A vulnerability assessment can detect the maximum number of security defects in a given timeframe. It involves both manual and automated techniques. You can target different layers of technology, such as host, network, and application layers.

In short, vulnerability testing can help identify flaws and vulnerabilities in software before a compromise takes place. You can ensure a systematic review of your software for security weaknesses.

Vulnerability assessment has three essential goals:

• evaluates if the system is susceptible to any vulnerabilities.

• assign severity levels to those vulnerabilities.

• recommend remediation or mitigation depending on the vulnerability.

## Types of vulnerability assessments

There are several types of vulnerability assessment:

### Host assessment

It is the assessment of critical servers that can be vulnerable to attacks. Thus, it prevents those parts of your system, which may be a victim of attack if not tested adequately.

### Network and wireless assessment

It prevents unauthorized access to public or private networks and network-accessible resources.

### Database assessment

It assesses databases or big data systems for vulnerabilities and misconfiguration. It classifies sensitive data across an organization’s infrastructure.

### Application scans

It is to identify security vulnerabilities in web applications.

## How it works

There are various forms of vulnerability testing. One form is dynamic application security testing, and the other is static application testing. Both approach the system with different methodologies. Similarly, they are effective at different levels of the software development life cycle.

### Dynamic application security testing

DAST analysis the security defects by providing inputs. In this approach, an outside-in testing approach helps you detect security vulnerabilities.

### Static application testing

SAST is for analysis of source code. You can detect critical vulnerabilities such as cross-site scripting and SQL injection. These usually take place in the early stages of SDLC.

## Security scanning process

The security scanning process involves four steps:

• testing

• analysis

• assessment

• remediation

### Vulnerability testing

The goal of this step is to evaluate application vulnerabilities with the help of automated tools.

### Vulnerability analysis

In this step, the root cause of vulnerabilities is found. It further involves the identification of system components that are responsible for causing the vulnerabilities.

### Risk assessment

In this step, priorities are set for each vulnerability. Security analyst ranks the vulnerabilities based on various factors.

### Remediation

Finally, in these steps, the security gaps are closed. It requires security staff, operation teams, and development teams who determine the best path of remediation.

## Conclusion

It is best if you practice vulnerability assessment tests regularly to keep your system safe.