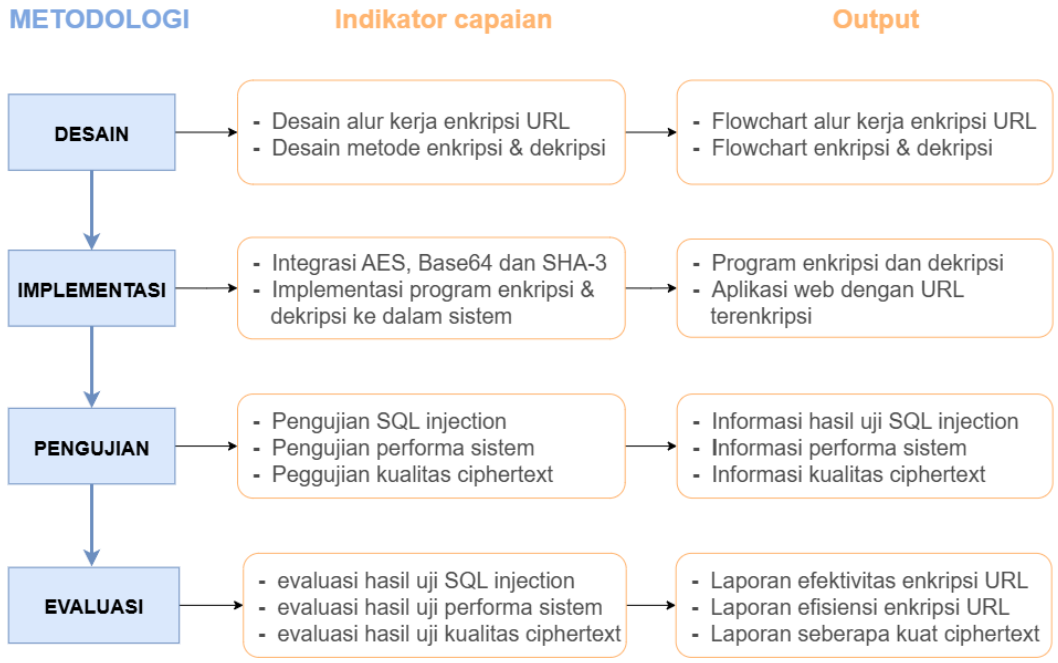
BAB III

METODOLOGI

Penelitian ini dilakukan melalui beberapa tahapan yang mencakup desain, implementasi, pengujian, dan evaluasi seperti yang diperlihatkan pada Gambar 3.1



Gambar 3. 1 Metodologi penelitian

3.1 Desain

Tahap ini menjelaskan rancangan skema alur kerja enkripsi URL secara dinamis dalam komunikasi *client-server* serta merancang mekanisme enkripsi dan dekripsi yang digunakan dalam penelitian untuk melindungi URL dari serangan *SQL Injection*. Desain ini mencakup konsep dan pendekatan yang diterapkan untuk memastikan keamanan dan efisiensi sistem. Kejelasan dalam perancangan ini menjadi aspek krusial, karena kesalahan pada tahap ini dapat berdampak pada keamanan serta efektivitas enkripsi dalam melindungi URL dari ancaman serangan.

3.1.1 Desain Skema Alur Kerja Enkripsi URL

Tahap ini menjelaskan rancangan alur proses pertukaran data antara *client* dan server yang melibatkan mekanisme enkripsi URL secara dinamis. Skema ini menggambarkan tahapan ketika *client* melakukan *request* dengan parameter yang telah dienkripsi, serta bagaimana server mendekripsi dan mengenkripsi ulang parameter tersebut. Desain ini berfungsi untuk memastikan bahwa seluruh komunikasi yang memanfaatkan parameter URL dapat berlangsung secara aman tanpa mengubah struktur logika dasar *request* HTTP antara *client* dan server.

3.1.2 Desain Mekanisme Enkripsi dan Dekripsi

Tahap ini mencakup perancangan mekanisme enkripsi dan dekripsi URL dengan menggunakan kombinasi algoritma AES, SHA-3, dan Base64. Perancangan dilakukan dalam bentuk *flowchart* yang menggambarkan alur proses enkripsi dari data *plaintext* menjadi *ciphertext*, serta proses dekripsi untuk mengembalikan data ke bentuk semula. *Flowchart* ini bertujuan untuk memvisualisasikan tahapan-tahapan utama yang akan diterapkan pada tahap implementasi

3.2 Implementasi

Tahap ini mencakup implementasi teknis dari desain yang telah dibuat. Proses implementasi meliputi integrasi algoritma dalam bentuk *pseudocode* serta penerapannya dalam sistem yang dikembangkan.

