BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya teknologi informasi, layanan *web* di internet menjadi suatu hal yang penting untuk menyimpan berbagai informasi. Kondisi ini menyebabkan meningkatnya kasus peretasan pada laman *web*, untuk itu keamanan pada *web* menjadi sangat penting untuk diperhatikan supaya dapat meminimalisir kasus pencurian data penting yang tersimpan (Maniraj et al., 2024).

Keamanan *web* menjadi semakin penting di era digital, hal ini disebabkan banyaknya aktivitas yang dilakukan secara *online*, seperti bertransaksi *online*, menyimpan data pribadi, dan lain-lainnya. Kekurangan pada keamanan *web* dapat menciptakan peluang bagi para penjahat siber untuk melakukan tindakan kriminal seperti pencurian data pribadi, penipuan online, dan *malware*. Dampak pelanggaran keamanan *web* dapat sangat parah, baik bagi individu maupun organisasi. Individu dapat mengalami kerugian finansial, pencurian identitas, dan kerusakan reputasi. Organisasi dapat mengalami kerugian finansial, kehilangan data, dan kerusakan reputasi. Oleh karena itu, penting untuk meningkatkan keamanan *web* dengan menerapkan berbagai langkah pencegahan, seperti memasang perangkat lunak antivirus dan *anti-malware*, memasang *firewall*, dan melakukan *backup* data secara teratur. Menurut laporan dari Badan Siber dan Sandi Negara (BSSN) Indonesia, antara Januari hingga 29 April 2019, dari 895 laporan yang diterima, *SQL Injection* dan *XSS* merupakan kerentanan yang paling banyak ditemukan, dengan total 637 laporan (Harahap, 2021).

Menurut (Orisa & Ardita, 2021) pemahaman mengenai aspek keamanan merupakan suatu hal yang *esensial* bagi seorang ahli *web*. *WAF* yang tertanam pada infrastruktur *server* dapat meningkatkan aspek keamanan aplikasi *web* (Riska & Alamsyah, 2021).

Berdasarkan penelitian dari (Prasetyo et al., 2024) penggunaan *WAF* dapat melindungi *web* dari berbagai serangan contohnya serangan *SQL injection*. *Website* yang tidak dilindungi oleh *WAF* rentan menjadi target peretasan oleh *Hacker*. Dalam sistem keamanan *web*, *WAF* bekerja dengan cara memilah *request* atau *query* yang masuk dan memblok *request* yang berpotensi membahayakan bagi keamanan situs *web* (Sukmana et al., 2024).

Mengimplementasikan *WAF* pada situs *web*, *ModSecurity* dapat menjadi pilihan utama. Berdasarkan penelitian yang dilakukan oleh (Wiguna et al., 2020) *ModSecurity* efektif dalam mendeteksi dan mencegah serangan seperti *SQL injection* dan *Cross-Site Scripting (XSS)*. Berdasarkan penelitian tersebut, kemampuan *ModSecurity* dapat secara signifikan melindungi informasi sensitif dalam *website*. Selain itu, *ModSecurity* tidak memerlukan lisensi karena bersifat *open source* (Dhiatama Ayunda et al., 2021).

Proses dalam membantu mengidentifikasi dan mengevaluasi keamanan pada situs *web*, *VA* merupakan langkah yang penting untuk dilaksanakan dan membantu pengelola *web* mengidentifikasi kerentanan yang ada pada layanannya sehingga pengelola dapat menerapkan *rules-rules* yang tepat dan meningkatkan efektivitas perlindungannya (Jurnal & Lana Rahardian, 2022). *VA* dapat dilakukan dengan melakukan *scanning* laman *web* dengan *tools* yang tersedia seperti *OWASP*

ZAP. *Tools* tersebut dapat melakukan *scanning* pada situs *web* untuk menilai keamanannya dengan melakukan penyerangan terukur pada *web* tersebut, hasilnya *tools* tersebut dapat memberikan informasi terkait kerentanan yang dimiliki situs *web*. Terdapat 4 kategori kerentanan pada *tools* tersebut yaitu, *high risk, medium risk, low risk* dan *informational risk* (Wahyudin, 2024).

