

**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 QURAI 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 QURAI 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

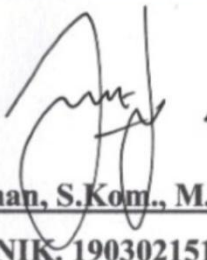
Muhammad Qurais Sihab

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

Arifiyanto Hadinegoro, S.Kom., M.T.
NIK. 190302289

Arif Akbarul Huda, S.Si., M.Eng.
NIK. 190302287

Lukman, S.Kom., M.Kom.
NIK. 190302151

Tanda Tangan



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 Pujiyanto, 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

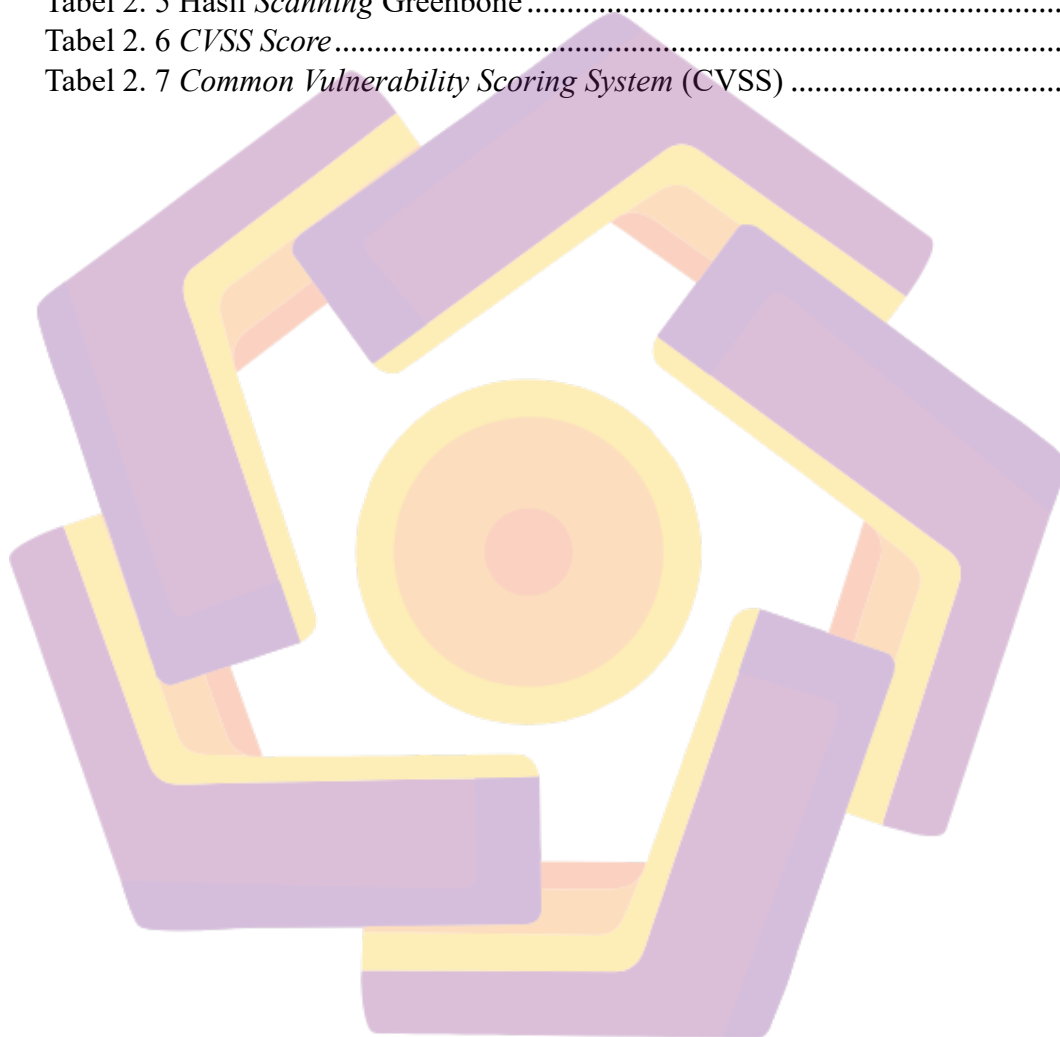
HALAMAN JUDUL.....	i
HALAMAN JUDUL.....	i
Halaman Persetujuan.....	ii
Halaman Pengesahan	iii
Halaman Pernyataan Keaslian Karya.....	iv
Kata Pengantar	v
Daftar Isi.....	vi
Daftar Tabel.....	ix
Daftar Gambar.....	x
Daftar Lampiran	xii
Intisari	xiii
<i>Abstract</i>	xiv
Bab I Pendahuluan	1
1.1. Gambaran Umum.....	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah.....	3
1.4. Tujuan.....	4
Bab II Teori dan METODE.....	5
2.1. Teori	5
2.1.1. <i>Information System Security</i>	5
2.1.2. <i>Vulnerability</i>	8
2.1.3. <i>Vulnerability Assessment and Penetration Testing</i>	9
2.1.4. <i>Method of Pentesting</i>	11
2.1.5. <i>Framework and Security Standard</i>	13
2.2. Analisis.....	24
2.2.1. <i>Black-Box Testing</i>	24
2.2.2. <i>Vulnerability Assessment and Penetration Testing Process</i>	25
BAB III Hasil dan Pembahasan	32
3.1. Hasil	32
3.1.1. <i>Planning and Preparation</i>	33

