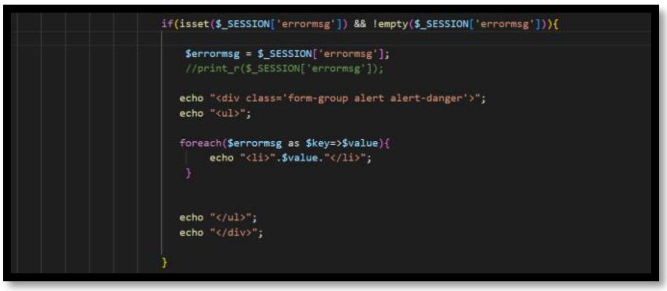
□ I'm not a robot

Forgot your password?

Don't have an account yet? Register here

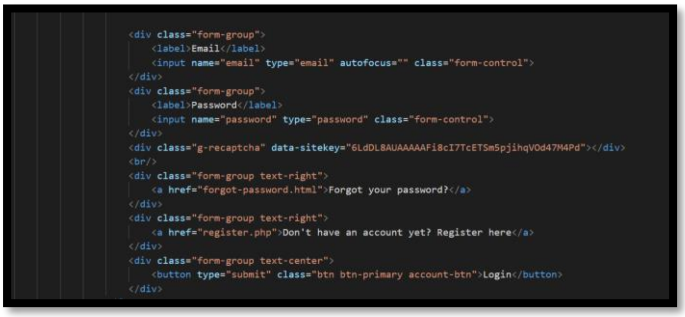
Figure 4.7 Login

Code of the system:



```php
if(isset($_SESSION['errormsg']) && !empty($_SESSION['errormsg'])){

    $errormsg = $_SESSION['errormsg'];
    //print_r($_SESSION['errormsg']);

   echo "<div class='form-group alert alert-danger'>";
   echo "<ul>";

   foreach($errormsg as $key=>$value){
       echo "<li>".$value."</li>";
    }


   echo "</ul>";
   echo "</div>";

}
```

Figure 4.8 Login Page (Code 1)



```html
<div class="form-group">
    <label>Email</label>
    <input name="email" type="email" autofocus="" class="form-control">
</div>
<div class="form-group">
    <label>Password</label>
    <input name="password" type="password" class="form-control">
</div>
<div class="g-recaptcha" data-sitekey="6LdDL8AUAAAAAFi8cI7TcETSm5pjihqVOd47M4Pd"></div>
<br/>
<div class="form-group text-right">
    <a href="forgot-password.html">Forgot your password?</a>
</div>
<div class="form-group text-right">
    <a href="register.php">Don't have an account yet? Register here</a>
</div>
<div class="form-group text-center">
    <button type="submit" class="btn btn-primary account-btn">Login</button>
</div>
```

Figure 4.9 Login Page (Code 2)

In order to get access to a secure website or form, authentication credentials are submitted on a login page. On the login form, there are separate fields for the username and password. When the login form is submitted, the underlying programming validates the validity of the credentials and grants the user access to the restricted page.

Module lab in the E-learning: Securing Web Application System

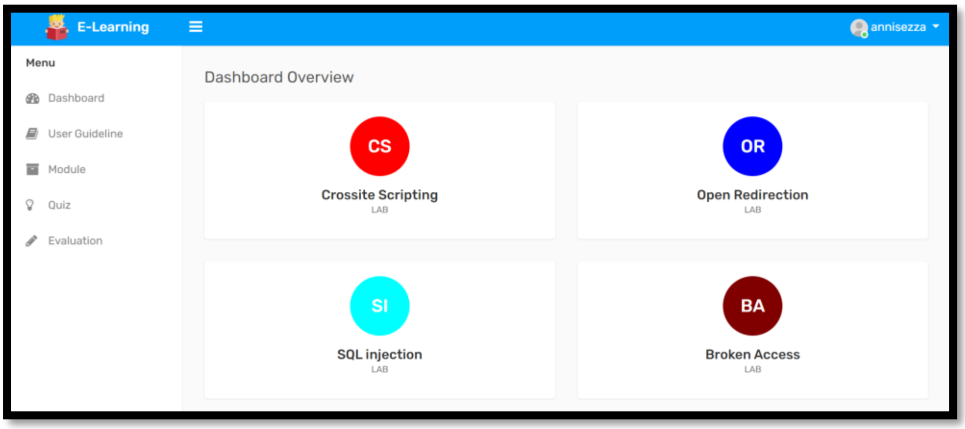
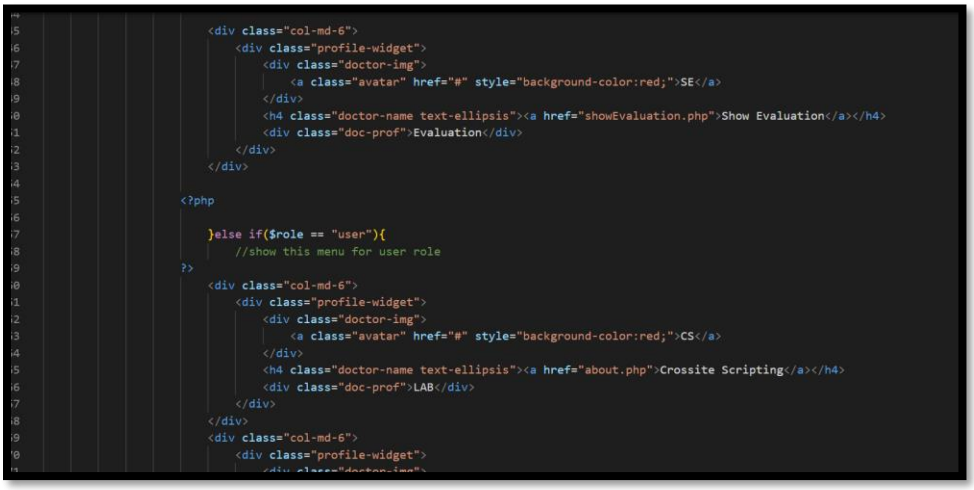


Figure 4.10 Dash Board Overview



```
        <div class="col-md-6">
            <div class="profile-widget">
                <div class="doctor-img">
                    <a class="avatar" href="#" style="background-color:red;">SE</a>
                </div>
                <h4 class="doctor-name text-ellipsis"><a href="showEvaluation.php">Show Evaluation</a></h4>
                <div class="doc-prof">Evaluation</div>
            </div>
        </div>

    <?php

        }else if($role == "user"){
            //show this menu for user role
    ?>
        <div class="col-md-6">
            <div class="profile-widget">
                <div class="doctor-img">
                    <a class="avatar" href="#" style="background-color:red;">CS</a>
                </div>
                <h4 class="doctor-name text-ellipsis"><a href="about.php">Crossite Scripting</a></h4>
                <div class="doc-prof">LAB</div>
            </div>
        </div>
        <div class="col-md-6">
            <div class="profile-widget">
                <div class="doctor-img">
```

Figure 4.11 Dash Board (code)

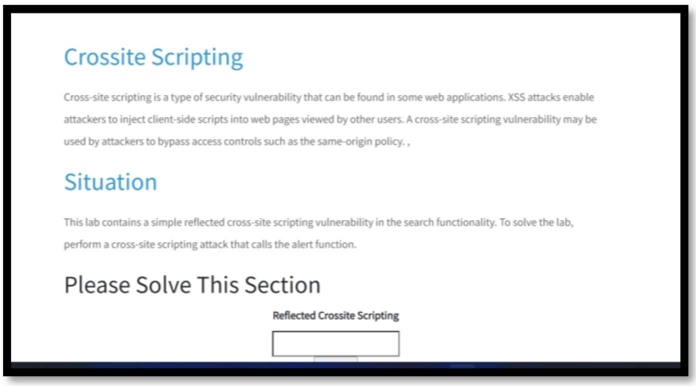
This is the interface of the dashboard; this project is a E-learning web application is a software project that incorporates security vulnerabilities on purpose for educational reasons for students and newcomer on cybersecurity industries. Moreover, this project focused on 5 vulnerabilities from the OWASP Top 10 security, include cross site scripting, Open redirection, Sql Injection, Broken Access and unrestricted file upload.

i. Cross-Site Scripting

Cross-Site Scripting (XSS) attacks are injection attacks that introduce malicious scripts into otherwise trustworthy and harmless websites. An XSS attack occurs when an attacker uses an online application to communicate malicious code to a different end user, often through a browser-side script. When a web application accepts user input in its output without validating or encoding it, it is susceptible to the weaknesses that enable these attacks to succeed.

An attacker may use XSS to transmit a malicious script to an unsuspecting user. The user's browser is incapable of determining that the script should not be trusted and will execute it anyhow. Since the browser thinks the script originated from a trustworthy source, the malicious script may access any cookies, session tokens, or other sensitive information saved by the browser and used with that site.

i. Figure below shows the Cross-site Scripting prototype system. This lab provide situation for user to answer the question



Crossite Scripting

Cross-site scripting is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy. ,

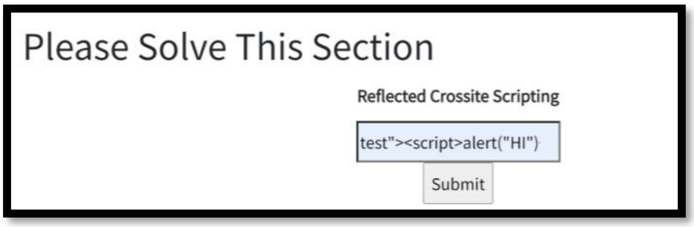
Situation

This lab contains a simple reflected cross-site scripting vulnerability in the search functionality. To solve the lab, perform a cross-site scripting attack that calls the alert function.

Please Solve This Section

Reflected Crossite Scripting

Figure 4.12 Cross-Site Scripting



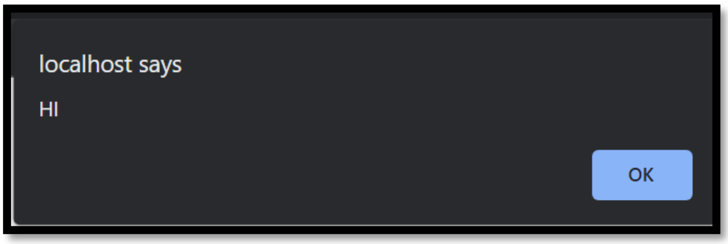
Please Solve This Section

Reflected Crossite Scripting

test"><script>alert("HI")

Figure 4.13 Inject Script

Users need to inject the malicious java/HTML code at the box given.



