ABSTRAK

Menurut OWASP *Top* 10 *Most Critical Web Application Security Risks*, menempatkan *Cross Site Scripting* berada diposisi ketiga dengan tipe serangan injeksi. Pada proses pembuatan *website* Akademik Penunjang Administrasi di Institusi XYZ, Perlu dilakukan *Security Testing* terhadap celah keamanan *Cross Site Scripting* dikarenakan celah ini memiliki potensi kerentanan yang tinggi dan berpotensi untuk pencurian data sensitif sehingga dapat dilakukan manipulasi data, jika hal tersebut terjadi dapat menghilangkan kredibilitas institusi terkait. Penelitian ini dilakukan untuk mengetahui celah *Cross Site Scripting* terhadap *Website* Administrasi Penunjang Administrasi di Institusi XYZ dan melakukan mitigasi celah tersebut dengan cara pengujian celah keamanan. Identifikasi celah *Cross Site Scripting* dilakukan menggunakan *tool* OWASP ZAP dengan hasil celah tersebut teridentifikasi pada parameter *"warn"*. Proses eksploitasi dilakukan untuk membuktikan celah *Cross Site Scripting* menggunakan *tool* XSStrike dan Burp Suite dengan hasil keberhasil mengeksploitasi website target mengunakan beberapa *payload* yang diinjeksikan. Dapat disimpulkan bahwa pada parameter *"warn"* tidak menerapkan filter dan validasi input sebagai pencegah XSS dengan baik sehingga proses mitigasi dapat dilakukan terhadap *website* tersebut. Proses mitigasi dilakukan dengan menambahkan *header* CSP, penggunaan fungsi htmlspecialchars(), dan menggunaan *Secure Socket Layer* (SSL). Hasil yang didapatkan pasca mitigasi adalah *popup* dialog konfirmasi sudah tidak terdeteksi dan *alert error* masih dapat di modifikasi sehingga proses mitigasi berhasil mengurangi celah keamanan tersebut.

Kata Kunci: ***Cross Site Scripting, Website, Mitigation,*** **PTES.**