ABSTRAK

Saat ini kerentanan keamanan suatu website atau pun domain masih sering ditemukan. Dikarenakan seiring update nya suatu website namun blum maksimalnya pengujian kerentanan keamanan (Pengujian penetrasi) yang dilakukan yang membuat suatu website dan domain rentan untuk diserang. *Open web applicatin project* (*Owasp*) merupakan metode yang dapat diterapkan dalam melakukan pengujian kerentanan keamanan pada website maupun domain yang dimana *Open web applicatin project* (*Owasp*) merupakan standarisasi untuk melakukan pengecekan kerentanan keamanan, dengan melakukan pengujian penetrasi dalam suatu *web* domain dengan mengikuti langkah - langkah atau metode yang ada dan dalam menggunakan alat - alat yang beragam yang dapat berfungsi untuk pengujian celah keamanan berdasarkan metode yang ada tersebut.

Kata kunci: *Open web applicatin project*, Keamanan Data, Evaluasi, Pengujian Penetrasi.

ABSTRACT

Currently, security vulnerabilities of a website or domain are still often found. Due to the fact that as a website updates, the maximum security vulnerability testing (penetration testing) is not carried out which makes a website and domain vulnerable to attack. The Open web application project (Owasp) is a method that can be applied in conducting security vulnerability testing on websites and domains where the Open web application project (Owasp) is a standard for checking security vulnerabilities, by conducting penetration testing in a web domain by following the steps - existing steps or methods and in using various tools that can function for testing security holes based on these existing methods.

***Keywords**: Open web applicatin project, Safety Data, Evaluation, Penetration Testing.*