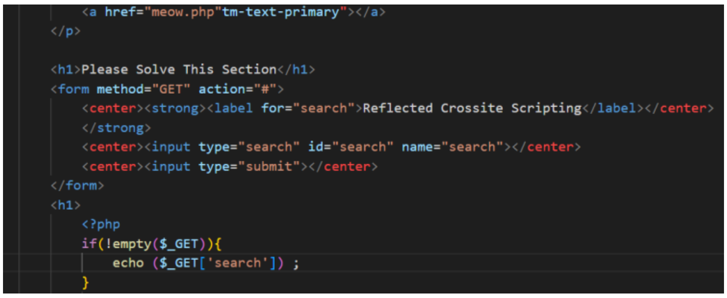
localhost says

HI

Figure 4.14 Inject result

The crosstie scripting vulnerabilities have been popup at the page and the user successfully complete the task given.

The code of the system



```
        <a href="meow.php"tm-text-primary"></a>
    </p>

    <h1>Please Solve This Section</h1>
    <form method="GET" action="#">
        <center><strong><label for="search">Reflected Crossite Scripting</label></center>
        </strong>
        <center><input type="search" id="search" name="search"></center>
        <center><input type="submit"></center>
    </form>
    <h1>
        <?php
        if(!empty($_GET)){
            echo ($_GET['search']) ;
        }
```

Figure 4.15 Sensitization

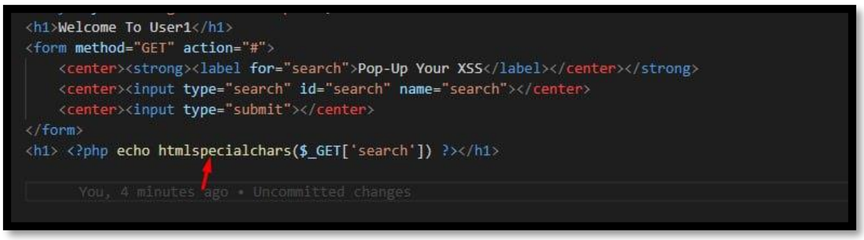
Client-side Cross-Site Scripting (XSS) is a kind of code injection attack. The attacker tries to run dangerous scripts on the victim's web browser by inserting malicious code in a legitimate online page or web application.

It is known as reflected cross-site scripting when an attacker hides malicious script in the data given by a website's search or contact form. A search form is an excellent illustration of mirrored cross-site scripting since it sends the visitor's search query to the server and only displays the result to the visitor.

Countermeasure

When the environment being administered supports it, the second line of protection is to perform a technique called escaping to any untrusted data before it is utilized as output. To prevent JavaScript or other code from being mistakenly executed, certain text characters are substituted by an escape code. The larger than and less than symbols (and >) that are used to bracket HTML tags are two of the most common characters to escape. These characters are substituted with the escape codes and > to sanitize untrusted text. Although the web browser detects these unique codes and displays the appropriate character, there is no chance of the web browser being confused and running untrusted code.

- Inject script **echo htmlspeacialchars** to prevent attacker to do cross site scripting vulnerabilities.



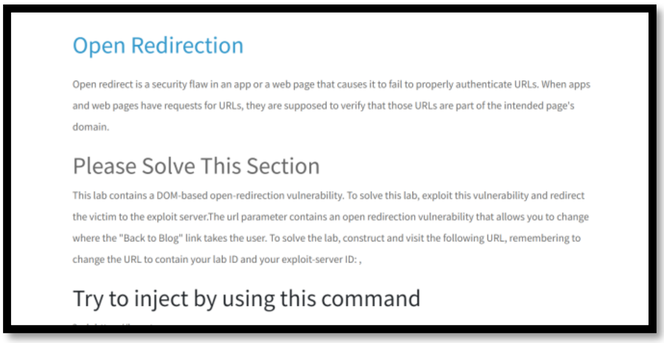
```
<h1>Welcome To User1</h1>
<form method="GET" action="#">
    <center><strong><label for="search">Pop-Up Your XSS</label></center></strong>
    <center><input type="search" id="search" name="search"></center>
    <center><input type="submit"></center>
</form>
<h1> <?php echo htmlspecialchars($_GET['search']) ?></h1>

      You, 4 minutes ago • Uncommitted changes
```

Figure 4.16 Inject script

ii. **Open Redirection**

Open redirection vulnerabilities occur when an application insecurely combines user-controllable data into a redirection's destination. An attacker may establish a URL inside the programme that leads to any external domain. This function may be used to facilitate phishing attacks against app users. The ability to leverage a legitimate application URL, targeting the correct domain, and with a valid SSL certificate (if SSL is used) provides credibility to the phishing effort since many customers will not notice the subsequent redirection to a different site.

i. Figure below shows the Open Redirection prototype system. This lab provide situation for user to answer the question.



Open Redirection

Open redirect is a security flaw in an app or a web page that causes it to fail to properly authenticate URLs. When apps and web pages have requests for URLs, they are supposed to verify that those URLs are part of the intended page's domain.

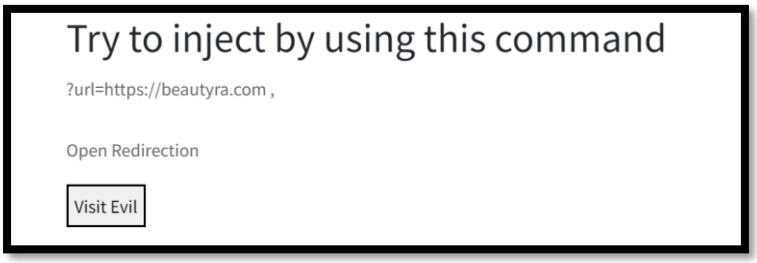
Please Solve This Section

This lab contains a DOM-based open-redirection vulnerability. To solve this lab, exploit this vulnerability and redirect the victim to the exploit server.The url parameter contains an open redirection vulnerability that allows you to change where the "Back to Blog" link takes the user. To solve the lab, construct and visit the following URL, remembering to change the URL to contain your lab ID and your exploit-server ID: ,

Try to inject by using this command

Figure 4.17 Open Redirection

The situation has been given for the Open redirection lab.



Try to inject by using this command

?url=https://beautyra.com ,

Open Redirection

Figure 4.18 Successful Inject

User need to inject by using the code given **?url=https://beautyra.com to** redirect this website page.

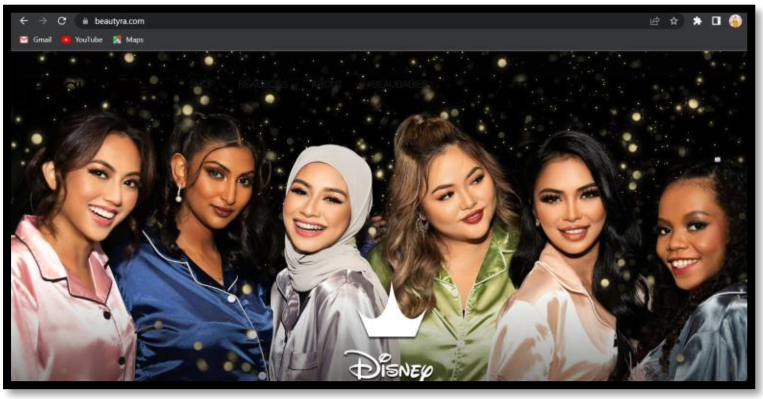
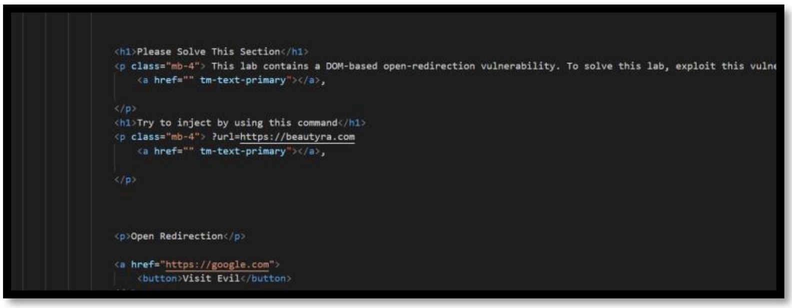


Figure 4.19 Try inject at beautyra page

User successfully open redirect to the beautyra page and this page has been detected have open redirection vulnerabilities.

Open redirection vulnerabilities occur when an application insecurely combines user-controllable data into a redirection's destination. An attacker may generate a URL inside the software that leads to any desired external domain. This function may be used to facilitate phishing attacks against app users. The ability to leverage a legitimate application URL, targeting the correct domain, and with a valid SSL certificate (if SSL is used) provides credibility to the phishing effort since many customers will not notice the subsequent redirection to a different site.

The code of the system



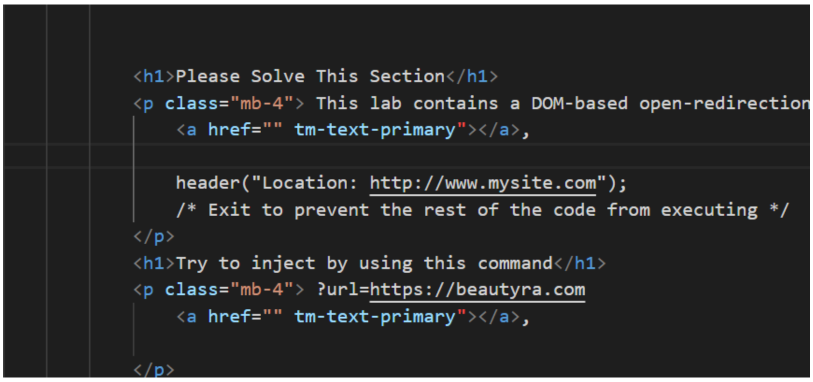
```
<h1>Please Solve This Section</h1>
<p class="mb-4"> This lab contains a DOM-based open-redirection vulnerability. To solve this lab, exploit this vulne
    <a href="" tm-text-primary"></a>,

</p>
<h1>Try to inject by using this command</h1>
<p class="mb-4"> ?url=https://beautyra.com
    <a href="" tm-text-primary"></a>,

</p>



<p>Open Redirection</p>

<a href="https://google.com">
    <button>Visit Evil</button>
```

Figure 4.20 Code of the System

When a user has control over a redirect or forward to another URL, this is known as an open redirect vulnerability. An attacker could offer a URL that redirects an unsuspecting victim from a legal domain to an attacker's phishing site if the app does not authenticate untrusted user input. Open redirections are used by attackers to give their phishing assaults more credibility. The majority of users see the real, trustworthy domain but are unaware of the phishing site redirection.

Countermeasure

To minimize the risk of unwanted redirects, avoid user-controllable data in URLs where possible and carefully sanitize it when it must be used



```
<h1>Please Solve This Section</h1>
<p class="mb-4"> This lab contains a DOM-based open-redirection
    <a href="" tm-text-primary"></a>,

    header("Location: http://www.mysite.com");
    /* Exit to prevent the rest of the code from executing */
</p>
<h1>Try to inject by using this command</h1>
<p class="mb-4"> ?url=https://beautyra.com
    <a href="" tm-text-primary"></a>,

</p>
```

Figure 4.21 Countermeasure

Open redirection, like many other vulnerabilities, are mostly created by processing unvalidated user inputs, particularly URL query strings. When possible, avoid user-controllable data in URLs and carefully sanitize it when it must be used to reduce the possibility of undesired redirects.

