

## INTISARI

*Website* merupakan kumpulan halaman yang menampilkan informasi yang bersifat statis maupun dinamis yang saling terkait dan dihubungkan dengan jaringan *internet*. Seiring dengan perkembangan *website*, *website* tidak sekedar menjadi media informasi saja melainkan juga sebagai *e-commerce*, *video sharing*, publikasi digital dan platform *e-learning* sehingga sangat penting bagi seorang pengembang *web* atau praktisi keamanan untuk memperhatikan dan menjaga keamanan sebuah *website*. Salah satu serangan siber yang dapat mengancam keamanan *website* adalah *SQL injection*. *SQL injection* merupakan teknik serangan keamanan pada sebuah *website* dengan memanipulasi masukkan pengguna menggunakan *queri SQL* berbahaya. Serangan *SQL injection* dapat mengakibatkan kerusakan pada *database* dan kebocoran data sensitif. Salah satu cara untuk mengantisipasi serangan *SQL injection* adalah dengan melakukan pengujian kerentanan *SQL injection* pada *website* secara berkala. Pengujian kerentanan *SQL injection* dapat dilakukan dengan berbagai cara salah satunya adalah pengujian menggunakan *tools* khusus kerentanan *SQL injection*. SQLMap, Havij dan Ghauri merupakan beberapa contoh *tools* khusus yang dapat digunakan untuk melakukan pengujian kerentanan *SQL injection*. Sangat penting bagi seorang penguji untuk mengetahui *tools* yang dapat memberikan informasi secara lengkap dan *detail*. Oleh karena itu, penelitian ini bertujuan untuk menemukan *tools* yang efektif diantara SQLMap, Havij dan Ghauri dalam melakukan serangan *SQL injection* pada *website*. *Tools* yang memiliki kompleksitas serangan paling kompleks dan dapat memberikan hasil pengujian secara *detail* serta memiliki dukungan fitur paling lengkap akan dianggap sebagai *tools* yang paling efektif. Berdasarkan hasil pengujian, SQLMap merupakan *tools* yang paling efektif karena dapat memiliki kompleksitas serangan paling kompleks dan dapat memberikan hasil pengujian secara *detail* serta memiliki dukungan fitur paling lengkap.

Kata kunci: Kerentanan, Keamanan, *Website*, *SQL injection*, SQLMap, Havij, Ghauri

## **ABSTRACT**

*The website is a collection of pages displaying information that is both static and dynamic, interconnected, and linked to the internet. With the evolution of websites, they have become not only informational platforms but also e-commerce, video-sharing, digital publishing, and e-learning platforms. Therefore, it is crucial for a web developer or security practitioner to pay attention to and safeguard the security of a website. One of the cyber attacks that can threaten website security is SQL injection. SQL injection is a security attack technique on a website that manipulates user inputs using malicious SQL queries. SQL injection attacks can result in damage to the database and leakage of sensitive data. One way to anticipate SQL injection attacks is by conducting periodic vulnerability testing on the website. Vulnerability testing for SQL injection can be performed in various ways, one of which is testing using specialized tools for SQL injection vulnerabilities. SQLMap, Havij, and Ghauri are examples of specialized tools that can be used for vulnerability testing against SQL injection. It is crucial for a tester to be aware of tools that can provide comprehensive and detailed information. Therefore, this research aims to identify the effective tool among SQLMap, Havij, and Ghauri in conducting SQL injection attacks on websites. The tool with the most complex attack complexity, detailed testing results, and the most comprehensive feature support will be considered the most effective. Based on the test results, SQLMap is the most effective tool because it has the most complex attack complexity, provides detailed testing results, and has the most comprehensive feature support.*

*Keyword: Vulnerability, Security, Website, SQL injection, SQLMap, Havij, Ghauri*