Security Testing Measurement Framework.

Contents.

Introduction.

Purpose

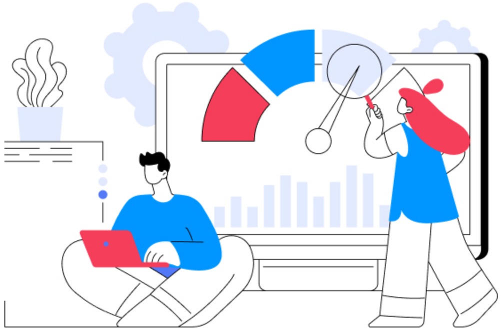
The purpose of this document is to provide a detailed security testing measurement framework that guides the application security testing team to identify, analyze, and report relevant measures and metrics. This guide can facilitate the teams in selecting metrics based on the testing cycles and reporting needs at multiple levels of the application development cycle and ongoing maintenance.

Context

In its annual assessment of cloud security threats, Thales surveyed nearly 3,000 IT and security professionals across 18 countries, providing valuable insights into the current landscape.

> "The study reveals compelling statistics that underscore the critical need for robust application security testing frameworks."

References:



1. Increasing Cloud Data Breaches

Last year, 39% of businesses experienced a data breach in their cloud environment, marking a notable increase from the 35% reported in 2022. This trend emphasizes the growing challenges and vulnerabilities present in cloud ecosystems.

2. Human Error as a Major Factor

The study identifies human error as the leading cause of cloud data breaches, with 55% of respondents attributing security incidents to this factor. This highlights the importance of addressing human-related vulnerabilities through comprehensive security measures.

3. Sensitivity of Cloud-Stored Data

A significant revelation is that 75% of businesses reported that more than 40% of data stored in the cloud is classified as sensitive. This emphasizes the criticality of safeguarding sensitive information and the need for heightened security measures.

4. Targeted Areas for Hackers

The study found that Software as a Service (SaaS) applications (38%) and cloud-based storage (36%) are the top targets for hackers. These insights underscore the necessity for a focused approach to securing these specific areas in cloud environments.

> "In light of these findings, the statistics underscore the urgency for organizations to adopt robust application security testing frameworks."

Such frameworks become imperative tools for identifying and mitigating vulnerabilities, safeguarding against human error, and ensuring the security of sensitive data stored in the cloud. By prioritizing security measures and addressing specific areas vulnerable to cyber threats, businesses can proactively enhance their overall security posture.

As more and more applications move to the cloud, there is a need to ensure that apps are more secure than ever. Independent security testing teams will need to provide insights into their testing process as well as the target under test. Only with such reports can application owners make timely decisions and have enough confidence to release apps.

Approach

As an independent security testing team, we perform **Vulnerability Assessment and Penetration Testing (VAPT)**. To create the measurement framework, we looked at our data needs with respect to vulnerabilities and associated risks across the areas of product, process, and business. This provided a basic outline for reporting and along with the industry standard **Common Vulnerability Scoring System (CVSS)** tool, we were able to provide an ongoing view of overall security posture during testing to our customers who are looking to get the security assessment of their applications.

Though CVSS tool v3.1 could be used to score the vulnerabilities, getting holistic metrics like vulnerability remediation effectiveness and overall risk exposure reduction was difficult. There seemed a need to demonstrate how security testing reduced the risk exposure for our customers.

