



**ANALISIS KEAMANAN SISTEM PADA *WEBSITE* PERUSAHAAN CV.
KAZAR TEKNOLOGI INDONESIA DENGAN METODE
*VULNERABILITY ASSESMENT AND PENETRATION TESTING (VAPT)***

SKRIPSI

Adha Maliq Ibrahim

1710511002

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2022



**ANALISIS KEAMANAN SISTEM PADA *WEBSITE* PERUSAHAAN CV.
KAZAR TEKNOLOGI INDONESIA DENGAN METODE
*VULNERABILITY ASSESMENT AND PENETRATION TESTING (VAPT)***

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Komputer**

Adha Maliq Ibrahim

1710511002

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2022

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Adha Maliq Ibrahim

NIM : 1710511002

Tanggal : 18 Januari 2022

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 18 Januari 2022

Yang menyatakan,



(Adha Maliq Ibrahim)

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMISI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, Saya yang bertanda tangan dibawah ini:

Nama : Adha Maliq Ibrahim

NIM : 1710511002

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah Saya yang berjudul:

**ANALISIS KEAMANAN SISTEM PADA *WEBSITE* PERUSAHAAN CV. KAZAR
TEKNOLOGI INDONESIA DENGAN METODE *VULNERABILITY ASSESMENT
AND PENETRATION TESTING (VAPT)***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir Saya selama tetap mencantumkan nama Saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 18 Januari 2022

Yang Menyatakan



(Adha Maliq Ibrahim)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut:

Nama : Adha Maliq Ibrahim
NIM : 1710511002
Program Studi : Informatika
Judul Tugas Akhir : Analisis Keamanan Sistem pada *Website* Perusahaan CV. Kazar Teknologi Indonesia dengan Metode *Vulnerability Assesment and Penetration Testing (VAPT)*

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Yuni Widiastiwi, S.Kom, M.Si.
Penguji I



Bayu Hananto, S.Kom., M.Kom.
Penguji II



Heri Bayu Seta, S.Kom, MTI.
Dosen Pembimbing I



I Wayan Widi P, S.Kom., MTI
Dosen Pembimbing II



Dr. Ermatita, M. Kom.
Dekan



Yuni Widiastiwi, S.Kom, M.Si.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 15 Desember 2021



**ANALISIS KEAMANAN SISTEM PADA WEBSITE PERUSAHAAN CV.
KAZAR TEKNOLOGI INDONESIA DENGAN METODE
VULNERABILITY ASSESMENT AND PENETRATION TESTING (VAPT)**

Adha Maliq Ibrahim

ABSTRAK

Website adalah aplikasi yang dijalankan melalui *software browser* yang mengakses informasinya menggunakan protokol HTTP atau HTTPS, *website* berisikan konten-konten multimedia. Mengakses sebuah laman *website* dapat dilakukan melalui perangkat yang memiliki *browser* dan juga *website* selalu diakses oleh pengguna saat ini. Kebutuhan akan penggunaan *website* menjadi ancaman keamanan informasi bagi penggunanya. CV. Kazar Teknologi Indonesia merupakan sebuah perusahaan bergerak dibidang barang dan jasa teknologi informasi. Penelitian ini menggunakan metode *Vulnerability Assessment and Penetration Testing* (VAPT). VAPT merupakan gabungan dari dua metode uji keamanan pada suatu aplikasi atau jaringan. Metode VAPT memiliki alur tahapan yang dimulai dengan *scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting, dan clean-up*. Hasil penelitian ini ditemukan kerentanan dari hasil Nessus sebanyak 42 kerentanan, OpenVAS sebanyak 10 kerentanan, OWASP ZAP sebanyak 10 kerentanan, dan WPScan kerentanan informasi. *Penetration testing* menggunakan teknik seperti analisis jaringan menggunakan Wireshark, *bypass password, brute force, inspect element* melalui *web browser*, dan *port scanning* dengan perintah dari nmap. Untuk menjaga server dan aplikasi web tetap aman, dapat dilakukan kegiatan *maintenance* oleh perusahaan untuk menjaga server dan aplikasi web sehingga mengurangi dampak jika terjadi eksploitasi oleh *attacker*.