Yayasan Sakata Innovation Center (YSIC) merupakan perusahaan *startup* yang bergerak di bidang pendidikan dan teknologi dengan fokus pada peningkatan *skill, knowledge*, dan *attitude*. YSIC mempunyai *website* yang bernama "Sakattaku.com" yang dimana *web* Sakattaku dibuat untuk memberikan informasi lengkap dan terkini tentang organisasi kepada pengunjung *web*. Pada isi *web* tersebut terdapat beberapa informasi yaitu memperkenalkan perjalanan Sakata, Visi dan Misi, memperlihatkan kegiatan Sakata, konten dan keunggulan lainnya. YSIC memiliki kegiatan sehari-hari yaitu menyediakan pelatihan, *workshop*, membuat konten, dan *short course* yang dilaksanakan secara online melalui program Sakata MOOC.

Berdasarkan hal-hal yang telah dibahas sebelumnya, maka peneliti melakukan *studi literatur* mengenai penelitian terdahulu yang berkaitan dengan penelitian ini. Penelitian (Jurnal & Lana Rahardian, 2022) melakukan pengujian keamanan situs *web* dengan menerapkan *VA* menggunakan aplikasi *acunetix*. Aplikasi ini memungkinkan untuk mendapatkan hasil yang terperinci dan menilai tingkat keamanan situs *web* dengan memanfaatkan *metrics* keamanan yang menampilkan kategori nilai *high*, *medium*, atau *low.* Penilaian ini diperoleh dengan menggunakan *security metriks* yang menghasilkan skor berbasis dengan rentang 1-

10, hasil pada *web* tersebut memiliki tingkat keamanan tinggi. Penelitian lainnya dilakukan oleh (Wahyudin, 2024) berfokus pada identifikasi celah dari *website sakupos.com* untuk kemudian dianalisis pada tahap *Vulnerabilies Scanning* dengan *Vulnerability Risk Medium*, 2 *tools* yaitu *OWASP ZAP* ditemukan 6 kerentanan dengan *vulnerabilituy Risk Medium*, 2 *risk low*, 2 *risk Informational* dan di *tools Nikto* ditemukan 1 *vulnerability risk Medium*, dan 1 *risk* di Tingkat *low.*

Penelitian (Narhudin et al., 2024) mengevaluasi *web* di PT Rachma Perkasa Utama dengan fokus pada serangan *injection SQL* dan *XSS* menggunakan metode *OWASP.* Mengidentifikasi kerentanan dengan risiko sedang hingga rendah dan ketidakpatuhan pada kebijakan keamanan. Penelitian selanjutnya dilakukan oleh (Wiguna et al., 2020) melakukan pengujian dan analisa terhadap penggunaan *WAF* dengan menggunakan *ModSecurity WAF* dan *OWASP WAF*, ujicoba *WAF* menunjukan bahwa serangan *SQL injection* dalam *tools ModSecurity* ini memungkinkan sistem untuk membatasi penyerang untuk mengevakuasi *SQL injection* di sebuah *website*, hasil ujicoba ini menunjukan penyerang tidak mendapatkan informasi apapun yang terkandung di dalam *website* karena sistem keamanan menemukan celah terbuka untuk dieksploitasi lebih lanjut.

Penelitian ini menguji keamanan website Desa Kragan menggunakan metode *PTES* dengan bantuan *empat tools: Whois, Zenmap, OWASP ZAP*, dan *SQLMap*. Pengujian dilakukan melalui lima tahapan mulai dari pengumpulan informasi hingga pelaporan. Dari hasil pemindaian *OWASP ZAP*, ditemukan 14 celah keamanan, termasuk yang bersifat kritis seperti *Cloud Metadata Exposure* dan *SQL Injection*. Beberapa celah berhasil dieksploitasi, namun *SQL Injection*

gagal karena terlindungi *WAF* dan *SSL*, penelitian ini belum menyertakan penilaian risiko secara kuantitatif dan tidak melakukan evaluasi ulang setelah rekomendasi perbaikan diterapkan (Fadila Burhani & Priyawati, 2024). Penelitian ini menguji efektivitas WAF sebagai sistem keamanan pada website wantilandesa.id dengan membandingkan kondisi sebelum dan sesudah WAF diterapkan. Pengujian dilakukan menggunakan SQL Injection, DDoS, dan pemindaian dengan OWASP ZAP. Sebelum WAF, ditemukan 20 celah dan serangan DDoS berhasil; setelah WAF aktif, celah berkurang menjadi 10 dan DDoS gagal. Pengujian juga didukung oleh Wireshark dan SSL. Namun, penelitian ini tidak melakukan eksploitasi langsung terhadap celah yang ditemukan, tidak menilai risiko secara kuantitatif, dan hanya fokus pada satu metode keamanan, sehingga hasilnya kurang bervariasi dan tidak menggambarkan perlindungan yang menyeluruh (Ardiansyah et al., 2023).

