BAB I PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi meningkatkan ketergantungan pada sistem digital, termasuk *Content Management System* (*CMS)* seperti WordPress yang menjadi salah satu platform terbesar untuk pengelolaan *website* (Secrieru & Stefănigă, 2025). WordPress mengandalkan plugin untuk melakukan kustomisasi seperti menambahkan fitur baru hingga modifikasi perilaku sistem (Lin dkk., 2023). Kemampuan plugin dalam melakukan kustomisasi disebabkan karena plugin memiliki akses seperti menjalankan kode PHP, mengakses database, dan mengirim serta menerima data dari server eksternal.

Plugin WordPress banyak dikembangkan oleh pihak ketiga dan tidak selalu melalui proses audit keamanan yang ketat sehingga menghasilkan banyak plugin berbahaya yang tersebar luas. Perilaku dari plugin berbahaya tersebut contohnya adalah melakukan *backdoor injection*, *data exfiltration*, *spam*, *SEO poisoning*, *privilege escalation*, dan *code obfuscation* (Kasturi dkk., 2022). Kebutuhan plugin pihak ketiga memberikan persentase kerentanan dengan jumlah besar pada WordPress yaitu sebesar 92%.

Proses deteksi plugin rentan dapat menggunakan plugin pada WordPress secara langsung. Meski demikian, penggunaan plugin WordPress secara langsung untuk melakukan deteksi kerentanan pada plugin lainnya sebagian besar gagal dalam mendeteksi kerentanan (Murphy dkk., 2021). Model deteksi plugin rentan menggunakan *machine learning* memberikan alternatif metode baru dalam mendeteksi plugin berbahaya.

Beberapa model *machine learning* yang umum untuk proses prediksi biner di antaranya adalah Logistic Regression, Naïve Bayes, dan Random Forest seperti yang dipakai pada penelitian (Ajayi dkk., 2025). Perbedaan antara penelitian tersebut dan penelitian ini terletak pada fokus pembahasan, yaitu pada improvisasi kinerja model untuk proses deteksi *malware* menggunakan data berupa perilaku *malware*, meskipun menggunakan model *machine learning* yang sama.

Pendekatan klasifikasi dari model Logistic Regression, Naïve Bayes, dan Random Forest berbeda-beda (Ajayi dkk., 2025). Logistic Regression efektif digunakan pada data observasional yang kompleks dan heterogen serta mampu memodelkan probabilitas kejadian secara langsung dan memiliki tingkat interpretabilitas yang tinggi (Dey dkk., 2025). Naïve Bayes merupakan algoritma klasifikasi berbasis probabilitas yang efektif untuk permasalahan klasifikasi biner dengan fitur yang relatif independen. Naïve Bayes mampu memberikan performa yang baik pada data berdimensi banyak dengan kompleksitas komputasi yang rendah (Islamanda & Sibaroni, 2024). Random Forest merupakan algoritma *ensemble learning* yang efektif dalam menangani hubungan non-linear dan interaksi kompleks antar fitur. Random Forest mampu memberikan performa yang stabil dan akurat pada data dengan banyak atribut serta tahan terhadap *noise* dan *overfitting* (Adetunji dkk., 2021).

Metadata seperti jumlah unduhan, *rating* pengguna, umur plugin, frekuensi pembaruan, dan versi WordPress yang diuji mampu digunakan sebagai fitur input dalam model *machine learning*. Struktur dataset metadata yang konsisten mampu bermakna prediktif (Gesese dkk., 2025).

Alat untuk melakukan pemrosesan *machine learning* terutama dengan kemampuan visualisasi data salah satunya adalah Orange. Fitur untuk melakukan *data management and preprocessing*, *classification*, *regression*, *association*, *ensembles*, *clustering*, *evaluation*, hingga *projections* tersedia pada Orange (Demšar dkk., 2013).

Berdasarkan latar belakang tersebut, penelitian ini berupaya menganalisis implementasi dan evaluasi model *machine learning* untuk prediksi plugin rentan WordPress kemudian membandingkan ketiga algoritma yang digunakan sehingga diharapkan dapat memberikan kontribusi bagi studi keamanan web berbasis teknik *machine learning*.