Kata kunci : *website, keamanan informasi, VAPT, Nessus, OpenVAS, OWASP ZAP, WPScan, penetration testing, maintenance.*

**ANALISIS KEAMANAN SISTEM PADA *WEBSITE* PERUSAHAAN CV.
KAZAR TEKNOLOGI INDONESIA DENGAN METODE
*VULNERABILITY ASSESMENT AND PENETRATION TESTING (VAPT)***

Adha Maliq Ibrahim

ABSTRACT

Website is an application that is run through a browser software that accesses information using the HTTP or HTTPS protocol, a website that contains multimedia content. Accessing a website page can be done through a device that has a browser and the website is always accessed by current users. The need for the use of the website is a threat to information security for its users. CV. Kazar Teknologi Indonesia is a company engaged in information technology goods and services. This study uses the Vulnerability Assessment and Penetration Testing (VAPT) method. VAPT is a combination of two security test methods on an application or network. The VAPT method has a flow of stages starting with scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting, and clean-up. The results of this study found 42 vulnerabilities from Nessus results, 10 vulnerabilities in OpenVAS, 10 vulnerabilities in OWASP ZAP, and WPScan only information vulnerabilities. Penetration testing using techniques such as network analysis using Wireshark, bypass passwords, brute force, inspect elements via a web browser, and port scanning with commands from nmap. To maintain the security of servers and web applications, maintenance activities can be carried out by companies to maintain servers and web applications so as to reduce the impact in the event of exploitation by attackers.

Keywords : website, information security, VAPT, Nessus, OpenVAS, OWASP ZAP, WPScan, Penetration testing, maintenance.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas nikmat dan karunia-Nya penulis berhasil menyelesaikan Skripsi ini. Penulis ingin mengucapkan terima kasih kepada:

1. Kedua orang tua penulis serta seluruh keluarga yang selalu memberi doa serta semangat sehingga penulis dapat menyelesaikan Skripsi ini.
2. Bapak Tomi Defisa, S.Kom., M.Kom. yang telah memberikan perizinan dalam penelitian pada perusahaan CV. Kazar Teknologi Indonesia.
3. Bapak Henki Bayu Seta, S.Kom., M.Kom. dan Bapak I Wayan Widi P., S.Kom., MTI. selaku dosen pembimbing I, dan dosen pembimbing II yang telah memberikan pembelajaran, semangat, serta saran yang bermanfaat.
4. Ibu Dr. Ermatita, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
5. Ibu Yuni Widiastiwi, S.Kom., Msi. selaku Ketua Program Studi Informatika Universitas Pembangunan Nasional Veteran Jakarta.
6. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta terima kasih yang telah memberikan ilmu-ilmu bermanfaat.
7. Teman-teman Informatika yaitu Khozi Ihza Humamda, Fuad Bawazir Alatas, Alvita Izana Kusumarini, Jose Alnevo Theora, dan Fajar Subkhi Sulaiman yang telah memberikan saran yang sangat bermanfaat.
8. Teman-teman Informatika 2017, dan seluruh rekan mahasiswa terima kasih atas bantuan, saran, dan dukungan yang telah diberikan.

Akhir kata, semoga Skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 5 Desember 2021

Penulis,

Adha Maliq Ibrahim

DAFTAR ISI

PERNYATAAN ORISINALITAS	i
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMISI	ii
LEMBAR PENGESAHAN	iii
ABSTRAK	iv
ABSTRACT	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR SIMBOL	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Ruang Lingkup	3
1.4 Tujuan Penelitian	4
1.5 Manfaat	4
1.6 Luaran yang Diharapkan	4
1.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Sistem Informasi	6
2.2 Keamanan Informasi	6
2.2.1 Aspek Keamanan Informasi	6
2.3 <i>Ethical Hacking</i>	8
2.4 <i>Common Vulnerability Scoring System (CVSS)</i>	9
2.5 <i>Vulnerability Assessment</i>	9
2.5.1 Teknik-teknik <i>Vulnerability Assessment</i>	10
2.5.2 Alur Proses <i>Vulnerability Assessment</i>	11
2.5.3 Tipe-tipe <i>Vulnerability Assessment</i>	12
2.5.4 Kelebihan dan Kekurangan dalam <i>Vulnerability Assessment</i>	13
2.6 <i>Penetration Testing</i>	14

