BAB I PENDAHULUAN

I.1 Latar Belakang

Di era digital saat ini, teknologi telah menjadi suatu bagian yang tidak dapat terpisahkan dari kehidupan sehari-hari. Salah satu teknologi yang telah menarik banyak perhatian yaitu *Application Programming Interface* (API). API memfasilitasi komunikasi antar suatu aplikasi dan berbagi data serta fungsionalitas. Akan tetapi, API yang sering dipakai sekarang saat ini yaitu REST API yang dimana API ini memiliki cukup banyak kemudahan yaitu dimana dia memiliki kinerja yang cukup baik, kompabilitasnya terhadap banyak platform dan arsitetkur yang terstruktur. Namun semua itu tidak ada bandingnya dengan salah satu jenis API yang telah mendapatkan popularitas adalah GraphQL. GraphQL merupakan bahasa *query* untuk API yang memberikan efisiensi, kekuatan, dan fleksibilitas yang luar biasa bagi pengembang yang dimana GraphQL mempunyai kelebihan yang tidak dimiliki oleh REST yaitu dapat melakukan pengambilan data yang lebih efisien dan dapat menghindari yang namanya *over-fetching*.

Namun, seperti semua teknologi yang ada. GraphQL juga mempunyai kerentanannya tersendiri. Salah satu kerentanan terbesar dalam penggunaan GraphQL adalah *injection vulnerabilities*. *Injection vulnerabilities* adalah salah satu jenis kerentanan keamanan yang dilakukan dengan memanipulasi *query* atau perintah yang dikirim ke aplikasi, dengan potensi untuk merusak ataupun mencuri data yang ada.

Dalam penelitian ini, penulis ingin mencari efektivitas dari teknik injeksi mana yang membutuhkan waktu secara efektif dalam melakukan eksploitasi terhadap GraphQL. Teknik injeksi yang digunakan dalam penelitian ini adalah *Log Injection, Spoof Injection,* dan *Command Injection*. Penelitian ini hanya berfokus pada serangan GraphQL. Dimana yang perlu diketahui serangan dengan menggunakan teknik injeksi sangat mengancam keamanan data aplikasi yang dimana pada penelitian ini waktu akan dijadikan sebagai perbandingan dalam melakukan eksploitasi.

I.2 Perumusan Masalah

Rumusan masalah yang mendasari penelitian ini adalah:

a. Bagaimana cara mengidentifikasi kerentanan dalam GraphQL?
b. Teknik serangan injeksi mana yang efektif untuk melakukan eksploitasi GraphQL?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Mengindentifikasi dan mengevaluasi serangan yang berkaitan dengan GraphQL, khususnya yang berbasis teknik injeksi.
b. Mengimplementasikan dan menganalisis teknik serangan injeksi yang efektif pada GraphQL dengan menggunakan *Command Injection*, *Spoof Injection* dan *Log Injection*.

I.4 Batasan Penelitian

Penelitian ini memiliki batasan penelitian seperti :

a. Penelitian ini tidak membahas mengenai algoritma dan implementasi pada mode *hardening* dan tanpa *hardening*.
b. Penelitian ini hanya meggunakan alat dan perangkat lunak yang tersedia secara gratis dan *open source* seperti *Altair* dan *GraphW00f*.

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Secara Teoritis :
    a) Dapat menambah pengetahuan dan pemahaman mengenai teknik-teknik serangan injeksi terhadap GraphQL.
    b) Dapat mengetahui tingkat kerentanan dari serangan injeksi terhadap GraphQL berdasarkan metrik *time*.
2. Secara Praktis :
    a) Dapat mengenali dan memahami teknik-teknik serangan injeksi yang berbeda dan berlangsung dengan langkah pada proses serangan injeksi.

b) Untuk tahapan lebih lanjut yaitu untuk aspek penguatan keamanan GraphQL pada aplikasi.