# 3. Reporting Practice

## Objective

The objective of this reporting practice was to develop the ability to **document penetration testing results in a structured, accurate, and actionable manner**, ensuring that both **technical teams** and **business stakeholders** clearly understand the identified risks, their impact, and the recommended remediation steps. Effective reporting bridges the gap between exploitation and risk reduction.

## Reporting Methodology

All findings were documented following **PTES-aligned reporting practices**, ensuring:

- Consistency in vulnerability documentation
- Clear risk prioritization using CVSS
- Actionable remediation guidance
- Audience-specific communication

## Report Template Structure

### 1. Executive Summary

The Executive Summary provides a **high-level overview** of the penetration test, written for senior management and non-technical stakeholders. It summarizes:

- Scope of testing
- Overall security posture
- Key high-risk findings
- Business impact and urgency

This section intentionally avoids technical terminology and focuses on **risk to the organization** rather than exploit mechanics.

**2. Technical Findings**

The Technical Findings section contains **detailed documentation of each vulnerability**, enabling developers and security teams to reproduce and remediate issues efficiently.

Each finding includes:

- Vulnerability name and classification
- Description and root cause
- Affected system or application component
- CVSS score and severity rating
- Proof of exploitation
- Security impact

This section serves as the **core technical evidence** of the penetration test.

**3. Remediation Plan**

The Remediation Plan provides **clear, prioritized corrective actions** mapped directly to each finding. Recommendations are written to be:

- Practical and implementable
- Aligned with secure coding standards
- Verifiable through retesting

Where applicable, remediation steps reference industry best practices such as **OWASP Secure Coding Guidelines**.

## Findings Table (Risk Summary)

| Finding ID | Vulnerability | CVSS Score | Severity | Remediation |
|---|---|---|---|---|
| F001 | SQL Injection | 9.1 | Critical | Use parameterized queries, validate input, apply least privilege to DB accounts |
| F002 | Weak Password Policy | 7.5 | High | Enforce strong password complexity, implement rate limiting and account lockout |

## Detailed Finding Explanation

### F001 – SQL Injection

**Description:**
The application fails to properly sanitize user-supplied input before using it in SQL queries. This allows attackers to manipulate backend queries and bypass authentication mechanisms.

**Impact:**
An attacker can access sensitive database information, bypass login controls, and potentially gain administrative access.

**Remediation:**
Implement prepared statements, enforce strict server-side input validation, and conduct regular code reviews to identify insecure query handling.

## Visualization: Network Attack Path Diagram (Draw.io)

A **network attack path diagram** was created using Draw.io to visually represent:

1. Attacker entry point (web application)
2. Exploitation of input validation weakness

3. Authentication bypass
4. Access to sensitive backend resources

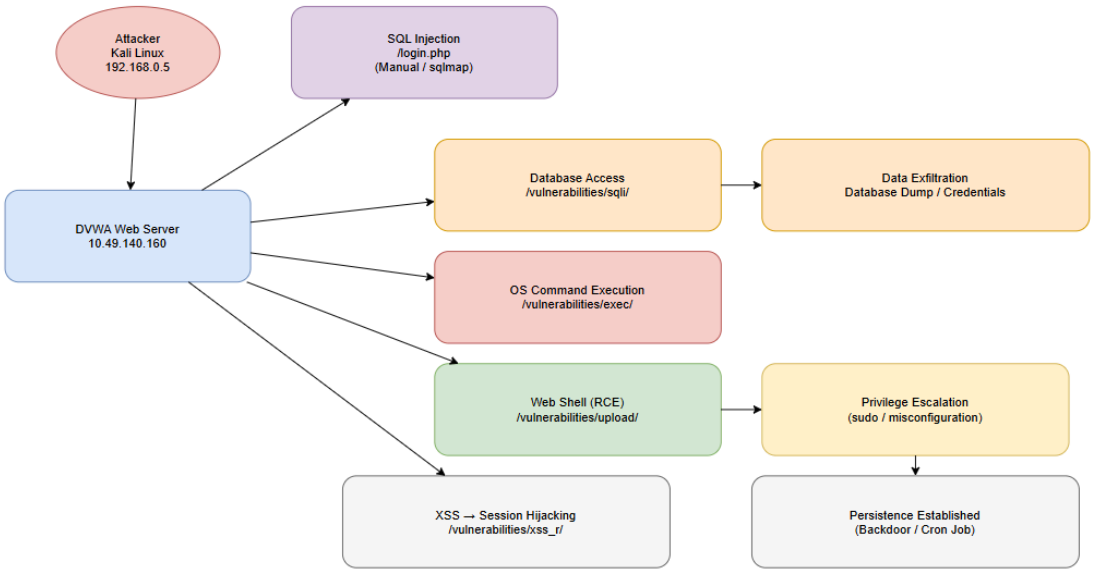


*Figure 3: Attack Path Diagram*

This visual aid helps stakeholders quickly understand **how vulnerabilities are chained** and why individual weaknesses pose systemic risk.

## Reporting Metrics & Risk Prioritization

To support risk-based decision making, the following metrics were emphasized:

- Number of vulnerabilities by severity
- Presence of exploitable critical flaws
- Likelihood of real-world exploitation
- Potential business impact

These metrics assist management in prioritizing remediation efforts.

**Document Information:**

Report Generated: December 19, 2025

Author: Soumendu Manna - CyArt VAPT Intern