ANALISIS KERENTANAN APLIKASI WEBSITE MENGGUNAKAN PENDEKATAN OWASP TOP 10 DAN GAP ANALYSIS ISO 27001:2022 PADA PT BUMI SUKSESINDO

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

WILLY AGUSTIANUS

22.83.0882

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

ANALISIS KERENTANAN APLIKASI WEBISTE MENGGUNAKAN PENDEKATAN OWASP TOP 10 DAN GAP ANALYSIS ISO 27001:2022 PADA PT BUMI SUSKESINDO

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

WILLY AGUSTIANUS

22.83.0882

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KERENTANAN APLIKASI WEBSITE MENGGUNAKAN PENDEKATAN OWASP TOP 10 DAN GAP ANALYSIS ISO 27001:2022 PADA PT BUMI SUKSESINDO

yang disusun dan diajukan oleh

WILLY AGUSTIANUS

22.83.0882

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 Mei 2026

Dosen Pembimbing,

Senie Destya, S.T., M.Kom.
NIK. 190302312

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KERENTANAN APLIKASI WEBSITE MENGGUNAKAN PENDEKATAN OWASP TOP 10 DAN GAP ANALYSIS ISO 27001:2022 PADA PT BUMI SUKSESINDO

yang disusun dan diajukan oleh

WILLY AGUSTIANUS

22.83.0882

Telah dipertahankan di depan Dewan Penguji
pada tanggal 25 Mei 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Eko Pramono, S.Si, M.T. **NIK. 190302580**	
Muhammad Koprawi, S.Kom., M.Eng. **NIK. 190302454**	
Senie Destya, S.T., M.Kom. **NIK. 190302312**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 25 Mei 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : WILLY AGUSTIANUS
NIM : 22.83.0882

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Kerentanan Aplikasi Website Menggunakan Pendekatan OWASP Top 10 dan Gap Analysis ISO 27001:2022 pada PT Bumi Suksesindo

Dosen Pembimbing : **Senie Destya, S.T., M.Kom.**

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 25 Mei 2026

Yang Menyatakan,

WILLY AGUSTIANUS

HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa atas segala rahmat, penyertaan, dan kasih-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi ini penulis persembahkan kepada kedua orang tua dan keluarga tercinta yang selalu memberikan doa, dukungan, semangat, serta motivasi kepada penulis selama menjalani proses perkuliahan hingga penyusunan skripsi ini.

Penulis juga mempersembahkan skripsi ini kepada dosen pembimbing, dosen penguji, pihak PT Bumi Suksesindo, sahabat, serta seluruh pihak yang telah memberikan bantuan, pengalaman, dan dukungan selama proses penelitian berlangsung. Semoga skripsi ini dapat memberikan manfaat dan menjadi hasil yang membanggakan bagi semua pihak yang telah mendukung penulis.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul "Analisis Kerentanan Aplikasi Website Menggunakan Pendekatan OWASP Top 10 dan Gap Analysis ISO 27001:2022 pada PT Bumi Suksesindo" dengan baik.

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Teknik Komputer, UNIVERSITAS AMIKOM YOGYAKARTA. Dalam proses penyusunan skripsi ini, penulis memperoleh bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada dosen pembimbing, seluruh dosen UNIVERSITAS AMIKOM YOGYAKARTA, pihak PT Bumi Suksesindo, kedua orang tua, keluarga, serta teman-teman yang telah memberikan dukungan dan bantuan kepada penulis.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi penyempurnaan penelitian ini. Semoga skripsi ini dapat memberikan manfaat bagi pembaca dan pihak yang membutuhkan.

