ABSTRACT

The rapid growth of the internet has driven the use of web applications across various sectors. However, alongside the convenience offered by web applications, security threats have also become more prevalent, one of which is SQL Injection, often exploiting URL parameters as entry points. This study proposes a dynamic URL encryption technique using a hybrid algorithm that combines AES, SHA-3, and Base64 to prevent SQL Injection attacks. AES is used to encrypt the data, SHA-3 ensures data integrity through verification, and Base64 maintains a valid ciphertext format within the URL. The evaluation was conducted in three stages: SQL Injection testing, system performance testing, and ciphertext quality testing. SQL Injection tests using Acunetix detected no vulnerabilities, while all attack attempts via SQLmap failed with a 403 Forbidden response. Performance testing with Google Lighthouse showed a slight score decrease in score, dropping by 0,2% *from 90.65% to 90.45% after URL encryption was applied, mostly influenced by external factors, indicating that encryption did not significantly impact system performance. Shannon entropy testing on 100 ciphertexts yielded an average score of 5.3995 out of 6 (89.99%), and Pearson correlation was 0.0004, indicating high randomness and no detectable pattern between ciphertexts.Thus, the proposed dynamic URL encryption technique is proven to be both effective and efficient in enhancing web application security without compromising system performance.*

Keyword: *AES, Base64, SHA-3, SQL Injection, URL Encryption*

ABSTRAK

Pesatnya perkembangan internet mendorong penggunaan aplikasi web di berbagai sektor. Namun seiring dengan kemudahan yang ditawarkan aplikasi web, semakin terbuka juga ancaman keamanan, salah satunya adalah *SQL Injection* yang sering memanfaatkan parameter URL sebagai titik masuk. Penelitian ini mengusulkan teknik enkripsi URL secara dinamis menggunakan algoritma *hybrid* yang menggabungkan AES, SHA-3, dan Base64 untuk mencegah serangan *SQL Injection.* AES digunakan untuk mengenkripsi data, SHA-3 untuk verifikasi integritas, dan Base64 untuk memastikan format *ciphertext* tetap valid dalam URL. Pengujian dilakukan dalam tiga tahap yaitu uji *SQL Injection*, uji performa sistem, dan uji kualitas *ciphertext*. Hasil pengujian *SQL Injection* menggunakan Acunetix menunjukkan tidak ada kerentanan yang terdeteksi, sementara setiap upaya serangan menggunakan SQLmap mengalami kegagalan dengan *response 403 Forbidden*. Uji performa dengan *Google Lighthouse* menunjukkan penurunan skor tipis yaitu 0,2% dari 90,65% menjadi 90,45% setelah enkripsi URL diterapkan, yang sebagian besar dipengaruhi oleh faktor eksternal, sehingga enkripsi URL tidak berdampak signifikan pada kinerja sistem. Uji entropi *Shannon* terhadap 100 *ciphertext* menghasilkan rata-rata 5,3995 dari 6 (89,99%), dan korelasi *Pearson* sebesar 0,0004, mengindikasikan *ciphertext* bersifat acak dan tidak ada hubungan antar *ciphertext*. Demikian teknik enkripsi URL ini terbukti efektif dan efisien dalam meningkatkan keamanan aplikasi web tanpa mengorbankan performa sistem.

Kata kunci: AES, Base64, Enripsi URL, SHA-3, *SQL Injection*