Vulnerability testing is a process of evaluating and identifying security weaknesses in a computer system, network, or software application. It involves systematically scanning, probing, and analyzing systems and applications to uncover potential vulnerabilities, such as coding errors, configuration flaws, or outdated software components.

The main goal of vulnerability testing is to discover and address these security gaps before they can be exploited by attackers, ultimately improving the overall security and resilience of the system.

Vulnerability testing is important for several reasons:

**Comprehensive understanding of the attack surface**

Vulnerability testing enables organizations to have a better understanding of their systems, networks, and applications. This comprehensive view helps to identify potential weak points and entry points that attackers might exploit.

**Adapting to evolving threats**

Cyber threats are constantly changing and evolving, with new vulnerabilities and attack vectors emerging regularly. Vulnerability testing helps organizations stay up-to-date with the latest security threats and take proactive measures to address them.

**Reducing attack vectors**

By identifying and addressing vulnerabilities, organizations can reduce the number of potential attack vectors available to cybercriminals. This decreases the likelihood of a successful cyberattack and helps safeguard critical systems and data.

**Enhanced security measures**

Vulnerability testing provides valuable information that can be used to improve security measures. This may include implementing new security controls, updating policies and procedures, or providing employee training on security best practices.

**Continuous improvement**

Vulnerability testing is an ongoing process, which allows organizations to continuously monitor their systems and applications for new vulnerabilities. This iterative approach enables organizations to make necessary adjustments and improvements, ensuring their security posture remains strong over time.

**Risk management**

Conducting vulnerability testing helps organizations understand and manage their security risks more effectively. By quantifying and prioritizing vulnerabilities based on their potential impact, organizations can make informed decisions about allocating resources and addressing risks.

**Vulnerability Testing Methods**

Vulnerability testing methods can be broadly categorized based on the approach taken to identify vulnerabilities. They are :

### **Active Testing**

Active testing is a vulnerability testing method in which testers interact directly with the target system, network, or application to identify potential security weaknesses. It typically involves sending inputs, requests, or packets to the target and analyzing the responses to discover vulnerabilities.

Active testing can be intrusive and may cause disruptions or performance issues in the target system, but it is usually more effective in finding vulnerabilities than passive testing. Examples of active testing include:

* Port scanning to identify open ports and services running on a network.
* Fuzz testing, which involves sending malformed or unexpected inputs to applications to discover vulnerabilities related to input validation and error handling.

### **Passive Testing**

Passive testing is a non-intrusive vulnerability testing method that involves observing and analyzing the target system, network, or application without directly interacting with it. Passive testing focuses on gathering information about the target, such as network traffic, configuration settings, or application behavior, to identify potential vulnerabilities.

This method is less likely to cause disruptions or performance issues but may be less effective in finding vulnerabilities compared to active testing. Examples of passive testing include:

* Traffic monitoring to identify patterns or anomalies that may indicate security weaknesses.
* Configuration reviews to assess security settings and identify misconfigurations.

### **Network Testing**

Network testing is a vulnerability testing method focused on identifying security weaknesses in network infrastructure, including devices, protocols, and configurations. It aims to discover vulnerabilities that could allow unauthorized access, eavesdropping, or Denial of Service (DoS) attacks on the network.

Network testing typically involves both active and passive testing techniques to evaluate the network’s security posture comprehensively. Examples of network testing include:

* Scanning for open ports and services on network devices.
* Analyzing network protocols and configurations for security flaws.

### **Distributed Testing**

Distributed testing is a vulnerability testing method that involves using multiple testing tools or systems, often deployed across different locations, to scan and analyze the target system, network, or application for vulnerabilities.

This approach can help provide a more comprehensive view of the target’s security posture, as it helps identify vulnerabilities that may be visible only from specific locations or under specific conditions. Distributed testing can also help distribute the load of vulnerability testing, reducing the impact on the target system and increasing the efficiency of the testing process.

Examples of distributed testing include:

* Using multiple vulnerability scanners from different locations to scan a web application for potential security flaws.
* Coordinating a team of testers in different geographical locations to perform simultaneous network vulnerability testing.

