BAB I PENDAHULUAN

I.1 Latar Belakang

Di era transformasi digital saat ini, pengelolaan data menjadi semakin kompleks, sehingga perlu pendekatan yang lebih efektif. GraphQL API, yang diperkenalkan pada tahun 2015, menawarkan keunggulan dibandingkan metode lain, seperti REST API. Keunggulannya terletak pada pengelolaan data nya, yaitu dapat meminta data secara spesifik sesuai kebutuhan, meningkatkan efisiensi dan mengurangi beban jaringan dengan menghindari pengambilan data yang tidak diperlukan.

Penggunaan GraphQL API berkembang mencapai 47% di kalangan pengembang global menurut laporan *The State of JavaScript 2023*. Platform besar seperti Facebook, GitHub, Shopify, Twitter, dan Airbnb telah mengintegrasikan GraphQL, ini menegaskan pentingnya GraphQL dalam industri teknologi saat ini. Penelitian sebelumnya oleh (Brito et al., 2019) menunjukkan bahwa dengan meningkatnya penerapan GraphQL, muncul kompleksitas dan masalah baru terkait keamanan API dan manajemen kinerja.

Dalam hal keamanan, salah satu ancaman yang dapat dihadapi GraphQL API adalah serangan *Denial-of-Service* (DoS). Serangan DoS bertujuan untuk menghabiskan sumber daya server, dan dalam konteks GraphQL, serangan ini dapat secara signifikan menghambat akses ke layanan, menyebabkan gangguan besar bagi pengguna dan mempengaruhi ketersediaan sistem.

Oleh karena itu, penelitian ini bertujuan untuk mengkaji kerentanan dan urutan dalam jenis serangan DOS berdasarkan jenis serangan dengan metrik ukuran cpu dan waktu saat eksploitasi. Hasilnya diharapkan dapat menjadi referensi bagi pengguna GraphQL dalam memilih dan mengimplementasikan API yang lebih aman dan meminimalisir risiko serangan DOS.

II.2 Rumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana cara mengidentifikasi serangan *Denial of Service* (Dos) dalam GraphQL?
b. Bagaimana mengetahui ukuran serangan *Denial Of Service* dalam melakukan eksploitasi GraphQL?
c. Apa dampak dari serangan *Denial of Service* (Dos) dalam GraphQL?

II.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengetahui dampak serangan *Denial of Service* (Dos) dengan teknik serangan *Circular Queries*, *Field Duplication*, *Alias Overloading*, dan *Object Limit Overloading* pada *API GraphQL* melalui eksploitasi pada kerentanan *API GraphQL*.
b. Mengimplementasikan dan menganalisis ukuran dengan menggunakan jenis teknik serangan *Denial of Service* (Dos) yang berbeda.
c. Menganalisis jenis serangan dengan metrik ukuran cpu dan waktu eksploitasi.

II.4 Batasan Penelitian

Adapun batasan penelitian pada penelitian ini adalah sebagai berikut:

a. Penelitian ini berfokus pada eksperimen dan simulasi pada serangan *Denial of Service* (DoS) pada API GraphQL dan tidak membahas jenis-jenis serangan lain yang mungkin terjadi pada GraphQL.
b. Pengujian penetrasi untuk GraphQL dilakukan hanya dengan menggunakan alat open source dan tersedia secara gratis yaitu (DVGA (Damn Vulnerable GraphQL Application)
c. Pengujian ini juga menggunakan *tools GraphQL Client* yang bernama Altair untuk menguji dan mengelola kueri dan mutasi GraphQL.

II.5 Manfaat Penelitian

Adapun manfaat yang didapatkan dengan adanya penelitian Tugas Akhir ini adalah sebagai berikut :

1. Secara Teoritis :
    a. Pemahaman tentang ancaman keamanan terhadap teknologi GraphQL.
    b. Memberikan landasan untuk penelitian lanjutan di bidang keamanan informasi dan serangan DoS pada GraphQL.
2. Secara praktis
    a. Peningkatan Keamanan Sistem: Memahami mekanisme serangan DoS menggunakan software Altair.
    b. Meningkatkan kinerja aplikasi dan sistem dengan berkurang nya *downtime* dan gangguan.
    c. API GraphQL memungkinkan perlindungan untuk data sensitif dan informasi pribadi yang diproses.