Faculty of Computer Science and Information Technology

OWASP A03 Injection vulnerability in Web Application Development

Andy Chieng Ging Wei

Bachelor of Computer Science with Honours (Software Engineering)

2023

OWASP A03 Injection vulnerability in Web Application Development

ANDY CHIENG GING WEI

This project is submitted in partial fulfilment of the requirements for the degree of Bachelor of Computer Science with Honours (Software Engineering)

Faculty of Computer Science and Information Technology

UNIVERSITI MALAYSIA SARAWAK

2023

KERENTANAN SUNTIKAN OWASP A03 DALAM PEMBANGUNAN APLIKASI WEB

ANDY CHIENG GING WEI

Projekinimerupakan salah satukeperluanuntuk Ijazah Sarjana Muda Sains KomputerdenganKepujian (KejuruteraanPerisian)

Fakulti Sains Komputer dan Teknologi Maklumat

UNIVERSITI MALAYSIA SARAWAK

2023

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE OWASP A03 Injection vulnerability in Web Application Development

ACADEMIC SESSION: _ 2022/2023

ANDY CHIENG GING WEI

(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☑	UNRESTRICTED	

Validated by

HUDI

_____ _____

(AUTHOR'S SIGNATURE) (SUPERVISOR'S SIGNATURE)

Permanent Address

2F, Jalan Kulas Timur

96000, Sibu Sarawak

Date: 30/6/2023 Date: _____

Note * Thesis refers to PhD, Master, and Bachelor Degree

** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

DECLARATION

I hereby declare that this project is my original work. I have not copied from any other student's work or from any other sources except where due reference or acknowledgement is not made explicitly in the text, nor has any part had been written for me by another person.

Hudi

…….

(Andy Chieng Ging Wei) 01July 2023

Matric No: 69073

ACKNOWLEDGEMENT

I would like to thank my supervisor, Dr. Lim Phei Chin for the advice, guidance, and encouragement throughout my final year project. I would also like to thank my examiner which is Dr.Ling Yeong Tyng for the advice on this project. Iwould also like to thank the God to give me wisdom in doing this project. I would also like to thank my friends and my family who gave me opinions and help me throughout my final year project.

ABSTRACT

In this information technologies era, more and more hacker appeared to attack the vulnerable web application on the internet. As a web developer to be, the junior web developer has to be equipped with knowledge and be prepared to handle the common vulnerability in web application. To accommodate with this goal, this project is being proposed and developed to teach the web developer on the fundamental about Open Web Application Security Project (OWASP) Top 10, focusing on OWASP Top 10 A03 - Injection vulnerability. OWASP A03 Injection vulnerability is one of the most common vulnerabilities can be found in the web application. In this web application, web developer will be well-educated on the vulnerability as well as the defencing ways to enhance the security of the web application developed that can defenceagainst this vulnerability. Besides, several research paper and the existing application related will be reviewed as a resource of requirement gathering which helps in designing on the functionality and features of web application complied with OWASP A03 Injection vulnerability. Other than that, the development of the web application will be documented. Besides, the result on testing on the web application will be analysed in this report. From the positive result gained from testers involved in both laboratory usability testing and usability testing using system usability scale, it is believed that this project can help to increase understanding of the web developer on the OWASP A03 vulnerability.

