Abstract

This research focuses on detecting Cross-site Scripting (XSS) attacks using the Long Short-term Memory (LSTM) method. XSS is a security vulnerability where an attacker injects malicious code, often JavaScript, into web pages. This can be used by attackers to steal credentials and manipulate content without user awareness, compromising the security of legitimate websites. To address this, user input on websites is analyzed using the LSTM method, a type of Recurrent Neural Network (RNN) architecture from the Deep Learning domain. LSTMs are effective for sequence prediction problems due to their ability to retain information over long periods and handle temporal dependencies. By training the LSTM model on a dataset of both benign and malicious inputs, it can distinguish between normal behavior and potential attacks, enhancing detection accuracy. The accuracy rate using this LSTM method is 99.25%, which is a high enough percentage to detect XSS. Extensive experiments and evaluations demonstrate that this method significantly improves the detection rate of XSS attacks compared to traditional methods, contributing to the development of more secure web applications by providing a reliable tool for early detection and prevention of XSS vulnerabilities.

Keywords : Cross-site scripting, Long short-term memory, Deep learning, Website

---