ANALISIS KERENTANAN *WEBSITE* PT. PITJARUS DENGAN TIGA *TOOLS SCANNING* DAN *PENETRATION TESTING BLACK BOX* BERDASARKAN OWASP TOP 10

SKRIPSI

CHATTELIN
2110314042

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
2026

ANALISIS KERENTANAN *WEBSITE* PT. PITJARUS DENGAN TIGA *TOOLS SCANNING* DAN *PENETRATION TESTING BLACK BOX* BERDASARKAN OWASP TOP 10

SKRIPSI

Diajukan untuk Memenuhi Persyaratan dalam Memperoleh Gelar Sarjana Teknik

CHATTELIN
2110314042

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK ELEKTRO
2026

HALAMAN PENGESAHAN PENGUJI

Skripsi yang diajukan oleh:

Nama	:	Chattelin
NIM	:	2110314042
Program Studi	:	S1 – Teknik Elektro
Judul Skripsi	:	Analisis Kerentanan *Website* PT. Pitjarus dengan Tiga *Tools Scanning* dan *Penetration Testing Black Box* berdasarkan OWASP Top 10

telah berhasil dipertahankan di hadapan tim penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Pembangunan Nasional Veteran Jakarta.

Ayu Mika Sherila, S.T., M.T.

Penguji Utama

Subekti Ari Santoso, S.T., M.Eng.

Penguji Lembaga

Silvia Anggraeni, S.T., M.Sc., Ph.D

Penguji I (Pembimbing)

Dr. Ir. Teguh Firmansyah, S.T., M.T., IPM

Dekan Fakultas Teknik

Luh Krisnawati, S.T., M.T.

Koordinator Program Studi Teknik Elektro

Ditetapkan di: Jakarta

Tanggal Ujian: *13 Januari 2026*

HALAMAN PENGESAHAN PEMBIMBING SKRIPSI

Analisis Kerentanan *Website* PT. Pitjarus dengan Tiga *Tools* *Scanning* dan *Penetration Testing Black Box* berdasarkan OWASP Top 10

Chattelin

NIM. 2110314042

Disetujui oleh,

Pembimbing I	Pembimbing II
Silvia Anggraeni, S.T., M.Sc., Ph.D	Dr. Muhamad Alif Razi, S.Pi., M.Sc.

Mengetahui,

Koordinator Program Studi Teknik Elektro

Fakultas Teknik

Universitas Pembangunan Nasional Veteran Jakarta

Luh Krisnawati, S.T., M.T.

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini merupakan hasil karya sendiri dan semua sumber yang dikutip ataupun digunakan sebagai rujukan telah saya nyatakan benar.

Nama	: Chattelin
NIM	: 2110314042
Program Studi	: S1 – Teknik Elektro

Apabila di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 13 Januari 2026

Yang menyatakan,

Chattelin

HALAMAN PERSETUJUAN PUBLIKASI UNTUK KEPENTINGAN AKADEMIS

Sebagai *civitas academica* Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama	: Chattelin
NIM	: 2110314042
Program Studi	: S1 – Teknik Elektro

menyetujui untuk memberikan Hak Bebas Royalti Non-eksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul:

Analisis Kerentanan *Website* PT. Pitjarus dengan Tiga *Tools Scanning* dan *Penetration Testing Black Box* berdasarkan OWASP Top 10

Dengan Hak Bebas Royalti Non-eksklusif ini, Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih-media/formatkan, mengelola (dalam bentuk pangkalan data, merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan pemilik hak cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 13 Januari 2026

Yang menyatakan,

Chattelin

ANALISIS KERENTANAN *WEBSITE* PT. PITJARUS DENGAN TIGA *TOOLS SCANNING* DAN *PENETRATION TESTING BLACK BOX* BERDASARKAN OWASP TOP 10

Chattelin

ABSTRAK

Pemanfaatan *website* sebagai sarana operasional bisnis berpotensi meningkatkan risiko ancaman siber terhadap data dan sistem informasi perusahaan. Penelitian ini bertujuan untuk menganalisis kerentanan keamanan *website* PT. Pitjarus menggunakan metode *penetration testing* dengan pendekatan *black box* berdasarkan standar NIST SP 800-115 dan kerangka kerja OWASP Top 10 2021. Metodologi penelitian mencakup fase *planning, discovery, attack*, dan *reporting*. Pada fase *discovery*, penggunaan Nslookup dan Nmap mengidentifikasi bahwa domain target berada di balik layanan *reverse proxy* Cloudflare yang menyembunyikan alamat IP server origin, sedangkan pemindaian menggunakan OWASP ZAP menemukan 9 indikasi awal kerentanan (*initial findings*) pada lapisan aplikasi, termasuk potensi SQL *Injection* dan *Cross-Site Scripting* (XSS) yang masuk ke dalam kategori *A03: Injection* pada OWASP Top 10 202. Temuan ini menjadi dasar penentuan fokus pengujian pada fase *attack*. Hasil validasi pada fase attack mengonfirmasi dua kerentanan utama, yaitu SQL *Injection* pada fitur autentikasi dan XSS pada fitur pembuatan tugas. Berdasarkan penilaian menggunakan CVSS v3.1, kerentanan SQL *Injection* memperoleh skor 7.5 (*High*), sedangkan XSS memperoleh skor 3.9 (*Low*). Hasil ini menunjukkan bahwa perlindungan *reverse proxy* belum sepenuhnya mampu mencegah eksploitasi pada lapisan aplikasi. Penelitian ini merekomendasikan penerapan *parameterized query*, validasi dan sanitasi input di sisi server, serta prinsip *least privilege* pada pengelolaan basis data untuk meningkatkan keamanan *website* PT. Pitjarus.

