Development of a Hybrid Model for Cross-Site Scripting (XSS) Attack Detection Using Random Forest and BERT Algorithms

BY

Anggaradiva Bendesa, Student ID 21151010167

Departement Of Informatics Engineering

Computer Science Study Program

ABSTRACT

Web applications continue to be vulnerable to Cross-Site Scripting (XSS) attacks, in which weak input validation enables attackers to inject and execute malicious scripts on the client side. Detecting such attacks is not straightforward, as XSS payloads frequently appear in varied forms—ranging from event handlers and JavaScript URIs to encoded or obfuscated content designed to evade filters. This research addresses that difficulty by constructing a hybrid detection approach that combines two complementary techniques: Random Forest, trained on character-based TF-IDF vectors along with handcrafted statistical features, and BERT, adapted through fine-tuning for the classification task at hand. The final hybrid model aggregates the confidence scores produced by both classifiers to arrive at a single prediction. On the test set, Random Forest and BERT each attained an accuracy of 99.21%, matched by the hybrid configuration at the same accuracy level, though the hybrid model showed a marginal advantage in F1-score (99.43%) and recall compared to the two individual models. These results support the case that combining statistical and contextual representations can serve as an effective supporting technique for XSS payload detection.

Keywords: XSS, Random Forest, BERT, hybrid model, payload detection

Pengembangan Model Hybrid Untuk Deteksi Serangan *XSS* Menggunakan Algoritma Random Forest dan BERT

Oleh

Anggaradiva Bendesa, NIM 21151010167

Jurusan Teknik Informatika

Program Studi Ilmu Komputer

ABSTRAK

Aplikasi web hingga kini masih rentan terhadap serangan Cross-Site Scripting (XSS), yang terjadi ketika validasi input yang lemah memungkinkan penyerang menyisipkan dan mengeksekusi skrip berbahaya pada sisi pengguna. Mendeteksi serangan semacam ini bukan hal yang sederhana, mengingat payload XSS kerap muncul dalam variasi bentuk—mulai dari event handler dan JavaScript URI, hingga konten yang di-encode atau di-obfuscate untuk melewati mekanisme filter. Penelitian ini berupaya menjawab tantangan tersebut dengan membangun model deteksi hybrid yang menggabungkan Random Forest, yang dilatih menggunakan vektor TF-IDF berbasis karakter beserta fitur statistik yang dirancang secara manual, dengan BERT, yang disesuaikan melalui fine-tuning untuk tugas klasifikasi terkait. Model hybrid akhir menggabungkan skor kepercayaan dari kedua model untuk menghasilkan satu keputusan klasifikasi. Pada data uji, Random Forest dan BERT masing-masing memperoleh akurasi 99,21%, setara dengan model hybrid pada tingkat akurasi yang sama, meskipun model hybrid menunjukkan keunggulan tipis pada nilai F1-score (99,43%) dan recall dibandingkan kedua model secara individual. Hasil ini mendukung argumen bahwa penggabungan representasi statistik dan kontekstual dapat menjadi teknik pendukung yang efektif untuk deteksi payload XSS.

Keywords: XSS, Random Forest, BERT, model hybrid, deteksi payload