PENERAPAN VULNERABILITY ASSESSMENT DAN PENETRATION TESTING (VAPT) MENGGUNAKAN METODE BLACK-BOX TESTING UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN

LAPORAN NON-REGULER

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

Disusun oleh :

MUHAMMAD QURAIS SIHAB

21.11.4407

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

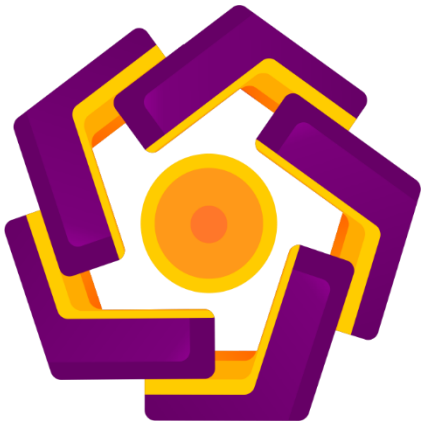
2025

PENERAPAN VULNERABILITY ASSESSMENT DAN PENETRATION TESTING (VAPT) MENGGUNAKAN METODE BLACK-BOX TESTING UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN

LAPORAN NON-REGULER

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika



Disusun oleh :

MUHAMMAD QURAIS SIHAB

21.11.4407

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

JALUR NON-REGULER

PENERAPAN VULNERABILITY ASSESSMENT DAN PENETRATION TESTING (VAPT) MENGGUNAKAN METODE BLACK-BOX TESTING UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN

yang disusun dan diajukan oleh

Muhammad Qurais Sihab

21.11.4407

telah disetujui oleh Dosen Pembimbing

pada tanggal 8 Januari 2025

Dosen Pembimbing,

Lukman, S.Kom., M.Kom.

NIK. 190302151

HALAMAN PENGESAHAN

JALUR NON-REGULER

PENERAPAN VULNERABILITY ASSESSMENT DAN PENETRATION TESTING (VAPT) MENGGUNAKAN METODE BLACK-BOX TESTING UNTUK MENGIDENTIFIKASI KERENTANAN KEAMANAN SISTEM INFORMASI PADA PERUSAHAAN

yang disusun dan diajukan oleh

Muhammad Qurais Sihab
21.11.4407

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Januari 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Arifiyanto Hadinegoro, S.Kom., M.T. **NIK. 190302289**	
Arif Akbarul Huda, S.Si., M.Eng. **NIK. 190302287**	
Lukman, S.Kom., M.Kom. **NIK. 190302151**	

Laporan ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Januari 2025

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN KARYA

Yang bertandatangan di bawah ini,

Nama mahasiswa : Muhammad Qurais Sihab

NIM : 21.11.4407

Menyatakan bahwa Laporan dengan judul berikut:

Penerapan Vulnerability Assessment dan Penetration Testing (VAPT) Menggunakan Metode Black-Box Testing Untuk Mengidentifikasi Kerentanan Keamanan Sistem Informasi Pada Perusahaan

Dosen Pembimbing : Lukman, S.Kom., 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 kegiatan 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 ketidak-benaran 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, 22 Januari 2025

Yang Menyatakan,

Muhammad Qurais Sihab

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan berjudul *"Penerapan Vulnerability Assessment dan Penetration Testing (VAPT) Menggunakan Metode Black-Box Testing untuk Mengidentifikasi Kerentanan Keamanan Sistem Informasi pada Perusahaan"*. Laporan ini disusun sebagai salah satu syarat untuk memenuhi tugas akhir pada Program Studi Informatika.