3.1.2.	<i>Information Gathering</i>	33
3.1.3.	<i>Vulnerability Scanning</i>	41
3.1.4.	<i>Gaining Access</i>	49
3.1.5.	<i>Maintaining Access</i>	64
3.1.6.	<i>Reporting</i>	64
3.1.7.	<i>Remediation</i>	67
3.1.8.	<i>Final Report</i>	68
3.2.	Evaluasi	69
3.2.1.	Efektivitas Metode <i>Black-Box Testing</i>	69
3.2.2.	Efektivitas <i>Tools</i> Pengujian dan Teknik Manual	77
3.2.3.	CVSS (<i>Common Vulnerability Scoring System</i>)	78
BAB IV	Kesimpulan	85
4.1.	Kesimpulan	85
4.2.	Saran	86
Referensi		87
Curriculum Vitae		90
Lampiran dan Bukti Pendukung		92
1.	Surat Tugas	92
1.1.	Surat Tugas Penetration Testing PT. Bank Jatim	92
1.2.	Surat Tugas Penetration Testing PT. Bank Kalbar	93
1.3.	Surat Tugas Penetration Testing PT. Bank SulutGo	94
1.4.	Surat Tugas Penetration Testing PT. BPR Danagung	95
2.	Bukti Pendapatan	96
2.1.	Fee Proyek Penetration Testing PT. Bank SulutGo	96
2.2.	Fee Proyek Penetration Testing PT. Bank Kalbar	98
2.3.	Fee saku Proyek Penetration Testing PT. Bank Jatim	100
3.	Dokumentasi Kegiatan	107
3.1.	Diskusi kegiatan Penetration Testing di PT. Bank SulutGo	107
3.2.	Kunjungan ke BDx Data Center dalam rangka Audit Internal PT. Bank SulutGo	108
3.3.	Kegiatan Penetration Testing di PT. Bank Kalbar	108
3.4.	Kegiatan Penetration Testing di PT. Bank Jatim	109