2.6.1	Metodologi <i>Penetration Testing</i>	14
2.6.2	Proses <i>Penetration Testing</i>	14
2.6.3	Strategi <i>Penetration Testing</i>	16
2.6.4	Kelebihan dan Kekurangan <i>Penetration Testing</i>	16
2.7	<i>Vulnerability Assessment and Penetration Testing (VAPT)</i>	17
2.7.1	Alur Proses <i>VAPT</i>	17
2.7.2	Alat-alat <i>VAPT</i>	20
2.8	<i>Tools</i> yang Digunakan.....	20
2.9	Perbedaan dengan Penelitian Terdahulu	24
2.10	Penelitian Terkait	24
BAB III METODE PENELITIAN		27
3.1	Tahapan Penelitian	27
3.1.1	Identifikasi Masalah	28
3.1.2	Studi Literatur	28
3.1.3	Observasi dan Wawancara	28
3.1.4	<i>Scope</i>	28
3.1.5	<i>Reconnaissance</i>	28
3.1.6	<i>Vulnerability Detection</i>	29
3.1.7	<i>Information Analysis and Planing</i>	30
3.1.8	<i>Penetration Testing</i>	30
3.1.9	<i>Privilage Escalation</i>	30
3.1.10	<i>Result Analysis</i>	31
3.1.11	<i>Reporting</i>	31
3.1.12	<i>Clean-up</i>	31
3.1.13	<i>Maintenance</i>	31
3.2	Alasan Penelitian di Perusahaan Terkait	31
3.3	Alat bantu Penelitian	32
3.4	Jadwal Penelitian	33
BAB IV HASIL DAN PEMBAHASAN		35
4.1	Topologi Jaringan.....	35
4.2	Observasi dan Wawancara	36
4.3	<i>Scope</i>	37
4.4	<i>Reconnaissance</i>	37
4.4.1	Whois	37

4.4.2	NSlookup	39
4.4.3	Sublist3r	39
4.4.4	Nmap	41
4.4.5	Wappalyzer	42
4.5	<i>Vulnerability Detection</i>	43
4.5.1	Nessus	43
4.5.2	OpenVAS	54
4.5.3	OWASP ZAP	58
4.5.4	WPScan	60
4.6	<i>Information Analysis and Planing</i>	66
4.6.1	Analisis Hasil Nessus	66
4.6.2	Analisis Hasil OpenVAS	86
4.6.3	Analisis Hasil OWASP ZAP	89
4.6.4	Hasil Analisis WPScan	92
4.7	<i>Penetration Testing</i>	92
4.7.1	<i>Penetration Testing</i> Berdasarkan Jaringan	93
4.7.2	<i>Penetration Testing</i> Berdasarkan Aplikasi	111
4.8	<i>Privilege Escalation</i>	116
4.9	<i>Result Analysis</i>	120
4.9.1	<i>Result Analysis</i> Berdasarkan Jaringan	121
4.9.2	<i>Result Analysis</i> Berdasarkan Aplikasi	124
4.10	<i>Reporting</i>	125
4.10.1	<i>Reporting</i> Berdasarkan Jaringan	126
4.10.2	<i>Reporting</i> Berdasarkan Aplikasi	128
4.11	<i>Clean-up</i>	130
4.12	<i>Maintenance</i>	130
BAB V PENUTUP		133
5.1	Kesimpulan	133
5.2	Saran	134
DAFTAR PUSTAKA		136
RIWAYAT HIDUP		139
LAMPIRAN		140

