LAPORAN VULNERABILITY ASSESSMENT

Format Standar Pelaporan Keamanan Siber

Versi Dokumen: 1.0

Tanggal: [DD/MM/YYYY]

Klasifikasi: **CONFIDENTIAL**

Disusun oleh: [Nama Tim / Vendor]

Klien: [Nama Perusahaan Klien]

Informasi Dokumen

Nomor Laporan	[VA-2025-001]
Tanggal Mulai	[DD/MM/YYYY]
Tanggal Selesai	[DD/MM/YYYY]
Scope	[Aplikasi Web / Jaringan Internal / dst.]
Metodologi	OWASP Testing Guide, NIST SP 800-115
Tools Digunakan	Nessus, Burp Suite, Nmap, OpenVAS
Status Laporan	Final

Daftar Isi

1. Executive Summary

Laporan ini merupakan hasil pelaksanaan *Vulnerability Assessment* (VA) yang dilakukan terhadap [nama sistem/aplikasi/jaringan] milik [nama klien] pada periode [tanggal mulai] hingga [tanggal selesai]. Tujuan pengujian adalah mengidentifikasi celah keamanan yang berpotensi dieksploitasi oleh pihak tidak berwenang, serta memberikan rekomendasi perbaikan yang dapat segera ditindaklanjuti.

Severity	Jumlah Temuan	Status Prioritas
● Critical	[ ]	Segera diperbaiki (0–3 hari)
● High	[ ]	Diperbaiki dalam 7 hari
● Medium	[ ]	Diperbaiki dalam 30 hari
● Low	[ ]	Diperbaiki dalam 90 hari
Total	[ ]	

Kesimpulan Umum: Berdasarkan hasil assessment, sistem [nama klien] ditemukan dalam kondisi [kritis / perlu perhatian / cukup baik]. Terdapat [X] temuan Critical yang memerlukan penanganan segera untuk mencegah potensi eksploitasi dan dampak bisnis yang signifikan.

2. Scope & Metodologi

2.1 Ruang Lingkup Pengujian

Tipe Pengujian	[Black Box / Grey Box / White Box]
Target Sistem	[URL / IP Address / Range Jaringan]
Lingkungan	[Production / Staging]
Jumlah Host/URL	[ ] host aktif dari [ ] total yang diidentifikasi
Yang Tidak Diuji	[Daftar sistem/komponen di luar scope]

2.2 Metodologi

Pengujian dilakukan mengacu pada standar industri berikut: **OWASP Testing Guide v4.2**, **NIST SP 800-115**, dan **PTES (Penetration Testing Execution Standard)**. Proses pengujian mencakup lima tahapan utama:

Fase	Nama Tahapan	Deskripsi
01	Reconnaissance	Pengumpulan informasi target secara pasif dan aktif
02	Vulnerability Scanning	Pemindaian otomatis menggunakan tools standar industri
03	Manual Analysis	Verifikasi temuan dan eliminasi false positive
04	Risk Assessment	Penilaian tingkat risiko menggunakan skor CVSS v3.1
05	Reporting	Dokumentasi temuan dan rekomendasi remediation

2.3 Tools yang Digunakan

Tool	Fungsi
Nessus Professional	Vulnerability scanning & patch audit
Burp Suite Pro	Web application security testing
Nmap / Zenmap	Network discovery & port scanning
OpenVAS	Open-source vulnerability scanner
Metasploit Framework	Validasi eksploitasi (jika dalam scope)
OWASP ZAP	Automated web application scanning

3. Temuan Vulnerability

3.1 Rekapitulasi Temuan

Berikut adalah distribusi temuan berdasarkan tingkat severity. Setiap temuan telah diverifikasi secara manual untuk mengeliminasi false positive.

Severity	Jumlah	CVSS Range	Rekomendasi Waktu Remediation
● Critical	[ ]	9.0 – 10.0	0 – 3 hari kerja
● High	[ ]	7.0 – 8.9	7 hari kerja
● Medium	[ ]	4.0 – 6.9	30 hari kerja
● Low	[ ]	0.1 – 3.9	90 hari kerja

3.2 Detail Temuan per Severity

Setiap temuan disajikan dengan komponen: **Deskripsi** — penjelasan celah keamanan; **Dampak** — risiko jika dieksploitasi; **Bukti Temuan** — dokumentasi teknis; dan **Rekomendasi** — langkah perbaikan spesifik.