Pada kesempatan ini, penulis ingin menyampaikan penghargaan dan terima kasih kepada berbagai pihak yang telah memberikan bimbingan, dukungan, dan motivasi selama proses penyusunan laporan ini. Ucapan terima kasih penulis sampaikan kepada:

1. Lukman, M.Kom, selaku dosen pembimbing, yang telah memberikan arahan, masukan, dan dukungan penuh selama proses penulisan laporan ini.
2. Enny Susana, S.Kom., M.M., selaku Project Leader di PT. Pilar Teknotama Sinergi, atas kesempatan, bimbingan, dan ilmu yang diberikan kepada penulis selama bekerja dan belajar di perusahaan.
3. Ade Pujianto, M.Kom, selaku Team Leader di PT. Pilar Teknotama Sinergi, yang telah membagikan wawasan dan pengalaman berharga kepada penulis.
4. Rekan-rekan di PT. Pilar Teknotama Sinergi, atas dukungan, kolaborasi, dan semangat yang diberikan selama proses belajar dan bekerja.
5. Orang tua tercinta, atas doa, dukungan, dan kasih sayang yang tiada henti dalam setiap langkah yang penulis ambil.
6. Teman-teman seperjuangan, yang telah memberikan motivasi, dukungan moral, serta kebersamaan yang sangat berarti selama proses penyusunan laporan ini.

Yogyakarta, 8 Januari 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Seiring dengan pesatnya perkembangan teknologi digital, upaya perlindungan terhadap data dan sistem informasi telah menjadi hal yang sangat penting bagi perusahaan dalam menghadapi ancaman siber yang semakin berkembang dan kompleks. Ancaman-ancaman ini memiliki potensi untuk menimbulkan kerugian finansial yang signifikan serta merusak reputasi perusahaan apabila tidak ditangani secara efektif. Penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan pada sistem informasi melalui penerapan *Vulnerability Assessment and Penetration Testing* (VAPT) dengan metode *Black-Box Testing*. Metode ini memungkinkan pengujian terhadap sistem dari sudut pandang eksternal tanpa memanfaatkan informasi internal, sehingga menghasilkan evaluasi yang objektif mengenai kelemahan dalam infrastruktur keamanan. Hasil pengujian menunjukkan bahwa pendekatan ini berhasil mendeteksi berbagai kerentanan dengan tingkat kritis, seperti *SQL Injection*, *Cross-Site Scripting* (XSS), kredensial yang lemah (*weak credentials*), serta *sensitive information disclosure*, termasuk *directory listing* dan konfigurasi *server*. Temuan ini memberikan gambaran yang komprehensif terkait titik lemah sistem, sekaligus menjadi dasar untuk menyusun rekomendasi perbaikan yang terarah. Implementasi langkah mitigasi yang disarankan diharapkan dapat meningkatkan tingkat keamanan sistem informasi perusahaan, mendorong peningkatan kesadaran keamanan siber di antara pemangku kepentingan, serta memastikan keberlanjutan operasional perusahaan dalam menghadapi ancaman siber di masa mendatang.

Kata kunci: Vulnerability Assessment, Penetration Testing, Black-Box Testing, Keamanan Siber, Sistem Informasi

ABSTRACT

With the rapid advancement of digital technology, the protection of data and information systems has become a critical priority for companies in addressing the increasingly complex and evolving cyber threats. These threats have the potential to cause significant financial losses and damage a company's reputation if not effectively managed. This study aims to identify potential vulnerabilities in information systems through the application of Vulnerability Assessment and Penetration Testing (VAPT) using the Black-Box Testing method. This approach enables system testing from an external perspective without utilizing internal information, thereby providing an objective evaluation of weaknesses in the security infrastructure. The results of the testing revealed that this approach successfully identified various critical vulnerabilities, including SQL Injection, Cross-Site Scripting (XSS), weak credentials, and sensitive information disclosure, such as directory listings and server configurations. These findings provide a comprehensive overview of system weaknesses and serve as a basis for formulating targeted improvement recommendations. The implementation of the suggested mitigation measures is expected to enhance the security level of the company's information systems, promote increased cybersecurity awareness among stakeholders, and ensure the continuity of the company's operations in facing future cyber threats.

Keyword: *Vulnerability Assessment, Penetration Testing, Black-Box Testing, Cybersecurity, Information Systems*