Deteksi Serangan Cross-site Scripting pada Aplikasi Web Menggunakan Metode LSTM

Naufal Ahmad Nur Hakim[1], Vera Suryani[2], Muhamad Irsan[3]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung

[1]naufalanh@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id,
[3]irsanfaiz@telkomuniversity.ac.id,

Abstrak

Penelitian ini berfokus pada pendeteksian serangan Cross-site Scripting (XSS) dengan menggunakan metode Long Short-term Memory (LSTM). XSS adalah kerentanan keamanan di mana penyerang menyuntikkan kode berbahaya, biasanya JavaScript, ke dalam halaman web. Hal ini dapat digunakan oleh penyerang untuk mencuri kredensial dan memanipulasi konten tanpa sepengetahuan pengguna, sehingga membahayakan keamanan situs web yang sah. Untuk mengatasi hal ini, input pengguna di situs web dianalisis menggunakan metode LSTM, sebuah jenis arsitektur Recurrent Neural Network (RNN) dari domain Deep Learning. LSTM efektif untuk masalah prediksi urutan karena kemampuannya menyimpan informasi dalam jangka panjang dan mengelola ketergantungan temporal. Dengan melatih model LSTM pada dataset yang terdiri dari input yang jinak dan berbahaya, LSTM dapat membedakan antara perilaku normal dan potensi serangan, sehingga meningkatkan akurasi deteksi. Tingkat akurasi menggunakan metode LSTM ini adalah 99.25%, yang merupakan persentase yang cukup tinggi untuk mendeteksi XSS. Eksperimen dan evaluasi ekstensif menunjukkan bahwa metode ini secara signifikan meningkatkan tingkat deteksi serangan XSS dibandingkan dengan metode tradisional, berkontribusi pada pengembangan aplikasi web yang lebih aman dengan menyediakan alat yang dapat diandalkan untuk deteksi dini dan pencegahan kerentanan XSS.

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