# TECHNICAL COMPLIANCE REVIEW

# REPORT



**MITRA INTEGRASI INFORMATIKA**

**PT. TOYOTA MOTOR MANUFACTURING INDONESIA**

📞 (62-21) 29345 777

✉ contact@mii.co.id

🌐 www.mii.co.id

CONSULTING ADVISORY SERVICES

# Contents

# 1 Project Overview

## 1.1 Description

TECH COMP REV '

'

## 2 Executive Summary

A penetration test report executive summary is a document that states the findings of a penetration test in a clear and concise way. The purpose of this summary is to provide management with a high-level overview of the test, so they can decide whether or not to pursue further action.

Disclaimer: This article is intended to assist our institute's students in writing penetration testing reports. The example offered is not factual, and it has been simplified for educational reasons to provide clear and straightforward instructions. Example

The findings of a penetration test conducted on ABC Hospital's network on March 1, 2019 are summarized in this report. A team of skilled security consultants from XYZ Security conducted the test.

A security penetration test is a simulated cyber-attack on a computer system or network. The goal of this test is to identify and exploit vulnerabilities in the system in order to assess the system's security posture. Penetration tests are an important part of a comprehensive security strategy and can help organizations identify and fix vulnerabilities before they are exploited by attackers.

Key Findings:

XYZ Security discovered various flaws that may be exploited by a malicious actor. The most important findings were:

```
1   A vulnerability in the firewall that could allow an attacker to gain access to the network
        from the Internet
2
3   A vulnerability in the web server that could allow an attacker to gain access to sensitive
        data
4
5   A vulnerability in the authentication system that could allow an attacker to gain access
        to user accounts
6
7   A vulnerability in the email server that could allow an attacker to spoof emails
```

These flaws could lead to serious breaches of confidentiality and integrity if they are exploited. Unauthorized access to personal identity information, patient information, and medical data would be gained by adversaries.

The consequences of a major cyber breach caused by these flaws could include lawsuits and financial losses. In one situation, XYZ Security could tamper with the real-time flow of medical information. The effects of a real-world attack could put patients' health at danger.

### 2.1 Summary of Findings Identified

Executive Summary

Breakdown by Categories

**# 1 Critical** SQLI

**# 2 Critical** CELAH KERENTANAN PADA SERVER BSSN

## 2.2  Scope

### 2.2.1  In Scope

TBC

### 2.2.2  Out of Scope

Based on the project scope example above, the following requests from the client would be out of scope rather than in scope:

```
1  Creating a QR code to add to marketing materials to make the app easy for customers to
      download
2  Publishing the finished app to the app store
3  Developing a second app for XYZ, Inc. to use for their in-house HR functions
4  Producing an email marketing campaign to spread the word about the app
```

Even if Company ABC offers the services named in the above out of scope examples, they do not fit the definition of in scope set by the project scope example. A project manager would need to explain this to the client and then refer them to the appropriate team within Company ABC that can handle that request.

## 2.3  Methodology

Penetration Testing Methodologies and Standards

There are various standards and methodologies that ensure the penetration test is authentic and covers all important aspects. Some of them are mentioned below:

```
1   OSSTMM
2   OWASP
3   NIST
4   PTES
5   ISSAF
```

What is OSSTMM?

OSSTMM is short for Open-Source Security Testing Methodology Manual. It is one of the most widely used and recognized standards of penetration testing. It's based on a scientific approach to penetration testing that contains adaptable guides for testers. You can use this to conduct an accurate assessment. What is OWASP?

OWASP stands for Open Web Application Security Project. Widely known, this standard is developed and updated by a community keeping in trend with the latest threats. Apart from application vulnerabilities, this also accounts for logic errors in processes. What is NIST?

National Institute of Standards and Technology (NIST) offers very specific penetration testing guidelines for pentesters to help them improve the accuracy of the test. Both large and small companies, in various industries, can leverage this framework for a penetration test. What is PTES?

PTES or Penetration Testing Execution Standards is a pentest methodology designed by a team of information security professionals. The goal of PTES is to create a comprehensive and up-to-date standard for penetration testing as well as to build awareness among businesses as to what to expect from a pentest.

## 2.4  Recommendations

Recommendations

Purpose: Guide the organization in fixing the identified issues before they can cause damage.

You can add your recommendations to the previous section. However, it's best to create a separate section because it will help readers see the way forward clearly.

Make sure to avoid generic suggestions – they are rarely helpful. Instead, write detailed and specific remediations that help developers fix issues and ideally achieve Defense-in-Depth. Also, use action words, like install, upgrade, or implement, to minimize confusion and encourage action. Conclusion

Purpose: Clarify the next steps.

The Conclusion section wraps up your report and includes the planned or in-progress steps.

For example, you could say any or all of the following:

```
1   X vulnerabilities were found and need to be addressed by..
2   To finalize this report, the risk score must be completed.
3   A retest is scheduled for Y to verify if remediations were completed and ensure compliance
        with this report.
```

## 3  Findings and Risk Analysis

### 3.1  SQLI

**Severity:** Critical
**CVSS Score:** 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**CWE**

89 - Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

**Description**

blabla

**Location**

TBC

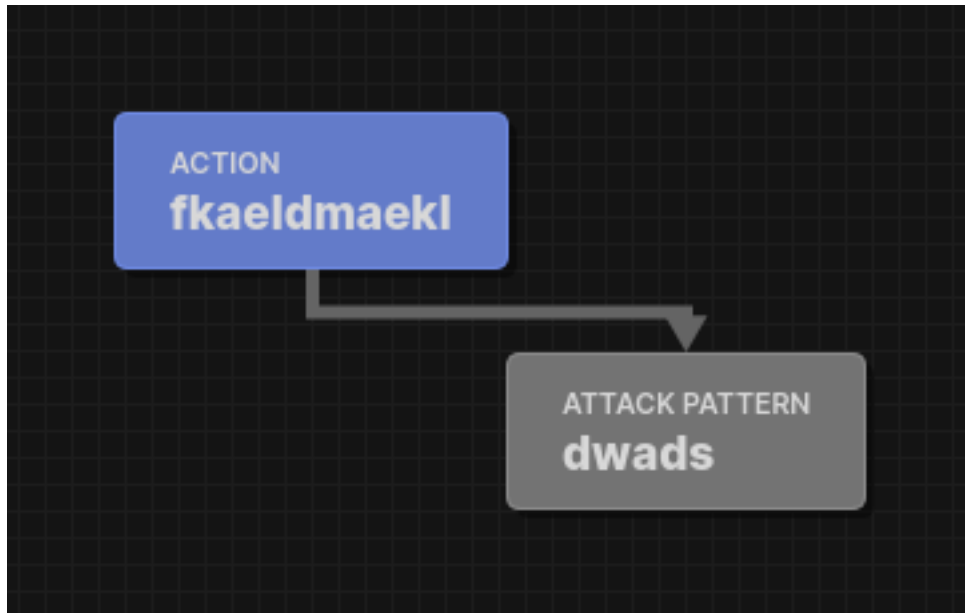**Impact**

TBC

**Recommendation**

TBC

**References**

TBC

**Attack Flow**

Untitled Document



**Figure 1:** Untitled Document

## 3.2  CELAH KERENTANAN PADA SERVER BSSN

**Severity:** Critical
**CVSS Score:** 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

**CWE**

0 - Insufficient Information

**Description**

ENGINEER COPO

**Location**

DATA CENTER

**Impact**

SERVER DOWN

**Recommendation**

REKRUT KAMI!

**References**

SUROSOWANCYBER.ORG

## 4  Additional Notes