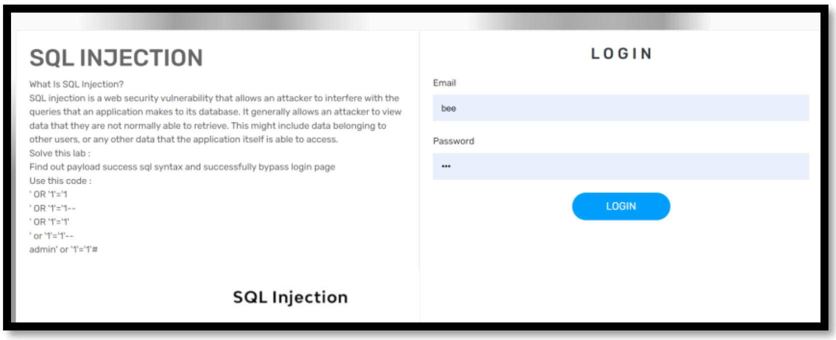
iii. SQL Injection

SQL injection is a code injection technique for attacking data-driven systems that includes executing malicious SQL statements inserted into an input field (e.g., to dump the database contents to the attacker). SQL injection must exploit a software security hole, such as when user input is incorrectly checked for string literal escape characters encoded in SQL queries or when user input is not strongly typed and executed unexpectedly. SQL injection is most often linked with website assaults, although it may be used to compromise any SQL database.
SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow full disclosure of all data on the system, destroy the data or make it otherwise unavailable, and gain administrative access to the database server.

i. Figure below shows the SQL Injection system. This lab provide situation for user to answer the question Figure 4.23 shows the source code involve

SQL syntax error

User will give the task and answer SQL syntax error task.



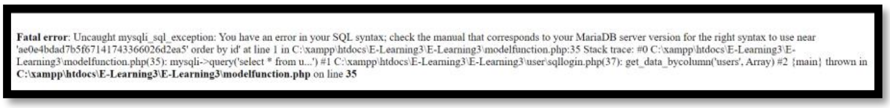
SQL INJECTION

What Is SQL Injection?
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access.
Solve this lab :
Find out payload success sql syntax and successfully bypass login page
Use this code :

```
' OR '1'='1
' OR '1'='1--
' OR '1'='1'
' or '1'='1'--
admin' or '1'='1'#
```

SQL Injection

Figure 4.22 SQL Injection



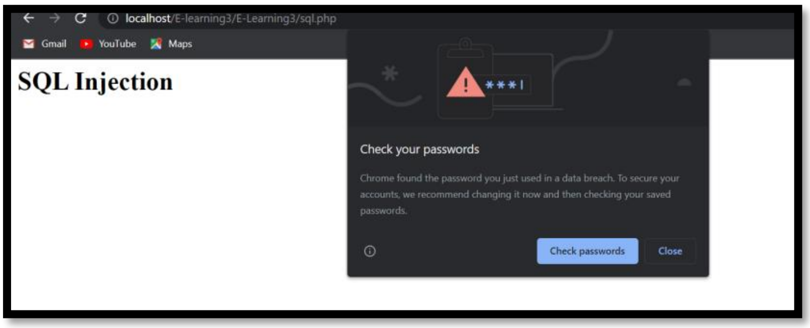
```
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
'ae0e4bdad7b5f67141743366026d2ea5' order by id' at line 1 in C:\xampp\htdocs\E-Learning3\E-Learning3\modelfunction.php:35 Stack trace: #0 C:\xampp\htdocs\E-Learning3\E-
Learning3\modelfunction.php(35): mysqli->query('select * from u...') #1 C:\xampp\htdocs\E-Learning3\E-Learning3\user\sqllogin.php(37): get_data_bycolumn('users', Array) #2 {main} thrown in
C:\xampp\htdocs\E-Learning3\E-Learning3\modelfunction.php on line 35
```

Figure 4.23 SQL injection Successful

This SQL error usually indicates that there is incorrect syntax somewhere in the query. Here are a few examples: Using a database-specific SQL for the incorrect database (for example, BigQuery supports DATE ADD, whereas Redshift allows DATEADD). In the SQL, there is a typo (missing comma, misspelt word, etc.)

SQL bypass login page

For second question lab SQL injection, user will be given task on how to inject the code and bypass the login page.



SQL Injection

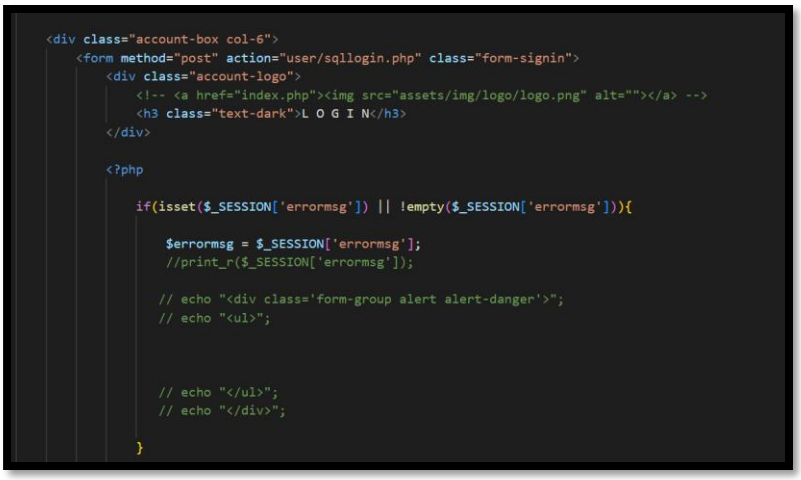
Check your passwords

Chrome found the password you just used in a data breach. To secure your accounts, we recommend changing it now and then checking your saved passwords.

Figure 4.24 Injection Bypass login

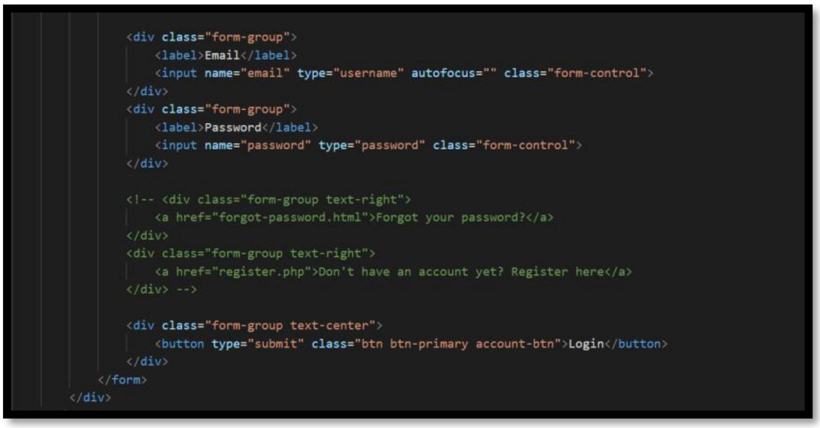
SQL injection is a method that exploits user data by inserting SQL commands as statements into web page inputs. In essence, malicious users may use these statements to affect the web server of the application.

The code of the system



```
<div class="account-box col-6">
    <form method="post" action="user/sqllogin.php" class="form-signin">
        <div class="account-logo">
            <!-- <a href="index.php"><img src="assets/img/logo/logo.png" alt=""></a> -->
            <h3 class="text-dark">L O G I N</h3>
        </div>

        <?php

            if(isset($_SESSION['errormsg']) || !empty($_SESSION['errormsg'])){

                $errormsg = $_SESSION['errormsg'];
                //print_r($_SESSION['errormsg']);

               // echo "<div class='form-group alert alert-danger'>";
               // echo "<ul>";



               // echo "</ul>";
               // echo "</div>";

            }
```

Figure 4.25 System Code 1

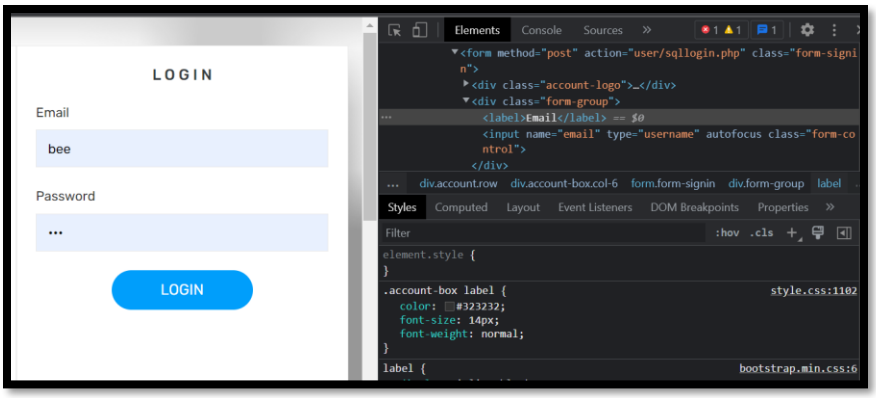


```
            <div class="form-group">
                <label>Email</label>
                <input name="email" type="username" autofocus="" class="form-control">
            </div>
            <div class="form-group">
                <label>Password</label>
                <input name="password" type="password" class="form-control">
            </div>

            <!-- <div class="form-group text-right">
                <a href="forgot-password.html">Forgot your password?</a>
            </div>
            <div class="form-group text-right">
                <a href="register.php">Don't have an account yet? Register here</a>
            </div> -->

            <div class="form-group text-center">
                <button type="submit" class="btn btn-primary account-btn">Login</button>
            </div>
        </form>
    </div>
```

Figure 4.26 System Code 2

Countermeasure

Only input validation and parametrized queries, including prepared statements, can reliably avoid SQL Injection attacks. Never utilise the input directly inside the application code. Not just online form inputs such as login forms, but every input must be sanitised by the developer. Never utilise the input directly inside the application code. Not just online form inputs such as login forms, but every input must be sanitised by the developer. For instance, single quotes are potentially dangerous code components that must be eliminated. On your production websites, you should also disable the display of database failures. SQL Injection may be used to get database information by exploiting database flaws.



```
<form method="post" action="user/sqllogin.php" class="form-signi
n">
  <div class="account-logo">…</div>
  <div class="form-group">
    <label>Email</label> == $0
    <input name="email" type="username" autofocus class="form-co
    ntrol">
  </div>
```

```
div.account.row  div.account-box.col-6  form.form-signin  div.form-group  label
```

```
element.style {
}
.account-box label {                                    style.css:1102
   color: #323232;
   font-size: 14px;
   font-weight: normal;
}
label {                                          bootstrap.min.css:6
```

