BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam UU No 3 Tahun 2002 tentang Pertahanan Negara, telah ditetapkan bahwa ancaman dalam sistem pertahanan negara terdiri dari ancaman militer dan ancaman non militer, termasuk diantaranya ancaman siber. Berdasarkan data *Indonesia Security Incident Response Team on Internet Infrastructure* (IDSIRTII) terdapat 48,8 juta serangan Internet sepanjang tahun 2015 di Indonesia [1]. Tingginya angka kejahatan dan peretas di bidang Internet ini menjadi ancaman di tengah masifnya pertumbuhan pengguna internet di Indonesia. Tercatat pada tahun 2020 terdapat 3 kejadian *data breach* yang menyita banyak perhatian publik, yang pertama terjadi pada bulan April Tokopedia mengalami data breach yang mengakibatkan 91 juta data penggunanya bocor ke internet [2], kedua pada bulan Mei 2020 Bukalapak juga mengalami data breach yang mengakibatkan 12 juta data penggunanya bocor, dan Lembaga Komisi Pemilihan Umum (KPU) juga mengalami hal serupa dimana ada 2,3 juta data penduduk Indonesia yang bocor [3]. Sedangkan pada tahun 2021 sendiri hingga bulan Juli tercatat ada 2 kasus serupa yang dialami 2 perusahaan BUMN yaitu BPJS pada bulan Mei tercatat ada sekitar 279 data pemegang BPJS bocor ke internet yang mengakibatkan kerugian sebesar 600 triliun rupiah [4], dan BRI tercatat 2 juta data, dan 463.000 dokumen pengguna layanan BRI *LIFE Insurance* telah bocor [5].

RASP (Runtime Application Self Protection) merupakan salah satu teknologi modern yang digunakan untuk melindungi aplikasi yang sedang berjalan secara real-time. Jika dibandingkan dengan WAF (Web Application Firewall), RASP melindungi aplikasi secara real-time, RASP dapat melindungi aplikasi dengan menganalisa perilaku aplikasi dan konteks perilaku tersebut. Dengan RASP aplikasi dapat memantau traffic dan melakukan tindakan prevensi jika RASP mengidentifikasi adanya perilaku mencurigakan pada aplikasi secara real-time. Sedangkan WAF hanya melakukan perlindungan dengan melakukan penyaringan request yang dianggap mencurigakan pada web server [6] dan [7].

Peter Cisar dan Sanja Maravic Cisar pada jurnalnya yang berjudul The Framework of Runtime Self-Application Protection pada tahun 2016, penulis mencoba membandingkan performa deteksi RASP dengan WAF pada web based application. Hasilnya RASP melakukan proteksi dari 2 sisi yaitu sisi aplikasi dan network sedangkan WAF hanya melakukan perlindungan pada sisi network saja. Sehingga WAF dinilai tidak terlalu efektif untuk melindungi aplikasi dari serangan yang berjalan secara client side [6]. Berdasarkan studi oleh tim Positive Technologies Security pada artikelnya berjudul Mobile Application Security and Threat 2019, hampir 76% pencurian data seperti password, informasi finansial dan data personal terjadi karena terdapat celah pada program khususnya di tempat penyimpanan data pada aplikasi, lalu hal ini dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mencuri data-data tersebut dengan

memasukan malware pada mobile device milik korban, dan serangan yang disebutkan diatas merupakan serangan yang bersifat client-side attack [6].

Dari permasalahan diatas, penulis akan menganalisis bagaimana RASP melakukan pengamanan dan meminimalisir serangan pada platform aplikasi *mobile* jika dibandingkan dengan aplikasi yang hanya menerapkan WAF atau dengan kata lain hanya menerapkan proteksi pada API saja. Lalu apakah RASP dapat menjadi solusi instan terhadap masalah keamanan aplikasi dan dapat menggantikan WAF.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka muncul pernyataan berikut :

1. Perbandingan antara RASP dengan WAF terkait jumlah dan jenis serangan yang dapat terdeteksi ?
2. Seberapa jauh RASP dalam mencegah serangan pada aplikasi *mobile* ?
3. Apakah RASP dapat menjadi solusi instan terhadap masalah keamanan pada aplikasi *mobile* ?

1.3 Batasan Masalah

Berdasarkan masalah diatas, maka batasan dari persoalan ini adalah :

1. Ada beberapa bahasa pemrograman yang tidak *compatible* dengan RASP.
2. Versi RASP AppSealing yang digunakan adalah versi 2.25.0
3. RASP menggunakan versi *trial*, sehingga fitur seperti *logging* dan *real-time* logging tidak diterapkan.

1.4 Maksud dan Tujuan Penelitian

Adapun tujuan yang hendak dicapai dalam penggunaan RASP adalah :

1. Mendeteksi secara *real-time* serangan atau *traffic* mencurigakan pada aplikasi.
2. Membandingkan jumlah serangan yang dapat dicegah antara aplikasi *mobile* yang menggunakan RASP dengan yang tidak menggunakan atau hanya menggunakan WAF saja.

1.5 Manfaat Penelitian

Penulis :

1. Sebagai salah satu syarat dalam menuntaskan jenjang strata satu untuk memperoleh gelar Sarjana (S.Kom).
2. Menerapkan ilmu serta teori yang telah didapatkan selama masa perkuliahan.
3. Sebagai dokumentasi bagi penulis terhadap dunia *cyber security* terutama pada bidang *mobile application security*.

Pemilik Aplikasi :

1. Meminimalisir serangan siber dan kebocoran data.
2. Meminimalisir kerugian materi dan tenaga jika terjadi insiden siber bagi perusahaan/pemilik aplikasi.
3. Meningkatkan kepercayaan pengguna terhadap aplikasi yang dikelola oleh pemilik aplikasi.
4. Sebagai pertimbangan penerapan RASP.

1.6 Metode Penelitian

1.6.1 Metode Pengumpulan Data

Data yang digunakan pada penelitian ini adalah data keberhasilan deteksi serangan pada RASP maupun WAF pada target mobile application dan API pada mobile application yang akan digunakan sebagai perbandingan antara ke-2 hal tersebut.

1.6.2 Metode Analisis

Pada tahap ini penulis melakukan analisis terhadap deteksi serangan oleh RASP maupun WAF yang ditujukan pada aplikasi yang berguna untuk bahan perbandingan performa.

1.6.3 Metode Pengujian

Pada tahap ini penulis melakukan pengujian serangan terhadap aplikasi yang sudah dipasangi RASP dan aplikasi yang sudah dipasangi WAF.

1.6.4 Sistematika Penulisan

Sistematika penulisan dibuat untuk mempermudah penulis dalam penyusunan skripsi. Adapun sistematika penulisan ini dikelompokan kedalam beberapa bab. Setiap bab diuraikan sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini menjelaskan tentang dasar penelitian, yang berisi latar belakang, rumusan masalah, Batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II METODE PENELITIAN

Pada bab ini berisi tinjauan Pustaka yang mirip dengan penelitian ini. Pada bab ini juga berisi tentang landasan-landasan teori yang mendukung dalam penelitian ini.

BAB III METODE PENELITIAN

Pada bab ini berisi tentang alur dari penelitian yang berupa perancangan perangkat dan bahan apa saja yang akan digunakan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini berisi tentang hasil dari tahapan penelitian yang dilakukan secara menyeluruh termasuk hasil dari pengujian.

BAB V PENUTUP

Bagian terakhir dari penelitian yang berisi tentang kesimpulan dan saran untuk memperbaiki kekurangan yang ada pada penelitian ini.