ANALISIS PENGARUH NEXT.JS UNTUK MENINGKATKAN KEAMANAN *WEBSITE* MENGGUNAKAN METODE PENGUJIAN *TOP 10 OWASP*.

STUDI KASUS: IDEABOX MULTI-TENANT

SKRIPSI

Diajukan untuk memenuhi sebagian dari syarat untuk memperoleh gelar Sarjana Komputer pada Program Studi Rekayasa Perangkat Lunak

oleh

Reihan Manzis Syahputra

2008580

PROGRAM STUDI REKAYASA PERANGKAT LUNAK

KAMPUS UPI DI CIBIRU

UNIVERSITAS PENDIDIKAN INDONESIA

2024

ANALISIS PENGARUH NEXT.JS UNTUK MENINGKATKAN KEAMANAN *WEBSITE* MENGGUNAKAN METODE PENGUJIAN *TOP 10 OWASP*. STUDI KASUS: IDEABOX MULTI-TENANT

Oleh

Reihan Manzis Syahputra

2008580

Diajukan untuk Memenuhi Sebagian Syarat Memperoleh Gelar Sarjana Komputer
pada Program Studi Rekayasa Perangkat Lunak

Universitas Pendidikan Indonesia April 2024

LEMBAR PENGESAHAN SKRIPSI

REIHAN MANZIS SYAHPUTRA

2008580

ANALISIS PENGARUH NEXT.JS UNTUK MENINGKATKAN KEAMANAN *WEBSITE* MENGGUNAKAN METODE PENGUJIAN *TOP 10 OWASP*. STUDI KASUS: IDEABOX MULTI-TENANT

Disetujui dan disahkan oleh Pembimbing

Pembimbing 1

Raditya Muhammad, M.T.

NIP 920190219920507101

Pembimbing 2

M. Iqbal Ardimansyah, S.T., M.Kom.

NIP 920190219910328101

Mengetahui,

Ketua Program Studi S-1 RPL.

M. Iqbal Ardimansyah, S.T., M.Kom.

NIP 920190219910328101

ABSTRAK

ANALISIS PENGARUH NEXT.JS UNTUK MENINGKATKAN KEAMANAN *WEBSITE* MENGGUNAKAN METODE PENGUJIAN *TOP 10 OWASP*. STUDI KASUS: IDEABOX MULTI-TENANT

Reihan Manzis Syahputra

2008580

Latarbelakang penelitian ini berasal dari pentingnya sebuah ide dan inovasi bagi suatu organisasi dalam mempertahankan keunggulannya dalam berkompetisi, sehingga menjadikan ide dan inovasi penting untuk dilindungi karena dampak yang dapat ditimbulkan dari pencurian ide dan inovasi tersebut. Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan aplikasi *website IdeaBox Multi-tenant* dan menganalisis pengaruh dari implementasi fitur Next.js untuk meningkatkan keamanan *website IdeaBox Multi-tenant*. Pengujian pada penelitian ini menggunakan pengujian metode *top 10 owasp* yang mencakup serangkaian pengujian untuk mengidentifikasi kerentanan keamanan yang ada dalam aplikasi *website IdeaBox Multi-tenant* menggunakan aplikasi *Zed Attack Proxy* dengan metode penyerangan *ajax spider* dan *active scan*. Hasil penelitian menunjukan bahwa sebelum mengimplementasi fitur Next.js, *website IdeaBox Multi-tenant* memiliki total 12 kategori celah keamanan, 6 kategori kerentanan pada aspek *Broken Access Control*, 3 kategori kerentanan pada aspek *Cryptographic Failures*, 6 kategori kerentanan pada aspek *Security Misconfiguration* dan 1 kategori kerentanan pada aspek *Identification and Authentication Failures.* Sedangkan setelah menerapkan fitur Next.js, *website IdeaBox Multi-tenant* memiliki total 7 kategori celah keamanan, 2 kategori kerentanan pada aspek *Broken Access Control*, 2 kategori kerentanan pada aspek *Cryptographic Failures* dan 3 kategori kerentanan pada aspek *Security Misconfiguration*. Berdasarkan hasil pengujian, pengaruh dari implementasi Next.js menunjukan hasil yang positif dengan dapat meningkatkan keamanan *website*, serta menurunkan resiko yang dapat ditimbulkan terhadap kerentanan yang ditemukan.

Kata Kunci : Keamanan Website, Next.js, Pengujian OWASP, Zed Attack Proxy, Top 10 OWASP.