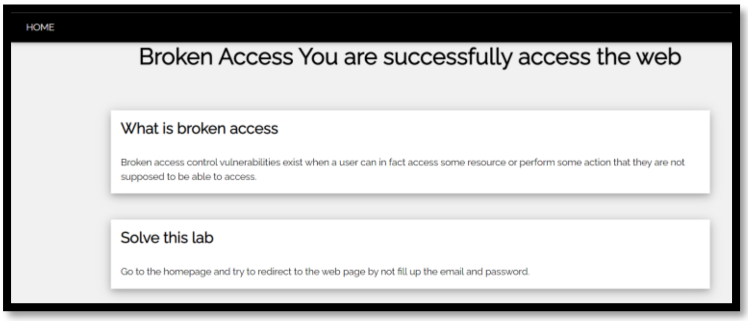
Figure 4.27 countermeasures

iv. Broken Access

Access control ensures that users cannot operate beyond the scope of their authorization. Failures often result in unauthorised information exposure, change or loss of all data, or the execution of a business function outside the user's permissions. The following are frequent instances of access control flaws:

- By modifying the URL, the internal state of the application, or the HTML page, or by utilising a custom API attack tool, it is possible to circumvent access control tests.Allowing the primary key to be changed to another user's record, allowing someone else's account to be seen or edited.
- Privilege is being raised. Performing as a user while signed in as a user or as an administrator when logged in as a user.

ii. Figure below shows the Broken Access system. This lab provide situation for user to answer the question



Broken Access You are successfully access the web

What is broken access

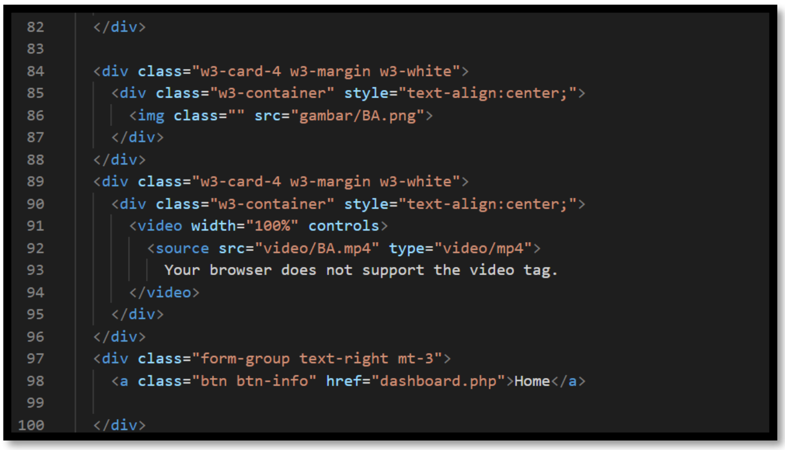
Broken access control vulnerabilities exist when a user can in fact access some resource or perform some action that they are not supposed to be able to access.

Solve this lab

Go to the homepage and try to redirect to the web page by not fill up the email and password.

Figure 4.28 Broken Access

The code of the system



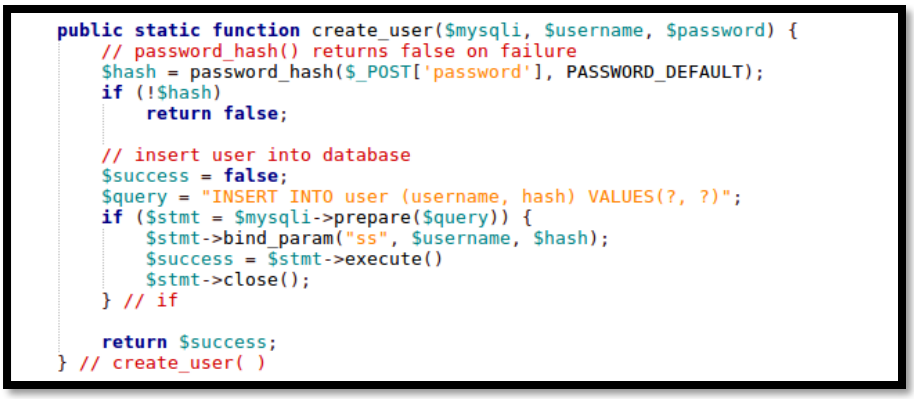
```
</div>

<div class="w3-card-4 w3-margin w3-white">
  <div class="w3-container" style="text-align:center;">
    <img class="" src="gambar/BA.png">
  </div>
</div>
<div class="w3-card-4 w3-margin w3-white">
  <div class="w3-container" style="text-align:center;">
    <video width="100%" controls>
      <source src="video/BA.mp4" type="video/mp4">
        Your browser does not support the video tag.
    </video>
  </div>
</div>
<div class="form-group text-right mt-3">
  <a class="btn btn-info" href="dashboard.php">Home</a>

</div>
```

Figure 4.29 Broken Access Code

Countermeasure

Access control is only effective if it is enforced by trustworthy server-side code or a server-less API where the attacker cannot modify the access control check or metadata. Access to functionality is prohibited by default. Utilize authentication systems that are based on roles and access control lists.

Always use a unique identifier when searching for anything in a database. This ID is typically used in URLs to indicate the kind of information the user is seeking.



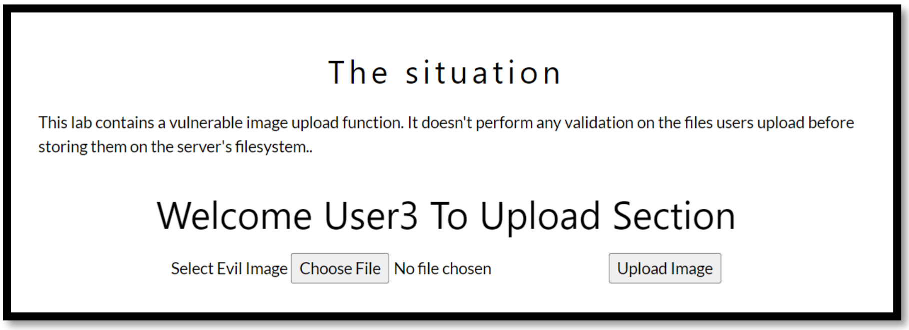
```
public static function create_user($mysqli, $username, $password) {
    // password_hash() returns false on failure
    $hash = password_hash($_POST['password'], PASSWORD_DEFAULT);
    if (!$hash)
        return false;

    // insert user into database
    $success = false;
    $query = "INSERT INTO user (username, hash) VALUES(?, ?)";
    if ($stmt = $mysqli->prepare($query)) {
        $stmt->bind_param("ss", $username, $hash);
        $success = $stmt->execute()
        $stmt->close();
    } // if

    return $success;
} // create_user( )
```

Figure 4.30 Broken Access Countermeasures

v. Unrestricted file upload

File upload vulnerabilities occur when a web server let users to upload files to its filesystem without adequately checking their name, type, content, and size. If these restrictions are not sufficiently enforced, even a basic picture upload facility might be exploited to upload arbitrary and possibly harmful data. This may also include script files on the server that enable remote code execution.

In rare situations, posting the file alone is sufficient to create troubles. Other attacks may include sending a second HTTP request for the file, often to compel the server to run it.



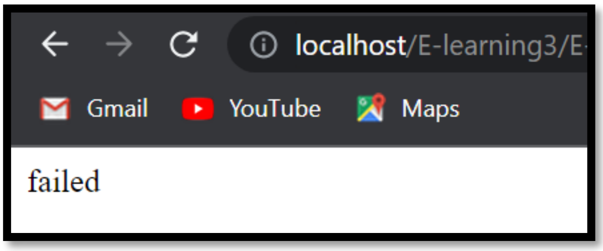
The situation

This lab contains a vulnerable image upload function. It doesn't perform any validation on the files users upload before storing them on the server's filesystem..

Welcome User3 To Upload Section

Figure 4.31 Unrestricted File Upload

Users need to answer the question and do the vulnerabilities testing, as you can see here user need to upload the file location for validation.

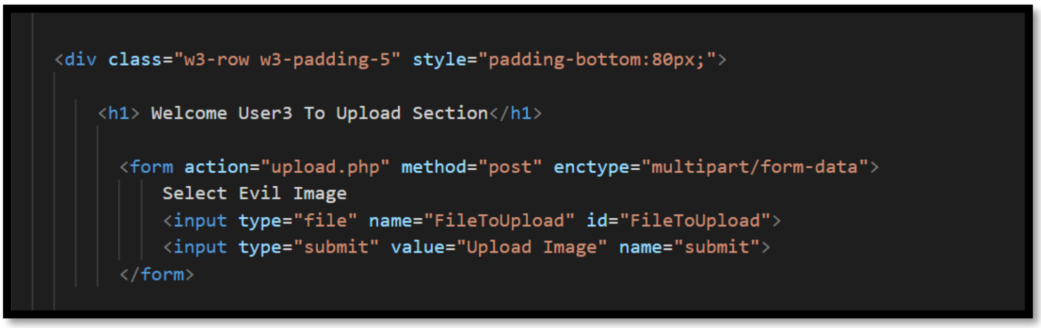


failed

Figure 4.32 Uploaded Validation

User not able to view the file uploaded validation.

The code of the system



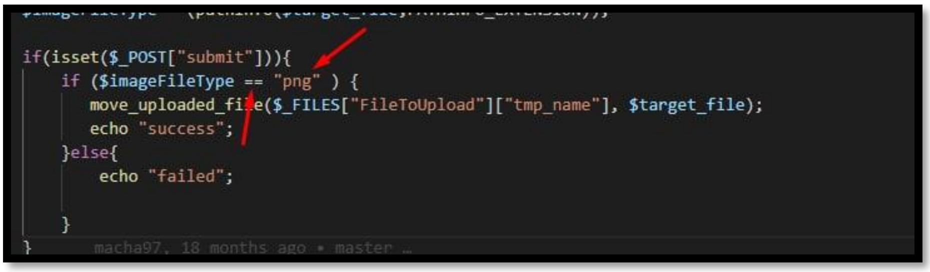
```
<div class="w3-row w3-padding-5" style="padding-bottom:80px;">

    <h1> Welcome User3 To Upload Section</h1>

      <form action="upload.php" method="post" enctype="multipart/form-data">
          Select Evil Image
          <input type="file" name="FileToUpload" id="FileToUpload">
          <input type="submit" value="Upload Image" name="submit">
      </form>
```

Figure 4.33 System Code

Countermeasure

Identifying vulnerabilities in a web server's setup when it parses files with double extensions or executes them by employing a sensitive extension after a delimiter character like as "/" or ";" (e.g. "/file.jpg/index.php" when the "file.jpg" file submitted contains PHP code)

To circumvent case-sensitive restrictions, capitalise a handful of letters (e.g. "file.aSp" or "file.PHp3").