Yogyakarta, 7 Mei 2026

WILLY AGUSTIANUS

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

API	Application Programming Interface
BSSN	Badan Siber dan Sandi Negara
CIA	Confidentiality, Integrity, Availability
CPU	Central Processing Unit
CSP	Content Security Policy
CSRF	Cross-Site Request Forgery
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DLP	Data Lekage Prevention
DRP	Disaster Recovery Plan
GB	Gigabyte
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information Communication and Technology
IEC	International Electrotechnical Commission
IKU	Indikator Kinerja Utama
IoT	Internet of Things
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organization for Standardization
KPI	Key Performance Indicator
MB	Megabyte

MFA	Multi-Factor Authentication
OWASP	Open Web Application Security Project
PTES	Penetration Testing Execution Standard
RAM	Random Access Memory
RKA	Rencana Kerja dan Anggaran
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	Software Development Life Cycle
SMKI	Sistem Manajemen Keamanan Informasi
SOP	Standard Operating Procedure
SQL	Structured Query Language
UI	User Interface
URL	Uniform Resource Locator
VA	Vulnerability Assessment
WAF	Web Application Firewall
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

DAFTAR ISTILAH

- OWASP (Open Web Application Security Project)
  Organisasi terbuka yang berfokus pada peningkatan keamanan aplikasi web melalui standar, dokumentasi, dan pengujian keamanan.
- OWASP Top 10:2021
  Daftar 10 kategori kerentanan keamanan aplikasi web yang paling kritis berdasarkan analisis risiko dan tren serangan terbaru.
- Penetration Testing
  Metode pengujian keamanan sistem dengan mensimulasikan serangan untuk mengidentifikasi kerentanan pada aplikasi atau jaringan.
- Vulnerability Assessment
  Proses identifikasi, analisis, dan evaluasi terhadap kelemahan keamanan pada suatu sistem informasi.
- Kerentanan (Vulnerability)
  Kelemahan pada sistem, aplikasi, atau konfigurasi yang dapat dimanfaatkan oleh pihak tidak berwenang.
- Risiko Keamanan Informasi
  Potensi kerugian yang timbul akibat ancaman yang memanfaatkan kerentanan pada aset informasi.
- ISO/IEC 27001:2022
  Standar internasional yang mengatur Sistem Manajemen Keamanan Informasi (SMKI) untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi.
- SMKI (Sistem Manajemen Keamanan Informasi)
  Kerangka kerja yang digunakan organisasi untuk mengelola keamanan informasi secara sistematis dan berkelanjutan.
- CIA Triad
  Konsep dasar keamanan informasi yang terdiri dari Confidentiality, Integrity, dan Availability.
- Confidentiality

Prinsip keamanan informasi yang memastikan data hanya dapat diakses oleh pihak yang berwenang.

- Integrity
  Prinsip keamanan infromasi yang menjamin keakuratan dan keutuhan data.
- Availability
  Prinsip keamanan informasi yang memastikan sistem dan data tersedia saat dibutuhkan.
- CVSS (Common Vulnerability Scoring System)
  Standar penilaian tingkat keparahan kerentanan keamanan berdasarkan skor risiko.
- Admin Page Exposure
  Kondisi ketika halaman administrasi sistem dapat diakses tanpa perlindungan atau pembatasan yang memadai.
- Security Misconfiguration
  Kerentanan yang terjadi akibat kesalahan konfigurasi keamanan pada server, aplikasi, atau layanan.
- Broken Access Control
  Kerentanan yang memungkinkan pengguna mengakses data atau fungsi tanpa otorisasi yang sesuai.
- XSS (Cross-Site Scripting)
  Jenis serangan injeksi yang memungkinkan penyerang menjalankan skirp berbahaya pada browser pengguna.
- SQL Injection
  Teknik Serangan dengan menyisipkan perintah SQL berbahaya untuk mengakses atau memanipulasi database.
- DDoS (Distributed Denial of Service)
  Jenis serangan siber yang bertujuan membanjiri server, jaringan, atau layanan dengan lalu lintas berlebihan sehingga sistem tidak dapat melayani pengguna secara normal
- Clickjacking

Teknik serangan pada aplikasi web dengan memanipulasi tampilan antarmuka sehingga pengguna tanpa sadar melakukan klik pada elemen berbahaya atau tersembunyi.

