SKRIPSI

PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)

MOCHAMMAD YOGA FIRNANDA
NPM 21081010152

DOSEN PEMBIMBING
Henni Endah Wahanani, S.T., M.Kom.
Achmad Junaidi, S.Kom., M.Kom.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA

2025

SKRIPSI

PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)

MOCHAMMAD YOGA FIRNANDA
NPM 21081010152

DOSEN PEMBIMBING

Henni Endah Wahanani, S.T., M.Kom.

Achmad Junaidi, S.Kom., M.Kom.

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAWA TIMUR
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
SURABAYA

2025

Halaman ini sengaja dikosongkan

LEMBAR PENGESAHAN

PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)

Oleh :
MOCHAMMAD YOGA FIRNANDA
NPM. 21081010152

Telah dipertahankan dihadapan dan diterima oleh Tim Penguji Skripsi Prodi Informatika Fakulktas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jawa Timur pada tanggal 16 Mei 2025

Menyetujui

Henni Endah Wahanani, S.T., M.Kom. NIP. 19780922 2021212 005	.....	(Pembimbing I)
Achmad Junaidi, S.Kom., M.Kom. NIP. 3 7811 04 0199 1	.....	(Pembimbing II)
Yisti Vita Via, S.ST., M.Kom. NIP. 19860425 2021212 001	.....	(Ketua Penguji)
Afina Lina Nurlaili, S.Kom., M.Kom. NIP. 1993121 3202203 2010	.....	(Anggota Penguji)

Mengetahui,
Dekan Fakultas Ilmu Komputer

Prof. Dr. Ir. Novirina Hendrasarie, MT.
19681126 199403 2 001

Halaman ini sengaja dikosongkan

LEMBAR PERSETUJUAN

PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)

Oleh:

MOCHAMMAD YOGA FIRNANDA

NPM. 21081010152

Menyetujui,

Koordinator Program Studi

Fakultas Ilmu Komputer

Fetty Tri Anggraeny, S.Kom., M.Kom.

NIP. 19820211 2021212 005

Halaman ini sengaja dikosongkan

SURAT PERNYATAAN BEBAS PLAGIASI

Yang bertandatangan di bawah ini:

Nama	:	Mochammad Yoga Firnanda
NPM	:	21081010152
Program	:	Sarjana (S1)
Program Studi	:	Informatika
Fakultas	:	Ilmu Komputer

Menyatakan bahwa dalam dokumen ilmiah Tugas Skripsi ini tidak terdapat bagian dari karya ilmiah lain yang telah diajukan untuk memperoleh gelar akademik di suatu lembaga Pendidikan Tinggi, dan juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang/lembaga lain, kecuali yang secara tertulis disitasi dalam dokumen ini dan disebutkan secara lengkap dalam daftar pustaka.

Dan saya menyatakan bahwa dokumen ilmiah ini bebas dari unsur-unsur plagiasi. Apabila dikemudian hari ditemulan indikasi plagiat pada Skripsi, saya bersedia menerima sanksi sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya tanpa ada paksaan dari siapapun juga dan untuk dipergunakan sebagaimana mestinya.

Surabaya, 13 Juni 2025

Yang Membuat Pernyataan,

MOCHAMMAD YOGA FIRNANDA

NPM. 21081010152

Halaman ini sengaja dikosongkan

ABSTRAK

Nama Mahasiswa / NPM	:	Mochammad Yoga Firnanda / 21081010152
Judul Skripsi	:	PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)
Dosen Pembimbing	:	1. Henni Endah Wahanani, S.T., M.Kom. 2. Achmad Junaidi, S.Kom., M.Kom.