1.2. Rumusan Masalah

Rumusan masalah berdasarkan pemaparan latar belakang untuk penelitian ini sebagai berikut.

1. Bagaimana implementasi dan analisis model *machine learning* untuk proses prediksi kerentanan plugin WordPress menggunakan metadata?
2. Bagaimana performa model Logistic Regression, Naïve Bayes, dan Random Forest berdasarkan matriks evaluasi dalam melakukan prediksi plugin rentan WordPress?
3. Bagaimana analisis model yang memberikan performa terbaik berdasarkan matriks evaluasi untuk prediksi plugin rentan WordPress?

1.3. Tujuan Penelitian

Berdasarkan pada latar belakang dan rumusan masalah sebelumnya, maka tujuan penelitian ini adalah sebagai berikut:

1. Implementasi dan analisis proses prediksi plugin rentan WordPress dengan *machine learning* menggunakan metadata.
2. Menganalisis dan mengevaluasi performa dari model *machine learning* yang dipakai yaitu Logistic Regression, Naïve Bayes, dan Random Forest dalam melakukan proses prediksi plugin rentan WordPress.
3. Menganalisis model dengan performa terbaik dalam melakukan proses prediksi plugin rentan WordPress menggunakan faktor berupa hasil dari evaluasi matriks.

1.4. Manfaat Penelitian

Manfaat yang dapat diambil dari penelitian ini adalah sebagai berikut:

1. Manfaat akademis, penelitian ini memberikan kontribusi ilmiah dalam bidang *machine learning* dan keamanan aplikasi web dengan menyajikan analisis perbandingan performa algoritma Logistic Regression, Naïve Bayes, dan Random Forest dalam memprediksi kerentanan plugin WordPress berbasis metadata.
2. Manfaat penelitian lanjutan: Penelitian ini dapat dijadikan sebagai acuan bagi penelitian selanjutnya dalam pengembangan metode deteksi kerentanan plugin WordPress, baik dengan menambahkan algoritma lain, mengintegrasikan teknik *Feature Extraction* and *Engineering* yang lebih

kompleks, maupun mengembangkan pendekatan berbasis *Deep Learning* atau data temporal.

3. Manfaat untuk Universitas Siliwangi: sebagai bahan tambahan untuk penelitian lainnya yang berkaitan dengan deteksi plugin rentan berbasis *machine learning* di lingkungan akademik studi Informatika Universitas Siliwangi.
4. Manfaat untuk penulis, memberikan wawasan keilmuan baru pada bidang keamanan web dan pemodelan *machine learning* terutama untuk deteksi plugin rentan secara otomatis.

1.5. Batasan Masalah

Batasan masalah dijadikan sebagai batas pencapaian dari penelitian yang berlangsung yang dijelaskan sebagai berikut:

1. Penelitian ini membahas prediksi kerentanan plugin WordPress dan tidak mencakup analisis keamanan pada inti (*core*) WordPress maupun tema (*theme*).
2. Data yang digunakan dalam penelitian ini terbatas pada metadata plugin WordPress yang diperoleh melalui WordPress Plugin API.
3. Algoritma *machine learning* yang digunakan dalam penelitian ini dibatasi pada Logistic Regression, Naïve Bayes, dan Random Forest.
4. Proses klasifikasi dilakukan dalam bentuk klasifikasi biner, yaitu plugin dikategorikan sebagai rentan atau tidak rentan.
5. Evaluasi performa model dibatasi pada metrik akurasi, presisi, *recall*, dan *F1-score*.

6. Dataset yang digunakan merupakan data yang dikumpulkan pada periode waktu satu hingga dua bulan, sehingga hasil penelitian tidak mempertimbangkan perubahan status keamanan plugin di masa mendatang.
7. Penelitian ini berfokus pada analisis implementasi dan perbandingan performa algoritma, bukan pada pengembangan atau optimasi metode baru, termasuk penyesuaian *hyperparameter* secara ekstensif.