Journal of Basrah Researches ((Sciences)) Vol. (47). No. 1 (2021)

Available online at: https://www.iasj.net/iasj/journal/260/issues

ISSN –1817 –2695

Received date: 6-5-2021 Accepted date: 18-8-2021 Available online date: 31-12-2021

Proposed Method to Detect and Prevent Reflected Cross-Site Script Attack

Iman Fareed Khazal[1], Mohammed Abdulridha Hussain[2]

[1,2] *Computer Science Department, College of Education for Pure Science, University of Basrah, Basrah, Iraq*

E-mail: imanfared88@gmail.com, mohsubber@gmail.com

Abstract

Due to the widespread use of web applications and the dramatic increase in the number of application users, most web applications contain flaws that make them vulnerable to a variety of attacks. One of the most common attacks is Cross-Site Script (XSS). In an XSS attack, the attacker exploits an XSS vulnerability in a web application and injects a malicious script into it. The majority of preventive measures are client-side, reducing the performance of the web browser. It has been suggested as a server side method in this paper. The Prevent Reflected-XSS Server (PRS) is a suggestion server that checks the domain name of a link's Uniform Resource Locator (URL) to see if it is on the untrusted list of malicious sites. If it does not exist, Check that link to see if it contains any malicious script. If the URL is injected, the malicious URL is replaced with a sterilized URL. This method was tested using an open-source application and was successful in determining the harmful code within the URL and sterilizing it in an average of 0.33 seconds.

Keywords: cross site script(XSS), Reflected(non-persistent) XSS, Web application, sterilized URL, preventing XSS.

1. Introduction

Since the first case of Covid-19 (Coronavirus) disease was reported in China (Wuhan District) in December 2019, the disease has spread throughout the world [1]. The COVID-19 epidemic has prompted a call for the use of novel techniques to mitigate the epidemic's impact. Telemedicine, online education, and telework are becoming increasingly important in assisting society in slowing the spread of the virus [2]. COVID-19 prevalence posed a significant threat to the "technology-driven society," and internet criminals took advantage of this opportunity to expand their attacks [3]. Internet