Abstract

GraphQL is a query language that allows clients to request specific data from an API, making it more efficient and flexible compared to traditional REST APIs. This makes applications faster and more efficient by reducing data over-fetching, combining various data sources into a single request, and supporting schema changes without disrupting the integrity of existing applications. This study focuses on security testing and exploiting Denial of Service (DoS) vulnerabilities within GraphQL APIs. As a query language that is growing in popularity, GraphQL offers flexibility in data retrieval but is also vulnerable to DoS attacks. The research centers on DoS attacks using various exploitation techniques such as *Circular* Queries, Field Duplication, Alias Overloading, and Object Limit Overriding. Testing was conducted using the Kali Linux operating system and testing applications such as Altair and DVGA, employing the Threat Modeling Attack Tree method. The results of the testing show that the Field Duplication attack is the most effective, with the fastest execution time and relatively high CPU usage (2.5 seconds/88.5% reduced to 1.86 seconds/75.50%), while the lowest risk was found in Alias Overloading (1412.05 seconds/99% reduced to 691.29 seconds/93%). Although Alias Overloading posed the lowest risk, it still resulted in high CPU usage, burdening the server significantly. This study provides an understanding of the importance of testing and strengthening API security to prevent DoS attacks.

Keywords –API GraphQL, Attack Tree, Denial of Service, exploitation, Cpu, Time