PlexTrac

PENTEST REPORT

(OUTLINE & SUMMARY)

PLEXTRAC FOR PENTEST REPORTING
EST. 2025
PENTEST REPORTING
BOOTCAMP
SECURE • STREAMLINE • STANDOUT

1: EXECUTIVE SUMMARY (CISO-FOCUSED)

- **Purpose & Objectives:** Clear explanation of why the pentest was conducted and what it aimed to assess.
- **High-Level Findings:** A summarized list of critical, high, and moderate risks across network and application layers.
- **Business Impact:** Explanation of how identified vulnerabilities could affect operations, data confidentiality, integrity, availability, compliance, and brand reputation.
- **Risk Scorecard:** Visual or tabular risk ratings using CVSS or a custom severity scale.
- **Recommendations Overview:** Strategic suggestions such as policy changes, funding needs, or security roadmap items.
- **Compliance Mapping (if applicable):** Relation of findings to standards like SOC 2, ISO 27001, PCI-DSS, etc.

2: SCOPE & METHODOLOGY (CROSS-AUDIENCE)

- **In-Scope Assets:** List of web applications, internal IP ranges, servers, endpoints, and APIs.
- **Out-of-Scope Items:** Anything deliberately excluded from testing (e.g., production databases, third-party services).
- **Testing Window:** Dates, times, and access granted.
- **Approach Used:**
  - Black-box, gray-box, or white-box
  - Manual vs. automated techniques
  - Tools and frameworks employed (e.g., Nmap, Burp Suite, Metasploit)
- **Rules of Engagement:** Constraints, authorization, and escalation procedures during testing.

3: NETWORK INFRASTRUCTURE FINDINGS (NETWORK ADMIN-FOCUSED)

- **Topology Overview:** Brief network architecture description relevant to discovered vulnerabilities.
- **Findings:**
  - Vulnerabilities/CVE’s
  - Misconfigurations (e.g., open ports, weak firewall rules)
  - Legacy systems or unpatched software
  - Internal lateral movement risks
  - Unencrypted protocols or poor segmentation
- **Risk Ratings:** CVSS scoring and potential business impact.
- **Proof-of-Concept:** Screenshots, command output, or payloads used to demonstrate issues.
- **Remediation Guidance:** Detailed steps aligned with best practices and minimal operational disruption.

4: WEB APPLICATION FINDINGS (DEVELOPER-FOCUSED)

- **Application Overview:** Tech stack, user roles tested, authentication/authorization flows.
- **Findings:**
  - Input validation flaws (e.g., SQLi, XSS)
  - Access control issues (IDOR, privilege escalation)
  - Authentication weaknesses (e.g., brute-force susceptibility, session mismanagement)
  - Business logic flaws
- **Risk Ratings:** Contextualized impact, especially in relation to data exposure and user trust.
- **Reproduction Steps:** Clear, developer-friendly steps to recreate the vulnerability.
- **Remediation Suggestions:** Secure coding practices, references (e.g., OWASP), and framework-specific advice.

5: REMEDIATION TRACKER / APPENDIX

- **Findings Matrix:** A consolidated table with ID, title, severity, asset, status (e.g., Open, Remediated, Risk Accepted).
- **Remediation SLA Recommendations:** Timeframes based on severity (e.g., critical within 7 days).
- **Appendices:**
  - Tool outputs (redacted as necessary)
  - Credential use (temporary accounts, if applicable)
  - Full list of URLs, IPs, and testing artifacts

FINAL NOTES:

The report should be **well-structured and modular**, enabling each stakeholder group to extract what they need without wading through irrelevant technical detail. It should be delivered in both **PDF** (for recordkeeping) and/or **HTML/XLS/CSV/interactive format** (for filtering and tracking).