

## ABSTRAK

Tragedi serangan siber saat ini sudah menjadi hal yang lumrah terjadi pada berbagai *website*. Pada tahun 2022 Indonesia mengalami peningkatan kasus serangan siber, selain itu serangan terhadap *website* menjadi tiga insiden serangan teratas. Serangan siber ini juga berpotensi terjadi pada *website* milik Yayasan Dana Sosial Al-Falah Surabaya. Selain itu serangan siber seperti kebocoran data maupun serangan terhadap *website* dapat menyebabkan kerugian bagi perusahaan, sehingga jika ditemukan kerentanan pada sistem seperti kerentanan *SQL Injection* yang dapat digolongkan sebagai kerentanan dengan risiko tinggi yang dapat memberikan kemungkinan bagi peretas untuk mendapatkan informasi dari *database website* dan pada kasus tertentu mampu merusak konten pada halaman *website (Defaceing)*. Tujuan dari penelitian ini untuk menganalisis keamanan sistem informasi pada *website* YDSF – LAZNAS menggunakan kerangka kerja uji penetrasi ISSAF (*Information System Security Assessment Framework*). *Penetration Testing* ini adalah salah satu cara untuk melihat tingkat keamanan sebuah sistem, membantu mengidentifikasi celah potensial pada sistem yang dapat dieksploitasi oleh penyerang atau peretas. ISSAF juga digunakan untuk menghubungkan langkah-langkah *pentesting* dengan tujuan untuk memberikan panduan komprehensif dalam melakukan *penetration testing*. Kriteria keberhasilan penelitian ini meliputi peningkatan kesadaran pihak YDSF – LAZNAS akan keamanan sistem informasi, dan peningkatan perlindungan data donatur dengan cara memberikan hasil uji penetrasi melalui *Final Report* yang dibuat menggunakan kerangka kerja ISSAF. Oleh karena itu uji penetrasi yang dilakukan dapat memberikan beberapa kesimpulan seperti masih dideteksinya beberapa kerentanan, *port* terbuka dan eksploitasi yang berhasil dilakukan dimana strategi perlindungan dan mitigasi resiko beserta perbaikan berdasarkan solusi dari kerentanan yang didapatkan perlu dilakukan. Dikarenakan hal tersebut, prioritas perbaikan terhadap keamanan sistem informasi pada *website* YDSF – LAZNAS perlu berfokus pada beberapa kerentanan yang teridentifikasi saat berlangsungnya uji penetrasi.

*Kata kunci*— **Keamanan Sistem Informasi, ISSAF, Pentest, OWASP, YDSF-LAZNAS**