VA-001	[Nama Vulnerability — Contoh: SQL Injection pada Parameter Login]				CRITICAL
CVSS Score	**9.8**	**CVE**	CVE-XXXX-XXXXX	**Sistem Terdampak**	[URL / IP / Komponen yang terdampak]
Deskripsi	Ditemukan celah injeksi SQL pada parameter [nama parameter] di endpoint [URL/endpoint]. Celah ini memungkinkan penyerang mengirimkan input berbahaya yang dieksekusi langsung oleh database, tanpa validasi atau sanitasi yang memadai.				
Dampak	Eksploitasi celah ini dapat mengakibatkan: akses tidak sah ke seluruh database, kebocoran data sensitif pengguna, modifikasi atau penghapusan data, hingga pengambilalihan server database sepenuhnya.				
Bukti Temuan	Screenshot / output tools / payload yang digunakan untuk mereplikasi temuan ini tersedia pada Lampiran A.				
Rekomendasi	1. Implementasikan *parameterized queries* atau *prepared statements*. 2. Terapkan input validation dan sanitasi pada seluruh parameter input. 3. Gunakan prinsip least privilege pada akun database. 4. Aktifkan Web Application Firewall (WAF) sebagai mitigasi tambahan.				

VA-002	[Nama Vulnerability — Contoh: Outdated SSL/TLS Configuration]				HIGH
CVSS Score	**7.5**	**CVE**	CVE-XXXX-XXXXX	**Sistem Terdampak**	[URL / IP / Port yang terdampak]
Deskripsi	Server menggunakan protokol SSL/TLS versi lama (TLS 1.0/1.1) yang telah dinyatakan deprecated dan rentan terhadap berbagai serangan seperti BEAST, POODLE, dan downgrade attack.				
Dampak	Penyerang yang berada dalam posisi man-in-the-middle dapat mendekripsi komunikasi yang seharusnya terenkripsi, berpotensi mencuri kredensial dan data sensitif yang ditransmisikan.				
Bukti Temuan	Hasil scan Nessus (Plugin ID: XXXXX) dan output testssl.sh tersedia pada Lampiran B.				
Rekomendasi	1. Nonaktifkan TLS 1.0 dan TLS 1.1 pada konfigurasi server. 2. Aktifkan hanya TLS 1.2 dan TLS 1.3. 3. Perbarui cipher suite — hapus cipher yang lemah (RC4, DES, 3DES). 4. Implementasikan HSTS (HTTP Strict Transport Security).				

VA-003	[Nama Vulnerability — Contoh: Missing Security Headers]				MEDIUM
CVSS Score	**5.3**	**CVE**	N/A	**Sistem Terdampak**	[URL / Seluruh endpoint aplikasi web]
Deskripsi	Aplikasi tidak mengimplementasikan HTTP security headers yang direkomendasikan, termasuk Content-Security-Policy (CSP), X-Frame-Options, dan X-Content-Type-Options.				
Dampak	Ketiadaan security headers meningkatkan risiko serangan seperti Cross-Site Scripting (XSS), clickjacking, dan MIME-type sniffing yang dapat digunakan untuk memanipulasi perilaku browser pengguna.				
Bukti Temuan	Output Burp Suite dan curl headers response tersedia pada Lampiran C.				
Rekomendasi	1. Tambahkan header Content-Security-Policy dengan policy yang sesuai. 2. Set X-Frame-Options: DENY atau SAMEORIGIN. 3. Set X-Content-Type-Options: nosniff. 4. Tambahkan Referrer-Policy dan Permissions-Policy.				

** Temuan selanjutnya mengikuti format yang sama. Urutkan dari severity tertinggi ke terendah.*

4. Tabel Rekapitulasi Seluruh Temuan

Tabel berikut merangkum seluruh temuan dalam satu halaman untuk memudahkan tracking dan prioritisasi oleh tim IT maupun manajemen.