3.5.	Diskusi Internal Bersama Divisi IT Security PT. Bank Jatim.....	109
3.6.	Kegiatan Penetration Testing di PT. Bank Jatim.....	110
3.7.	Sesi Diskusi dan Penetration Testing di PT. Bank Jatim.....	111
3.8.	Kegiatan Penetration Testing di PT. Bank Jatim.....	112
3.9.	Sesi Diskusi Daring Terkait Kegiatan Penetration Testing Bersama Tim PT. Pilar Teknotama Sinergi	113
3.10.	Sesi Diskusi Daring Terkait Remediasi Kegiatan Penetration Testing di PT. Bank Jatim	113
3.11.	Kegiatan Penetration Testing di PT. BPR Danagung	114
3.12.	Perayaan Hari Ulang Tahun PT. Pilar Teknotama Sinergi	114
4.	Dokumen Penunjang (Penghargaan dan Sertifikasi).....	115
4.1.	Apresiasi Dinas Komunikasi dan Informatika Daerah Istimewa Yogyakarta atas kegiatan Vulnerability Assessment dan Penetration Testing Pada Sistem Elektronik Pemerintah Daerah DIY.....	115
4.2.	Lulus Sertifikasi Sebagai Penunjang Layak di Industri	116
4.3.	Evaluasi Hasil Kerja dan Kinerja Karyawan	117

DAFTAR TABEL

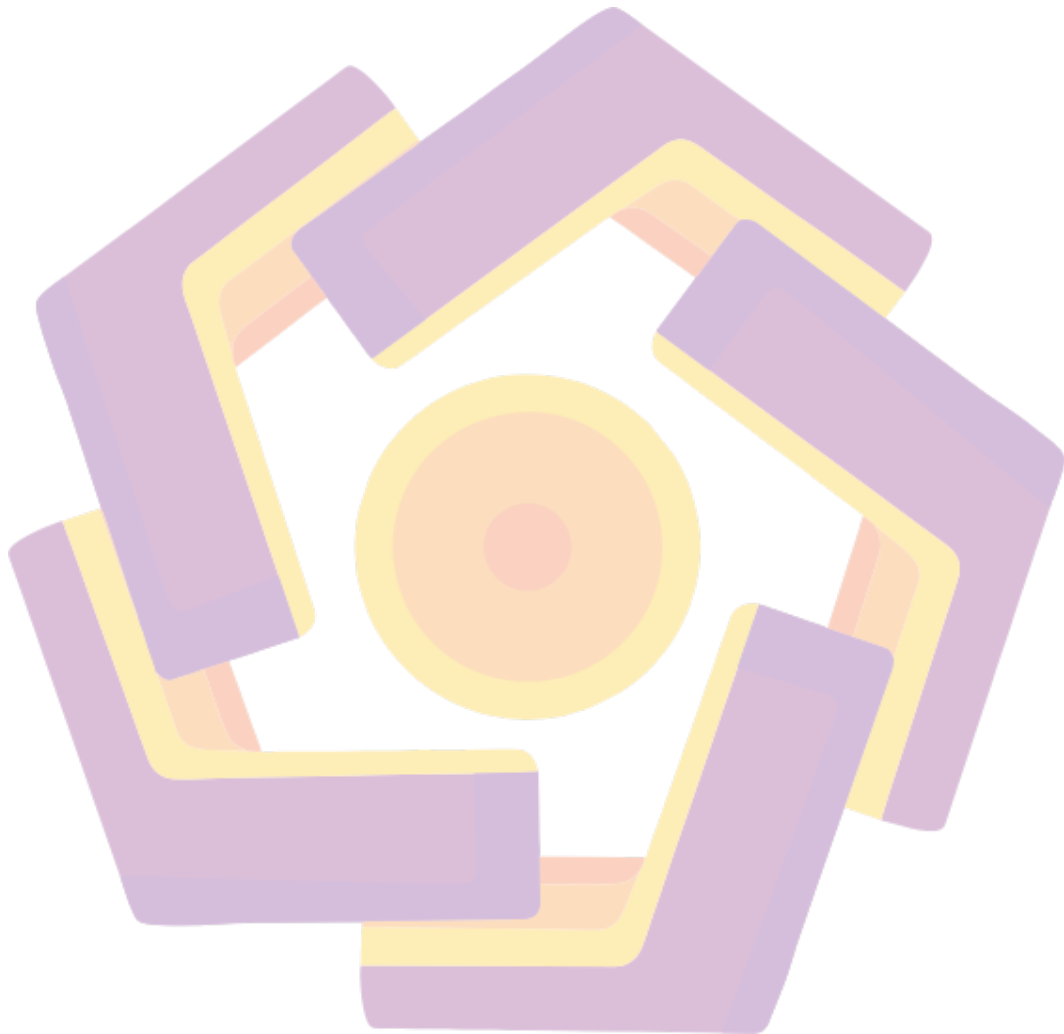
Tabel 2. 1 OWASP MASVS <i>Control Groups</i>	18
Tabel 2. 2 PCI-DSS <i>Compliance</i>	22
Tabel 2. 3 Hasil <i>Scanning</i> Invicti	42
Tabel 2. 4 Hasil <i>Scanning</i> Acunetix	44
Tabel 2. 5 Hasil <i>Scanning</i> Greenbone	46
Tabel 2. 6 <i>CVSS Score</i>	66
Tabel 2. 7 <i>Common Vulnerability Scoring System (CVSS)</i>	78