DAFTAR GAMBAR


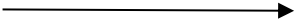


Gambar 2. 1 CIA TRIAD (NDK, 2021)	7
Gambar 2. 2 Proses Vulnerability Assessment (Chandrakant and Prakash, 2019)11	
Gambar 2. 3 Proses Penetration Testing (Chandrakant and Prakash, 2019).....	15
Gambar 2. 4 Alur Proses VAPT(Zulfi, 2017).....	18
Gambar 3. 1 Tahapan Penelitian	27
Gambar 4. 1 Topologi Jaringan ISP.....	35
Gambar 4. 2 Topologi Jaringan VPN.....	36
Gambar 4. 3 Hasil NSlookup	39
Gambar 4. 4 Hasil Nmap.....	42
Gambar 4. 5 Hasil Wappalyzer	42
Gambar 4. 6 Hasil Nessus	44
Gambar 4. 7 Hasil Nessus Severity Info	45
Gambar 4. 8 Hasil OpenVAS Severity Medium.....	55
Gambar 4. 9 Hasil OpenVAS Severity Medium-Low	55
Gambar 4. 10 Hasil OWASP ZAP.....	58
Gambar 4. 11 Hasil WPScan Header, Robots.....	61
Gambar 4. 12 Hasil WPScan XML, WordPress	61
Gambar 4. 13 Hasil WPScan WP-Cron, Wordpress	62
Gambar 4. 14 Hasil WPScan User Identified.....	62
Gambar 4. 15 Tampilan wp-login.php	93
Gambar 4. 16 Tampilan Gagal Login Admin wp-login.php.....	94
Gambar 4. 17 Hasil Wireshark TLS.....	95
Gambar 4. 18 Informasi pada TLSv1.2.....	95
Gambar 4. 19 Hasil mengakses pada user identified	96
Gambar 4. 20 Pencarian Wireshark TLSv1.0	97
Gambar 4. 21 Hasil Pengujian HSTS.....	98
Gambar 4. 22 Hasil Akses kazar.co.id/robots.txt.....	98
Gambar 4. 23 Hasil Wireshark HTTP	100
Gambar 4. 24 Proses Login FTP	101
Gambar 4. 25 Hasil Wireshark FTP	102
Gambar 4. 26 Proses Login IMAP	102
Gambar 4. 27 Hasil Wireshark IMAP	103
Gambar 4. 28 Proses Login POP3.....	104
Gambar 4. 29 Hasil Wireshark POP3	105
Gambar 4. 30 Hasil Nmap Diffie-Helman	106
Gambar 4. 31 Hasil Nmap HTTP Server Information	108
Gambar 4. 32 Hasil Nmap port 443	111
Gambar 4. 33 Message Form kazar.co.id.....	112

Gambar 4. 34 Inspect Element Message Form	113
Gambar 4. 35 Cookie pada kazar.co.id	113
Gambar 4. 36 Menambahkan Cookie pada kazar.co.id	114
Gambar 4. 37 Inspect Element Button Submit.....	114
Gambar 4. 38 Burpsuite HTTP Response	115
Gambar 4. 39 Informasi user identified kazar.co.id.....	116
Gambar 4. 40 CV Tomi.....	118
Gambar 4. 41 Proses Brute Force WPScan user admin	119
Gambar 4. 42 Proses Brute Force WPScan user tomi.....	120

DAFTAR TABEL

Tabel 2. 1 VAPT Tools (Chandrakant and Prakash, 2019, hlm. 75-76).....	20
Tabel 3. 1 Reconnaissance Tools	29
Tabel 3. 2 Vulnerability Detection Tools.....	29
Tabel 3. 3 Penetration Testing Tools	30
Tabel 3. 4 Jadwal Penelitian.....	34
Tabel 4. 1 Hasil Whois.....	38
Tabel 4. 2 Hasil sublist3r	40
Tabel 4. 3 Hasil Scanning Nessus	46
Tabel 4. 4 Hasil Scanning OpenVAS.....	56
Tabel 4. 5 Hasil Scanning OWASP ZAP.....	59
Tabel 4. 6 Hasil Scanning WPScan.....	63
Tabel 4. 7 Analisis Kerentanan pada Hasil Nessus.....	66
Tabel 4. 8 Analisis Kerentanan pada Hasil OpenVAS	86
Tabel 4. 9 Analisis Kerentanan pada Hasil OWASP ZAP.....	89
Tabel 4. 10 Wordlist Password Brute Force	117
Tabel 4. 11 Result Analysis berdasarkan Jaringan	121
Tabel 4. 12 Result Analysis berdasarkan Aplikasi	124
Tabel 4. 13 Reporting berdasarkan Jaringan.....	126
Tabel 4. 14 Reporting berdasarkan Aplikasi.....	129

DAFTAR SIMBOL

Simbol	Nama Simbol	Keterangan
	Simbol Proses	Digambarkan sebagai proses yang terjadi
	Simbol arah data dan arus data	Petunjuk arah pada data dan arus data pada sebuah proses
	Simbol <i>Terminator</i>	Simbol untuk kegiatan awalan atau akhiran dari suatu proses
	Simbol Proses yang Ditetapkan	Simbol untuk kegiatan yang sudah ditentukan pada proses yang dijalankan