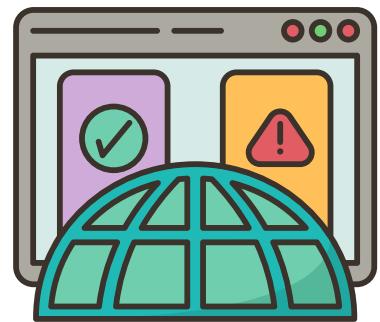




Evaluasi Keamanan Sistem ERP Weskonek dengan PTES Black-Box dan Klasifikasi Kerentanan CWE

Latar Belakang



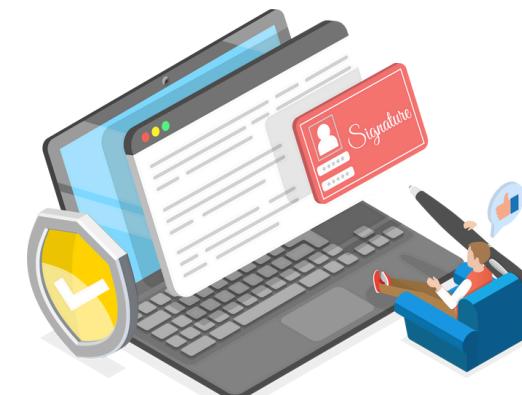
PENTINGNYA KEAMANAN
APLIKASI WEB



SERANGAN KE SISTEM ERP
PERNAH TERJADI



ERP MERUPAKAN SISTEM
INTI BISNIS



BELUM ADA PENELITIAN
KHUSUS TENTANG ERP
WESKONEK

"The information compromised most often according to this research is the highest regulated in today's business ecosystem," Onapsis said. Still, 62 percent of the study's participants said their ERP applications are vulnerable to cyber attacks.

Hacker Attacks Target These ERP Applications, Data

Among the 64 percent of enterprises that have experienced breaches of large ERP platforms in the last 24 months, information compromised includes sales data (50 percent), HR data (45 percent), customer PII (41 percent), intellectual property (36 percent) and financial data (34 percent).

Sumber : <https://www.msspalert.com/news/hackers-target-erp-applications>

Penelitian Sebelumnya

CESS

(Journal of Computing Engineering, System and Science) 8(2) July 2023 518-528

e-ISSN: 2502-714x

p-ISSN: 2502-7131

Contents list available at www.jurnal.unimed.ac.id

CESS
(Journal of Computing Engineering, System and Science)

journal homepage: <https://jurnal.unimed.ac.id/2012/index.php/cess>



**Implementasi Penetration Testing Pada Website Menggunakan Metode
Penetration Testing Execution Standard (PTES)**

**Implementation of Penetration Testing on the Website Using the Penetration
Testing Execution Standard (PTES) Method**

Bagus Kurniawan^{1*}, Ikhwan Ruslianto², Syamsul Bahri³

^{1,2,3} Program Studi Rekayasa Sistem Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Jalan Prof. Dr. H. Hadari Nawawi Pontianak

email: ¹kurniawanbagus55@gmail.com, ²ikhwanruslianto@siskom.untan.ac.id,
³syamsul.bahri@siskom.untan.ac.id

JIRE (Jurnal Informatika & Rekayasa Elektronika)
<http://e-journal.stmiklombok.ac.id/index.php/jire>

Volume 8, No 1, April 2025

PENGUJIAN WEBSITE DINAS SOSIAL SURABAYA MENGGUNAKAN METODE PENETRATION TESTING DAN OWASP TOP 10

Bregas Arya Bagaskara¹, Mohammad Idhom², Henni Endah Wahana^{1,3}

^{1,2,3}Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jawa Timur

Jln. Rungkut Madya, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur 60294

¹bregas909@gmail.com, ²idhom@upnjatim.ac.id, ³henniendah@upnjatim.ac.id

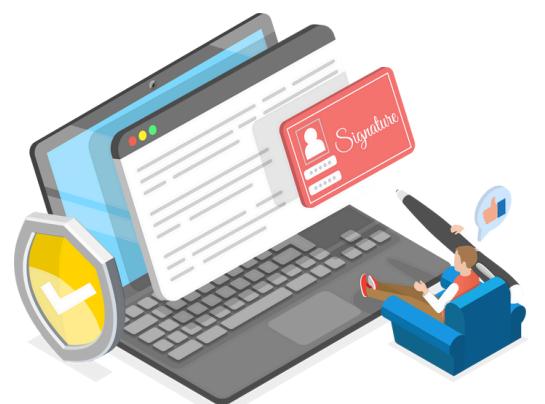
Gap Pada Penelitian



PENDEKATAN YANG
DIGUNAKAN SEBELUMNYA
TERBATAS PADA OWASP TOP 10
ATAU PTES SAJA, TANPA
INTEGRASI ANTARSTANDAR.