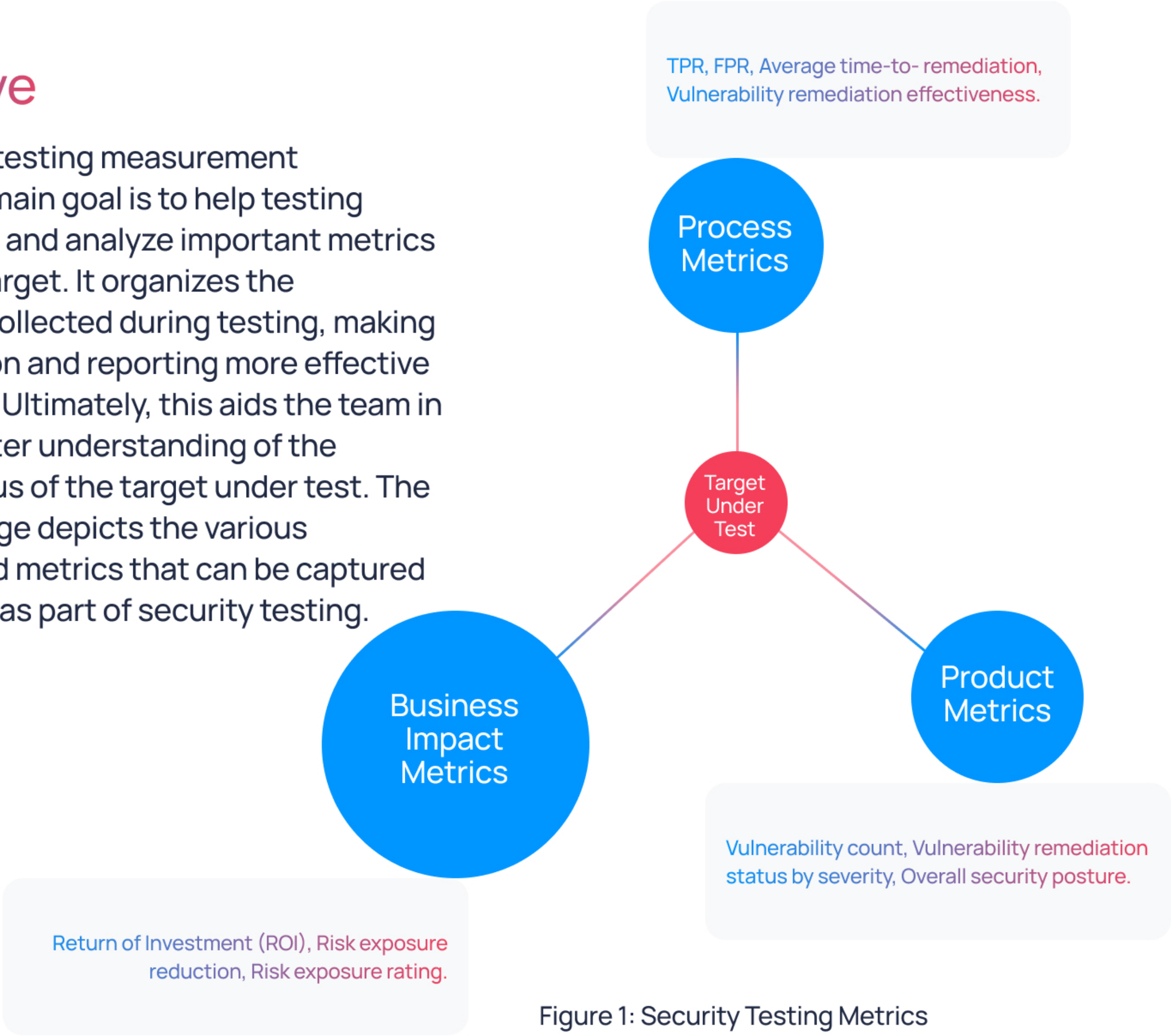
Terms and Definitions.

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

Security Testing Measurement Framework.

Objective

The security testing measurement framework's main goal is to help testing teams gather and analyze important metrics about their target. It organizes the information collected during testing, making data collection and reporting more effective and efficient. Ultimately, this aids the team in gaining a better understanding of the security status of the target under test. The following image depicts the various measures and metrics that can be captured and reported as part of security testing.



TPR, FPR, Average time-to- remediation, Vulnerability remediation effectiveness.

Vulnerability count, Vulnerability remediation status by severity, Overall security posture.

Return of Investment (ROI), Risk exposure reduction, Risk exposure rating.