DAFTAR GAMBAR

Gambar 2. 1 CIA Triad.....	5
Gambar 2. 2 <i>Black-Box Testing</i>	11
Gambar 2. 3 <i>White-Box Testing</i>	12
Gambar 2. 4 <i>Gray-Box Testing</i>	12
Gambar 2. 5 OWASP Top 10	14
Gambar 2. 6 Owasp top 10.....	16
Gambar 2. 7 OWASP MASVS.....	17
Gambar 2. 8 <i>Natioanl Instite of Standards and Technology</i>	19
Gambar 2. 9 PCI-DSS	21
Gambar 2. 10 <i>Black-Box Testing Method</i>	24
Gambar 2. 11 <i>VAPT Process</i>	25
Gambar 3. 1 <i>IP Server</i>	33
Gambar 3. 2 <i>Hasil Port Scanning</i>	34
Gambar 3. 3 <i>SSL Enumeration</i>	35
Gambar 3. 4 <i>Directory Scanning</i>	36
Gambar 3. 5 <i>Nmap Scanning</i>	38
Gambar 3. 6 <i>Directory Listing</i>	39
Gambar 3. 7 <i>Information Disclosure</i>	40
Gambar 3. 8 <i>Information Disclosure phpinfo.php</i>	41
Gambar 3. 9 <i>Hasil Scanning Invicti</i>	42
Gambar 3. 10 <i>Hasil Scanning Acunetix</i>	44
Gambar 3. 11 <i>Hasil Scanning Greenbone</i>	46
Gambar 3. 12 <i>HTTP request POST</i>	50
Gambar 3. 13 <i>Cross-Site Scripting (XSS)</i>	50
Gambar 3. 14 <i>Port Scanning</i>	51
Gambar 3. 15 <i>Weak Credential Web Application</i>	51
Gambar 3. 16 <i>Port Scanning</i>	52
Gambar 3. 17 <i>Weak Credential PostgreSQL</i>	53
Gambar 3. 18 <i>Port Scanning</i>	54
Gambar 3. 19 <i>Weak Credential Microsoft SQL Server</i>	54
Gambar 3. 20 <i>Access Database via HeidiSQL</i>	55
Gambar 3. 21 <i>Halaman Login Aplikasi Web</i>	56
Gambar 3. 22 <i>Command SQLMap</i>	56
Gambar 3. 23 <i>Hasil SQLMap</i>	57
Gambar 3. 24 <i>Clickjacking via Iframe HTML</i>	58
Gambar 3. 25 <i>Proof of Concept Clickjacking</i>	58
Gambar 3. 26 <i>Hasil Scanning Port Nmap</i>	59
Gambar 3. 27 <i>CVE MikroTik Winbox Arbitrary File Read</i>	59
Gambar 3. 28 <i>MikroTik Winbox Arbitrary File Read</i>	60
Gambar 3. 29 <i>Non-Standart Port SSH (Secure Shell)</i>	60
Gambar 3. 30 <i>MikroTik Access via SSH (Sevure Shell)</i>	61