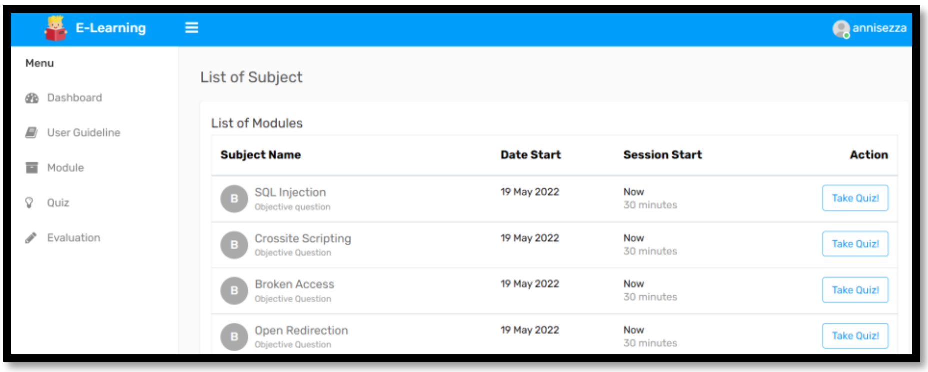


```
if(isset($_POST["submit"])){
    if ($imageFileType == "png" ) {
        move_uploaded_file($_FILES["FileToUpload"]["tmp_name"], $target_file);
        echo "success";
    }else{
         echo "failed";

    }
}       macha97, 18 months ago • master …
```

Figure 4.34 Countermeasure

vi. Quiz (Quizizz)

Quizizz is a learning platform that offers a number of features to make classrooms more interesting, dynamic, and stimulating. As a developer, you may create interactive courses, formative assessments, labs, and other student interactions (of all ages).



List of Subject

List of Modules

Subject Name	Date Start	Session Start	Action
B SQL Injection Objective question	19 May 2022	Now 30 minutes	Take Quiz!
B Crossite Scripting Objective Question	19 May 2022	Now 30 minutes	Take Quiz!
B Broken Access Objective Question	19 May 2022	Now 30 minutes	Take Quiz!
B Open Redirection Objective Question	19 May 2022	Now 30 minutes	Take Quiz!

Figure 4.35 List of Modules

The dashboard for list of subjects for user to answer the quizizz

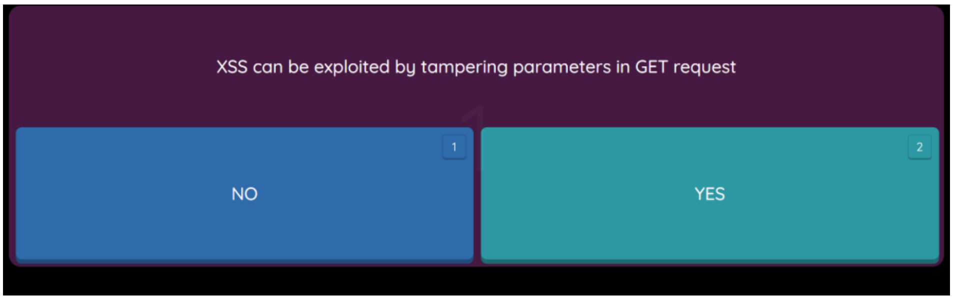
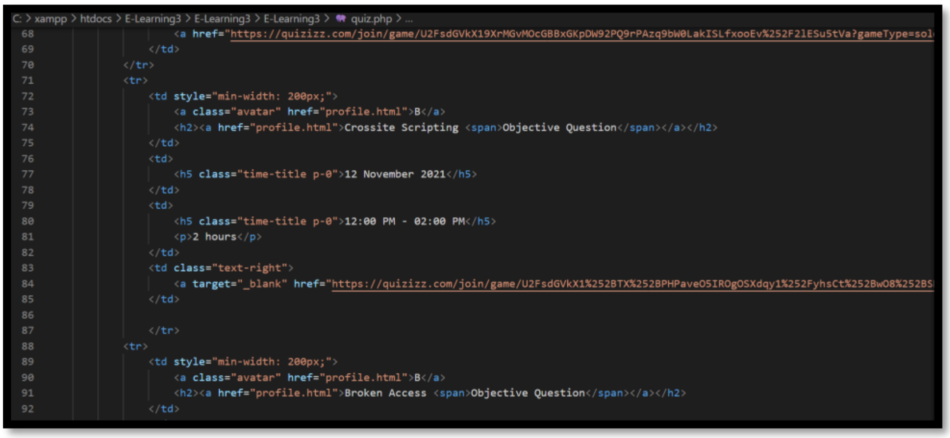

XSS can be exploited by tampering parameters in GET request

Figure 4.36 Quiz in quizizz

This E-learning platform have collaborated with quizizz to make more interactive for user to answer the quiz.

The code of the system:



C: > xampp > htdocs > E-Learning3 > E-Learning3 > E-Learning3 > quiz.php > ...

```
                <a href="https://quizizz.com/join/game/U2FsdGVkX19XrMGvMOcGBBxGKpDW92PQ9rPAzq9bW0LakISLfxooEv%252F21ESu5tVa?gameType=sol
            </td>
        </tr>
        <tr>
            <td style="min-width: 200px;">
                <a class="avatar" href="profile.html">B</a>
                <h2><a href="profile.html">Crossite Scripting <span>Objective Question</span></a></h2>
            </td>
            <td>
                <h5 class="time-title p-0">12 November 2021</h5>
            </td>
            <td>
                <h5 class="time-title p-0">12:00 PM - 02:00 PM</h5>
                <p>2 hours</p>
            </td>
            <td class="text-right">
                <a target="_blank" href="https://quizizz.com/join/game/U2FsdGVkX1%252BTX%252BPHPaveO5IROgOSXdqy1%252FyhsCt%252BwO8%252BS
            </td>

            </tr>
        <tr>
            <td style="min-width: 200px;">
                <a class="avatar" href="profile.html">B</a>
                <h2><a href="profile.html">Broken Access <span>Objective Question</span></a></h2>
            </td>
```

Figure 4.37 System Code

CHAPTER 5: TESTING AND RESULT

5.0 Introduction

In this chapter 5, testing and results will be fully describe and explain. It will include the explanation about security testing, system testing, system functionality testing and the result of the overall testing. Testing and results is an important element before the developer can publish to the public user for them to use the system or the software.

Security testing is a technique aimed to identify flaws in information security processes that safeguard data and retain functioning. Passing security testing does not indicate that there are no flaws or that the system is completely safe, but it does verify that the project has minimal susceptibility to unauthorised users in order to preserve the confidentiality, integrity, and availability of authorised users.The following are the test cases of E-learning: Securing Web Application Hacking and Web Implementation of the Hardening on the Vulnerabilities that involves security requirements.

In brief, the tester will be conduct on nine (9) modules which are:

i. SQL Injection Module (Script Inject)
ii. SQL Injection Module (SQLmap Tool)
iii. Broken Authentication Module (Complex Password)
iv. Broken Authentication Module (Session ID)
v. Broken Authentication Module (Auto Logout)
vi. Broken Authentication Module (System Disabled Temporary)
vii. Sensitive Data Exposure Module (Encrypted Traffic)
viii. Sensitive Data Exposure Module (Encrypted Database)

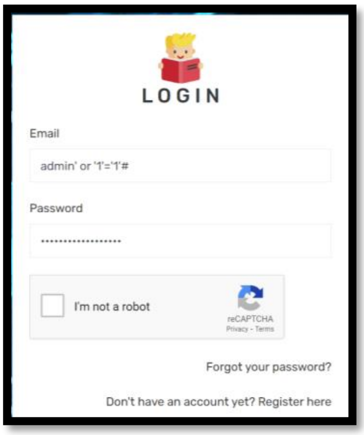
The detail of each of the tests will be explained in the next section.

Test case for register page of E-learning: Securing Web Application Hacking and Web Implementation of the Hardening on the Vulnerabilities

i. Table shows the test case of SQL Injection Module (Script Insertion). This test is to ensure that this E-leaning is secured from Script for SQL Injection Attack.

TEST	ID TID07
Description	To test the SQL Injection for Script Insertion vulnerability at the login page.
Precondition	User needs to have access to input box in the web browser (email and password) such as below.
Input definition	• Insert script (' OR '1'='1) in the email and password box • Insert script (' OR '1'='1--) in the email and password box • Insert script ('OR '1'='1'(payload success sql syntax error)) in the email and password box • (' or '1'='1'--)in the email and password box • Insert script (admin' or '1'='1'#)(payload success sql redirect to sql page error) in the email and password box
Output Definition	System refresh to Login Page.
Remark	E-learning is not vulnerable to SQL Injection for Script Insertion based on Figure below

Table 5.1 Injection Module



LOGIN

Email

admin' or '1'='1'#

Password

....

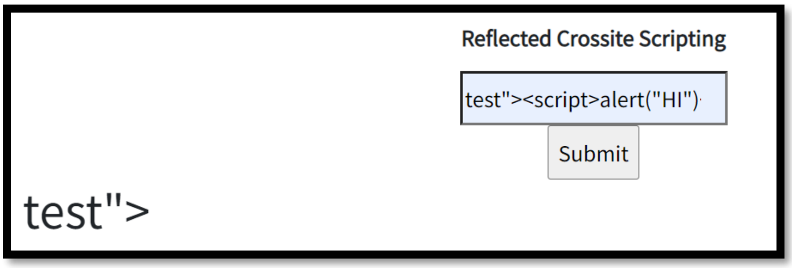
Figure 5.1 Login

ii. **Cross site Scripting for E-learning page**

Table 5.2 shows the test case of Cross site Scripting Module (Script Insertion). This test is to ensure that this E-leaning is secured from Script for crosstie scripting Attack.

TEST	ID WSTG-INPV-01
Description	To test crosstie scripting Insertion vulnerability at the dashboard E-learning page.
Precondition	User needs to have access to input box of malicious HTML script in the web browser such as below.
Input definition	• test"><script>alert("HI")</script> at the box given.
Output Definition	System refresh and not popup the cross site scripting vulnerabilities
Remark	E-learning is not vulnerable to crosstie scripting for Script Insertion malicious HTML and Java script based on Figure below

Table 5.2 Cross site Scripting



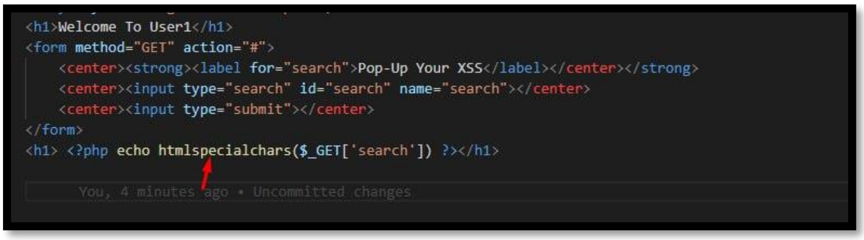
Reflected Crossite Scripting

test"><script>alert("HI")

test">

Figure 5.2 Cross site Scripting

Countermeasure:



```
<h1>Welcome To User1</h1>
<form method="GET" action="#">
    <center><strong><label for="search">Pop-Up Your XSS</label></center></strong>
    <center><input type="search" id="search" name="search"></center>
    <center><input type="submit"></center>
</form>
<h1> <?php echo htmlspecialchars($_GET['search']) ?></h1>

    You, 4 minutes ago • Uncommitted changes
```

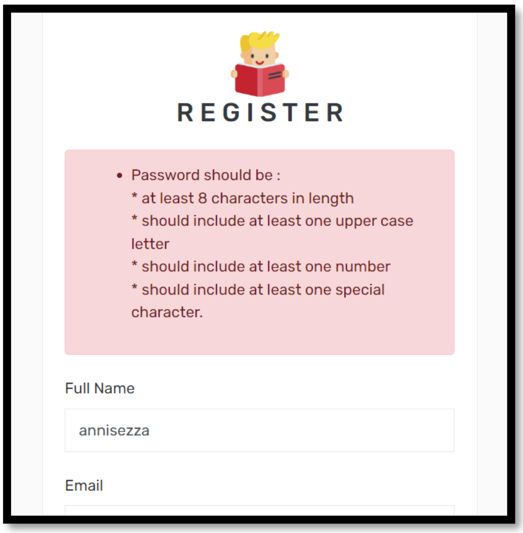
Figure 5.3 Countermeasures

iii. Broken Authentication Module (Complex Password)

Table 5.3 shows the test case of Broken Authentication Module (Complex Password). This test is to ensure the E-learning platform require complex password registration only.

