<https://www.imperva.com/learn/application-security/vulnerability-assessment/>

**Vulnerability Assessment**

49.5k views

[App Security](https://www.imperva.com/learn/application-security/)Essentials

**What is vulnerability assessment**

A [vulnerability](https://www.imperva.com/learn/application-security/vulnerability-management/) assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Examples of threats that can be prevented by vulnerability assessment include:

1. [SQL injection](https://www.imperva.com/learn/application-security/sql-injection-sqli/), [XSS](https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/) and other code injection attacks.
2. Escalation of privileges due to faulty authentication mechanisms.
3. Insecure defaults – software that ships with insecure settings, such as a guessable admin passwords.

There are several types of vulnerability assessments. These include:

1. **Host assessment** – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
2. **Network and wireless assessment** – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
3. **Database assessment** – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization’s infrastructure.
4. **Application scans** – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

**Vulnerability assessment: Security scanning process**

The security scanning process consists of four steps: testing, analysis, assessment and remediation.



**1. Vulnerability identification (testing)**

The objective of this step is to draft a comprehensive list of an application’s vulnerabilities. Security analysts test the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually. Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and [threat intelligence](https://www.imperva.com/learn/application-security/threat-intelligence/) feeds to identify security weaknesses.

**2. Vulnerability analysis**

The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one.

It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability. For example, the root cause of a vulnerability could be an old version of an open source library. This provides a clear path for remediation – upgrading the library.

**3. Risk assessment**

The objective of this step is the prioritizing of vulnerabilities. It involves security analysts assigning a rank or severity score to each vulnerability, based on such factors as:

1. Which systems are affected.
2. What data is at risk.
3. Which business functions are at risk.
4. Ease of attack or compromise.
5. Severity of an attack.
6. Potential damage as a result of the vulnerability.

**4. Remediation**

The objective of this step is the closing of security gaps. It’s typically a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.

Specific remediation steps might include:

1. Introduction of new security procedures, measures or tools.
2. The updating of operational or configuration changes.
3. Development and implementation of a vulnerability patch.

Vulnerability assessment cannot be a one-off activity. To be effective, organizations must operationalize this process and repeat it at regular intervals. It is also critical to foster cooperation between security, operation and development teams – a process known as [DevSecOps](https://www.csoonline.com/article/3245748/devops/what-is-devsecops-developing-more-secure-applications.html).

**Vulnerability assessment tools**

Vulnerability assessment tools are designed to automatically scan for new and existing threats that can target your application. Types of tools include:

1. Web application scanners that test for and simulate known attack patterns.
2. Protocol scanners that search for vulnerable protocols, ports and network services.
3. Network scanners that help visualize networks and discover warning signals like stray IP addresses, spoofed packets and suspicious packet generation from a single IP address.

It is a best practice to schedule regular, automated scans of all critical IT systems. The results of these scans should feed into the organization’s ongoing vulnerability assessment process.

See how Imperva Web Application Firewall can help you with vulnerability assessment.

Request demo[Learn more](https://www.imperva.com/products/web-application-firewall-waf/)

**Vulnerability assessment and WAF**

[Imperva’s web application firewall](https://www.imperva.com/products/web-application-firewall-waf/) helps protect against application vulnerabilities in several ways:

1. As a gateway for all incoming traffic, it can proactively filter out malicious visitors and requests, such as SQL injections and XSS attacks. This eliminates the risk of data exposure to malicious actors.
2. It can perform virtual-patching — the auto-applying of a patch for a newly discovered vulnerability at the network edge, giving developers and IT teams the opportunity to safely deploy a new patch on the application without concern.
3. Our WAF provides a view of security events. [Attack Analytics](https://www.imperva.com/products/attack-analytics/) helps contextualize attacks and expose overarching threats, (e.g., showing thousands of seemingly unrelated attacks as part of one big attack campaign).
4. Our WAF integrates with all leading [SIEM platforms](https://www.imperva.com/learn/application-security/siem/) to provide you with a clear view of the threats you’re facing and help you prepare for new attacks.