Gambar 3. 31 Hasil <i>Scanning Nmap</i>	62
Gambar 3. 32 <i>Weak Credential FTP</i>	62
Gambar 3. 33 <i>File Transfer Protocol</i>	63
Gambar 3. 34 <i>FTP Unencrypted Cleartext Login</i>	63



DAFTAR LAMPIRAN

Lampiran 1. 1 Surat Tugas <i>Penetration Testing</i> PT. Bank Jatim	92
Lampiran 1. 2 Surat Tugas <i>Penetration Testing</i> PT. Bank Kalbar	93
Lampiran 1. 3 Surat Tugas <i>Penetration Testing</i> PT. Bank Jatim	94
Lampiran 1. 4 Surat Tugas <i>Penetration Testing</i> PT. Bank Jatim	95
Lampiran 2. 1 Fee Proyek <i>Penetration Testing</i> PT. Bank SulutGo.....	96
Lampiran 2. 2 Uang Saku Proyek <i>Penetration Testing</i> PT. Bank SulutGo.....	97
Lampiran 2. 3 Uang Saku Proyek <i>Penetration Testing</i> PT. Bank Kalbar	98
Lampiran 2. 4 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Kalbar.....	99
Lampiran 2. 5 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim.....	100
Lampiran 2. 6 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim	101
Lampiran 2. 7 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim	102
Lampiran 2. 8 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim	103
Lampiran 2. 9 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim	104
Lampiran 2. 10 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim	105
Lampiran 2. 11 Uang saku Proyek <i>Penetration Testing</i> PT. Bank Jatim	106
Lampiran 3. 1 Diskusi kegiatan <i>Penetration Testing</i> di PT. Bank SulutGo.....	107
Lampiran 3. 2 Kunjungan ke BDx Data Center dalam rangka Audit Internal PT. Bank SulutGo.....	108
Lampiran 3. 3 Kegiatan <i>Penetration Testing</i> di PT. Bank Kalbar.....	108
Lampiran 3. 4 Kegiatan <i>Penetration Testing</i> di PT. Bank Jatim.....	109
Lampiran 3. 5 Diskusi Internal Bersama Divisi IT Security PT. Bank Jatim	110
Lampiran 3. 6 Kegiatan <i>Penetration Testing</i> di PT. Bank Jatim.....	110
Lampiran 3. 7 Sesi Diskusi dan <i>Penetration Testing</i> di PT. Bank Jatim.....	111
Lampiran 3. 8 Kegiatan <i>Penetration Testing</i> di PT. Bank Jatim.....	112
Lampiran 3. 9 Sesi Diskusi Daring Terkait Kegiatan <i>Penetration Testing</i> Bersama Tim PT. Pilar Teknotama Sinergi	113
Lampiran 3. 10 Sesi Diskusi Daring Terkait Remediasi Kegiatan <i>Penetration Testing</i> di PT. Bank Jatim.....	113
Lampiran 3. 11 Kegiatan <i>Penetration Testing</i> di PT. BPR Danagung	114
Lampiran 3. 12 Perayaan Hari Ulang Tahun PT. Pilar Teknotama Sinergi.....	114
Lampiran 4. 1 Apresiasi Diskominfo Daerah Istimewa Yogyakarta.....	115
Lampiran 4. 2 Sertifikasi Sebagai Penunjang Layak di Industri (CND)	116
Lampiran 4. 3 Sertifikasi Sebagai Penunjang Layak di Industri (ECIH).....	116
Lampiran 4. 4 Sertifikasi Sebagai Penunjang Layak di Industri (Security+)	117
Lampiran 4. 5 Evaluasi Hasil Kerja dan Kinerja Karyawan	117

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*