TEST	ID TID09
Description	To test the strength of password required in E-learning system by doing brute force attack using burp suite.
Precondition	Setup proxy as network preference at web browser. Setup proxy with port 8080 at burp suite.
Input definition	• User cannot simply create password by not contain combination characters ((e.g., a-z, A-Z, 0-9).
Output Definition	The payloads failed to guess and brute force the password due to complex password
Remark	E-learning is not vulnerable to broken authentication in registration platform.

Table 5.3 Broken Authentication



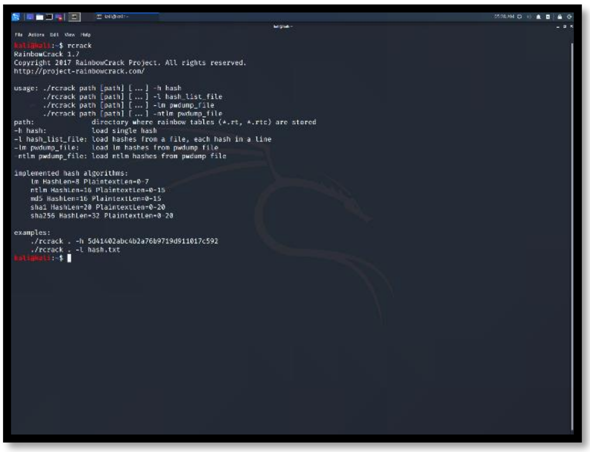
- Password should be :
  * at least 8 characters in length
  * should include at least one upper case letter
  * should include at least one number
  * should include at least one special character.

Full Name

annisezza

Email

Figure 5.4 Register



```
kali@kali:~$ rcrack
RainbowCrack 1.7
Copyright 2017 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: ./rcrack path [path] [...] -h hash
       ./rcrack path [path] [...] -l hash_list_file
       ./rcrack path [path] [...] -lm pwdump_file
       ./rcrack path [path] [...] -ntlm pwdump_file
path:              directory where rainbow tables (*.rt, *.rtc) are stored
-h hash:           load single hash
-l hash_list_file: load hashes from a file, each hash in a line
-lm pwdump_file:   load lm hashes from pwdump file
-ntlm pwdump_file: load ntlm hashes from pwdump file

implemented hash algorithms:
    lm HashLen=8 PlaintextLen=0-7
    ntlm HashLen=16 PlaintextLen=0-15
    md5 HashLen=16 PlaintextLen=0-15
    sha1 HashLen=20 PlaintextLen=0-20
    sha256 HashLen=32 PlaintextLen=0-20

examples:
    ./rcrack . -h 5d41402abc4b2a76b9719d911017c592
    ./rcrack . -l hash.txt
kali@kali:~$ 
```

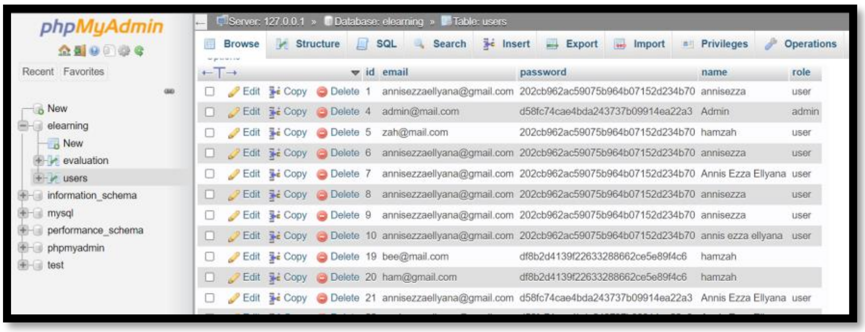
Figure 5.5 Attack

iv. **Sensitive Data Exposure Module (Encrypted Database)**

Table 5.4 shows the test case of Sensitive Data Exposure Module (Encrypted Database). This test is to ensure that data user such as password encrypt.

TEST	ID TID09
Description	Database encryption ensures that data in the system is saved in an encrypted format. This means that until an attacker or malware has access to your database, they won't be able to see the sensitive data.
Precondition	• E-learning system need to encrypt user's input by put the encryption code in the : • php configuration file. • User password. • User admin.
Input definition	• User insert Registration Key. • User clicks "Register" button. • User insert username, password, and email. • User clicks "Register" button. • User enter phpMyAdmin page with configured username and password.
Output Definition	User will see encrypted password to do a payload of password.
Remark	E-learning is not vulnerable to sensitive data exposure by encrypted password in the database system.

Table 5.4 Encrypted Database



Server: 127.0.0.1 » Database: elearning » Table: users

				id	email	password	name	role
□	Edit	Copy	Delete	1	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□	Edit	Copy	Delete	4	admin@mail.com	d58fc74cae4bda243737b09914ea22a3	Admin	admin
□	Edit	Copy	Delete	5	zah@mail.com	202cb962ac59075b964b07152d234b70	hamzah	user
□	Edit	Copy	Delete	6	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□	Edit	Copy	Delete	7	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	Annis Ezza Ellyana	user
□	Edit	Copy	Delete	8	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□	Edit	Copy	Delete	9	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□	Edit	Copy	Delete	10	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annis ezza ellyana	user
□	Edit	Copy	Delete	19	bee@mail.com	df8b2d4139f22633288662ce5e89f4c6	hamzah	
□	Edit	Copy	Delete	20	ham@gmail.com	df8b2d4139f22633288662ce5e89f4c6	hamzah	
□	Edit	Copy	Delete	21	annisezzaellyana@gmail.com	d58fc74cae4bda243737b09914ea22a3	Annis Ezza Ellyana	user

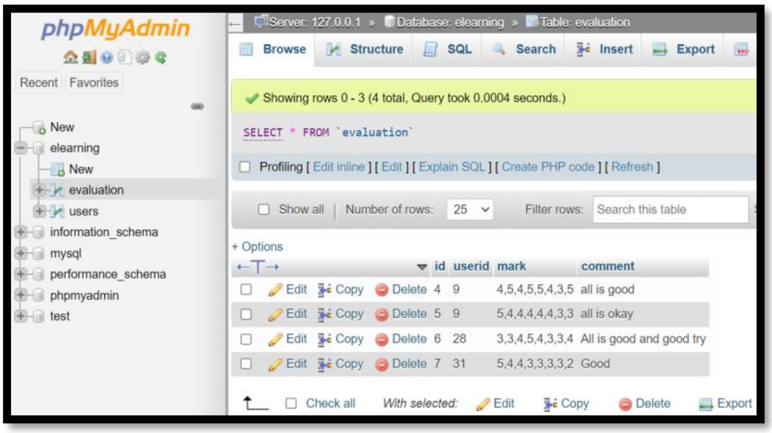
Figure 5.6 Database

v. Sensitive Data Exposure Module (Encrypted Database for admin)

Table 5.5 shows the test case of Sensitive Data Exposure Module (Encrypted Database password for admin). This test is to ensure that data user such as password encrypt.

Table 5.5 Encrypted Database for Admin

TEST	ID TID09
Description	• Database encryption ensures that data in the system is saved in an encrypted format. This means that until an attacker or malware has access to your database, they won't be able to see the sensitive data. • Using Unique ID for password to ensure public user cannot simply delete the database on the system.
Precondition	• E-learning system need to encrypt user's input by put the encryption code in the: • php configuration file. • User password. • User admin.
Input definition	• User insert Registration Key. • User clicks "Register" button. • User insert username, password, and email. • User clicks "Register" button. • User enter phpMyAdmin page with configured username and password.
Output Definition	User will see encrypted password to do a payload of password.
Remark	E-learning is not vulnerable to sensitive data exposure by encrypted password in the database system.



Showing rows 0 - 3 (4 total, Query took 0.0004 seconds.)

```
SELECT * FROM `evaluation`
```

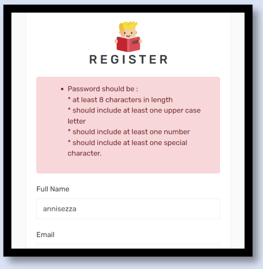
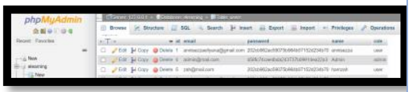
□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

□ Show all | Number of rows: 25 Filter rows: Search this table

	id	userid	mark	comment
□ Edit Copy Delete	4	9	4,5,4,5,5,4,3,5	all is good
□ Edit Copy Delete	5	9	5,4,4,4,4,4,3,3	all is okay
□ Edit Copy Delete	6	28	3,3,4,5,4,3,3,4	All is good and good try
□ Edit Copy Delete	7	31	5,4,4,3,3,3,3,2	Good

Figure 3 Database using Unique ID

vi. **Result Test Cases**

Test ID	Module	Description	Expected Result	Results
TID01	User Registration Module  REGISTER • Password should be : * at least 8 characters in length * should include at least one upper case letter * should include at least one number * should include at least one special character. Full Name annisezza Email	To check either user can simply create a simple password.	User create password by contain combination characters ((e.g., a-z, A-Z, 0-9).	**Pass**
TID02	User Authentication Module - Only admin and user registered can access the system  phpMyAdmin Recent Favorites New Browse Structure SQL Search Insert Export Import Privileges Operations email password Edit Copy Delete	To check multi-factor authentication for user to login	User can access surveillance system interphase after the multi-factor authentication which is password and email	**Pass**
TID03	SQL Injection Module (Content URL)	To test the SQL Injection for Content URL vulnerability	User cannot go to any other content page by editing the URL directly.	**Pass**
TID04	SQL Injection Module (Script Insertion)	To test the SQL Injection for	User/attacker cannot inject code	**Pass**

