

REPORT STRUCTURE

Standard Engagement Report Structure

Client: Engagement:

Classification: Confidential

1 • DOCUMENT CONTROL

FIELD	VALUE
Report reference	RT-REP-.....-.....
Version / Date	 •
Prepared by	
Reviewed by	
Distribution	

2 • EXECUTIVE SUMMARY

- Engagement objectives and testing tier in plain language.
- Overall risk posture — top risks in business terms, not just CVSS.
- Headline numbers: findings by severity, critical issues, assets affected.
- Recommended priorities for the next 30 / 60 / 90 days.

3 • ENGAGEMENT OVERVIEW

- Authorized scope (from the Authorization Form) and testing window.
- Personnel involved and access provided.
- Deviations from the SOW, if any, and approvals.

4 • METHODOLOGY

- Framework alignment: OWASP Top 10, ASVS, PTES, OSSTMM.
- Phases executed: recon → enumeration → exploitation (PoC) → validation.
- Tools and AI-assisted pipeline used (governed, scoped, audited).
- Limitations: anything not tested and why.

5 • FINDINGS SUMMARY

SEVERITY	COUNT
CRITICAL	
HIGH	
MEDIUM	
LOW	
INFO	

Each finding is ranked by real business risk and exploitability – severity alone does not drive priority.

6 • DETAILED FINDINGS

Each finding follows the same structure for reproducibility:

- **Title & ID** – unique reference, e.g., RED-001
- **Severity** – CRITICAL / HIGH / MEDIUM / LOW / INFO with CVSS score
- **Affected asset** – host, endpoint, or component
- **Description** – what the weakness is and why it matters
- **Reproduction steps** – exact steps to confirm
- **Evidence** – sanitized artifacts proving the finding (no live credentials or sensitive data)
- **Impact** – business and technical impact if exploited
- **Remediation** – concrete fix guidance with priority
- **References** – CWE / OWASP / vendor links where applicable

7 • RETEST RESULTS

- Status per finding after remediation: Resolved / Partially Resolved / Not Resolved / Not Retested.
- Retest window and method.
- Residual risk and recommended follow-up.

8 • APPENDIX

- Full scope confirmation (targets and dates).
- Tools and versions used.
- Engagement timeline and activity log summary.
- Evidence pack index.

9 • HANDLING & RETENTION

- This report is confidential under the NDA and for the named distribution only.
- Retained per the Rules of Engagement retention period, then securely destroyed.
- Re-disclosure only with written consent.