Permasalahan utama yang ingin diselesaikan pada penelitian ini adalah kurangnya perlindungan keamanan dan belum pernah dilakukannya pengujian keamanan terhadap *website* Sakattaku.com hal ini diketahui menurut pengelola *web* tersebut. Kurangnya aspek perlindungan pada *website* tersebut dapat menyebabkan *website* rentan terhadap berbagai ancaman dan jenis serangan siber, seperti *SQL injection*, *XSS*, dan *CSRF*, yang dapat mengakibatkan kebocoran data, gangguan operasional, dan kerusakan reputasi, padahal *website* tersebut menyimpan data penting bagi perusahaan.

Berbeda dengan penelitian sebelumnya, pada penelitian ini pemecahan masalah akan dilakukan dengan membandingkan hasil metode *VA* yang dilindungi dan yang tidak dilindungi oleh *WAF* pada *web,* dengan *VA menggunakan tools*

OWASP ZAP, dan *WAF* menggunakan *ModSecurity*. Metode *VA* digunakan bertujuan untuk secara sistematis mengidentifikasi, menganalisis, dan mengevaluasi potensi celah keamanan dalam aplikasi web, dengan pendekatan ini bertujuan untuk memahami sejauh mana kemampuan deteksi *WAF*, mengidentifikasi kelemahan yang tidak terdeteksi *WAF*, serta memberikan organisasi rekomendasi untuk memilih solusi yang tepat untuk membangun postur keamanan aplikasi *web* yang kuat dan efektif.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan, ada beberapa rumusan masalah yang akan dibahas dipenelitian ini yaitu :

1. Bagaimana metode *VA* dapat mengidentifikasi kerentanan keamanan pada *web* Sakattaku.com untuk menentukan *rules* pada *WAF* yang akan diimplementasikan?
2. Bagaimana perbandingan hasil evaluasi dari pengujian *web* dengan metode *VA* yang dilindungi dan yang tidak dilindungi oleh *WAF*, untuk keefektifan *WAF* dalam melindungi aplikasi *web* dari serangan siber?

1.3 Tujuan Penelitian

Tujuan penelitian ini berdasarkan rumusan masalah yang telah dibuat sebagai berikut :

1. Mengidentifikasi kerentanan pada *web* Sakattaku.com untuk menentukan *rules* yang dipakai pada *WAF* untuk meningkatkan keamanan pada *web* tersebut.

2. Mengevaluasi efektifitas *WAF* dalam melindungi aplikasi *web* dari serangan *siber* setelah *VA,* mengidentifikasi area yang perlu diperkuat, dan mengoptimalkan konfigurasi *WAF.*

1.4 Manfaat Penelitian

Manfaat penelitian ini dapat memberikan kontribusi dalam pengembangan metode yang efektif untuk mengidentifikasi dan mengatasi kerentanan pada aplikasi *web*, dengan memahami metode *VA* dapat membantu organisasi mengoptimalkan konfigurasi *WAF* mereka. Penting untuk memastikan bahwa *WAF* beroperasi dengan efektif dan memberikan perlindungan maksimal terhadap serangan *siber.*

1.5 Batasan Masalah

Ada beberapa batasan masalah yang perlu diperhatikan dalam penelitian ini, yaitu:

1. Penelitian ini menggunakan *website* Sakattaku yang merupakan *website* resmi dari Yayasan Sakata Innovation Center (YSIC).
2. Serangan ini menggunakan *SQL injection*, *Cross-Site Scripting* (*XSS*) dan *Cross-Site Request Forgency* (*CSRF*).
3. Alat yang digunakan untuk men*scanning vulnerability* yaitu *OWASP ZAP*.
4. Perangkat lunak yang dipakai oleh *Web Application Firewall* yaitu *ModSecurity.*