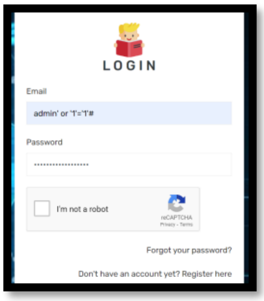
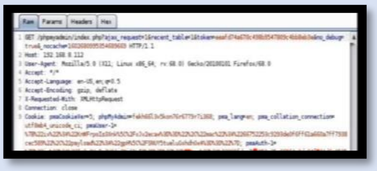
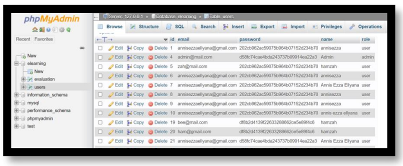
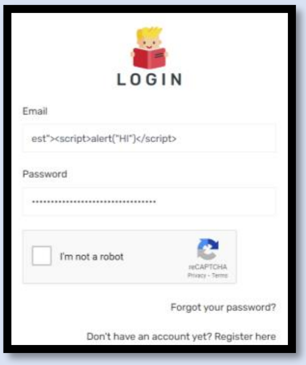
		Script Insertion vulnerability	database. System refresh to Login Page	
TID05	Broken Authentication Module (Complex Password) 	To test complex password feature using brute force attack	The user cannot brute force the username and password	**Pass**
TID06	Sensitive Data Exposure Module (Encrypted Database) 	To test either the system encrypts the data before saving into database	The system encrypts the data before saving into database via php code	**Pass**
TID07	Crosstie scripting 	User needs to have access to input box of malicious HTML script in the web browser.	E-learning is not vulnerable to crosstie scripting for Script Insertion malicious HTML and Java script	**Pass**

Table 5.6 Result Test Cases

LOGIN

Email: admin' or '1'='1'#

Password: ••••••••••••••••

□ I'm not a robot

```
GET /phpmyadmin/index.php?ajax_request=1&recent_table=1&token=[illegible]&no_debug=
true&_nocache=[illegible] HTTP/1.1
Host: 192.168.0.112
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Cookie: pmaCookieVer=5; phpMyAdmin=[illegible]; pma_lang=en; pma_collation_connection=
utf8mb4_unicode_ci; pmaUser-1=
[illegible]
[illegible]; pmaAuth-1=
```

	id	email	password	name	role
□ Edit Copy Delete	1	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□ Edit Copy Delete	4	admin@mail.com	d58fc74cae4bda243737b09914ea22a3	Admin	admin
□ Edit Copy Delete	5	zah@mail.com	202cb962ac59075b964b07152d234b70	hamzah	user
□ Edit Copy Delete	6	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□ Edit Copy Delete	7	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	Annis Ezza Ellyana	user
□ Edit Copy Delete	8	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□ Edit Copy Delete	9	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annisezza	user
□ Edit Copy Delete	10	annisezzaellyana@gmail.com	202cb962ac59075b964b07152d234b70	annis ezza ellyana	user
□ Edit Copy Delete	19	bee@mail.com	df8b2d4139f22633288662ce5e89f4c6	hamzah	
□ Edit Copy Delete	20	ham@gmail.com	df8b2d4139f22633288662ce5e89f4c6	hamzah	
□ Edit Copy Delete	21	annisezzaellyana@gmail.com	d58fc74cae4bda243737b09914ea22a3	Annis Ezza Ellyana	user

LOGIN

Email: est"><script>alert("HI")</script>

Password: ••••••••••••••••••••••••••••••

□ I'm not a robot

CHAPTER 6: CONCLUSION AND RECOMMENDATION

6.1 Introduction

This Chapter will explain the objectives that have been achieved in this project. This Chapter includes the achievement details, the conclusion, and the future recommendation of the project for future enhancement.

6.2 Conclusion

In conclusion, E-learning Securing Web Application Hacking Security and Implementation Hardening On The Vulnerabilities is application that is purposefully insecure. It assists web security enthusiasts, developers, and students in identifying and preventing web vulnerabilities. This E-learning web application training programme equips people to execute successful penetration testing and ethical hacking projects In addition to the function, there are secure coding, development and architecture which are the main components of this project. The prototype also has been tested to ensure the system works successfully. Plus, the testing result shows the system have meet the project goal and all the scopes mentioned in Chapter 1.

6.3 Review Objectives

The objectives of the project are to construct a E-learning: Securing Web Application Hacking Security and Implementation Hardening on The Vulnerabilities platform. The system should be secure and user-friendly. The main goal to be reviewed are: -

1. The purpose is to study on how to create a platform for educate student and new learner on how to secure the web application by implement the OWASP top 10 vulnerabilities
   - ➢ The objective is achieved. The developer studied all web vulnerabilities and chose top 5 OWASP vulnerabilities as the security scopes of this project.

2. To develop secured E-learning platform for beginner to learn secured web application based on selected OWASP ranking.
   - ➢ The objective is achieved. Based on the result, this E-learning platform, user able to answer the lab given and gain more knowledge based on the video and text given.

3. To test E-learning platform with countermeasure features.
   - ➢ The objective is achieved. The system E-learning platform are successfully complete by focusing lab on Top 10 OWASP which is, Sql Injection, Crosstie Scripting, Open Redirection, Broken Access, Unrestricted file upload.

6.4 Project Limitation

Each project has limitation when developing a system that is based on hardware and software. For this project, the limitation that we found is to harden the vulnerabilities based on the lab that have been created. It needs high knowledge to educate user especially for new beginner. Other than that, the limitation is do not able to access to the server (http) web, the module cannot be access for user.

Furthermore, limitation of high cost to do collaboration with quiz platform,lack skill and availability.

6.5 Recommendation

This project has been created and executed with success. In the following phase of study, however, it may be enhanced to focus on more sophisticated and superior systems. There are three recommendations for future enhancement to be done. To approve a legal user, the system must first replace the secondary authentication (PIN number) with a One-Time Password (OTP). To login, the user must enter the proper PIN number OTP.

Aside from that, we wish to partner with several developers to make the quiz more interactive.Next, in term of security development, our suggestion for future enhancement is to patch more security scopes which are Cross Site Scripting (XSS) and Broken Access Control. We suggest XSS because it is one of OWASP Top 10 and can be done remotely.. By implementing all of these security elements, we are confident that this system will be more robust and secure from all of the possible threats.

REFERENCES

(PDF) security issues in e-learning system - researchgate. (n.d.). Retrieved June 11, 2022, from https://www.researchgate.net/publication/339562121_Security_issues_in_E-Learning_system

Boyle, P. (2022, May 12). The best 20 online quiz makers for boosting user engagement in 2022. Retrieved June 11, 2022, from https://blog.hubspot.com/marketing/quiz-maker

IJCSIS, J. (2016, August 19). E-Learning Systems Risks and their security. Retrieved June 11, 2022, from https://www.academia.edu/27901621/E_Learning_Systems_Risks_and_their_Security

Owasp releases their top 10 most critical application security risks for 2017. (n.d.). Retrieved June 11, 2022, from https://www.titanhq.com/blog/owasp-releases-their-top-10-most-critical-application-security-risks-for-20/?utm_campaign=AD-PM-SpamTitan-T1&acctid=THQ&utm_source=Adwords&utm_medium=PPC&keyword=&matchtype=&campaignid=14035790152&adgroupid=&gclid=Cj0KCQjw-pCVBhCFARIsAGMxhAdm0r0f3bwDdk1y0lh4FoXamfkpVikOMcAhG2EaCjnbT0qJDdqK-p0aAsRYEALw_wcB&network=x&device=c

Rostrypa, D. (n.d.). How to create an e-learning platform: Tips & tricks. Retrieved June 11, 2022, from https://stormotion.io/blog/how-to-create-an-e-learning-platform-of-your-own/

Rostrypa, D. (n.d.). How to create an e-learning platform: Tips & tricks. Retrieved June 12, 2022, from https://stormotion.io/blog/how-to-create-an-e-learning-platform-of-your-own/

Security. (n.d.). Retrieved June 11, 2022, from https://www.elearninglearning.com/security/

TwitterGitHub, M., Nalpas, M., & TwitterGitHub. (n.d.). When to use HTTPS for local development. Retrieved June 11, 2022, from https://web.dev/when-to-use-local-https/

What is Data Encryption? (2021, May 06). Retrieved June 14, 2022, from https://www.forcepoint.com/cyber-edu/data-encryption

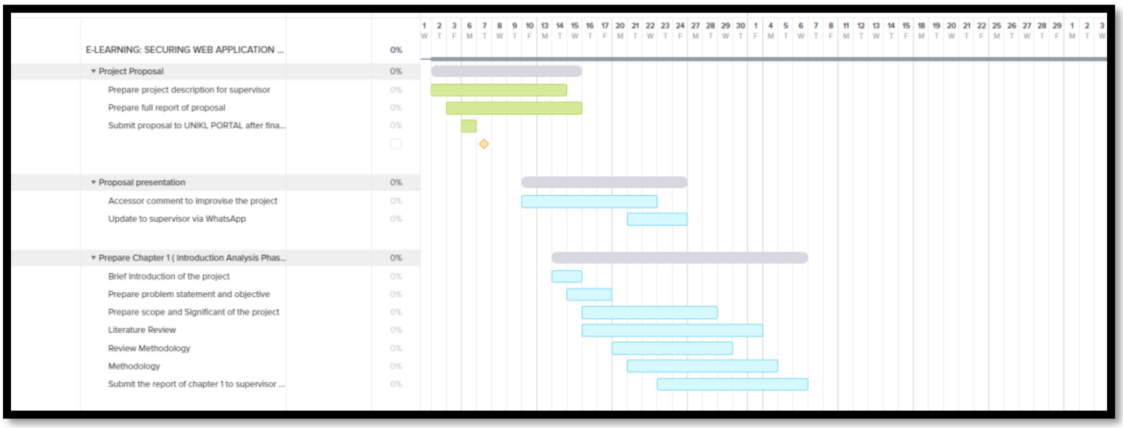
15 best ✳ interactive E-learning web apps for online classroom. (2022, May 26). Retrieved June 14, 2022, from https://colorwhistle.com/top-e-learning-web-apps/

Western province elearning. (n.d.). Retrieved June 14, 2022, from https://www.inclusiveducation.com/wp-elearning

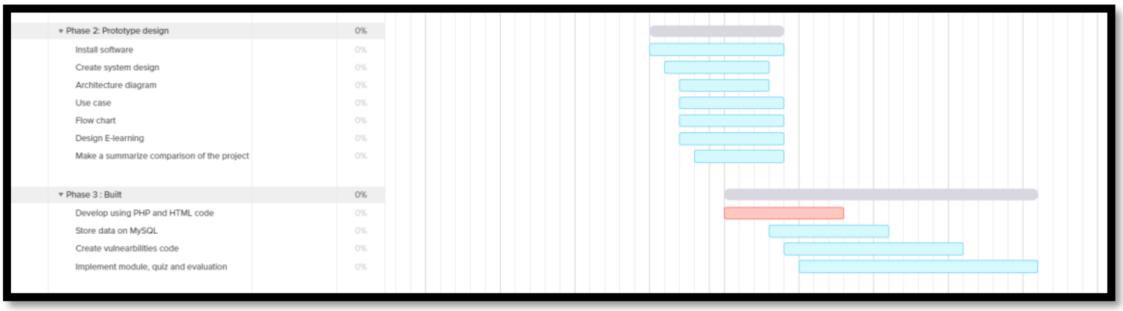
Janobe. (n.d.). Retrieved June 14, 2022, from https://www.sourcecodester.com/php/12808/e-learning-system-using-phpmysqli.html

10 essential steps to improve your website security. (n.d.). Retrieved June 14, 2022, from https://www.computer.org/publications/tech-news/trends/10-essential-steps-to-improve-your-website-security

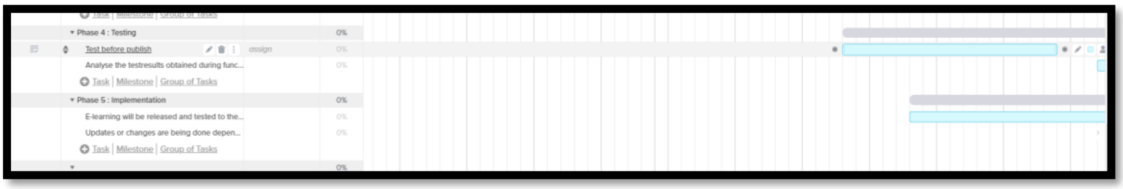
Grant chart.



