“ANALISIS KEAMANAN SISTEM INFORMASI DENGAN METODE *INPUT VALIDATION TESTING* PADA APLIKASI Z DI BAGIAN PENGADAAN BARANG DAN JASA SEKRETARIAT DAERAH KABUPATEN BULELENG”

Oleh

Kadek Nova Wardana, NIM 1815091011

Program Studi Sistem Informasi

Jurusan Teknik Informatika

Fakultas Teknik dan Kejuruan

Universitas Pendidikan Ganesha

ABSTRAK

Pengembangan aplikasi yang berbasiskan website menjadi suatu kebutuhan diera kemajuan internet, semakin tingginya penggunaan aplikasi berbasis web juga dilakukan oleh pihak-pihak yang berasal dari pemerintahan termassuk BPBJ Kabupaten Buleleng yang mengembangkan aplikasi pengajuan tender yaitu Z. Aplikasi Z merupakan aplikasi yang digunakan untuk dapat melakukan pengajuan tender, dimana pada aplikasi Z mengelola data-data yang sangat penting dan menyangkut hal yang sangat sensitif dan rahasia yang dimana keamanan pada aplikasi tersebut harus dapat dikatakan aman. Penyerangan pada sebuah website dijelaskan oleh OWASP mengenai OWASP *Top Ten* tahun 2017 yang mana memberikan peringkat bahwa keamanan paling rentan nomor satu adalah *injection*, dimana keamanan paling rentan tersebut dapat diuji dengan menggunakan metode *Input Validation Testing*. Metode *Input Validation Testing* berfokus menguji kerentanan *SQL Injection, Reflected Cross Site Scripting (XSS), Stored Cross Site Scripting (XSS), Command Injection, Http Smuggling* yang diuji secara *automation* dan manual menggunakan tools rekomendasi OWASP. Pengujian kelima kerentanan tersebut jika ditemukan, kemudian akan dicari nilai risiko dari kerentanan tersebut menggunakan OWASP *Risk Rating* untuk dinilai seberapa tingkat risiko yang dihasilkan dari kerentanan yang ditemukan. Hasil pengujian menunjukkan aplikasi Z memiliki kerentanan *Stored Cross Site Scripting likelihood* 5 (*Medium*) *impact* 5.75 (*Medium*), *Reflected Cross Site Scripting likelihood* 4.75 (*Medium*) *impact* 4.5 (*Medium*), *HTTP Smuggling likelihood* 6.125 (*High*) *impact* 5.625 (*Medium*).

Kata Kunci : Z, *Injection*, OWASP *Top Ten*, *Input Validation Testing*, OWASP *Risk Rating*.

"*ANALYSIS OF INFORMATION SYSTEM SECURITY USING INPUT VALIDATION TESTING METHOD ON Z APPLICATION IN THE PROCUREMENT OF GOODS AND SERVICES SECRETARIAT OF REGIONAL BULELENG DISTRICT*"

By

Kadek Nova Wardana, NIM 1815091011

Study Program in Information System

Department in Informatics Engineering

Faculty of Engineering and Vocational

Ganesha University of Education

ABSTRACT

Website-based application development has become necessity in the era of internet advancement, the increasing use of web-based applications is also being carried out by parties from the government, including BPBJ Buleleng Regency, which is developing a tender submission application, namely Z. The Z application is an application that is used to be able to submit tenders, where the Z application manages data that is very important and involves very sensitive and confidential matters where the security of the application must be safe. An attack on a website is explained by OWASP regarding the 2017 OWASP Top Ten which ranks the number one most vulnerable security is injection, where the most vulnerable security can be tested using the Input Validation Testing method. The Input Validation Testing method focuses on testing SQL Injection, Reflected Cross Site Scripting (XSS), Stored Cross Site Scripting (XSS), Command Injection, Http Smuggling vulnerabilities which are tested automatically and manually using OWASP recommendation tools. Testing the five vulnerabilities if found, then looking for the risk value of these vulnerabilities using the OWASP Risk Rating to assess what level of risk results from the vulnerabilities found. The test results show that the Z application has vulnerabilities Stored Cross Site Scripting likelihood 5 (Medium) impact 5.75 (Medium), Reflected Cross Site Scripting likelihood 4.75 (Medium) impact 4.5 (Medium), HTTP Smuggling likelihood 6.125 (High) impact 5.625 (Medium).

Keywords : Z, *Injection*, OWASP *Top Ten*, *Input Validation Testing*, OWASP *Risk Rating*.