BAB V
SIMPULAN, IMPLIKASI DAN REKOMENDASI

5.1 Simpulan

Pada pembahasan ini, peneliti memaparkan simpulan dari rumusan masalah yang telah ditentukan sebelumnya. Berikut simpulan yang telah dilaksanakan.

1. Penerapan Next.js pada aplikasi *website IdeaBox* mencakup beberapa fitur yang terkait dengan konteks keamanan, mencakup *Next.js Server-Side Rendering, Next.js Middleware, Formik, Yup Validation*, *Nookies* dan *bcrypt*. *Next.js Server-Side Rendering* mampu merubah konsep penarikan data pada *IdeaBox Multi-tenant* sehingga penarikan data pada aplikasi lebih aman, *Next.js Middleware* mampu menjaga *route* atau halaman yang dapat diakses hanya oleh pengguna yang sah, *Formik* dan *Yup Validation* mampu memvalidasi dan mensanitasi semua *input* yang dikirimkan oleh pengguna, *Nookies* mampu menyimpan dan menjaga data pengguna dengan baik, *bcrypt* mampu mengenkripsi kata sandi yang dikirim oleh pengguna. Fitur-fitur tersebut berhasil diimplementasikan dengan baik pada beberapa fungsi dan komponen *website IdeaBox Multi-tenant*, terbukti dengan dapat meningkatkan keamanan *website Ideabox Multi-tenant*.
2. Dengan implementasi fitur keamanan Next.js pada aplikasi website IdeaBox Multi-tenant, terdapat perubahan yang signifikan dalam tingkat keamanan sistem. Pengujian menggunakan metode Top 10 OWASP menunjukkan bahwa setelah penerapan fitur keamanan Next.js, kerentanan yang sebelumnya terdapat pada aplikasi berhasil diperbaiki dengan baik. Pada pengujian sebelum mengimplementasi fitur Next.js, *website IdeaBox Multi-tenant* memiliki total 12 kategori celah keamanan, 6 kategori kerentanan pada aspek *Broken Access Control* dengan tingkat kemungkinan terjadi kerentanan dan resiko yang ditimbulkan tinggi, 3 kategori kerentanan pada aspek *Cryptographic Failures* dengan tingkat kemungkinan terjadi kerentanan dan resiko yang ditimbulkan sedang, 6 kategori kerentanan pada aspek *Security Misconfiguration* dengan tingkat kemungkinan terjadi kerentanan yang tinggi dan tingkat resiko yang

ditimbulkan kritis, serta 1 kategori kerentanan pada aspek *Identification and Authentication Failures* dengan tingkat kemungkinan terjadi kerentanan dan resiko yang ditimbulkan sedang. Sedangkan setelah menerapkan fitur Next.js, *website IdeaBox Multi-tenant* memiliki total 7 kategori celah keamanan, 2 kategori kerentanan pada aspek *Broken Access Control* dengan tingkat kemungkinan terjadi kerentanan yang rendah dan tingkat resiko yang ditimbulkan sedang, 2 kategori kerentanan pada aspek *Cryptographic Failures* dengan tingkat kemungkinan terjadi kerentanan dan resiko yang ditimbulkan sedang, serta 3 kategori kerentanan pada aspek *Security Misconfiguration* dengan tingkat kemungkinan terjadi kerentanan dan resiko yang ditimbulkan sedang. Hal ini menandakan bahwa implementasi fitur keamanan Next.js memberikan dampak positif dalam meningkatkan keamanan aplikasi website *IdeaBox Multi-tenant*.

5.2 Implikasi

Dengan menggunakan pengujian metode *Top 10 OWASP*, implementasi fitur Next.js terbukti dapat meningkatkan keamanan aplikasi *website IdeaBox Multi-tenant*. Dari hasil pengujian serta perbandingan hasil pengujian yang telah dilakukan, dapat dilihat bahwa pengaruh implementasi fitur Next.js terhadap aplikasi *website IdeaBox Multi-tenant* menunjukan hasil yang positif dengan dapat menurunkannya tingkat kemungkinan terjadi dan resiko dampak yang dihasilkan terhadap beberapa kerentanan yang ditemukan. Penggunaan *Standard Risk Model* dan CVSS untuk mengukur tingkat kemungkinan terjadi kerentanan dan tingkat resiko yang dapat ditimbulkan dari masing-masing kerentanan, dapat menunjukan hasil yang membantu dalam mengidentifikasi tingkat kemungkinan terjadi dan resiko yang ditimbulkan. Fitur Next.js yang di implementasikan seperti Next.js *Server-side Rendering*, Next.js *Middleware*, *Nookies* dan *bcrypt* terbukti dapat memperbaiki kerentanan yang ditemukan pada kategori *Broken Access Control, Security Misconfiguration* dan *Identification and Authentication Failures*, sementara fitur *Formik* dan *Yup* dapat memperbaiki kerentanan *Cryptographic*

Failures dengan cara mengvalidasi dan mensanitasi semua *input* dan transaksi data yang dilakukan.

5.3 Rekomendasi

Setelah mengimplementasi fitur Next.js, masih terdapat kerentanan yang terdeteksi dalam aplikasi website IdeaBox Multi-tenant, meskipun dalam tingkat kemungkinan terjadi dan resiko yang lebih rendah dibandingkan sebelumnya. Hal ini menunjukkan bahwa meskipun fitur Next.js telah memberikan kontribusi positif dalam meningkatkan keamanan aplikasi *website*, namun masih diperlukan langkah-langkah tambahan untuk memperbaiki dan memperkuat pertahanan sistem secara keseluruhan. Dengan demikian, penting untuk terus melakukan pemantauan dan evaluasi secara berkala terhadap kerentanan yang terdeteksi serta melakukan tindakan perbaikan yang sesuai guna meminimalisir risiko keamanan yang mungkin timbul.

1. *Broken Access Control*

   Pastikan server *website*, server aplikasi maupun *load balancer* terkonfigurasi dengan baik untuk menyembunyikan header "X-Powered-By". Selain itu, hapus semua komentar yang memberikan informasi yang dapat membantu penyerang dan memperbaiki masalah mendasar yang mereka rujuk.

2. *Cryptographic Failures*

   Pastikan server *website*, server aplikasi maupun *load balancer* terkonfigurasi dengan baik untuk menyembunyikan header "X-Powered-By". Selain itu, hapus semua komentar yang memberikan informasi yang dapat membantu penyerang dan memperbaiki masalah mendasar yang mereka rujuk.

3. *Security Misconfiguration*

   Browser *website* yang modern, dapat mendukung *header HTTP Content-Security-Policy* dan *X-Frame-Options*, Pastikan untuk salah satunya disetel di semua halaman *website* yang ditampilkan pada halaman *website.* Selain itu, pertimbangkan untuk menerapkan arahan *Content Security Policy's* "*frame-ancestors*".