Figure 1: Security Testing Metrics

Key Metrics

The framework used the following metrics to collectively contribute to a comprehensive understanding of the security landscape, guide prioritization of security efforts, and enable organizations to make informed decisions to enhance their overall security posture.

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.

Benefit: Helps in minimizing wasted time and resources by identifying and reducing false alarms. A lower FPR means more accurate identification of genuine security issues.

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.

Benefit: Measures the effectiveness of the testing process or tool in correctly identifying actual vulnerabilities. A higher TPR indicates a more reliable security testing process.

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.

Benefit: Provides a quantitative measure of the security posture. Monitoring changes in vulnerability count over time helps assess the effectiveness of security measures and identify trends.

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.

Benefit: Allows prioritization of efforts by focusing on addressing the most critical vulnerabilities first. Helps in strategic planning for risk mitigation.

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.

Benefit: Measures the efficiency of the remediation process. A lower time-to-remediation indicates quicker responses to security issues, reducing the window of potential exploitation.

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.

Benefit: Assesses the success of the remediation efforts. Monitoring how well vulnerabilities are addressed provides insights into the overall security improvement.

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.

Benefit: Quantifies the reduction in potential risk as vulnerabilities are addressed. Offers a holistic view of the impact of security measures on overall risk exposure.

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.

Benefit: Evaluates the cost-effectiveness of security efforts. It helps organizations understand the value they gain from investing in security measures, considering both the cost of implementation and the reduction in potential damages.

Key Indicators

Overall Security Posture Score

The Overall Security Posture Score is a composite metric that provides a consolidated view of the applications under test for an organization. It considers various aspects of security testing, vulnerability management, and risk mitigation efforts. It is an indicator of the average of Base, Temporal, and Environment Metrics as per CVSS tool. Acting as a single-point indicator of current application security posture based on vulnerability, it helps in making release or no-release decisions.

Some of the key benefits are:

- **Simplicity:** Offers a single, easy-to-understand metric that summarizes the overall security health.
- **Benchmarking:** Enables organizations to track changes in security posture over time and compare scores against industry benchmarks.
- **Communication:** Facilitates communication between security teams and leadership by presenting a high-level overview of security effectiveness.

Risk Exposure Rating

The Risk Exposure Rating quantifies the level of risk an organization faces based on the severity and prevalence of vulnerabilities in their applications/infrastructure. It helps prioritize remediation efforts by focusing on the most critical issues. It is an indicator of a weighted index based on the likelihood and impact of the possible threats to identified vulnerabilities. It quantifies the magnitude of risk the company will face with the current state of vulnerability. This indicator also helps in making release or no-release decisions.

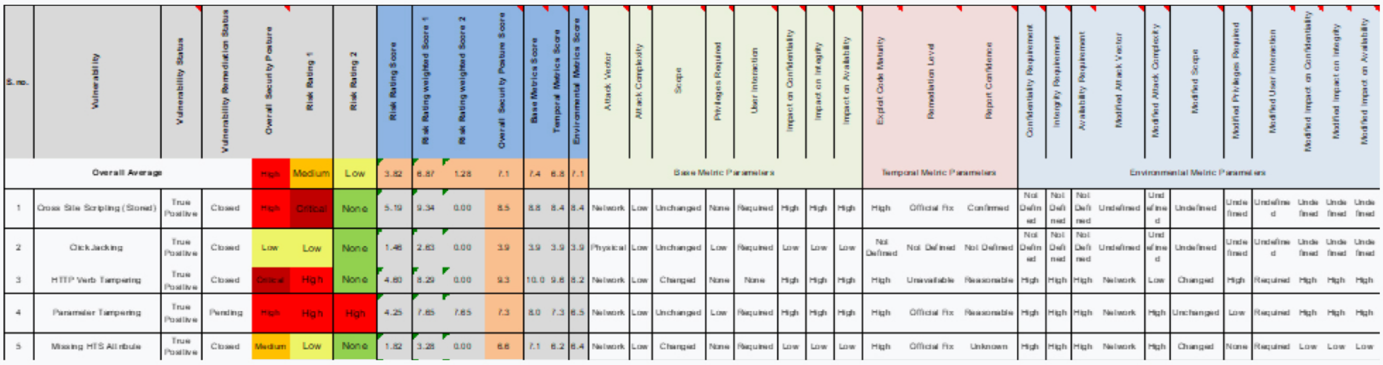
Some of the key benefits are:

- **Prioritization:** Guides organizations in prioritizing remediation efforts based on the potential impact of vulnerabilities.
- **Resource Allocation:** Helps allocate resources more effectively by addressing high-risk vulnerabilities first.
- **Decision Support:** Assists in making informed decisions about risk acceptance, mitigation, or transfer by providing a clear understanding of the overall risk exposure.

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

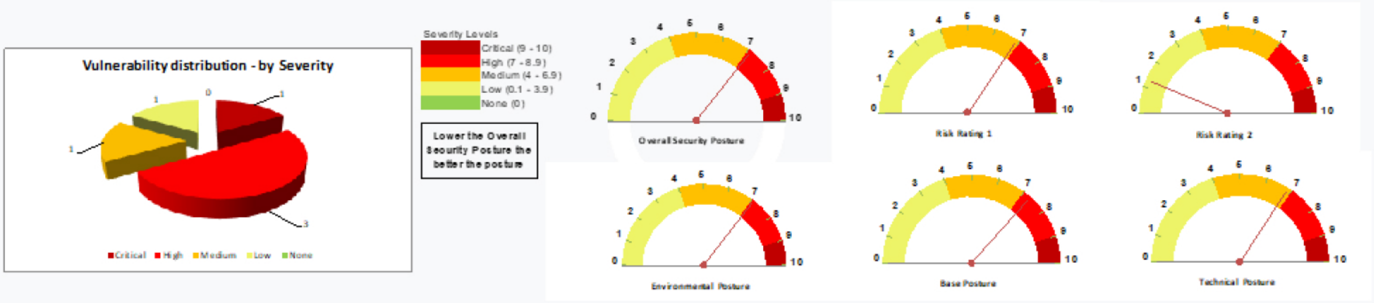


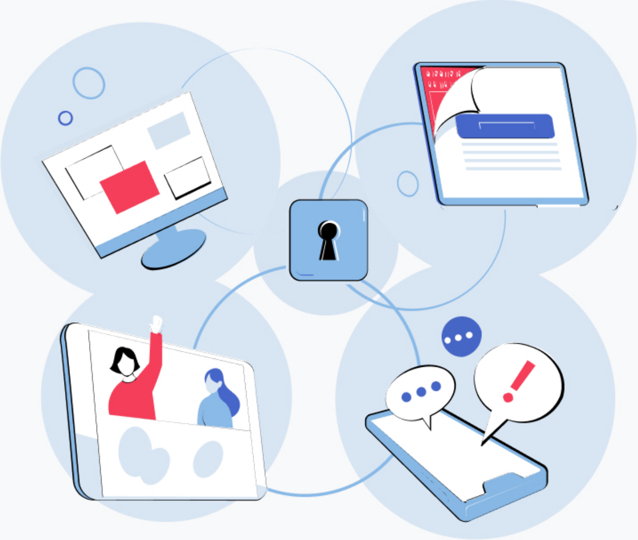
S. no.	Vulnerability	Vulnerability Status	Vulnerability Remediation Status	Overall Security Posture	Risk Rating 1	Risk Rating 2	Risk Rating Score	Risk Rating weighted Score 1	Risk Rating weighted Score 2	Overall Security Posture Score	Base Metrics Score	Temporal Metrics Score	Environmental Metrics Score
	Overall Average			High	Medium	Low	3.82	6.87	1.28	7.1	7.4	6.8	7.1
1	Cross Site Scripting (Stored)	True Positive	Closed	High	Critical	None	5.19	9.34	0.00	8.5	8.8	8.4	8.4
2	Click Jacking	True Positive	Closed	Low	Low	None	1.46	2.63	0.00	3.9	3.9	3.9	3.9
3	HTTP Verb Tampering	True Positive	Closed	Critical	High	None	4.60	8.29	0.00	9.3	10.0	9.8	8.2
4	Parameter Tampering	True Positive	Pending	High	High	High	4.25	7.65	7.65	7.3	8.0	7.3	6.5
5	Missing HTS Attribute	True Positive	Closed	Medium	Low	None	1.82	3.28	0.00	6.6	7.1	6.2	6.4

