

ABSTRAK

Perkembangan teknologi informasi berkembang pesat seiring pertumbuhan penggunaannya. Pemanfaatan teknologi informasi dalam bentuk *website* sudah banyak digunakan oleh berbagai macam pihak. Universitas XYZ merupakan lembaga pendidikan yang menggunakan *website* untuk keperluan akademik, kegiatan belajar mengajar dan berbagai macam kebutuhan entitas internalnya. Salah satu *website* yang digunakan oleh Universitas XYZ bertujuan untuk mengakomodasi keperluan absensi kegiatan praktikum bagi praktikan dan asisten praktikum di Fakultas XYZ. Seiring perkembangan teknologi selain banyaknya manfaat yang dirasakan, terdapat peningkatan serangan keamanan dengan berbagai macam teknik ancaman terhadap *website* oleh pihak yang tidak bertanggung jawab dengan tujuan untuk merugikan pemilik dan pengguna *website*. Oleh karena itu, diperlukan *vulnerability assessment* untuk mengetahui celah keamanan pada *website* fakultas XYZ menggunakan metode VAPT dengan penggunaan *tools automated scanning*. Pada pengujian ini menggunakan beberapa *tools*, yaitu Nessus, Burp Suite, dan OWASP ZAP. Celah keamanan pada *website* dilakukan analisis untuk menentukan tingkat risiko dan tahapan mitigasi. Pada pengujian analisis kerentanan menggunakan *tool* Nessus ditemukan 5 celah kerentanan. *Tool* Burp Suite ditemukan 8 celah kerentanan, dan *tool* OWASP ZAP ditemukan 14 celah kerentanan. Kemudian dilakukan penetapan kerentanan dari ketiga *tools*, menjadi 9 kerentanan untuk dilakukan eksploitasi dan mitigasi. Hasil dari tahapan mitigasi menunjukkan bahwa 3 dari 9 celah kerentanan berhasil dimitigasi.

Kata kunci— **Kerentanan, VAPT, *automated scanning*, eksploitasi, mitigasi.**