ABSTRAK

Perkembangan sistem informasi mendorong lembaga pendidikan untuk mengadopsi *website* sebagai media ujian daring. SMAN 20 Bandung merupakan salah satu institusi yang telah mengimplementasikan sistem ujian berbasis web. Pemilihan SMAN 20 Bandung sebagai objek penelitian didasarkan pada keterbukaan institusi dalam mendukung proses pengujian serta kebutuhan akan evaluasi keamanan pada aplikasi yang digunakan secara aktif. Penelitian ini bertujuan untuk mengidentifikasi, menguji, dan merekomendasikan perbaikan terhadap potensi celah keamanan yang ada pada sistem ujian tersebut.

Metode yang digunakan mengacu pada *Penetration Testing Execution Standard* (PTES) dengan tiga alat bantu utama: Nessus *Essentials*, Burpsuite *Professional*, dan OWASP ZAP. Dari ketiga alat tersebut ditemukan total 160 kerentanan yang diklasifikasikan berdasarkan tingkat *severity*, mulai dari *informational* hingga *critical*. Seluruh temuan kemudian dianalisis menggunakan pendekatan *vulnerability analysis*, di mana proses eliminasi dilakukan berdasarkan tiga kriteria utama: tingkat *severity*, keberulangan antar *tools*, dan efisiensi mitigasi.

Tujuh kerentanan prioritas dipilih dan diuji melalui tahapan eksploitasi, yang kemudian diikuti dengan perancangan mitigasi baik pada sisi konfigurasi server maupun kode aplikasi. Pengujian ulang pasca mitigasi menunjukkan bahwa sebagian besar kerentanan berhasil diminimalisasi secara signifikan. Namun, beberapa isu seperti *Content Security Policy* (CSP) dan token CSRF masih membutuhkan penanganan lanjutan di tingkat pengembangan aplikasi. Penelitian ini memberikan gambaran menyeluruh terhadap keamanan website ujian SMAN 20 Bandung dan menjadi pijakan awal dalam peningkatan keamanan sistem secara berkelanjutan.

Kata kunci — **Keamanan Website, PTES, Nessus, Burpsuite, OWASP ZAP, Eksploitasi.**