

BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya teknologi informasi, pesatnya penggunaan aplikasi berbasis website sebagai sarana berbagi informasi, komunikasi, pengelolaan data berbagai bidang, terutama dalam lingkungan pendidikan. Menurut (Herdianto et al., 2022) salah satu hal yang berkembang cukup pesat adalah aplikasi berbasis web [1]. Aplikasi web dapat dijalankan di berbagai platform dan juga termasuk aplikasi yang ringan digunakan. Website ialah sebuah halaman data berbasis web yang menyediakan berbagai informasi, dokumen ataupun tautan yang menghubungkan halaman data satu dengan halaman data lainnya yang dapat kita akses saat terkoneksi dengan internet kapanpun dan dimanapun melalui browser [2].

Antarmuka pengguna menjadi elemen yang paling sering berinteraksi langsung dengan pengguna. Antarmuka pengguna (UI) mengacu pada sistem serta pengguna yang akan berinteraksi satu sama lain melalui perintah atau teknik untuk mengoperasikan sistem, memasukkan data, dan menggunakan konten [3]. Meski demikian, banyak terjadi serangan *siber* pada antarmuka pengguna. Ancaman ini meliputi *SQL injection*, *cross-site scripting (XSS)*, dan *cross-site request forgery (CSRF)*, dll yang dapat merusak integritas dan kerahasiaan data. Praktik untuk keamanan antarmuka pengguna bisa ditangani dengan sanitasi input, validasi input [4].

Banyak pengembang hanya berfokus pembuatan tampilan dan fungsionalitas antarmuka tanpa mempertimbangkan sisi keamanannya. Sehingga banyak pengembang menambahkan keamanan setelah sistem atau aplikasi web selesai dibangun. Keamanan sebuah website sangatlah penting mengingat begitu banyak data penting dan tersimpan di dalam server website. Oleh karena itu, penting bagi para pengembang website untuk memahami dan menerapkan praktik keamanan pada setiap website yang dikelola [5]

Website yang digunakan untuk mengimplementasikan kode keamanan ini, yang dapat dianggap belum sepenuhnya matang dalam pengelolaan keamanannya, adalah

Akalink. Akalink adalah salah satu web sistem informasi akademik yang menjadi sarana berbagi informasi dan pengelolaan data. Pada aplikasi web akalink sistem ini melibatkan beberapa pengguna yaitu admin, guru. Namun, sebagai aplikasi web masih tahap pengembangan belum menerapkan strategi pengamanan antarmuka.

Dengan latar belakang yang telah dijelaskan, penulis melakukan penelitian ini bertujuan untuk melakukan penerapan strategi pengamanan kode perangkat lunak berbasis web sehingga dapat mengurangi serangan atau ancaman siber.

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah:

1. Bagaimana menerapkan strategi pengamanan kode perangkat lunak berbasis web?
2. Sejauh mana efektivitas penerapan pengamanan kode perangkat lunak dalam meningkatkan keamanan website?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini ialah:

1. Menerapkan strategi pengamanan pada website untuk meminimalkan potensi ancaman sebelum sistem dipublikasikan.
2. Mengidentifikasi jenis ancaman keamanan yang umum terjadi pada perangkat lunak.
3. Sebagai acuan ataupun panduan untuk seorang pengembang.

1.4 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah:

1. Menambah wawasan dan pemahaman tentang pentingnya penerapan strategi pengamanan, guna mencegah celah dalam pengembangan website.
2. Menambah literatur dan referensi bagi peneliti lanjutan
3. Memberikan kontribusi dalam meningkatkan pemahaman dan kesadaran developer pentingnya menjaga keamanan.

1.5 Batasan Penelitian

Terdapat batasan masalah penelitian yaitu:

1. Ruang lingkup pengujian sebagai objek penelitian hanya dilakukan terhadap website akalink, tidak termasuk pada aplikasi mobile (siswa).
2. Penerapan pengamanan hanya difokuskan pada keamanan aplikasi web pada sisi kode, meliputi pengamanan terhadap serangan CSRF token, validasi input, validasi upload file, controlled file storage, blade escaping, enkripsi data, rate limiting, dan content security policy.
3. Pengujian dilakukan sebatas pada simulasi serangan dasar untuk mengetahui efektivitas penerapan pengamanan yang telah diimplementasikan.