

## ABSTRAK

Masalah keamanan sistem sekarang ini sedang menjadi topik yang sangat banyak dibahas dikarenakan banyak perusahaan besar yang terkena masalah keamanan sistem yang tentunya bukan hanya user yang menjadi rugi tapi perusahaan pun terdampak kerugian seperti kerugian finansial atau kepercayaan yang hilang dari pengguna. Pada Paper ini, Penulis membahas mengenai uji penetration testing pada sistem Universitas Islam Negeri Sunan Gunung Djati Bandung untuk menemukan masalah security yang dapat mengganggu user experience atau tercurinya data user atau organisasi. Penelitian ini menggunakan owasp top 10 sebagai acuan pengujian penetration testing. Metode owasp banyak digunakan oleh security expert dikarenakan kerentanan yang dicari merupakan kerentanan yang baru dan banyak di manfaatkan oleh hacker. Penetration testing yang dibahas pada paper ini memiliki beberapa Langkah-langkah, seperti information gathering dan scanning, exploitation dan reporting. Pada pengujian sistem ditemukan beberapa kerentanan yang memiliki severity low sampai high hal tersebut sesuai dengan dampak yang diberikan oleh bug tersebut, semakin tinggi severity maka semakin merugikan atau merusak kerentanan tersebut. Oleh karena itu kerentanan yang memiliki severity tinggi harus segera diperbaiki agar tidak dimanfaatkan oleh hacker.

Kata kunci : web, security, pentesting, pentesting report, web information application disclosure, Owasp top 10, Bypass Login, Gaining Access