QUALIZEAL

Presented by Mahendra Y N
Date: 30-Nov-23

Security Testing Measurement Framework.

A comprehensive toolkit to depict the security posture for the target under test.

Contents.

Introduction.

Purpose

This document aims to establish a comprehensive measurement framework for security testing, providing operational definitions for metrics and indicators for informed decision-making regarding new releases.

Context

Independent security testing teams play a pivotal role in exhaustive testing, offering insights crucial for customers when deciding on new apps or planned releases. This paper outlines a set of measures and metrics that have proven instrumental in facilitating these decisions.

Approach

In the process of Vulnerability Assessment and Penetration Testing (VAPT) and other security testing methodologies, we systematically map phase-based data points to gauge the extent of vulnerabilities and associated risks. We use the industry standard Common Vulnerability Scoring System (CVSS) tool to provide an ongoing view of overall security posture during testing.

One limitation that we face with the existing CVSS tool (v3.1) is that it does not address the risk factor which is one of the primary goals of security testing. We need to show how security testing can reduce the risk exposure for the customer. To address this key requirement, we extended the tool to include an assessment of threat.

Our approach involves utilizing the Common Vulnerability Scoring System (CVSS) metrics, extending the interpretation by considering the likelihood of threats and their potential impact on confidentiality, integrity, and availability.

This fine tuning provides an extra level of insight with the data that we are already collecting as part of the tool.

While this measurement framework is not foolproof, it significantly enhances the depth of security testing reporting and data analysis, providing a multifaceted view of the target under test (application or network).

Terms and Definitions.

- CVSS - an open framework for communicating the characteristics and severity of software vulnerabilities.
- Base metrics - these represent the intrinsic qualities of a vulnerability that is constant over time and across the environments. Calculated as per CVSS tool.
- Temporal metrics - these reflect the qualities of a vulnerability that change over time. Calculated as per CVSS tool.
- Environmental metrics - characteristics of a vulnerability that are unique to a user's environment. Calculated as per CVSS tool.

Security Testing Measurement Framework.

Objective

The primary objective of the security testing measurement framework is to establish a systematic approach for evaluating and reporting effectiveness and efficiencies of security testing. This framework aims to provide quantitative and qualitative insights into the security posture of the target under test.

Below image depicts the various metrics and measures that are captured and reported during the security testing phase.

