BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, keamanan aplikasi web menjadi salah satu prioritas utama dalam pengembangan perangkat lunak. Website yang tidak aman dapat menjadi target serangan siber yang dapat merugikan pengelola situs dan penggunanya. Salah satu jenis serangan yang sering dihadapi dalam pengembangan aplikasi web adalah *Cross-Site Request Forgery* (CSRF).

Cross-Site Request Forgery (CSRF) adalah sebuah sebuah serangan eksploitasi web yang membuat pengguna tanpa sadar mengirim sebuah permintaan atau *request* ke website melalui website yang sedang digunakan saat itu. Salah satu jenis serangan CSRF adalah serangan melalui *form,* penyerang membuat *form* palsu yang meniru *form* yang ada di situs target. *Form* palsu ini dapat berisi permintaan yang tidak diinginkan atau jahat. Ketika pengguna yang terinfeksi mengisi *form* tersebut, data yang dimasukkan akan dikirimkan ke situs target sehingga menyebabkan tindakan yang tidak sah. Oleh karena itu, salah satu pencegahan dari serangan tersebut adalah menggunakan token anti-CSRF, dimana token ini disertakan setiap ada permintaan *HTTP* dan divalidasi oleh *server* untuk memastikan bahwa permintaan tersebut benar-benar berasal dari pengguna yang sah.

PT. Baracipta Esa Engineering (Beecons) merupakan perusahaan konsultan dan kontraktor yang bergerak di bidang arsitektur dan perencanaan, manajemen konstruksi, pemetaan dan survey. Salah satu platform aplikasi yang dikembangkan adalah Tenderplus.id, yaitu sebuah platform aplikasi yang dikembangkan untuk memudahkan pengguna dalam memantau paket tender terbaru di LPSE (Layanan Pengadaan Secara Elektronik) pemerintah Indonesia. Beberapa fitur di website tersebut antara lain menyediakan notifikasi realtime melalui WhatsApp dan email, serta fitur analisis kinerja perusahaan kompetitor, untuk membantu pengguna

menjadi lebih unggul dalam pengajuan penawaran di tender yang sedang diikuti. Oleh karena itu, penting untuk meningkatkan keamanan aplikasi web, salah satunya mencegah serangan CSRF.

Website ini belum menerapkan proteksi CSRF. Sehingga berdasarkan permasalahan diatas, proyek akhir ini bertujuan untuk mengimplementasikan proteksi CSRF pada website Tenderplus.id dengan tujuan untuk mencegah tindakan yang tidak diinginkan dengan memastikan bahwa permintaan yang dilakukan pengguna adalah permintaan yang sah dan berasal dari pengguna yang berwenang.

1.2 Rumusan Masalah

Berdasarkan permasalahan yang telah diuraikan pada latar belakang, maka rumusan masalah yang diidentifikasikan pada Proyek Akhir ini adalah bagaimana mengimplementasikan proteksi CSRF pada website Tenderplus.id yang menggunakan framework Codeigniter 3.

1.3 Tujuan

Tujuan dari Proyek Akhir ini adalah mengimplementasikan proteksi CSRF pada website Tenderplus.id untuk melindungi pengguna yang telah masuk ke sistem (*authenticate users*) dari tindakan yang tidak diinginkan atau tidak sah yang mungkin dilakukan oleh pihak lain.

1.4 Batasan Masalah

Dalam penyelesaian Proyek Akhir ini, penulis membatasi permasalahan sebagai berikut:

1. Implementasi proteksi CSRF hanya berfokus apabila ada proses *request POST* yang dilakukan pengguna .
2. Implementasi proteksi CSRF hanya berfokus pada halaman login, halaman *manage marketing*, halaman plot tim dan halaman CRM (*Customer Relationship Management*) .
3. Fokus utama adalah proteksi CSRF, tidak mencakup jenis serangan lainnya.