BAB I
PENDAHULUAN

1.1 Latar Belakang

Website dapat memberikan akses informasi dimana dan kapan saja asalkan akses internet tersedia. Dengan semakin populernya internet, jumlah pesan *cyber* juga meningkat[1]. Selain dampak negatifnya, *malware* juga memberikan ancaman pada jaringan komputer yang terhubung ke internet, seperti virus dan *trojan horse*. Untuk memitigasi dampak negatifnya, integritas jaringan perlu dijaga. Keamanan jaringan akan memberikan layanan dan perlindungan pada jaringan komputer yang terhubung ke internet, memungkinkan pengguna untuk beroperasi secara normal dan mengambil data dengan aman dan terjamin.

Namun, semakin banyaknya ancaman keamanan *cyber* yang terus berkembang membuat *website* rentan terhadap serangan yang dapat merugikan baik bagi pengelola maupun pengguna[2][3]. Hal ini juga berlaku pada *website* Dukcapil Kabupaten Nganjuk (sedudo.nganjukkab.go.id), yang menyimpan berbagai informasi vital terkait administrasi kependudukan seperti KTP, KK, NIK, Akta Kelahiran, Akta Kematian, dll. Menjaga keamanan *website* sangatlah penting, mengingat *website* Dukcapil Kabupaten Nganjuk menyimpan data sensitif yang melibatkan informasi pribadi masyarakat Kabupaten Nganjuk. Ancaman seperti serangan *peretasan, injeksi kode* dan kerentanan keamanan lainnya dapat mengakibatkan tercurinya data, pencemaran nama baik, atau bahkan penyalahgunaan informasi yang dapat membahayakan masyarakat[4]. Oleh karena itu, melakukan analisis celah keamanan dan mitigasi yang efektif menjadi krusial untuk melindungi *website* Dukapil Kabupaten Nganjuk dari berbagai potensi serangan yang memungkinkan terjadi.

Untuk mencari celah keamanan pada sistem digunakan teknik *penetration testing*. Beberapa tools yang digunakan untuk *penetration testing* adalah *Owasp Zap* dan *Nikto*. Pada penelitian lain menerapkan *Owasp Zap* sebagai tools *penetration testing* terhadap *Website E-learning ITERA* [5], didapatkan hasil bahwa *Website E-learning ITERA* berhasil diserang menggunakan metode reverse brute forse dan ditemukan tiga *URL* dengan risiko tinggi serangan *SQL Injection*.

Sedangkan penelitian lain yang menerapkan *Nikto* terhadap *Website Sekolah Menengah Atas ABC* [6], didapatkan hasil bahwa ditemukan beberapa header yang tidak umum, yang dimana *Nikto* lebih bersifat informatif terkait masalah file, direktori yang tidak aman dan perangkat lunak yang usang.

Untuk melakukan monitoring dan pendeteksi serangan digunakan tools monitoring *Wazuh*. Pada penelitian lain menerapkan *Wazuh* sebagai tools monitoring terhadap *website Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan* [7], didapatkan hasil bahwa *wazuh* berhasil mendeteksi serangan *DDOS Slowloris* dan *Brute Force* serta dapat mengklasifikasikan keduanya serangan di level 3 hingga 10.

Dengan menggabungkan kedua alat tersebut, yaitu *Owasp Zap* dan *Wazuh* dapat meningkatkan kemampuan mendeteksi kerentanan secara menyeluruh. *Wazuh* dapat memantau aktivitas sistem dan mendeteksi kerentanan yang mungkin tidak terdeteksi oleh *Owasp Zap*. Hal ini dapat memperkuat sistem keamanan dan memungkinkannya untuk menghadapi berbagai jenis ancaman keamanan yang kompleks.

Sesuai beberapa uraian yang telah disampaikan serta perlunya evaluasi mengenai analisis celah keamanan menggunakan, *OWASP ZAP* dan *WAZUH* di *Website* Dukcapil Kab.Nganjuk, maka peneliti berminat untuk melakukan penelitian dengan judul "Analisis Celah Keamanan dan Monitoring Website Menggunakan Owasp Zed Attack Proxy (ZAP) & Wazuh (Studi Kasus: Website Dukcapil Kab.Nganjuk)".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang telah dijelaskan sebelumnya, permasalahan dapat dirumuskan sebagai berikut :

a) Apa saja celah keamanan yang mungkin ada pada *website* Dukcapil Kabupaten Nganjuk yang dapat dieksploitasi oleh penyerang?
b) Seberapa besar tingkat resiko keamanan yang terdapat pada *website* Dukcapil Kabupaten Nganjuk?

1.3 Tujuan Penelitian

Mengevaluasi tingkat keamanan *Website* Dukcapil Kab.Nganjuk dengan menggunakan *Owasp Zed Attack Proxy (ZAP)* guna mengidentifikasi celah keamanan yang mungkin ada dan *Wazuh* guna memonitoring kegiatan yang terdapat pada website serta mendokumentasikan celah keamanan yang ada pada *Website* Dukcapil Kab.Nganjuk, termasuk jenis-jenis celah seperti *SQL Injection, cross-site scripting (XSS), cross-site request forgery (CSRF),* dll.

1.4 Batasan Masalah

Untuk mencapai tujuan masalah penelitian, berikut ini merupakan batasan masalah penelitian yaitu :

a) Studi kasus yang digunakan pada penlitian ini adalah *website* Dukcapil Kabupaten Nganjuk.
b) Pada penelitian ini *operating system* yang digunakan adalah Kali Linux dan Virtual Box sebagai *software* virtualisasi dalam pengujian.
c) Pada penelitian ini percobaan serangan yang akan dilakukan yaitu : *cross-site scripting (XSS), sql injection, clickjacking* dan *distributed denial of service (ddos).*
d) Proses perhitungan kerentanan website menggunakan *Common Vulnerability Scoring System* versi 3.
e) Pada penelitian ini tidak dilakukan implementasi peningkatan keamanan *website* yang sudah ada.