

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 bukti pembayaran kegiatan praktikum bagi praktikan untuk mengambil sertifikasi 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 pengujian kerentanan untuk mengetahui celah keamanan pada *website* fakultas XYZ menggunakan metode PTES. Pada pengujian ini menggunakan beberapa *tools*, yaitu SQLMap, Bupsuite, jSQL Injection, dan Havij. Celah keamanan pada *website* dilakukan analisis untuk menentukan tahapan mitigasi. Hasil analisis dari pengujian keamanan pada *website* akademik penunjang pengajaran Institusi XYZ menggunakan metode SQL Injection menunjukkan bahwa dari empat *tools* yang digunakan menunjukkan hasil penyerangan tidak ditemukan *parameter* celah kerentanan pada *website* tersebut yang berarti tidak adanya manipulasi data yang terjadi melalui penyerangan dengan metode SQL Injection. Kelanjutan dari penelitian dapat memilih *tools* yang beragam, akurat, dan luas untuk mengidentifikasi kerentanan keamanan dan menggunakan metode yang berbeda agar hasil penelitian lebih bervariasi. Selain itu, lakukan pemeliharaan rutin pada *website* untuk meminimalisir celah keamanan.

Kata kunci – **eksploitasi, Kerentanan, PTES, Mitigasi**