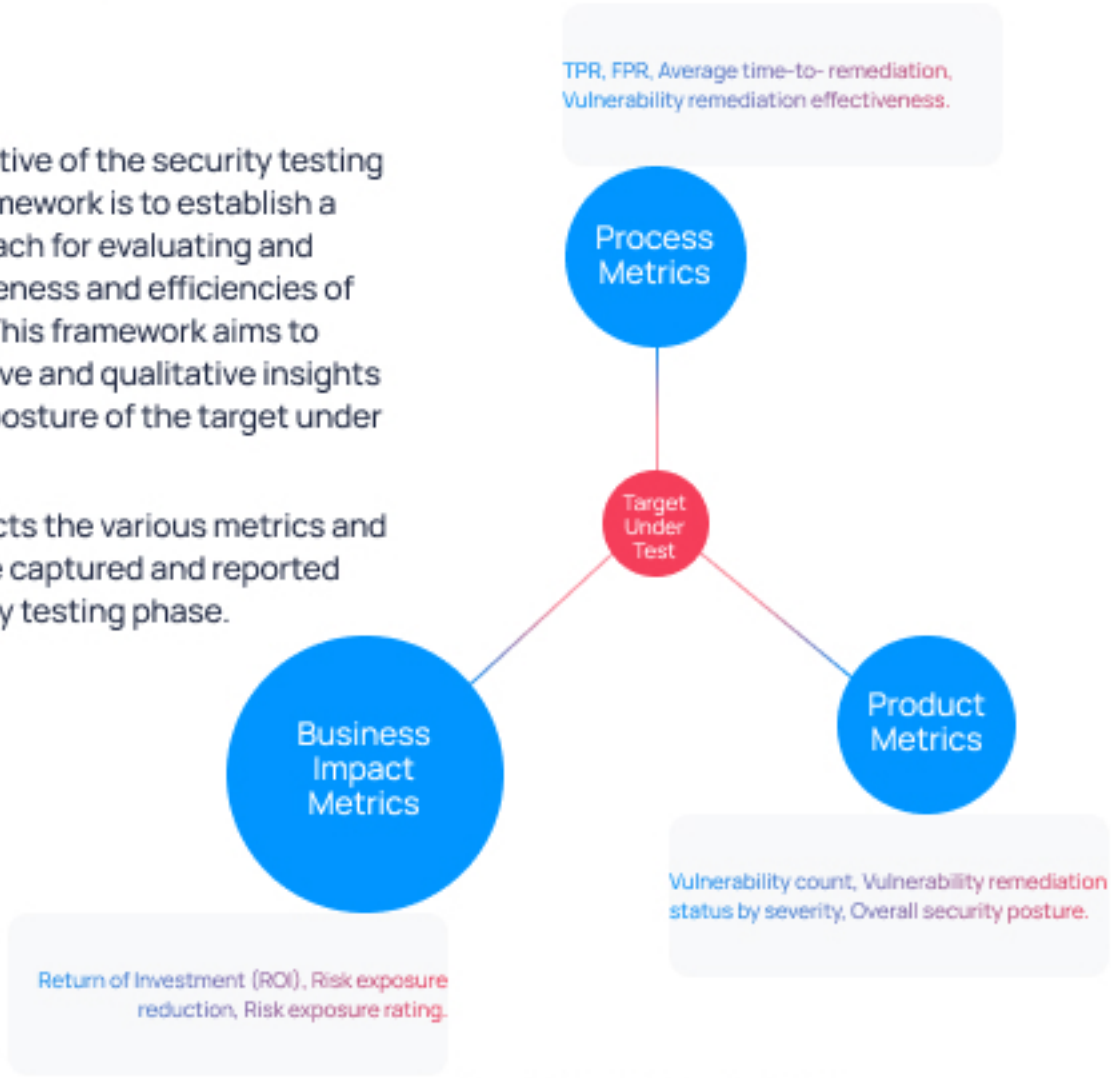


Figure 1: Security Testing Metrics

Key Metrics

False Positive Rate (FPR)

Metric: Percentage of vulnerabilities marked as "false positive" of all vulnerabilities reported.

Purpose: To know how effective the tool is in identifying valid vulnerabilities. Helps to strategize the testing approach.

True Positive Rate (TPR)

Metric: Percentage of vulnerabilities marked as "true positive" of all vulnerabilities reported.

Purpose: To know how effective the tool is in identifying valid vulnerabilities. Helps to strategize the testing approach.

Vulnerability count

Measure: The count of "true positive" vulnerabilities reported for the system under test.

Purpose: To know the extent of vulnerabilities found as part of testing. Helps to plan the number of testing cycles required and when to stop testing.

Vulnerability remediation status by severity

Measure: The open versus closed status of vulnerabilities shown by severity.

Purpose: To show open versus closed vulnerabilities status by severity. Helps to plan the number of testing cycles required and when to stop testing.

Average Time-to-remediation

Measure: Average number of days taken to fix "true positive" vulnerabilities.

Purpose: To know how much time is spent to fix a vulnerability. Helps in planning resource allocation and release/no release decision.

Vulnerability Remediation Effectiveness

Metric: Percentage of "closed" vulnerabilities from the total "true positive" vulnerabilities found.

Purpose: To know how many of the total vulnerabilities are fixed. Helps in planning resource allocation and release/no release decision.

Risk Exposure Reduction

Metric: Percentage of overall reduction in risk score post-remediation.

Purpose: To know how much of the risk the company is able to contain from the previous cycle. Helps to identify any negative impact of fix or new functionality issue.

Return on Investment (ROI)

Metric: Percentage of total cost of return on the total cost of testing.

Purpose: To know how much organization saves by investing in detecting vulnerabilities before release. Also, helps to know when the application is reaching a stable point.

Key Indicators

Overall Security Posture Score

Indicator: The average of Base, Temporal and Environment Metrics as per CVSS tool.