KATA KUNCI: *Penetration Testing*, *Black Box*, NIST SP 800-115, OWASP Top 10, Keamanan *Website*

VULNERABILITY ANALYSIS OF PT. PITJARUS WEBSITE USING THREE SCANNING TOOLS AND BLACK BOX PENETRATION TESTING BASED ON OWASP TOP 10

Chattelin

ABSTRACT

The use of websites as core business platforms increases the potential risk of cyber threats to organizational data and information systems. This study aims to assess security vulnerabilities on the PT. Pitjarus website through penetration testing using a black-box approach, guided by the NIST SP 800-115 standard and the OWASP Top 10 2021 framework. The research was conducted through four stages: planning, discovery, attack, and reporting. During the discovery phase, Nslookup and Nmap identified that the target domain is protected by the Cloudflare reverse proxy service, which masks the origin server's IP address. In addition, scanning with OWASP ZAP detected nine initial indicators of vulnerabilities at the application layer, including potential SQL Injection and Cross-Site Scripting (XSS), classified under the A03: Injection category in the OWASP Top 10 2021. These findings directed the execution of targeted testing in the attack phase, which confirmed two primary vulnerabilities: SQL Injection in the authentication feature and XSS in the task creation feature. Based on CVSS v3.1 scoring, SQL Injection received a score of 7.5 (High), while XSS received a score of 3.9 (Low). The findings demonstrate that reverse proxy protection alone is insufficient to mitigate attacks at the application layer. Accordingly, this study recommends implementing parameterized queries, enforcing server-side input validation and sanitization, and applying the principle of least privilege in database management to further enhance the security posture of the PT. Pitjarus website.

KEYWORDS: *Penetration Testing, Black Box, NIST SP 800-115, OWASP Top 10, Website Security*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yesus Kristus karena atas kasih dan penyertaan-Nya, penulis dapat menyelesaikan skripsi yang berjudul "Analisis Kerentanan *Website* PT. Pitjarus dengan Tiga *Tools Scanning* dan *Penetration Testing Black Box* berdasarkan OWASP Top 10". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro.

Penyusunan skripsi ini tidak terlepas dari berbagai kendala dan tantangan. Namun, berkat bantuan, dukungan, serta doa dari berbagai pihak, skripsi ini dapat diselesaikan dengan baik. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Tuhan Yesus Kristus**,** atas segala berkat, kekuatan, dan penyertaan-Nya yang senantiasa menyertai penulis selama proses perkuliahan hingga penyusunan skripsi ini.
2. Kedua orang tua tercinta**,** Ibu Rosma dan Bapak Ian Michael, atas kasih sayang, doa, dukungan moral maupun materi, serta kepercayaan yang selalu diberikan kepada penulis.
3. Ibu Silvia Anggraeni, S.T., M.Sc., Ph.D, selaku Dosen Pembimbing Utama, atas bimbingan, arahan, kesabaran, dan ilmu yang telah diberikan selama proses penyusunan skripsi.
4. Bapak Dr. Muhamad Alif Razi, S.Pi., M.Sc. dan Ibu Yosy Rahmawati, S.ST., M.T., selaku Dosen Pembimbing II, atas masukan, saran, serta evaluasi yang sangat membantu dalam penyempurnaan skripsi ini.
5. Kenneth Maynard M., selaku CTO PT. Pitjarus sekaligus kakak laki-laki penulis, atas izin yang diberikan kepada penulis untuk melaksanakan penelitian di lingkungan PT. Pitjarus, serta arahan, dukungan, dan masukan yang sangat berharga selama proses penelitian dan penyusunan skripsi ini.
6. Teman-teman angkatan 2021 Teknik Elektro, khususnya Cantika, Iul, Aisyah, Rania, dan Raissa, Dika yang telah menemani, mendukung, dan berbagi cerita selama masa perkuliahan hingga penyusunan skripsi.

7. Sahabat-sahabat penulis, Melita dan Aqis, atas kebersamaan, semangat, serta dukungan yang diberikan selama proses penyusunan skripsi ini.
8. Assyarif Rahman**,** atas peran, kesabaran, dan ketulusan dalam mendampingi penulis, menyaksikan setiap proses dan perjuangan yang dilalui, serta selalu memberikan dukungan, ide, dan penguatan hingga skripsi ini dapat diselesaikan.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan dan kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun demi kesempurnaan skripsi ini. Semoga skripsi ini dapat memberikan manfaat dan kontribusi bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan aplikasi web.

Jakarta, Januari 2026

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN