BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Ide dan inovasi memiliki peranan yang penting bagi organisasi yang berupaya mempertahankan keunggulan kompetitifnya. Ide merujuk pada proses menghasilkan gagasan baru yang bermanfaat, seperti produk atau solusi baru (Acar et al., 2019). Di sisi lain, inovasi melibatkan penerapan ide-ide tersebut untuk menciptakan manfaat yang nyata. Kedua konsep ini krusial bagi kesuksesan organisasi, karena mereka mendorong kemajuan dan adaptasi terhadap perubahan permintaan pasar serta kemajuan teknologi. Namun, dalam proses berinovasi, pencurian ide menjadi kekhawatiran utama bagi individu dan organisasi yang terlibat (Acar et al., 2019). Pencurian ide terjadi ketika pihak lain mengambil kredit atau menggunakan ide tanpa izin, yang dapat berdampak pada kerugian finansial dan kerusakan reputasi bagi pencipta aslinya.

Terdapat berbagai macam sarana, *platform* dan cara untuk mengelola ide dan inovasi (Acar et al., 2019), seperti aplikasi *website IdeaBox Multi-Tenant*. *IdeaBox Multi-tenant* merupakan sebuah aplikasi website *idea and innovation collaboration,* dimana fitur utama dari aplikasi ini adalah pengguna dapat membuat dan mengunggah ide miliknya, melihat, melakukan komentar, like, dan bergabung pada ide milik orang lain, serta dapat mengelola ide mereka sendiri.

Aplikasi website telah menjadi fondasi bagi banyak aspek kehidupan kita (Hassan et al., 2023). Mereka menyediakan berbagai layanan mulai dari komunikasi, transaksi bisnis secara online, hingga layanan sarana untuk berinovasi (Surentu et al., 2020). Namun, dengan meningkatnya peran aplikasi website, juga muncul ancaman serius terhadap keamanan data yang disimpan dan diproses dalam platform ini (Tania et al., 2018). Aplikasi website sudah seharusnya memiliki keamanan dari serangan *hacker* atau serangan *cyber,* karena aplikasi website tersebut pasti memiliki banyak data penting penggunanya yang disimpan dalam sebuah database (Risky & Yuhandri, 2021), seperti data pribadi pengguna, data

transaksi, data akun, dan lain-lain. Oleh karena itu, pengujian keamanan menjadi sangat krusial untuk mengidentifikasi dan menutup potensi celah keamanan (Fata, 2023) sehingga dapat mencegah risiko serangan *cyber* seperti terjadinya kebocoran data yang berdampak merugikan bagi pengguna.

Serangan *cyber* yang bertujuan untuk mencuri data pribadi, merusak integritas data, atau mengekspos kerentanan dalam aplikasi web semakin umum terjadi (Rusdan, 2019), risiko serangan *cyber* merupakan suatu risiko operasional terhadap aset informasi dan teknologi yang mampu memengaruhi kerahasiaan, ketersediaan dan integritas dari sistem informasi (Febriyanti et al., 2023).

Serangan cyber juga sangat penting untuk diperhatikan dalam konteks perlindungan data sensitif dan penganggulangan serangan *cyber* yang terus berkembang (Permana & Nurnaningsih, 2018). Dalam era digital yang semakin terhubung, menjaga kerahasiaan data pengguna seperti data pribadi dan data inovasi dalam aplikasi seperti "*IdeaBox Multi-Tenant"* menjadi krusial, mengingat potensi dampak serius yang dapat ditimbulkan oleh pelanggaran keamanan data yang kemungkinan besar akan merugikan dan membahayakan pemilik data.

Menurut Hardianto dan Sutabri (2023), berdasarkan survey Acunetix tahun 2021, serangan *cyber* terhadap aplikasi website menunjukkan peningkatan setiap tahunnya, baik jumlah maupun skala serangannya. Dalam survei tersebut, mencatat bahwa sekitar 21% aplikasi web mempunyai resiko yang sangat tinggi terhadap serangan Cross-Site Scripting (XSS) dan SQLinjections. Bahkan lebih dari 63% aplikasi web mempunyai kerentanan tingkat menengah terhadap serangan Cross-Site Request Forgery (CSRF).

