Abstrak

GraphQL adalah bahasa kueri yang memungkinkan klien untuk meminta data khusus dari API, membuatnya lebih efisien dan fleksibel dibandingkan REST API tradisional. Ini membuat aplikasi lebih cepat dan efisien dengan mengurangi over-fetching data, menggabungkan berbagai sumber data dalam satu permintaan, dan mendukung perubahan skema tanpa mengganggu integritas aplikasi yang sudah ada. Pada penelitian ini berfokus pada pengujian keamanan dan eksploitasi kerentanan *Denial of Service* (DoS) dalam API GraphQL nya. GraphQL, sebagai bahasa kueri yang semakin populer, memiliki fleksibilitas dalam pengambilan data namun juga rentan terhadap serangan DoS. Penelitian ini berfokus pada serangan *Denial of Service* (DoS) menggunakan berbagai teknik eksploitasi seperti *Circular Queries, Field Duplication, Alias Overloading,* dan *Object Limit Overriding*. Pengujian dilakukan dengan sistem operasi Kali Linux dan aplikasi pengujian seperti Altair dan DVGA. Dan dalam proses nya menggunakan metode *Threat Modelling Attack Tree*. Sehingga mendapatkan hasil dari pengujian bahwa serangan *Field Duplication* paling efektif dengan waktu eksekusi *time* tercepat dan penggunaan CPU yang cukup tinggi (2,5 detik/88.5% menjadi 1,86 detik /75.50%) dan risiko paling rendah yaitu Alias Overloading (1412,05 detik/99% menjadi 691,29 detik/93%), namun walaupun risiko paling rendah namun menghasilkan penggunaan CPU yang tinggi dalam membebani *server.* Penelitian ini memberikan pemahaman pentingnya pengujian dan penguatan keamanan API untuk mencegah serangan DoS.

Kata kunci – Graphql API, *Attack Tree, Denial of Service*, eksploitasi, *cpu, Time*