BELUM ADA PENELITIAN YANG
MENGGABUNGKAN METODE
PTES DENGAN KLASIFIKASI
CWE UNTUK MENGHASILKAN
EVALUASI KEAMANAN YANG
LEBIH TERSTRUKTUR DAN
TERSTANDAR INTERNASIONAL.



BELUM ADA PENELITIAN
KHUSUS TENTANG ERP
WESKONEK



Rumusan Masalah

- ✓ Bagaimana mengidentifikasi kerentanan keamanan pada sistem ERP Weskonek menggunakan pendekatan PTES Black-Box?
- ✓ Bagaimana mengklasifikasikan hasil temuan kerentanan tersebut berdasarkan standar CWE?

Tujuan Penelitian



Mengevaluasi keamanan ERP Weskonek.

Penelitian ini bertujuan untuk mengetahui sejauh mana sistem ERP PT Tekno Konek Solusi (Weskonek) aman dari potensi serangan siber dengan pendekatan penetration testing.



Mengidentifikasi potensi kerentanan.

Proses pengujian dilakukan untuk menemukan celah-celah keamanan pada aplikasi ERP, baik dari sisi input, autentikasi, maupun konfigurasi sistem.



Mengklasifikasikan kerentanan menggunakan CWE.

Hasil temuan dikelompokkan berdasarkan standar Common Weakness Enumeration (CWE) agar lebih spesifik, detail, dan sesuai standar internasional.



Memberikan rekomendasi perbaikan.

Penelitian ini menyajikan saran mitigasi atau langkah perbaikan terhadap kerentanan yang ditemukan, sehingga dapat meningkatkan keamanan ERP Weskonek.



Batasan Masalah

- ✓ Fokus hanya pada aplikasi web ERP Weskonek.
- ✓ Pengujian menggunakan black-box, tanpa akses source code/server.
- ✓ Metodologi PTES (penetration testing execution standard)
- ✓ Klasifikasi kerentanan CWE (Common Weakness Enumeration)