S. no.	Attack Vector	Attack Complexity	Scope	Privileges Required	User Interaction	Impact on Confidentiality	Impact on Integrity	Impact on Availability	Exploit Code Maturity	Remediation Level	Report Confidence
	Base Metric Parameters								Temporal Metric Parameters		
1	Network	Low	Unchanged	None	Required	High	High	High	High	Official Fix	Confirmed
2	Physical	Low	Unchanged	Low	Required	Low	Low	Low	Not Defined	Not Defined	Not Defined
3	Network	Low	Changed	None	None	High	High	High	High	Unavailable	Reasonable
4	Network	Low	Unchanged	Low	Required	High	High	High	High	Official Fix	Reasonable
5	Network	Low	Changed	None	Required	Low	Low	Low	High	Official Fix	Unknown

S. no.	Confidentiality Requirement	Integrity Requirement	Availability Requirement	Modified Attack Vector	Modified Attack Complexity	Modified Scope	Modified Privileges Required	Modified User Interaction	Modified Impact on Confidentiality	Modified Impact on Integrity	Modified Impact on Availability
	Environmental Metric Parameters										
1	Not Defined	Not Defined	Not Defined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined
2	Not Defined	Not Defined	Not Defined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined	Undefined
3	High	High	High	Network	Low	Changed	High	Required	High	High	High
4	High	High	High	Network	High	Unchanged	Low	Required	High	High	High
5	High	High	High	Network	High	Changed	None	Required	Low	Low	Low

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 security testing metrics framework builds on the industry's 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 aligns with business objectives.

Comprehensiveness-

While CVSS primarily focuses on the vulnerability of the application/system under test and its severity, we have included process metrics of "Vulnerability Remediation Status" and "Vulnerability Remediation Effectiveness" that extend the visibility to the closure of identified vulnerabilities.

Business Context-

Metrics of "Return on Investment" and "Risk Exposure Reduction" bring in the impact on business due to the identified vulnerabilities and the investment in security testing. This helps align security efforts with overall business goals with the need of continuous quick releases.

Accuracy Assessment-

Metrics of "False Positive Rate" and "True Positive Rate" highlight the accuracy of security testing, ensuring that the information provided is reliable.

Resource Optimization-

The process and business metrics hold the key to real-time decisions on testing strategy and resource allocation. With these metrics, testing teams and customers can plan and optimize testing resources to ensure that the system under test is indeed secure for release.

Conclusion.

The proposed security testing metrics and reporting framework addresses several challenges in security testing. It enables teams to provide insights into the identification and prioritization of vulnerabilities, the remediation process, and the business impact of overall security testing. The stakeholders benefit by having a complete picture of the target under test, the quality of the security testing process, and the impact of the business decisions. The framework is not just vulnerability-driven but is also risk-driven so the teams can collaborate and actively assess and manage associated risks.

As we work with multiple customers and scenarios, the independent security testing teams can build on these additional aspects of process and business metrics to create a collection of measures and metrics that can give deep insights into security testing. This will ensure that testing teams and customers work in tandem to achieve business objectives while successfully addressing ever-evolving cyber threats.

In conclusion, we encourage independent security testing teams to enhance their existing metrics dashboard to provide visibility into the entire vulnerability lifecycle, security testing process, and risk assessment to meet business objectives. This will not only strengthen efforts towards building the security testing baselines, and support customer business objectives but also build secure applications and networks for end users.