Sebagai aplikasi *website*, *IdeaBox Multi-tenant* memiliki potensi serangan siber seperti XSS, SQL *Injection* dan CSRF jika tidak dilakukan langkah-langkah pencegahan dan fitur keamanan yang memadai. Oleh karena itu, keamanan aplikasi *website* menjadi sangat penting, terutama dalam konteks aplikasi kolaborasi inovasi seperti *IdeaBox Multi-Tenant*. Dalam lingkungan di mana ide dan informasi berharga dipertukarkan, menjaga keamanan data akan menjadi prioritas utama.

Dalam rangka meningkatkan keamanan aplikasi website, teknologi untuk mengembangkan aplikasi website semakin berkembang, pengembangan di sisi *front-end* atau bagian yang ditampilkan ke pengguna memainkan peran penting dalam pengembangan aplikasi website, karena itu merupakan apa yang ditampilkan dan digunakan langsung oleh pengguna (Lazuardy & Anggiani, 2022). Salah satu framework pengembangan web yang populer saat ini adalah Next.js (Lazuardy & Dyah Anggiani, 2022). Next.js adalah framework React yang kuat yang memungkinkan pengembangan aplikasi web yang responsif, cepat, dan aman. Dengan memanfaatkan fitur-fitur keamanan Next.js, seperti *server-side rendering* (SSR), routing yang dinamis dan *middleware* (Dinku, 2022), pengembang dapat membangun aplikasi web yang memiliki keamanan yang baik.

Untuk menguji tingkat keamanan dari sebuah website, diperlukan pendekatan yang terstruktur dan terpercaya. Menurut Abdan (2022), Salah satu pendekatan yang terkenal dan banyak digunakan dalam pengujian keamanan aplikasi web adalah melalui pendekatan yang disusun oleh OWASP (Open Web Application Security Project). OWASP adalah sebuah komunitas global yang berfokus pada peningkatan keamanan aplikasi web melalui pengembangan panduan, alat, dan sumber daya yang ditujukan untuk membantu organisasi dan pengembang dalam mengatasi kerentanan keamanan yang umum ditemui dalam aplikasi web.

Salah satu kerangka kerja dari OWASP adalah daftar "*Top 10 OWASP*" yang merupakan kerangka kerja yang paling aktif dan secara rutin diperbarui untuk terus memberikan pedoman mengenai ancaman terkini dalam dunia siber (Abdan, 2022). Top 10 OWASP menjadi referensi utama bagi profesional keamanan siber dan pengembang perangkat lunak yang bertanggung jawab dalam dunia serangan siber dalam mengidentifikasi dan memahami kerentanan keamanan yang paling umum dalam aplikasi website.

Berdasarkan pemaparan masalah tersebut, maka penelitian ini dimaksudkan untuk mengukur dan menguji tingkat keamanan aplikasi website menggunakan 10 standarisasi keamanan website yang dikenal dengan "*Top 10 OWASP"* atau *Open Web Application Security Project*" sebelum dan sesudah menerapkan fitur Next.js

pada aplikasi *website IdeaBox Multi-Tenant*. Harapannya, penelitian ini dapat memberikan pemahaman yang lebih mendalam mengenai pengaruh fitur Next.js terhadap keamanan aplikasi website, serta mengidentifikasi perubahan dalam tingkat keamanan sebelum dan sesudah implementasi fitur Next.js.