Purpose: A one point indicator of current application security posture based on vulnerability. Helps in release/no release decision.

Risk Exposure Rating

Indicator: A weighted index based on the likelihood and impact of the possible threats to identified vulnerabilities.

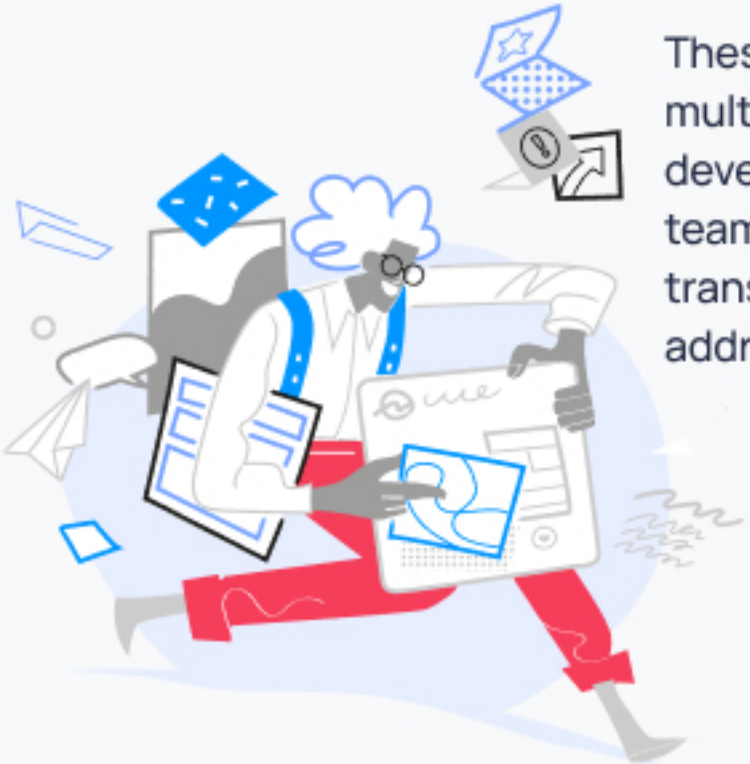
Purpose: To know how much of a risk the company will face with the current state of vulnerability. Helps in release/no release decision.

Reporting and Review

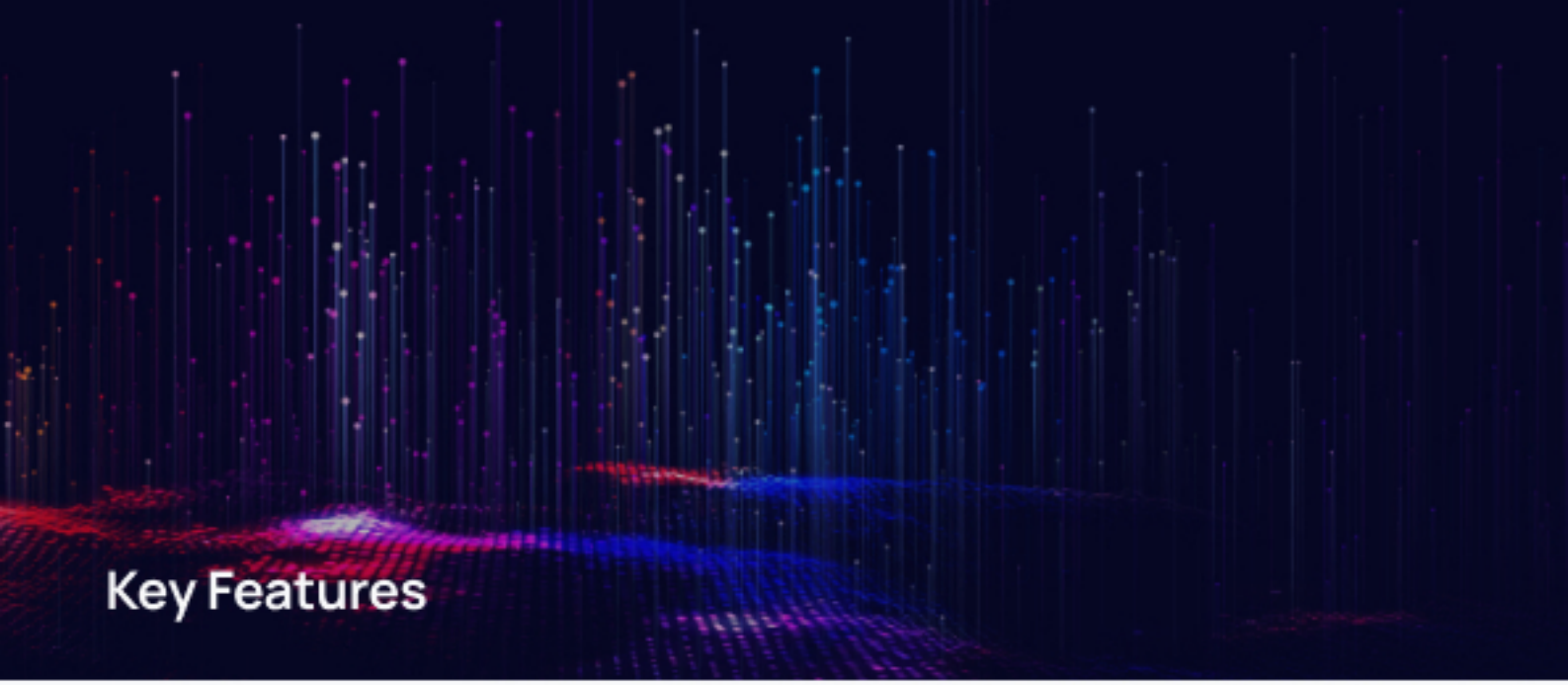
There are two supporting templates, Vulnerability Scoring Sheet, and Executive Metric sheets, to provide comprehensive reporting based on the above-mentioned metrics across multiple testing cycles.