ABSTRAK

Pada era teknologimaklumatini, semakinbanyakpenggodammenyerangaplikasi web yang rentan di internet. Sebagaipembangun web, pembangun web junior harusdilengkapidenganpengetahuan dan bersediauntukmenanganikerentananumumdalamaplikasi web. Untukmemenuhitujuanini, projekinidicadangkan dan dikembangkanuntukmengajarpembangun web mengenaiasasmengenai Open Web Application Security Project (OWASP) Top 10, memberitumpuankepada OWASP Top 10 A03 - Kerentanansuntikan. Kerentanansuntikan OWASP A03 adalah salah satukelemahan yang paling biasadijumpaidalamaplikasi web. Dalamaplikasi web ini, pembangun web akanberpendidikantinggimengenaikerentanansertacara-carapertahananuntukmeningkatkankeselamatanaplikasi web yang dikembangkan yang dapatmempertahankandiridarikerentananini. Selainitu, beberapamakalahpenyelidikan dan aplikasi yang adaakandikajisebagaisumberpengumpulankeperluan yang membantudalammerancangfungsi dan ciriaplikasi web yang mematuhikerentananSuntikan OWASP A03. Selainitu, pengembanganaplikasi web akandidokumentasikan. Selainitu, hasilpengujian pada aplikasi web akandianalisisdalamlaporanini. Dari hasilpositif yang diperolehdaripadapenguji yang terlibatdalamujiankebolehgunaanmakmal dan ujiankebolehgunaanmenggunakanskalakebolehgunaansistem, dipercayaibahawaprojekinidapatmembantumeningkatkanpemahamanpembangun web mengenaikerentanan OWASP A03.

Table of Contents

List of Figures

List of Tables

CHAPTER ONE: INTRODUCTION

1.1 Background

Starting from a few decades ago, informationtechnology has grown exponentially. Various information technology like World Wide Web (WWW) hademerged in the current market. Talking about the world wide web,Jacksi and Abass (2019) defined web as "Sharing of information, document and resource between users across the internet and also it is as tunnel to access storage data on serves and display it on client by browser through the internet, information is related to on client by browser through the internet, information is related to gather by links that include text, picture, sound, video." The very first web is developed by the British scientist, Tim Berners-Lee. The concept of Web1.0 was then designed as the first model of web which can only display information to the client without posting anything. In 1999, Darcy DiNucci announced the Web 2.0 which became famous in the year 2004. In web 2.0,it has the capability to perform read and write operation and is known as Participative and Social Web. One of the most famous Web 2.0 applications is Facebook where the clients can connect and interact with each other across the internet. In 2015, Web 2.0 is further upgraded to Web 3.0, established as semantic network or in the other words, "Internet of Things".

As web technologies expand, web application security becomes one of the biggest concerns especially for large organizations or companies. This is because there are getting more and more illegal cyber-attack had been carried out towards the web application for stealing clients' personal data, like Personal Identifiable Information (PII) and Personal Health Information (PHI)(Singh et al., 2021) by cybercriminal like Black Hat Hackers. Thepersonal data of the client might be used by the hacker to do illegal activity, for example, uses of victims' identity to pretend as the victim, and carry out scam activities among the victims' friend zones. Thus, it is very necessary to have the proper and effective way to prevent cyber-attack to minimize the chance for the leakage of the web users' personal data.

To accommodate this situation, a non-profit organization, Open Web Application Security Project (OWASP) has come up with a standard which can be used as a guideline by the web developer to enhance their web application's security. Those standards or guidelines are also known as OWASP Top 10.

Lala et al. (2021) claims that currently there is an overwhelming number of vulnerability in any of the web application during development phase. OWASP Top 10 provides resources, documentation, and tools that assist security analysts, pen testers, developers, and hobbyists in addressing vulnerabilities. Hence, having OWASP Top 10 as a security guildline for the developer to patch the vulnerabilities listed in OWASP Top 10 is the most efficient way to enhance the web security.

OWASP Top 10 contains top 10 common web application security risks in the current market. This standard will be updated once in four year. According to the latest OWASP version, which is OWASP Top 10 2021(Introduction, 2021), the rank of the common web application security risks are:

A01: Broken Access Control

A02: Cryptographic Failures

A03: Injection

A04: Insecure Design

A05: Security Misconfiguration

A06: Vulnerable and Outdated Components

A07: Identification and Authentication Failures

A08: Software and Data Integrity Failures

A09: Security Logging and Monitoring Failures

A10: Server-Side Request Forgery

1.2 Problem Statement

In this era with exponential growth of information technologies, there are more and more web applications developed by the web developer which are widely being used by the public. Those web applications might require user's personal data such as name, ID number or even bank card number or bank account for web application like e-commerce application. If the web security of those web applications is not high enough, hackers can attack the web application through injection attack. According to OWASP (Introduction, 2021), the injection attack is categorized as A03 Injection vulnerability which rank at the top 3 in the OWASP Top 10. The most common injection attack in A03 injection vulnerability are SQL Injection and Cross-Site Scripting (XSS) injection(Williams, Jmanico, & Kingthorin, 2021). Through the injection attack like SQL Injection, the attacker can have full access to the web application database. This situation may lead to the exposure of the users' personal data or their sensitive data. Sensitive data like bank card numbers might be used by the attacker to transfer the users' wealth. Thus, it is very important to protect user personal data and their sensitive. Besides, another type of injection attack is XSS injection. In XSS injection attack, the attacker can do malicious actions like malware spreading, cookies-stealing, session hijacking to steal users' credentials or even redirect user to a malicious web application (Farea et al., 2021). Hence, it is very necessary to have the knowledge on A03 Injection vulnerability so that this vulnerability can be prevented and prohibited.

1.3 Objectives

- To design and develop a vulnerable web application of A03 Injection detection for educational purposes.
- To test the effectiveness of the implemented web application in improving knowledge on A03 Injection.

1.4Project Scopes

Develop a web application prototype that complies with OWASP Top 10 A03 – Injection vulnerability. This web application is aimed to deliver knowledges on the OWASP A03 – injection vulnerability and provides lessons to the user on the implement the defensive techniques to defense against injection attack.

1.5Significant of the Project

This project aims to develop a web application prototypecomplying with OWASP Top 10 A03 – Injection vulnerability. This web application prototype aims to raise awareness about injection vulnerabilities and educate users about the impact of such vulnerabilities. Web application prototype is aimed to teach about injection attacks, including how they occur and their potential consequences.The prototype also provides a hands-on session where users can practice attacking the web application correctly. In case users encounter difficulties or are unsure about the next steps, the prototype offers features such as hints or tips to guide them in correctly attacking the web application.Upon completion of the hands-on session, the web application prototype suggests the best practices to users to prevent the specific vulnerability they targeted during the lesson.Through this interactive experience, the web application prototype will raise user's awareness of injection vulnerabilitiesand learn how to prevent them while developing their own web applications.

1.6Project Outline

Theoutline of the project is organized as follows:

- Chapter one introduces the background, problem statement, objectives and significant of the project.

- Chapter two includes the literature review made to gather the information related to the project.
- Chapter three discuss on the methodology used, requirement analysis, system design and prototyping of the proposed web application.
- Chapter four discuss about development process of the web application, including the screenshot of the web application developed as well as the core coding of the web application.
- Chapter five shows the result of how web application developed in achieving the objectives of this project in testing process.
- Chapter six shares about the conclusion, limitation and future work on this project

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

In chapter 2, several coursework and research papers related to the OWASP Top 10 which are done by other researchers will be reviewed. From reviewing through the coursework and research paper, we can get the knowledge which is related to the project topics. That knowledge will be useful and act as a guideline for us throughout this project. Other than reviewing coursework and research papers, several web applications which are compiled to the OWASP Top 10 vulnerabilities will also be reviewed. The applicationsthat will be reviewed in this chapter are OWASP Webgoat, Damn Vulnerable Web Application, OWASP Juice Shop, Free Online Bank Web by Micro Focus Fortify and Hacksplaning.

After reviewing the coursework and the existing web applications, a summary for each of the reviewed itemswill be extracted. For the reviewing of the existing web application, a comparative table will be made to compare the offering features of each of the existing web application. Those extracted information will be used in analyzing and designing the requirements and features that should be included in this project. To conclude this chapter, a summary conclusion will be done at the end of the chapter.

2.2 OWASP Top 10 A03 - Injection Vulnerability

According to Marashdeh et al. (2021), SQL injection refers to the type of attack towards the web application database through injecting malicious code to gain the information or the data existing in the database without proper authentication. Other than that, the attacker can perform dangerous actions such as retrieving data without authorization from the database, deleting MySQL tables and others. Those dangerous actions are irreversible and will cost permanent damage to the web application that had been attacked.