

ABSTRAK

**ANALISIS KERENTANAN *WEBSITE* MENGGUNAKAN PENDEKATAN
BLACK BOX TESTING
STUDI KASUS *WEBSITE* DATA POKOK PENDIDIKAN PEMERINTAH
DAERAH XYZ**

Oleh:

ATHO' NOVIAN AWLARIJAL

NIM: 1202164087

:

Di era saat ini, keamanan informasi sangat krusial. Menurut *Open Web Application Security Project (OWASP)* pada tahun 2017 ada beberapa kerentanan yang sering terjadi pada situs web seperti kelemahan injeksi, otentikasi rusak, data sensitif yang terpajan (terekspose), kontrol akses yang rusak, kesalahan konfigurasi keamanan, kelemahan *Cross-Site Scripting (XSS)*, dll. Kerentanan ini akan berdampak pada penyerang dalam mengeksploitasi sistem, mengambil informasi atau data penting di web. Menurut ID-SIRTII *domain* paling banyak yang menjadi target serangan siber di Indonesia adalah *domain .go.id*. Dinas Pendidikan di Pemerintah Daerah XYZ menggunakan situs web untuk menyebarkan informasi kepada pihak luar. Dinas Pendidikan menggunakan web untuk mengelola data pokok pendidikan (Dapodik). Oleh karena itu, keamanan harus dipastikan untuk menjaga integritas informasi di situs web. Salah satu cara untuk menjaga integritas informasi di situs web adalah dengan melakukan *vulnerability assessment*. *Vulnerability assessment* adalah serangkaian tindakan untuk mengidentifikasi dan menganalisis kemungkinan kerentanan keamanan dalam sistem (ISACA, 2017). Tugas akhir ini menggunakan pendekatan pengujian *black box* untuk penilaian kerentanan aplikasi web dengan menganalisis dan menggunakan beberapa tool untuk mendeteksi celah keamanan, sehingga dapat segera menanggulangi kerentanan sebelum terjadi serangan.

Kata Kunci: informasi, keamanan, aplikasi web, *vulnerability assessment*, *black box testing*