# 05-Penetration-Testing-Report-Template

# Penetration Testing Report Template

*A professional report structure suitable for client-facing web application / infrastructure penetration test engagements.*

---

## Cover Page

- Client Name
- Engagement Name / Target Scope
- Report Version & Date
- Classification (e.g., Confidential)
- Author / Tester Name & Contact
- Reviewed/Approved By

## Document Control

| Version | Date | Author | Description |
|---|---|---|---|
| 0.1 | | | Draft |
| 1.0 | | | Final |

---

## 1. Executive Summary

- Brief, non-technical overview for leadership/stakeholders
- Engagement objective and business context
- High-level summary of findings and overall risk posture
- Summary table of findings by severity (Critical / High / Medium / Low / Informational)
- Key recommendations (top 3–5 priorities)

## 2. Engagement Overview

### 2.1 Scope

- In-scope assets (URLs, IP ranges, applications, API endpoints)
- Out-of-scope assets
- Testing type (Black-box / Grey-box / White-box)
- Testing window (start/end dates)

### 2.2 Methodology

- Standards followed (OWASP WSTG, PTES, NIST 800-115, OWASP ASVS)
- Testing phases: Reconnaissance → Scanning/Enumeration → Vulnerability Analysis → Exploitation → Post-Exploitation → Reporting
- Tools used (Burp Suite, Nmap, OWASP ZAP, custom scripts, etc.)

### 2.3 Rules of Engagement

- Authorized testing hours
- Emergency contacts

- Any restrictions (no DoS testing, no social engineering, production vs. staging)

## 3. Risk Rating Methodology

- Explanation of severity scale used (e.g., CVSS v3.1 base score mapped to Critical/High/Medium/Low/Info)
- Formula/criteria: Likelihood × Impact, or CVSS ranges:
  - Critical: 9.0–10.0
  - High: 7.0–8.9
  - Medium: 4.0–6.9
  - Low: 0.1–3.9
  - Informational: N/A

## 4. Summary of Findings

| # | Finding | Severity | CVSS | Status |
|---|---|---|---|---|
| 1 | | | | Open |
| 2 | | | | Open |

## 5. Detailed Findings

*(Repeat this structure for each finding)*

### Finding 5.X: [Title]

- **Severity:** Critical / High / Medium / Low / Informational
- **CVSS v3.1 Score & Vector:**
- **CWE Reference:**
- **Affected Component(s)/URL(s):**
- **Description:** Clear technical explanation of the vulnerability.
- **Proof of Concept:** Step-by-step reproduction, including requests/responses, screenshots, or payloads used.
- **Business Impact:** What this means in real terms (data loss, account takeover, financial/reputational impact).
- **Remediation:** Specific, actionable fix guidance (not generic advice).
- **References:** OWASP/CWE/vendor links.

## 6. Positive Security Observations

- Controls that were tested and found effective (builds credibility and balance)

## 7. Recommendations Roadmap

| Priority | Recommendation | Effort | Owner |
|---|---|---|---|
| Immediate | | | |
| Short-term (30 days) | | | |
| Long-term (90+ days) | | | |

## 8. Conclusion

- Overall security posture assessment
- Retest recommendation and timeline

## Appendix A — Tools & Versions Used

## Appendix B — Testing Timeline/Log

## Appendix C — Full Request/Response Evidence (if not inline)

## Appendix D — Glossary of Terms

---

### Tips for Use

- Keep the Executive Summary jargon-free — it's often the only section leadership reads.
- Always include reproducible PoC evidence; unverifiable claims undermine credibility.
- Tailor remediation advice to the client's actual tech stack, not generic boilerplate.
- Map findings to CWE and OWASP categories for consistency across engagements.