PGD/M 11

Kube PCI Compliance validator

R.W.M.A.S.Rathnayake
（Reg. No.: MS21901812）
M.Sc. in IT
Specialized in Information Technology

Supervisor: Mr. Amila Senarathne

November 2022

Department of Information Technology
Sri Lanka Institute of Information Technology

PGD/M 11

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

…….. ……29/03/2023 ……

Mr. Amila Senarathne (Supervisor)

Approved for MSc. Research Project:

……

Head/<Department >

Approved for MSc:

……...

Head – Graduate Studies

DECLARATION

Sign: 

Anuruddha Shanaka Rathnayake

Date: 25/11/2022

ABSTRACT

With the development of the Internet and the proliferation of computing power, web-based applications have become commonplace. Despite this, vulnerabilities in these online apps are on the rise, which has resulted in the theft of personal information, the loss of data, and the denial of data access during data transmission. A common form of assault on the security of web applications is known as cross-site scripting (XSS), and it consists of injecting malicious code from a third-party website or server. Recent web application security studies have focused on attack prevention and safe coding techniques; however these methods sometimes falsely flag legitimate attacks and ignore the users who are the true targets of malicious ones. This study presents a clever method for finding cross-site scripting flaws in web-based software. This article explains how fuzzy logic was used to create a method for detecting common XSS flaws and provides some preliminary findings from that method's implementation. Compared to the work of Koliet al., our detection approach is far more accurate, with a false-positive rate of only 0.01%. One other function of our method is to aid in user judgment.

The volume, variety, and methods of information transmission across several media types and geographies have exploded on the Internet during the last decade. Particularly, the Internet has surpassed the success of traditional marketing tactics to become the primary avenue via which international corporations undertake marketing. Since practically all businesses in the modern day want to expand internationally, the Internet has come to play a pivotal role in virtually every aspect of human activity and global development. Building this essential presence on the web may be accomplished in several ways. Internet-based tasks can be accomplished by using web apps, which are computer programs that employ web technologies. As a result, it's not unexpected that the proliferation of web-based apps and other intelligent gadgets like smartphones, tablets, and other mobile phones has radically altered the nature of cross-platform communication and information sharing. To avoid falling victim to hackers and web attackers who are constantly scouring the Internet for improper coding practices that they can exploit to steal sensitive data and commit their evil deeds, application developers must reevaluate their development strategies and model their security concerns as the number and variety of these applications on the Internet continues to grow. Moreover, as the number of online applications grows, so do vulnerabilities, which

have become a major issue of debate in the development and security of multiple web applications. Frequently, Web applications acquire, process, store, and transport sensitive client data (such as personal information, credit card numbers, and social security numbers) for immediate and recurring use. Consequently, online applications have become a key target for hackers who exploit poor coding practices, weaknesses in application code, insufficient user input authorization, and software developers' failure to comply with security regulations. These vulnerabilities may reside either on the server or, more dangerously, on the client. The vulnerabilities include SQL injection, cross-site request forgery, information leakage, session hijacking, and cross-site scripting. The aim of this study is the detection of cross-site scripting assaults. Cross-site scripting refers to the injection of malicious code into vulnerable internet programs to redirect users to unreliable websites. Even if the servers and database engine have no vulnerabilities, XSS may still occur, and it is certainly one of the most widespread flaws in web applications today.

ACKNOWLEDGEMENT

TABLE OF CONTENTS

List of Figures

List of Tables