Vulnerability Scoring Data

Dashboard



These reports can be provided to multiple stakeholders, including development teams, security teams, and leadership, to ensure transparency and collaboration in addressing security concerns.



Key Features

The proposed security testing metrics framework builds on the industry best practices and standards. These metrics are essential to monitor and report security testing results, optimize resources in real time, improve processes, showcase performance, and facilitate decision making that align with business objectives.

Unmatched Comprehensiveness-

While CVSS primarily focuses on the technical aspects of vulnerabilities, metrics, such as "Vulnerability Remediation Status" and "Vulnerability Remediation Effectiveness," bring in the crucial element of remediation progress and effectiveness. This adds a layer of comprehensiveness by considering the lifecycle of vulnerabilities.

Strategic Business Context-

Metrics like "Return on Investment" and "Risk Exposure Reduction" go beyond the technical realm and bring in a business-oriented perspective. This aligns security efforts with overall business goals, a critical need in today's interconnected and business-driven landscape.

Precision in Accuracy Assessment-

Metrics like "False Positive Rate" and "True Positive Rate" address the accuracy of security testing, ensuring that the information provided is reliable. While CVSS provides a standardized approach, it may not inherently include these accuracy-checking elements.

Efficient Resource Optimization-

In an environment where cybersecurity teams often face resource constraints, having insights into the effectiveness of remediation efforts is invaluable for optimizing the use of available resources.

Conclusion.

The proposed security testing metrics and reporting framework addresses a spectrum of challenges in security testing—from initial identification and prioritization to ongoing remediation efforts and the business impact of security measures. This broader perspective is beneficial for organizations looking to not only identify and prioritize vulnerabilities but also actively manage and mitigate security risks. It reflects a more comprehensive understanding of security that aligns with both technical and business objectives.

The proposed reporting framework contributes to advancing the maturity of the cybersecurity industry, aligning it with broader organizational objectives and empowering organizations to stand resilient in the face of ever-evolving cyber threats. It represents a proactive and strategic approach that positions cybersecurity as an integral component of overall business strategy.

In summary, this approach goes beyond the traditional CVSS scoring methodology by incorporating metrics that span the entire vulnerability lifecycle, consider business impact, assess accuracy and efficacy, and provides invaluable insights for the return of investment in security testing.