Judul tesis : PENDETEKSI SERANGAN XSS DENGAN MACHINE LEARNING DAN METODE N-GRAM

ABSTRAK

Abstract - Cross Site Scripting (XSS) merupakan serangan yang paling sering dilakukan oleh penyerang untuk menyerang suatu website, dengan cara menyisipkan skrip berbahaya ke situs web. Serangan ini akan membawa pengguna ke halaman web yang sudah dirancang khusus untuk mengambil session dan cookies pengguna. Hampir 68% situs web rentan terhadap serangan XSS. Dalam penelitian ini, penulis melakukan penelitian dengan membanding beberapa metode machine learning dan kemudian menambahkan metode n-gram pada masing-masing fitur script, sehingga akan diketahuai machine learning manakah yang memiliki kemampuan pendeteksian terbaik terhadap serangan XSS. Berdasarkan penelitian yang dilakukan dengan membandingkan beberapa methode machine learning menunjukkan bahwa metode machine learnig SVM memiliki kemampuan pendeteksian yang sangat baik setelah di tambahkan metode n-gram pada fitur script nya.

Keywords – *XSS attack, malicious script, n-gram, vulnerable, detection script, machine learning.*

ABSTRACT

Cross Site Scripting (XSS) is an attack that is most often carried out by attackers to attack a website, by inserting malicious scripts into a website. This attack will take the user to a webpage that has been specifically designed to retrieve user sessions and cookies. Nearly 68% of websites are vulnerable to XSS attacks. In this study, the authors conducted a study by comparing several machines learning methods and then adding the n-gram method to each script feature, so that it would be known which machine learning has the best detection capability for XSS attacks. Based on research conducted by comparing several machine learning methods shows that the SVM machine learnig method has a very good detection ability after adding the n-gram method to its script features.

Keywords - XSS attack, malicious script, n-gram, vulnerable, detection script, machine learning.