ABSTRACT

Graph Query Language (GraphQL) is a query language designed to facilitate interactions between clients and Application Programming Interfaces (APIs). GraphQL was created to simplify data exchange between the backend and frontend, providing a clear and easy-to-understand description of the data. The popularity of GraphQL continues to grow due to its effective capabilities in managing and retrieving data from APIs. As GraphQL gains more popularity, the need for best security practices and tools to test and protect GraphQL APIs will become increasingly important. Like other technologies, GraphQL also has some weaknesses, one of which is its introspection feature that can reveal sensitive information that should not be exposed. Therefore, this research aims to identify information disclosure vulnerabilities in GraphQL APIs and determine the most effective time between two security modes: before and after hardening. Two Methods and two tools are used to implement this, namely Introspection with InQL and Field Suggestion with Clairvoyance. By combining these two Methods, the research can effectively and efficiently identify and exploit weaknesses in GraphQL APIs, which are then visually represented through Data Flow Diagrams and Attack Trees to provide a comprehensive overview of the exploitation paths and potential attacks. After implementation, it was found that the most successful and efficient Methods for exploiting information disclosure vulnerabilities before hardening was the Field Suggestion Method, with a total time of 7.94 seconds. The most efficient time before and after hardening turned out to be the same, with the Field Suggestion Method taking a total time of 8.99 seconds after hardening. Thus, from this time comparison, it can be concluded that the shorter the time required, the faster an attacker can obtain harmful information from GraphQL.

Keywords – **GraphQL, Information Disclosure Vulnerability, Hardening, Introspection, Field Suggestion Method**