1.2 Rumusan Masalah Penelitian

Berdasarkan penjelasan yang dipaparkan pada latar belakang, maka rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana penerapan Next.js pada *website IdeaBox Multi-tenant*.
2. Bagaimana tingkat keamanan *website IdeaBox Multi-tenant* sebelum dan sesudah menerapkan fitur keamanan *Next.js* serta pengaruhnya terhadap keamanan *website* yang diuji menggunakan metode pengujian *Top 10 OWASP*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Penerapan Next.js pada *website IdeaBox Multi-tenant*.
2. Menguji dan menganalisis tingkat keamanan *website IdeaBox Multi-tenant* sebelum dan sesudah menerapkan fitur *Next.js* serta pengaruhnya terhadap keamanan *website* menggunakan metode pengujian *Top 10 OWASP*.

1.4 Manfaat Penelitian

Adapun manfaat yang diharapkan dari dilakukannya penelitian ini adalah sebagai berikut.

1. Dengan mengadopsi fitur *Next.js,* dapat membantu meningkatkan tingkat keamanan aplikasi website dengan mengidentifikasi dan mengatasi kerentanan keamanan yang mungkin mengancam data pengguna.
2. Mengurangi risiko terjadinya serangan siber yang mengancam keamanan aplikasi website dengan menerapkan fitur *Next.js* dan menguji tingkat keamanannya.
3. Memberikan gambaran tingkat keamanan sebuah website dengan menerapkannya fitur *Next.js*.

4. Memberikan gambaran hasil evaluasi dari penerapan fitur *Next.js* dalam menjaga keamanan aplikasi website.
5. Memberikan kontribusi pada peningkatan kesadaran dan praktik keamanan di industri pengembangan aplikasi web secara keseluruhan.

1.5 Batasan Masalah

Adapun batasan masalah yang ada pada penelitian ini adalah sebagai berikut.

1. Menggunakan metode *Top 10 OWASP 2021* dari *Open Web Application Security Project* (OWASP) sebagai pendekatan pengujian keamanan website.
2. Fitur yang terkait dengan konteks keamanan dari *Next.js* yang akan diimplementasikan terdiri dari *Next.js Server-Side Rendering, Next.js Middleware, Formik, Yup Validation*, *Nookies* dan *bcrypt.*
3. *Metrics* yang digunakan dalam menghitung skor *Common Vulnerability Scoring System* berfokus pada *Base Metrics.*

1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini terdiri dari:

BAB I PENDAHULUAN

Bab ini merangkum pandangan keseluruhan penelitian yang akan dijalankan, mencakup gambaran latar belakang penelitian, perumusan masalah penelitian, tujuan penelitian, manfaat penelitian, batasan penelitian, serta struktur penulisan yang akan diikuti.

BAB II KAJIAN PUSTAKA

Bab ini berisi penjelasan tentang berbagai teori yang relevan dengan subjek yang sedang diteliti, serta informasi dan kemajuan penelitian terdahulu yang memiliki relevansi dengan studi yang sedang dilakukan oleh penulis. Bagian ini juga mencakup kerangka acuan berdasarkan hasil penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Bab ini membahas mengenai metode dan langkah-langkah yang akan digunakan untuk menyelesaikan masalah penelitian. Beberapa komponen yang

akan dijelaskan mencakup desain penelitian yang akan diterapkan, alat dan bahan penelitian, instrumen penelitian, hipotesis, proses analisis data, dan model dampaknya.

BAB IV TEMUAN DAN PEMBAHASAN

Bab ini memaparkan hasil dan analisis penelitian sesuai dengan tujuan dan masalah penelitian. Bagian ini mencakup penjelasan tentang desain arsitektur dari *Next.js*, proses implementasi fitur *Next.js* sesuai studi kasus, pengujian tingkat keamanan kerahasiaan data, evaluasi pengujian yang telah dilakukan, serta pembahasan dari hasil analisis pengujian keamanan kerahasiaan data dan evaluasi hasil pengujian keamanan kerahasiaan data.

BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Bab ini berisi kesimpulan dari hasil penelitian yang didasarkan pada rumusan masalah, implikasi penelitian ini, dan saran untuk penelitian selanjutnya.