ABSTRACT

ANALYSIS OF THE INFLUENCE OF NEXT.JS TO ENHANCE WEBSITE SECURITY USING THE TOP 10 OWASP TESTING METHOD. CASE STUDY: IDEABOX MULTI-TENANT

Reihan Manzis Syahputra

2008580

The background of this research stems from the importance of ideas and innovation for an organization to maintain its competitive edge, making ideas and innovation crucial to protect due to the potential impacts of their theft. This study aims to evaluate the security level of the IdeaBox Multi-tenant website application and analyze the influence of implementing Next.js features to enhance the security of the IdeaBox Multi-tenant website. The research testing employs the top 10 OWASP testing method, which includes a series of tests to identify security vulnerabilities existing in the IdeaBox Multi-tenant website application using the Zed Attack Proxy application with AJAX spider and active scan methods. The research findings indicate that before implementing Next.js features, the IdeaBox Multi-tenant website had a total of 12 categories of security vulnerabilities, including 6 categories of vulnerabilities in Broken Access Control aspects, 3 categories of vulnerabilities in Cryptographic Failures aspects, 6 categories of vulnerabilities in Security Misconfiguration aspects, and 1 category of vulnerability in Identification and Authentication Failures aspect. Whereas after implementing Next.js features, the IdeaBox Multi-tenant website had a total of 7 categories of security vulnerabilities, including 2 categories of vulnerabilities in Broken Access Control aspects, 2 categories of vulnerabilities in Cryptographic Failures aspects, and 3 categories of vulnerabilities in Security Misconfiguration aspects. The influence of implementing Next.js features shows positive results by enhancing website security and reducing the impact risks associated with identified vulnerabilities.

***Keywords* : *Website Security, Next.js, OWASP Testing, Zed Attack Proxy, Top 10 OWASP*.**

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

Abdan, M. K. (2022). *Pengujian Keamanan Sistem Informasi Berbasis Web Berdasarkan Framework OWASP WSTG v4.2 (Studi Kasus: Sistem Sekawan v1 Universitas Islam Indonesia*. Universitas Islam Indonesia.

Aurelia, A., Wasino, W., Chandra, D., and Jap, T. B. (2023). Developing Website-based information system applications to map PT. XYZ's properties using Next.JS framework with haversine method. *International Journal of Application on Sciences, Technology and Engineering (IJASTE)*, *1*(1), 59–64.

Blessing, L., Chakrabarti, A., and Wallace, K. M. (1998). An overview of descriptive studies in relation to a general design research methodology. In E. Frankenberger, H. Birkhofer, and P. Badke-Schaub (Eds.), *Designer*. Springer.

Budi, E., Wira, D., dan Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234.

Chai, K. Y., and Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT In Education (JICTIE)*, *8*(2), 34–42.

Dermawan, I., Baidawi, A., Iksan, I., dan Dewi, S. M. (2023). Serangan cyber dan kesiapan keamanan cyber terhadap Bank Indonesia. *Jurnal Informasi Dan Teknologi*, *5*(3), 20–25.

Dinku, Z. (2022). *React.js vs. Next.js* [Bachelor's Thesis]. Metropolia University of Applied Sciences.

Fata, D. (2023). *Evaluasi risiko celah keamanan menggunakan metodologi open web application security project (OWASP) pada aplikasi web sistem informasi akademik (SIAKAD) UIN Ar-Raniry*. Universitas Islam Negeri Ar-Raniry .

Febriana, R. (2022). Blackbox testing sistem informasi absensi pegawai karawang dengan metode Top 10 Owasp Attack. *Jurnal Ilmiah Wahana Pendidikan*, *8*(12), 327–334.

Febryanti, P. C., Subartini, B., dan Riaman, R. (2023). Perhitungan tingkat risiko cyber pada layanan keuangan digital berdasarkan biaya kerugian agrerat. *FIBONACCI: Jurnal Pendidikan Matematika Dan Matematika*, *9*(1), 95–104.

Ghelani, D. (2022). Cyber security, cyber threats, implication and future perspectives: A review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19.

Hardianto, H., and Sutabri, T. (2023). Analisis cyber crime handling pada aplikasi web dengan WAF ModSecurity. *PETIR: Jurnal Pengkajian Dan Penerapan Teknik Informatika*, *16*(1), 91–99.

Hariyadi, D., dan Nastiti, F. E. (2021). Analisis keamanan sistem informasi menggunakan sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *Jurnal Komtika (Komputasi Dan Informatika)*, *5*(1), 35–42.

Hassan, A. A., Rony, M. A., Yuliazmi, dan Putra, B. C. (2023). Implementasi e-commerce menggunakan content management system (CMS) pada toko Linda Collection. *2nd Seminar Nasional Mahasiswa Fakultas Teknologi (SENAFTI)*, *2*(1), 659–667.

Jartarghar, H. A., Salanke, G. R., A.R, A. K., G.S, S., and Dalali, S. (2022). React Apps with server-side rendering: Next.js. *Journal of Telecommunication, Electronic and Computer Engineering*, *14*(4), 25–29.