3.2.1 Integrasi Algoritma AES, SHA-3 & Base64

Tahap ini melibatkan implementasi algoritma AES, SHA-3, dan Base64 dalam bentuk *pseudocode* yang merepresentasikan proses enkripsi dan dekripsi URL. Setiap algoritma berkontribusi pada tahapan tertentu dalam proses

transformasi data, mulai dari penyandian hingga perlindungan integritas. Ketiga algoritma tersebut diintegrasikan ke dalam satu alur proses secara terpadu, sesuai dengan desain yang telah dirancang sebelumnya.

3.2.2 Implementasi Program Enkripsi URL ke dalam Sistem

Tahap ini menjelaskan proses integrasi kode program enkripsi dan dekripsi URL yang telah dikembangkan ke dalam sistem secara menyeluruh. Implementasi mencakup proses enkripsi URL sebelum *response* dikirim ke *client*, serta proses dekripsi saat sistem perlu membaca kembali informasi asli dari URL tersebut. mplementasi ini memungkinkan parameter URL disamarkan melalui enkripsi, namun tetap dapat didekripsi secara akurat tanpa mengganggu kinerja sistem.

3.3 Pengujian

Bagian ini menjelaskan metode pengujian yang digunakan untuk menguji keamanan sistem terhadap serangan *SQL Injection*, mengukur performa sistem setelah dilengkapi enkripsi URL, dan mengukur tingkat keacakan *ciphertext* yang dihasilkan. Setiap pengujian dilakukan dengan metode yang sistematis dan disertai hasil analisis berdasarkan alat bantu yang digunakan.

3.3.1 Uji *SQL Injection*

Tahap ini menjelaskan bagaimana sistem diuji terhadap berbagai jenis serangan *SQL Injection* menggunakan beberapa *tools* agar hasilnya tidak bersifat subjektif. Pengujian dilakukan menggunakan Acunetix dan SQLmap. Masing-masing *tools* akan menguji sistem tanpa enkripsi URL serta sistem dengan enkripsi URL untuk membandingkan tingkat keamanannya.

3.3.2 Uji Performa Sistem

Uji performa dilakukan untuk mengukur dampak penambahan fitur enkripsi URL terhadap kecepatan akses dan waktu muat halaman pada sistem. Pengujian ini membandingkan kondisi sistem sebelum dan sesudah penerapan enkripsi URL dengan menggunakan alat bantu *Google Lighthouse*. Hasil pengujian ini digunakan sebagai dasar evaluasi performa pada tahap selanjutnya.

3.3.3 Uji Kualitas *Ciphertext*

Uji kualitas *ciphertext* dilakukan untuk memastikan bahwa *ciphertext* yang dihasilkan tidak menunjukkan pola tertentu dan memiliki sifat acak yang kuat. Pengujian dilakukan menggunakan uji korelasi *Pearson* untuk menguji dinamika atau keterkaitan antar *ciphertext* serta uji entropi *Shannon* untuk menguji tingkat keacakan *ciphertext* yang dihasilkan. Pengujian ini diimplementasikan melalui bahasa pemrograman Python.

3.4 Evaluasi

Tahap ini melakukan analisis menyeluruh terhadap efektivitas, performa, dan kualitas hasil enkripsi URL berdasarkan hasil pengujian yang telah dilakukan. Evaluasi ini bertujuan untuk menilai sejauh mana sistem mampu menangkal serangan SQL Injection, mengukur dampak enkripsi terhadap kinerja halaman web, serta memastikan tingkat keacakan *ciphertext*.

3.4.1 Evaluasi Hasil Uji *SQL injection*

Tahap ini menganalisis hasil pengujian *SQL Injection* dan menentukan apakah sistem yang telah menerapkan enkripsi URL berhasil mencegah serangan

tersebut. Evaluasi dilakukan berdasarkan keberhasilan enkripsi URL melindungi sistem dalam menangkal berbagai skenario serangan yang diuji menggunakan Acunetix dan SQLmap.

3.4.2 Evaluasi Hasil Uji Performa Sistem

Hasil uji performa dianalisis untuk mengevaluasi sejauh mana enkripsi URL memengaruhi kinerja sistem. Evaluasi dilakukan dengan membandingkan nilai parameter performa sebelum dan sesudah enkripsi, guna menilai apakah terdapat perubahan signifikan terhadap waktu muat halaman. Analisis ini bertujuan untuk memastikan bahwa penerapan enkripsi tidak mengorbankan efisiensi sistem secara keseluruhan.

3.4.3 Evaluasi Hasil Uji Kualitas *Ciphertext*

Evaluasi dilakukan dengan menganalisis nilai koefisien korelasi *Pearson* untuk menilai dinamika *ciphertext* serta hasil uji entropi *Shannon* untuk menentukan tingkat keacakan *ciphertext*. Jika hasil pengujian menunjukkan bahwa *ciphertext* memiliki tingkat keacakan yang tinggi dan tidak memiliki pola keterkaitan yang signifikan, maka dapat disimpulkan bahwa metode enkripsi yang digunakan telah berhasil memenuhi tujuan penelitian.