Kemajuan teknologi yang pesat membawa banyak manfaat bagi sektor industri, sehingga banyak perusahaan yang bergantung pada teknologi untuk mendukung operasionalnya, namun ketergantungan ini juga membuka peluang bagi *hacker* untuk mengeksploitasi kerentanan sistem dan mencuri informasi sensitif. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan mengeksploitasi kerentanan pada website ERP PT. XYZ, khususnya pada halaman yang dapat diakses oleh pengguna dengan *role* SPV Marketing, dengan teknik *penetration testing* menggunakan metode PTES yang mengacu pada OWASP Top 10 tahun 2021. Metode PTES yang digunakan mencakup tujuh tahapan, yaitu *pre-engagement interaction*, *intelligence gathering*, *threat modeling*, *vulnerability analysis* menggunakan ZAP, *exploitation*, *post-exploitation*, dan *reporting*. Berdasarkan pemindaian ZAP, ditemukan 23 celah keamanan, dengan 18 di antaranya termasuk dalam kategori OWASP Top 10, seperti *Broken Access Control*, *Injection*, *Insecure Design*, dan *Security Misconfiguration*, *Vulnerable and Outdated Components, dan Software* and *Data Integrity Failures*. Simulasi serangan yang berhasil dilakukan mencakup *Cross-Site Scripting* (XSS), *Session Hijacking*, dan *Cross-Site Request Forgery* (CSRF). Pengujian ini difokuskan pada kerentanan dengan risiko *tinggi*, seperti *Cloud Metadata Potentially Exposed* dan *Vulnerable JS Library*, serta risiko sedang, seperti *Absence of Anti-CSRF Tokens*, *Application Error Disclosure*, *CSP Header Not Set*, dan *Missing Anti-clickjacking Header*. Selain itu, juga ditemukan risiko rendah, seperti *Big Redirect Detected*, *Cookie No HttpOnly Flag*, *Cookie Without Secure Flag*, *Cookie without SameSite Attribute*, *Cross-Domain Javascript Source File Inclusion*, *Server Leaks Version Information via "Server" HTTP Response*, *Strict-Transport-Security Header Not Set*, *Timestamp Disclosure – Unix*, dan *X-Content-Type-Options Header Missing*. Rekomendasi perbaikan disesuaikan dengan teknologi ERP untuk memudahkan pemahaman tim pengembang dan meningkatkan keamanan sistem sesuai pedoman keamanan yang ditetapkan dalam OWASP Top 10.

Kata Kunci : Pengujian Keamanan, PTES, OWASP Top 10, Website ERP

Halaman ini sengaja dikosongkan

ABSTRACT

Student Name / NPM	:	Mochammad Yoga Firnanda / 21081010152
Thesis title	:	ERP WEBSITE SECURITY TESTING USING PENETRATION TESTING TECHNIQUES WITH PTES METHOD BASED ON OWASP TOP 10 (STUDY CASE: PT. XYZ)
Advisor	:	1. Henni Endah Wahanani, S.T., M.Kom. 2. Achmad Junaidi, S.Kom., M.Kom.

Rapid technological advancements have brought numerous benefits to the industrial sector, leading many companies to rely on technology to support their operations. However, this dependency also opens opportunities for hackers to exploit system vulnerabilities and steal sensitive information. This research aims to identify, evaluate, and exploit vulnerabilities on the ERP website of PT. XYZ, particularly on pages accessible by users with the SPV Marketing role, using penetration testing techniques with the PTES method referring to the 2021 OWASP Top 10. The PTES method used includes seven stages: pre-engagement interaction, intelligence gathering, threat modeling, vulnerability analysis using ZAP, exploitation, post-exploitation, and reporting. Based on the ZAP scan, 23 security vulnerabilities were found, 18 of which are included in the OWASP Top 10 categories, such as Broken Access Control, Injection, Insecure Design, and Security Misconfiguration, Vulnerable and Outdated Components, and Software and Data Integrity Failures. Successful attack simulations include Cross-Site Scripting (XSS), Session Hijacking, and Cross-Site Request Forgery (CSRF). The testing focused on high-risk vulnerabilities, such as Cloud Metadata Potentially Exposed and Vulnerable JS Library, as well as medium-risk vulnerabilities such as Absence of Anti-CSRF Tokens, Application Error Disclosure, CSP Header Not Set, and Missing Anti-clickjacking Header. Additionally, low-risk vulnerabilities were also found, such as Big Redirect Detected, Cookie No HttpOnly Flag, Cookie Without Secure Flag, Cookie without SameSite Attribute, Cross-Domain Javascript Source File Inclusion, Server Leaks Version Information via 'Server' HTTP Response, Strict-Transport-Security Header Not Set, Timestamp Disclosure - Unix, and X-Content-Type-Options Header Missing. The improvement recommendations are tailored to ERP technology to facilitate the understanding of the development team and enhance system security in accordance with the security guidelines set forth in the OWASP Top 10.