E-LEARNING: SECURING WEB APPLICATION ...	0%
▾ Project Proposal	0%
Prepare project description for supervisor	0%
Prepare full report of proposal	0%
Submit proposal to UNIKL PORTAL after fina...	0%
	□
▾ Proposal presentation	0%
Accessor comment to improvise the project	0%
Update to supervisor via WhatsApp	0%
▾ Prepare Chapter 1 (Introduction Analysis Phas...	0%
Brief Introduction of the project	0%
Prepare problem statement and objective	0%
Prepare scope and Significant of the project	0%
Literature Review	0%
Review Methodology	0%
Methodology	0%
Submit the report of chapter 1 to supervisor ...	0%



▾ Phase 2: Prototype design	0%
Install software	0%
Create system design	0%
Architecture diagram	0%
Use case	0%
Flow chart	0%
Design E-learning	0%
Make a summarize comparison of the project	0%
▾ Phase 3 : Built	0%
Develop using PHP and HTML code	0%
Store data on MySQL	0%
Create vulnearbilities code	0%
Implement module, quiz and evaluation	0%

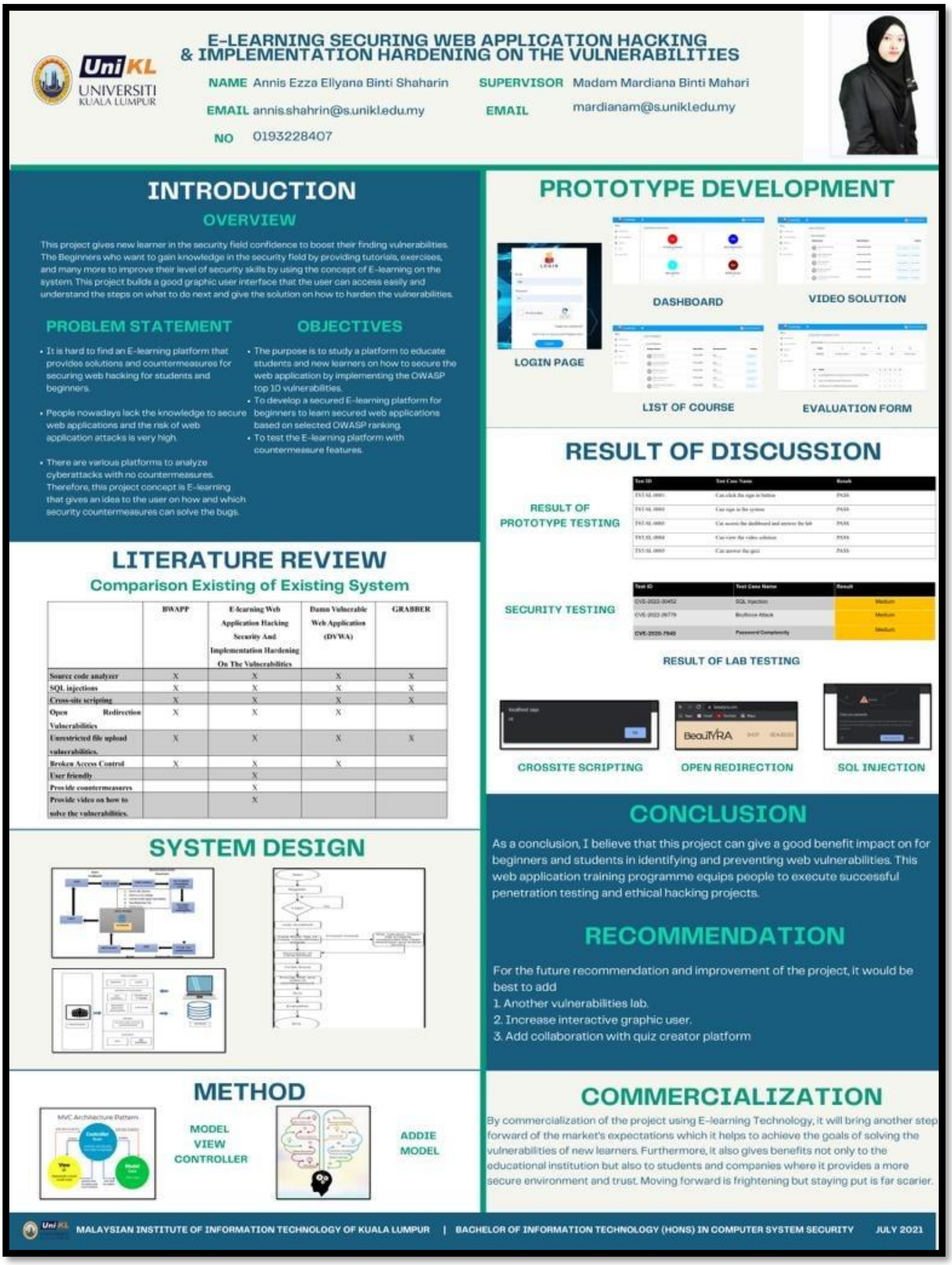


Task | Milestone | Group of Tasks

▾ Phase 4 : Testing		0%
Test before publish	assign	0%
Analyse the testresults obtained during func...		0%
▾ Phase 5 : Implementation		0%
E-learning will be released and tested to the...		0%
Updates or changes are being done depen...		0%
▾		0%

Task | Milestone | Group of Tasks
Task | Milestone | Group of Tasks

Poster



E-LEARNING SECURING WEB APPLICATION HACKING & IMPLEMENTATION HARDENING ON THE VULNERABILITIES

UniKL UNIVERSITI KUALA LUMPUR

NAME Annis Ezza Ellyana Binti Shaharin
EMAIL annis.shahrin@s.unikl.edu.my
NO 0193228407

SUPERVISOR Madam Mardiana Binti Mahari
EMAIL mardianam@s.unikl.edu.my

INTRODUCTION

OVERVIEW

This project gives new learner in the security field confidence to boost their finding vulnerabilities. The Beginners who want to gain knowledge in the security field by providing tutorials, exercises, and many more to improve their level of security skills by using the concept of E-learning on the system. This project builds a good graphic user interface that the user can access easily and understand the steps on what to do next and give the solution on how to harden the vulnerabilities.

PROBLEM STATEMENT

- It is hard to find an E-learning platform that provides solutions and countermeasures for securing web hacking for students and beginners.
- People nowadays lack the knowledge to secure web applications and the risk of web application attacks is very high.
- There are various platforms to analyze cyberattacks with no countermeasures. Therefore, this project concept is E-learning that gives an idea to the user on how and which security countermeasures can solve the bugs.

OBJECTIVES

- The purpose is to study a platform to educate students and new learners on how to secure the web application by implementing the OWASP top 10 vulnerabilities.
- To develop a secured E-learning platform for beginners to learn secured web applications based on selected OWASP ranking.
- To test the E-learning platform with countermeasure features.

LITERATURE REVIEW

Comparison Existing of Existing System

	BWAPP	E-learning Web Application Hacking Security And Implementation Hardening On The Vulnerabilities	Damn Vulnerable Web Application (DVWA)	GRABBER
Source code analyzer	X	X	X	X
SQL injections	X	X	X	X
Cross-site scripting	X	X	X	X
Open Redirection Vulnerabilities	X	X	X	
Unrestricted file upload vulnerabilities.	X	X	X	X
Broken Access Control	X	X	X	
User friendly		X		
Provide countermeasures		X		
Provide video on how to solve the vulnerabilities.		X		

SYSTEM DESIGN

METHOD

MODEL VIEW CONTROLLER

ADDIE MODEL

PROTOTYPE DEVELOPMENT

LOGIN PAGE

DASHBOARD

VIDEO SOLUTION

LIST OF COURSE

EVALUATION FORM

RESULT OF DISCUSSION

RESULT OF PROTOTYPE TESTING

Test ID	Test Case Name	Result
TST-SL-0001	Can click the sign in button	PASS
TST-SL-0002	Can sign in the system	PASS
TST-SL-0003	Can access the dashboard and answer the lab	PASS
TST-SL-0004	Can view the video solution	PASS
TST-SL-0005	Can answer the quiz	PASS

SECURITY TESTING

Test ID	Test Case Name	Result
CVE-2022-30452	SQL Injection	Medium
CVE-2022-26779	Bruteforce Attack	Medium
CVE-2020-7840	Password Complexity	Medium

RESULT OF LAB TESTING

CROSSITE SCRIPTING

OPEN REDIRECTION

SQL INJECTION

CONCLUSION

As a conclusion, I believe that this project can give a good benefit impact on for beginners and students in identifying and preventing web vulnerabilities. This web application training programme equips people to execute successful penetration testing and ethical hacking projects.

RECOMMENDATION

For the future recommendation and improvement of the project, it would be best to add

1. Another vulnerabilities lab.
2. Increase interactive graphic user.
3. Add collaboration with quiz creator platform

COMMERCIALIZATION

By commercialization of the project using E-learning Technology, it will bring another step forward of the market's expectations which it helps to achieve the goals of solving the vulnerabilities of new learners. Furthermore, it also gives benefits not only to the educational institution but also to students and companies where it provides a more secure environment and trust. Moving forward is frightening but staying put is far scarier.

MALAYSIAN INSTITUTE OF INFORMATION TECHNOLOGY OF KUALA LUMPUR | BACHELOR OF INFORMATION TECHNOLOGY (HONS) IN COMPUTER SYSTEM SECURITY JULY 2021