Lazuardy, M. F. S., and Anggraini, D. (2022). Modern front end web architectures with React.Js and Next.Js. *International Research Journal of Advanced Engineering and Science*, *7*(1), 132–141.

Nafi'ah, R. (2020). Pelanggaran data dan pencurian pada e-commerce. *Cyber Security Dan Forensik Digital*, *3*(1), 7–13.

Nguyen, A. (2022). *Building an e-commerce website using Next.js, Mantine, and Strapi*. Centria University of Applied Science.

Nurnaningsih, D., dan Permana, A. A. (2018). Rancangan aplikasi pengamanan data dengan algortima advanced encyption standard (AES). *JURNAL TEKNIK INFORMATIKA*, *11*(2), 177–186.

Purba, P. M., Amandha, A. C., Purnama, R. H., dan Ikhwan, A. (2022). Analisis keamanan website prodi sistem informasi UINSU menggunakan metode application scanning. *JINTEKS (Jurnal Informatika Teknologi Dan Sains)*, *4*(4), 325–329.

Risky, M. A. Z., dan Yuhandri, Y. (2021). Optimalisasi dalam penetrasi testing keamanan website menggunakan teknik SQL Injection dan XSS. *Jurnal Sistim Informasi Dan Teknologi*, *3*(4), 215–220.

Rochman, A., Salam, R. R., dan Maulana, S. A. (2021). Analisis keamanan website dengan information system security framework (ISSAF) dan open web application security project (OWASP) di Rumah Sakit XYZ. *Jurnal Indonesia Sosial Teknologi*, *2*(4), 506–619.

Rosaliah, Y. T. A., Jayanta, J., dan Hananto, B. (2021). Pengujian celah keamanan website menggunakan teknik Penetration Testing dan metode OWASP TOP 10 pada website SIM xxx. *Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA) Jakarta-Indonesia*, 752–761.

Rusdan, M. (2019). Pengembangan keamanan cyber pada cloud computing untuk usaha kecil dan menengah. *JITTER: Jurnal Ilmiah Teknologi Informasi Terapan*, *5*(3), 22–29.

Samonas, S., and Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *JISSec: Journal of Information System Security*, *10*(3), 21–45.

Susanto, F. G. P., Fadlan, N. I. Y., and Haryani, P. (2023). Design of Web-Based management information system for student organizations in Kendal Regency using Next.js framework. *Compiler*, *12*(1), 9.

Tania, A. M., Setiyadi, D., dan Khasanah, F. N. (2018). Keamanan website menggunakan vulnerability assessment. *INFORMATICS FOR EDUCATORS AND PROFESSIONALS*, *2*(2), 171–180.

Tonge, A. M., Kasture, S. S., and Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of Computer Engineering (IOSR0JCE)*, *12*(2), 67–75.

Willberg, M. (2019). *Web application security testing with OWASP TOP 10 framework* [BACHELOR'S THESIS]. Turku University Of Applied Science.

Yudiana, Elanda, A., dan Lintang Buana, R. (2021). Analisis kualitas kemanan sistem informasi e-office berbasis website pada STMIK ROSMA dengan menggunakan OWASP TOP 10. *CESS (Journal of Computer Engineering System and Science)*, *6*(2), 2502–2714.

Yuniarti, D. R., Alfarizy, H. F., Siallagan, Z., dan Rizkyanfi, M. W. (2023). Analisis potensi dan strategi pencegahan cyber crim dalam sistem logistik di era digital. *Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN)*, *3*(1), 23–32.

Mell, P., Scarfone, K., and Romanosky, S. (2006). Common Vulnerability Scoring System. IEEE Security & Privacy, 4(6), 85-89.

Abdulghaffar, K., Elmrabit, N., and Yousefi, M. (2023). Enhancing web application security through automated penetration testing with multiple vulnerability scanners. Computers, 12(11).

Kalaani, C. (2023). OWASP ZAP vs snort for SQLi vulnerability scanning [Georgia Southern University].

Nisa, K., Putra, A. M., Siregar, R. A., dan Irawan, M. D. (2022). Analisis website Tapanuli Tengah menggunakan metode open web application security project zap (Owasp Zap). Bulletin of Information Technology (BIT), 3(4), 308–316.

Priyawati, D., Rokhmah, S., and Utomo, I. C. (2022). Website vulnerability testing and analysis of internet management information system using OWASP. International Journal of Computer and Information System (IJCIS) , 03(03), 2745–9659.

Yudiana, Y., Elanda, A., dan Buana, R. L. (2021). Analisis kualitas keamanan sistem informasi e-office berbasis website pada STMIK Rosma dengan menggunakan OWASP TOP 10. Journal of Computer Engineering Syctem Science (CESS), 6(2), 2502–2714.