BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Penelitian ini termasuk ke dalam *Rapid Application Development (RAD),* metode yang digunakan untuk mengembangkan sistem yaitu metode berulang. Cara kerjanya adalah dengan membangun model kerja pada tahap awal pembangunan sistem agar dapat memenuhi kebutuhan dari user.

Penelitian ini bertujuan untuk mendapatkan hasil berupa akurasi dan dan dapat mendeteksi serta membedakan jika bukan virus SQL Injection. Software ini berguna untuk mempermudah para admin dalam proses deteksi dengan mudah, efisien, dan meminimalisir biaya yang keluar terlalu mahal. Metode yang dikatakan optimal adalah metode yang memiliki nilai lebih besar yang menunjukkan jumlah produksi optimal.

Teknik pengumpulan data menggunakan studi literatur / Pustaka. Data-data khususnya Payload Dataset serangan code injection dikumpulkan dari internet. Dataset untuk serangan masing-masing adalah SQL Payload Dataset dan XSS Payload Dataset. XSS Payload Dataset diambil dari repository GitHub, Kaggle, dan OWASP.

Data Source
https://www.kaggle.com/datasets/syedsaqlainhussain/sql-injection-dataset (10851) https://www.kaggle.com/datasets/sajid576/sql-injection-dataset (30919)

Tabel 3.1 Sumber Dataset

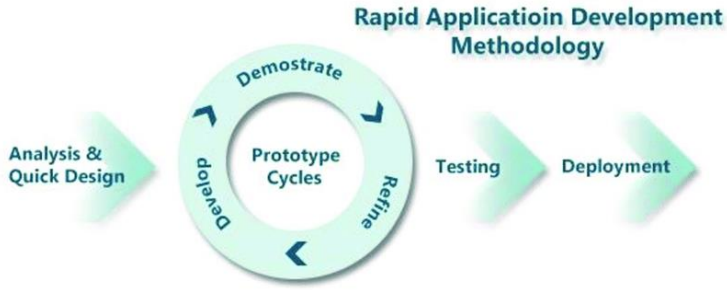
Attack Type	Dataset	Data Source
SQL Innjection	SQL Injection Payloads	https://github.com/payloadbox/sql-injection-payload-list/blob/master/Intruder/exploit/Auth_Bypass.txt

Tabel 3.2 Payloads Dataset

Melalui kolaborasi kedua tahap tersebut sehingga menghasilkan tahapan penelitian yang sesuai dengan rumusan masalah dan tujuan penelitian yaitu:

1. Analysis
2. Prototype Cycles
3. Testing
4. Deployment

Adapun proses dan prosedur pada saat penelitian yang dilakukan mengikuti alur penelitian yang dapat kami berikan dapat dilihat pada gambar dibawah



Gambar 3.1 RAD Methodologies

(Sumber: https://www.researchgate.net/)

Dalam RAD prototyping, analisis, develop, dan testing dilakukan pada waktu bersamaan untuk menghasilkan sistem dalam skala kecil dengan fungsi yang minim setelah itu akan dilakukan proses pengembangan secara iteratif sampai menghasilkan suatu sistem.

3.2 Metode Pengumpulan Data

Adapun teknik untuk pengumpulan data adalah sebagai berikut:

3.2.1 Riset

Merupakan suatu penelitian yang mana dalam penelitian tersebut saya meriset sebuah dataset yang ada pada sebuah website atau situs resmi untuk dijadikan acuan perjalanan sebuah coding yang akan diterapkan.

3.2.2 Collecting

Yaitu metode pengumpulan data dengan cara mengadakan tinjauan secara digital ke objek yang diteliti. Untuk mendapatkan data dan meyakinkan maka penulis melakukan riset, dan Collecting pada beberapa website untuk diambil dan diterapkan datanya.

3.2.3 Studi Pustaka

Untuk mendapatkan data-data yang bersifat teoritis maka penulis melakukan pengumpulan data dengan cara membaca dan mempelajari buku-buku, makalah ataupun referensi lain yang berhubungan dengan masalah yang dibahas.

3.3 Alat Pembuatan

Kebutuhan sistem yang digunakan dalam pengembangan tersebut terdiri dari perangkat keras dan perangkat lunak yaitu:

3.3.1 Perangkat Keras (Hardware) terdiri dari:

1. Laptop Acer Aspire 5
2. Mouse

3.3.2 Perangkat Lunak (Software) terdiri dari:

1. Microsoft Windows 11 (64 bit).
2. Microsoft Word 2019
3. Software Jupyter
4. Visual Studio Code
5. Anaconda
6. Browser Chrome

3.4 Analisis

Pada tahap Analisis dilakukan untuk memberikan jawaban dari pertanyaan siapa yang akan menggunakan perangkat lunak, apa yang akan dilakukan oleh perangkat lunak, dimana dan kapan perangkat lunak tersebut digunakan. Proses pengumpulan kebutuhan dilakukan secara intensif untuk

menspesifikasikan kebutuhan perangkat lunak agar dapat dipahami perangkat lunak seperti apa yang dibutuhkan oleh user. Pada tahapan ini peneliti akan menjelaskan bagaimana tahapan-tahapan untuk melakukan membangun konsep dari pembuatan "Aplikasi Deteksi *Cyber Attack SQL Injection* menggunakan *Algoritma Support Vector Machine"*. Kemudian melakukan pembuatan perangkat lunak baru.