Metodologi Penelitian

PENETRATION TESTING EXECUTION STANDARD

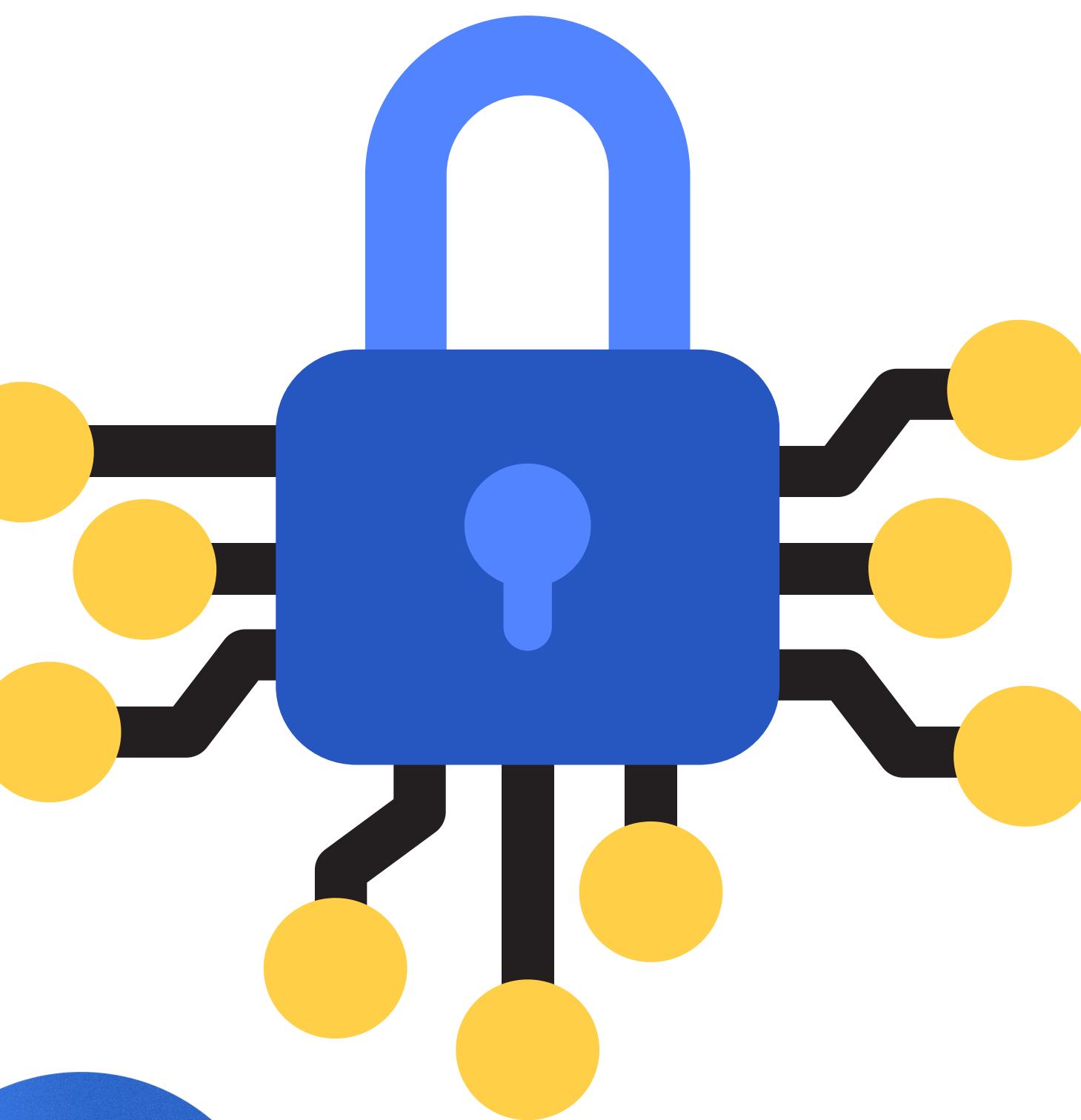
- Pre-engagement : menentukan ruang lingkup dan izin.
- Intelligence Gathering : mengumpulkan informasi target.
- Threat Modeling : memetakan potensi ancaman.
- Vulnerability Analysis : mencari kerentanan.
- Exploitation : mencoba memanfaatkan celah.
- Post-Exploitation : analisis dampak dan eksploitasi
- Reporting : penyusunan laporan hasil pengujian.



Manfaat Penelitian

- Akademis: jadi referensi untuk topik pentest ERP.
- Praktik: rekomendasi perbaikan keamanan untuk ERP Weskonek / PT Tekno Konek Solusi.
- Sosial: meningkatkan awareness keamanan sistem bisnis di Indonesia.





Rencana Hasil / Output

- Daftar kerentanan yang ditemukan.
- Klasifikasi kerentanan berdasarkan CWE.
- Skor risiko
- Rekomendasi mitigasi.

Jurnal Acuan

- PENGUJIAN WEBSITE DINAS SOSIAL SURABAYA MENGGUNAKAN METODE PENETRATION TESTING DAN OWASP TOP 10 | Bregas Arya Bagaskara¹, Mohammad Idhom², Henni Endah Wahanani³
- Analisis Keamanan Website Pada Instansi XYZ Melalui Penetration Testing Menggunakan Framework ISSAF & OWASP | Abdullah¹ , Muhammad Koprawi²
- Implementation of Penetration Testing on the Website Using the Penetration Testing Execution Standard (PTES) Method | Bagus Kurniawan^{1*} , Ikhwan Ruslianto² , Syamsul Bahri³
- Pengujian Keamanan Website XYZ Menggunakan Metode Vulnerability Assessment & Penetration Testing Security Testing of the XYZ Website Using Vulnerability Assessment and Penetration Testing Methods | Ian Vemas Silalahi¹ , Kasmawi²
- Security Testing of XYZ Website Application Using ISSAF and OWASP WSTG v4.2 Methods | Muhammad Firdaus Yusuf^{1*} , Ira Rosianal Hikmah² , Amiruddin³ , Septia Ulfa Sunaringtyas⁴
- Analisis Cela Keamanan Website Poltekkes Kemenkes Sorong Menggunakan Metode Penetration Testing | Gunawan Yudi Jayanto^{1*} Julius Panda Putra Naibaho² Alex De Kweldju³





**Sekian
Terimakasih**