BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Adapun beberapa penelitian terdahulu yang menjadi referensi untuk penelitian ini:

1. **H. Poston (*Mapping OWASP Top Ten to Blockchain*)**

   Berdasarkan penelitian terdahulu yang menggunakan kerangka kerja OWASP pada berbagai analisis dan kasus yang kompleks. Contohnya, adanya beberapa pembahasan penelitian pemetaan, kerentanan yang tercantum dalam 10 daftar teratas OWASP dengan versi terbaru menggunakan teknologi *blockchain*. OWASP merupakan perusahaan yang menyediakan segala informasi terkait sumber daya dalam edukasi pengembangan potensi masalah keamanan dalam kode mereka. 10 daftar teratas OWASP digunakan untuk mengidentifikasi kerentanan dalam *website*. Dalam hasil penelitian terdahulu ini memberikan hasil bahwa adanya proses identifikasi potensi kerentanan dalam sistem blockchain dengan memeriksa integrasi umum eksternal. Salah satunya, *blockchain* yang berbasis perangkat lunak. untuk kerentanan yang sama dapat diperjelas pada 10 daftar teratas OWASP yang juga berlaku dalam sistem *blockchain*. Kecuali pada kerangka XML *External Entities* yang tidak berlaku. Karena penggunaan XML pada sistem *blockchain* tergolong sedikit[8].

2. **T. Zhou, J. Yu dan D. Li (*Dynamic and lightweight framework for securing source addresses in SDN-based networks*)**

   Metode yang digunakan dalam penelitian sebelumnya dengan perbandingan penelitian yang dilakukan yaitu melakukan implementasi pada validasi alamat sumber di ruang lingkup SDN dengan membuat binding antara *IP address* dan juga struktur jaringan host untuk memfilter sebuah paket yang tidak cocok dengan efisiensi penerusan paket jaringan. Sehingga, fungsi *IP address* merupakan bagian penting dalam kerangka kerja yang diusulkan[9].

2.2 Studi Pustaka

2.2.1 Evaluasi Keamanan *Website*

Penelitian ini memberikan pemahaman yang komprehensif terkait beberapa aspek yang perlu dipertimbangkan dalam melakukan evaluasi keamanan *website*, termasuk jenis serangan yang sudah umum terjadi. Tidak hanya itu, adanya *scanning* kerentanan yang efektif, serta teknik mitigasi yang diterapkan untuk mengatasi temuan kerentanan[4].

2.3 OWASP ZAP

OWASP ZAP *(Zed Attack Proxy)* adalah *tools Scanning* keamanan aplikasi web yang dirancang untuk mengidentifikasi dan menguji keamanan aplikasi web kerentanan. *Tools* ini dikembangkan oleh *Open Web Application Security Project (OWASP)*, aplikasi web komunitas global yang berfokus pada keamanan. OWASP ZAP berkontribusi dalam mengidentifikasi celah keamanan dengan melakukan berbagai jenis pengujian dan analisis keamanan aplikasi web.

2.4 Wapiti

Wapiti adalah *tools scanning* kerentanan sumber terbuka dan resmi yang berjalan di OS Linux. Wapiti dapat melakukan proses pengujian berdasarkan penyesuaian komponen pembuatan *website*. Penelitian lain juga menjadi alasan mengapa *tools* ini digunakan[10]. Wapiti adalah pemindai kerentanan web sumber terbuka yang dievaluasi di koran. Ini diimplementasikan dengan antarmuka baris perintah (CLI) dan membutuhkan lebih banyak pengetahuan teknis dari pengguna. Studi evaluasi komparatif yang dilakukan di dalam penelitian tidak menunjukkan perbedaan yang signifikan di antara pemindai yang dievaluasi, termasuk Wapiti, dalam hal kemampuan mereka dalam mendeteksi kerentanan web yang umum. Fungsi dari *tools* Wapiti adalah sebagai berikut :

1. Wapiti adalah *tools* pengujian keamanan yang digunakan untuk mendeteksi kerentanan pada aplikasi web dengan menggunakan teknik serangan yang dikenal.
2. *Tools* ini dilakukan sebagai bentuk inspeksi terhadap parameter input yang dikirim ke *website* dan mencoba menemukan celah seperti SQL

injection, cross-site *script*ing (XSS), dan kerentanan terhadap file pengungkapan.

3. Wapiti juga dapat menguji keamanan halaman web dengan mengidentifikasi kerentanan seperti pembukaan direktori atau kelemahan terkait dengan pengaturan keamanan HTTP.

2.5 Nikto

Nikto adalah *tools* pengujian yang telah menguji sebanyak 6700 program yang tergolong file berbahaya, sedangkan 1250 versi aplikasi yang tidak mendapatkan pembaruan. Nikto dapat memeriksa beberapa indeks file melalui *server* HTTP[11]. HTTP merupakan gabungan antara HTTP dan SSL yang tergolong *website* yang ditandai dengan tampilan berwarna hijau di kolom pencarian *browser*. Alasan menggunakan Nikto sebagai *tools* analisis adalah[12].