No	ID	Nama Vulnerability	Severity	CVSS	Sistem	Status
1	VA-001	[Nama Vuln 1]	Critical	9.8	[Sistem]	Open
2	VA-002	[Nama Vuln 2]	High	7.5	[Sistem]	Open
3	VA-003	[Nama Vuln 3]	Medium	5.3	[Sistem]	In Progress
4	VA-004	[Nama Vuln 4]	Medium	4.1	[Sistem]	Open
5	VA-005	[Nama Vuln 5]	Low	3.1	[Sistem]	Open
...	...	...	...	...	...	...

Status Keterangan:	**Open** = Belum diperbaiki	**In Progress** = Sedang dalam proses remediation	**Resolved** = Sudah diperbaiki & diverifikasi

5. Rekomendasi Remediation

Rekomendasi berikut disusun berdasarkan prioritas severity. Tim IT disarankan untuk menyelesaikan seluruh temuan Critical dan High sebelum beralih ke temuan dengan severity lebih rendah. Setelah remediation selesai, disarankan untuk melakukan *retest* guna memverifikasi bahwa celah telah berhasil ditutup.

ID	Vulnerability	Langkah Remediation	Deadline	PIC
VA-001	[Nama Vuln 1]	Implementasi parameterized queries; validasi input; WAF	[DD/MM/YY]	[Nama/Tim]
VA-002	[Nama Vuln 2]	Nonaktifkan TLS 1.0/1.1; aktifkan TLS 1.3; update cipher suite	[DD/MM/YY]	[Nama/Tim]
VA-003	[Nama Vuln 3]	Tambahkan CSP, X-Frame-Options, X-Content-Type-Options	[DD/MM/YY]	[Nama/Tim]
...	...	...	...	...

6. Kesimpulan & Next Steps

Vulnerability assessment yang dilakukan pada [nama sistem/klien] telah berhasil mengidentifikasi total [ ] celah keamanan dengan distribusi [ ] Critical, [ ] High, [ ] Medium, dan [ ] Low. Kondisi keamanan sistem saat ini dinilai **[kritis / perlu perhatian / cukup baik]** dan memerlukan tindak lanjut segera pada temuan dengan severity Critical dan High.

Rekomendasi Next Steps:

#	Aktivitas	Deskripsi
01	Remediation Segera	Perbaiki seluruh temuan Critical dalam 3 hari kerja sejak laporan diterima.
02	Remediation Terencana	Buat jadwal perbaikan untuk temuan High, Medium, dan Low sesuai deadline yang disepakati.
03	Retest / Verifikasi	Jadwalkan sesi retest setelah remediation selesai untuk memverifikasi perbaikan.
04	Patch Management	Implementasikan proses patch management yang berkelanjutan agar vulnerability serupa tidak terulang.
05	Periodic Assessment	Lakukan VA secara rutin minimal 1x per tahun, atau setelah setiap perubahan sistem yang signifikan.

Lampiran — Referensi & Glosarium

Referensi Standar

- OWASP Testing Guide v4.2 — https://owasp.org/www-project-web-security-testing-guide/
- NIST SP 800-115 — Technical Guide to Information Security Testing
- CVSS v3.1 Specification — https://www.first.org/cvss/specification-document
- PTES — Penetration Testing Execution Standard — http://www.pentest-standard.org/

Glosarium

Istilah	Definisi
Vulnerability	Celah atau kelemahan dalam sistem yang dapat dieksploitasi oleh penyerang.
CVSS Score	Common Vulnerability Scoring System — skala 0–10 untuk mengukur tingkat keparahan vulnerability.
CVE	Common Vulnerabilities and Exposures — identifikasi unik untuk vulnerability yang telah dipublikasikan.
False Positive	Temuan yang terdeteksi oleh tools namun setelah verifikasi manual terbukti bukan vulnerability nyata.
Remediation	Proses perbaikan atau mitigasi celah keamanan yang ditemukan.
Retest	Pengujian ulang setelah remediation untuk memverifikasi bahwa celah telah berhasil ditutup.
Pentest / VAPT	Penetration Testing — pengujian yang melampaui VA dengan mencoba mengeksploitasi celah yang ditemukan.
Scope	Ruang lingkup yang disepakati — sistem, jaringan, atau aplikasi yang menjadi target pengujian.