Keyword : Security Testing, PTES, OWASP Top 10, ERP Website

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul **"PENGUJIAN KEAMANAN WEBSITE ERP DENGAN TEKNIK PENETRATION TESTING MENGGUNAKAN METODE PTES BERDASARKAN OWASP TOP 10 (STUDI KASUS: PT. XYZ)"** dengan baik. Penulisan buku skripsi ini tidak dapat terwujud tanpa bantuan, motivasi, dan dukungan dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan rasa hormat dan terima kasih kepada:

1. Kedua orang tua penulis yang selalu memberikan doa serta dukungan kepada penulis, baik dukungan materi dan non-materi, sehingga penulis dapat menyelesaikan perkuliahan dari awal hingga akhir dengan baik.
2. Bapak Prof. Dr. Ir. Akhmad Fauzi, M.MT., selaku Rektor Universitas Pembangunan Nasional "Veteran" Jawa Timur.
3. Ibu Dr. Novirina Hendrasarie, S.T, M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jawa Timur.
4. Ibu Fetty Tri Anggraeny S.Kom., M.Kom., selaku Koordinator Program Studi Informatika Universitas Pembangunan Nasional "Veteran" Jawa Timur.
5. Andreas Nugroho Sihananto, S.Kom., M.Kom., selaku Koordinator Skripsi Program Studi Informatika Universitas Pembangunan Nasional "Veteran" Jawa Timur.
6. Ibu Henni Endah Wahanani, S.T., M.Kom., selaku dosen pembimbing pertama dalam membimbing dan mengarahkan penulis selama proses penyelesaian buku skripsi.
7. Bapak Achmad Junaidi, S.Kom., M.Kom., selaku dosen pembimbing dalam membimbing dan mengarahkan penulis selama proses penyusunan, usulan hingga penyelesaian buku skripsi.
8. Seluruh dosen, dan staff program studi Informatika UPN "Veteran" Jawa Timur yang telah mengajar, memberikan ilmu, serta pengalaman berharga selama masa perkuliahan.
9. Terima kasih kepada Staff IT dan HRD PT. XYZ atas kesempatan, bantuan administrasi, dan penyediaan sumber daya selama penelitian skripsi terhadap website ERP PT. XYZ.

10. Teman-teman seperjuangan yang selalu memberikan semangat, motivasi, serta menemani dan membantu penulis selama masa perkuliahan.
11. Seluruh keluiarga besar dan kerabat yang senantiasa memberikan doa dan dukungan.
12. Semua pihak yang tidak dapat disebutkan satu per satu yang telah membantu secara langsung maupun tidak langsung dalam penyusunan skripsi.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih banyak terdapat kekurangan. Oleh karena itu, kritik dan saran yang membangun dari berbagai pihak sangat diharapkan demi perbaikan dan penyempurnaan skripsi ini. Semoga laporan skripsi ini dapat menjadi referensi yang bermanfaat, khususnya bagi mahasiswa yang sedang menempuh skripsi sebagai syarat kelulusan, baik dari instansi yang sama maupun yang berbeda.

Surabaya, 11 Juni 2025

Mochammad Yoga Firnanda

NPM. 21081010152

DAFTAR ISI

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

Halaman ini sengaja dikosongkan

DAFTAR TABEL

Halaman ini sengaja dikosongkan

DAFTAR LAMPIRAN