ABSTRAK

Perkembangan teknologi informasi pada saat ini telah menjadi suatu kebutuhan dalam meningkatkan efisiensi kinerja suatu organisasi, terutama aspek keamanan merupakan kunci penting yang perlu diperhatikan pada pengembangan *website* XYZ sebagai pintu utama bagi calon mahasiswa baru untuk mendaftar masuk dan mengakses informasi yang berkaitan dengan kegiatan mahasiswa baru seperti jadwal tes, pendaftaran, pengisian formulir data diri, jadwal seleksi dan kegiatan lainnya. Dengan banyaknya calon pendaftar yang masuk melalui *website*, maka akan semakin tinggi potensi terhadap risiko celah keamanan terhadap *website.* XYZ pernah mendapatkan laporan bahwa *website* XYZ masih rentan terhadap serangan *phising.* Hal ini juga menjadi ancaman yang serius sehingga dapat merugikan kepercayaan pengguna terhadap kredibilitas Universitas XYZ. Dengan semakin bertambahnya calon mahasiswa yang akan mendaftar masuk, maka keamanan sistem harus mendapatkan perhatian khusus sebagai langkah untuk pencegahan potensi kerentanan. Pada penelitian ini dilakukan *penetration testing* melalui pendekatan *Information System Security Assessment Framework* (ISSAF). Hasil *penetration testing* pada penelitian menemukan bahwa *website* XYZ terdapat celah keamanan *Local File Inclusion* melalui *path traversal* yang telah ditemukan serta memiliki 16 celah kerentanan dengan 4 tingkat *medium,* 8 tingkat *low* dan 4 tingkat *informational*. Pada prioritas perbaikan akan difokuskan menuju celah *Local File Inclusion,* dengan penerapan *whitelist,* membatasi akses pada *directory /etc, ssh/, home,* terapkan *deploy waf* seperti *modsecurity Apache.* Hal ini bertujuan ntuk menjaga kepercayaan masyarakat terhadap Universitas XYZ dan menjaga *website* dari serangan di masa yang akan datang.

Kata Kunci:.Keamanan Sistem Informasi, Penetration Testing, Website, ISSAF