- Indeks KAMI 5.0
  Instrumen evaluasi tingkat kesiapan keamanan informasi yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN)
- BSSN (Badan Siber dan Sandi Negara)
  Lembaga pemerintah Indonesia yang bertanggung jawab terhadap keamanan siber nasional.
- PSE (Penyelenggara Sistem Elektronik)
  Setiap orang, penyelenggara negara, badan usaha, atau masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik.

INTISARI

Keamanan aplikasi web menjadi aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi perusahaan. PT Bumi Suksesindo menggunakan website company profile dan sistem absensi karyawan yang dapat diakses melalui jaringan internal maupun external sehingga berpotensi mengalami ancaman keamanan siber. Penelitian ini menggunakan metode Penetration Testing dengan pendekatan OWASP Top 10:2021 untuk mengidentifikasi kerentanan aplikasi web. Tingkat risiko dianalisis menggunakan metode CVSS, sedangkan evaluasi keamanan informasi dilakukan menggunakan Gap Analysis berbasis Indeks KAMI 5.0 untuk mengukur kesiapan penerapan ISO/IEC 27001:2022. Selain itu, dilakukan pemetaan antara hasil Penetration Testing dengan kontrol keamanan pada Indeks KAMI 5.0 untuk mengetahui hubungan antara kerentanan teknis dan penerapan kontrol keamanan informasi organisasi.

Hasil penelitian menunjukkan bahwa aplikasi web PT Bumi Suksesindo masih memiliki kerentanan dengan tingkat risiko Medium hingga Critical. Hasil evaluasi Indeks KAMI 5.0 memperoleh skor 711 dengan kategori “Cukup Baik”, namun masih ditemukan beberapa kontrol keamanan yang belum diterapkan secara optimal. Hasil pemetaan menunjukkan bahwa kerentanan yang ditemukan berkaitan dengan kontrol keamanan yang belum diterapkan secara maksimal. Hal ini menunjukkan bahwa meskipun tingkat kesiapan keamanan informasi berada pada kategori “Cukup Baik”, kondisi keamanan aplikasi web belum sepenuhnya aman. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi bahan evaluasi serta acuan bagi perusahaan dalam meningkatkan keamanan informasi secara lebih optimal dan berkelanjutan.

Kata kunci: OWASP Top 10:2021, Penetration Testing, CVSS, Indeks KAMI 5.0, ISO/IEC 27001:2022

ABSTRACT

Web application security is an important aspect in maintaining the confidentiality, integrity, and availability of company information. PT Bumi Suksesindo utilizes a company profile website and a web-based attendance system that can be accessed through internal and external networks, making them vulnerable to cybersecurity threats. This research applied the Penetration Testing method using the OWASP Top 10:2021 approach to identify vulnerabilities in web applications. The vulnerability risk level was analyzed using the Common Vulnerability Scoring System (CVSS) method, while information security readiness was evaluated using Gap Analysis based on the Indeks KAMI 5.0 to measure the readiness for implementing ISO/IEC 27001:2022. In addition, mapping was conducted between the Penetration Testing results and the security controls in Indeks KAMI 5.0 to determine the relationship between technical vulnerabilities and the implementation of organizational information security controls.

The results showed that the web applications of PT Bumi Suksesindo still contained vulnerabilities with risk levels ranging from Medium to Critical. The Indeks KAMI 5.0 evaluation obtained a score of 711 with the category “Fairly Good,” however, several security controls had not been implemented optimally. The mapping results indicated that the identified vulnerabilities were related to security controls that had not been fully implemented. This indicates that although the organization’s information security readiness level was categorized as “Fairly Good,” the condition of the web application security was not yet fully secure. Therefore, the results of this study are expected to serve as evaluation material and a reference for the company in improving information security in a more optimal and sustainable manner.

***Keyword*:** OWASP Top 10:2021, Penetration Testing, CVSS, Indeks KAMI 5.0, ISO/IEC 27001:2022