3.4.1 Analisis Kebutuhan Fungsional

Pada analisis kebutuhan fungsional disini adalah bagian paparan mengenai bahan yang akan dimasukan kedalam pembuatan "Aplikasi Deteksi *Cyber Attack SQL Injection* menggunakan *support vector machine"* yang akan dibuat.

3.4.2 Analisis Kebutuhan Non-Fungsional

Pada analisis kebutuhan Non Fungsional ini terdapat dua komponen yaitu sebagai berikut:

1. **Analisis perangkat keras**

   Perangkat keras yang akan digunakan dalam melakukan coding dan pembuatan sistem presensi sebagai berikut:

   - Laptop Acer Aspire 5
   - Ram 8 GB DDR4
   - Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.19 GHz

2. **Analisis Perangkat Lunak**

   Software yang akan digunakan untuk melakukan proses pembuatan "Aplikasi Deteksi *Cyber Attack SQL Injection* menggunakan *Algoritma Support Vector Machine"* adalah menggunakan dua perangkat lunak yaitu sebagai berikut:

   a. ***Software* Untuk Pembuatan:**

      Berikut ini adalah software yang digunakan pada saat melakukan pembuatan aplikasi adalah sebagai berikut:

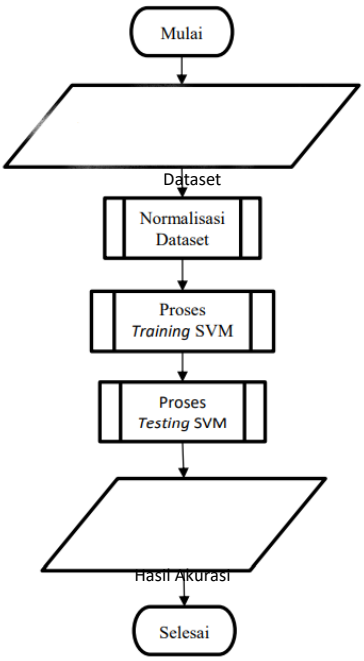
      - *Operating System* Menggunakan *Microsoft Window 10 (64 bit).*
      - *Microsoft Word 2019* adalah digunakan untuk melakukan proses pembuatan naskah tugas akhir skripsi.

- *Software Jupyter* digunakan untuk menerapkan atau menjalankan program deteksi SQL Injection.
- *Visual Studio Code* digunakan untuk deployment atau pembuatan aplikasi deteksi
- *Linux* digunakan sebagai IDE atau pendukung dalam pembuatan aplikasi

Nama Komponen	Spesifikasi	Keterangan
Laptop Acer	Intel(R) Core (TM) i3-1005G1 CPU @ 1.20GHz 1.19 GHz	Software utama dalam pembuatan sebuah program
Jupyter	3.7.11 Version	Pembuatan machine learning model dan model deteksi sql injection
Visual Studio Code	1.8.1 Version	Pembuatan aplikasi Deteksi SQL Injection
Chrome	Version 114.0.5735.199 (Official Build) (64-bit)	Wadah untuk menjalankan suatu program
Microsoft Word	2019	Pembuatan naskah tugas akhir skripsi

Tabel 3.3 Analisis Perangkat

3.5 Flowchart



Gambar 3.2 Flowchart

Pada gambar diatas menggambarkan fungsionalitas sebuah system atau program yang akan dijalankan.

3.6 Konsep

Nama	Keterangan
Judul	Aplikasi Deteksi *Cyber Attack SQL Injection* menggunakan Algoritma *Support Vector Machine*
Pengguna	Admin
Gambar	Menghasilkan informasi terkait keamanan suatu website pada SQL Injection.
Interaktif	Tersedia alat yang berfungsi untuk menjalankan perintah yang akan di jalankan oleh *user* pengguna.

Notifikasi	Tersedia notifikasi di tampilan jika termasuk dan bukan virus sql injection

Tabel 3.4 Konsep dan tujuan penggunaan aplikasi deteksi sql injection

Berikut ini konsep yang diterapkan:

1. Data Collecting

   Tahap pertama yang dilakukan yaitu Collecting Data, salah satunya pengumpulan data - data (Collecting), mengorganisir, transformasi data (Data Transformation), dan mempersiapkan data yang sesuai agar sesuai dengan kebutuhan analisis atau pemodelan yang akan dilakukan.

2. Model Selection

   Tahap Model Selection adalah tahap dimana semua objek atau bahan dibuat. Seperti halnya pembuatan kode program atau model Support Vector Machine (SVM) yang akan diimplementasikan, tapi sebelum itu data akan diseleksi terlebih dahulu agar sesuai dengan hasil nantinya. Pada tahap ini peneliti menggunakan Jupyter sebagai Integrated Development Environment (IDE).

3. Training

   Setelah melakukan selection model, langkah selanjutnya melakukan training dan testing data, yaitu melakukan percobaan model yang telah dibuat sebanyak 20 kali. Pada tahap akhir ini aplikasi akan diimplementasikan atau dijalankan kembali dengan cara menginput script SQL Injection kedalam model yang sudah dibuat sehingga menghasilkan akurasi yang sempurna pada web browser menggunakan Jupyter Notebook. Tahap ini ditujukan untuk memastikan apakah hasil deteksi sudah sesuai dengan tujuan yang diharapkan sebelumnya.

4. Detection

   Langkah selanjutnya yang dilakukan adalah Building a Attack Detection Model dan melakukan deteksi terhadap script Cyber Attack SQL Injectionn atau melakukan deteksi pada sebuah data yang sudah dikumpulkan menggunakan algoritma Support Vector Machine, target yang akan dideteksi adalah berupa virus SQL Injection.