Related content: Read our guide to [*vulnerability examples*](https://brightsec.com/blog/vulnerability-examples-common-types-and-5-real-world-examples/).

## What Are Vulnerability Testing Tools?

Vulnerability testing tools are software applications or services designed to help organizations identify and assess security weaknesses in their systems, networks, or applications. These tools automate the process of vulnerability testing, making it more efficient, accurate, and consistent.

There are several types of vulnerability testing tools, including:

* **Network vulnerability scanners:**

These tools scan networks for open ports, misconfigurations, and other security weaknesses.

* **Web application vulnerability scanners:**

These tools are specifically designed to identify vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and broken authentication.

* **Static application security testing (SAST) tools:**

Designed to analyze source code or compiled code to identify potential security vulnerabilities without executing the application.

* [**Dynamic application security testing (DAST) tools**](https://brightsec.com/blog/dast-dynamic-application-security-testing/)**:**

Built to interact with running applications to identify security weaknesses during runtime.

* **Fuzz testing tools:**

 Generate and send malformed or unexpected inputs to applications to identify vulnerabilities related to input validation and error handling.

* **Configuration management and compliance tools:**

These tools assess system and application configurations against established security best practices or compliance standards, such as CIS Benchmarks or PCI DSS.

* **Container and cloud security tools:**

These tools focus on identifying vulnerabilities and misconfigurations in cloud-based environments and containerized applications.

Organizations often use a combination of these vulnerability testing tools to achieve a comprehensive assessment of their security posture. It is important to keep these tools up-to-date to ensure they can effectively detect and analyze the latest security threats and vulnerabilities.

**5 vulnerability scanning case studies**

1. [SyCom](https://www.datamation.com/security/vulnerability-scanning-case-studies/#sycom)
2. [Visma](https://www.datamation.com/security/vulnerability-scanning-case-studies/#visma)
3. [California Polytechnic State University](https://www.datamation.com/security/vulnerability-scanning-case-studies/#cal_poly)
4. [Bitbrains](https://www.datamation.com/security/vulnerability-scanning-case-studies/#bitbrains)
5. [Hill & Smith](https://www.datamation.com/security/vulnerability-scanning-case-studies/#hill_and_smith)

## **1. SyCom**

With annual revenue of over $70 million, [SyCom](https://service.invicti.com/case-studies/sycom/) is one of the leading systems integrators in the East Coast of the U.S. It designs and supports IT solutions that help optimize business growth.

SyCom has been using Invicti’s Netsparker web application security scanner for about seven years. Until the deployment of Netsparker, the company administered manual scans annually to check for vulnerabilities. This meant the application was left open for potential cyberattacks for long periods in between the scans.

SyCom also uses the Netsparker web application security platform for continuous monitoring of its customers’ websites to check for vulnerabilities. A tool integral to this is Netsparker’s web application security scanning engine.

Netsparker automatically makes use of the detected vulnerabilities and feeds them into the SyCom framework. Security professionals can then reach out to customers and suggest remedies.

**Industry:** IT and telecommunications

**Vulnerability scanning provider:** Netsparker Enterprise by Invicti

**Outcomes:**

* Continuous web security scanning of client websites
* Automated reporting of identified vulnerabilities to the SyCom system
* Drastically reduced workload for security professionals

## **2. Visma**

With over one million customers across Europe and Latin America, [Visma](https://www.qualys.com/customers/success-stories/visma-drives-cloud-transformation-secure-development-delivery-saas-solutions/) is a leading provider of accounting, procurement, and payroll solutions. Visma employs over 5,500 professionals and includes 200 companies spanning over 20 countries across the world.

As the firm transformed into a software-as-a-service (SaaS) provider, newer challenges related to security emerged. Visma not only needs to ensure the security of its own systems, but it has the responsibility of safeguarding customer data as well. With a larger attack surface, Visma wanted to gain increased protection against potential cyberattacks by effectively detecting and remediating vulnerabilities.

To strengthen its defenses against potential threats, Visma adopted the Qualys Cloud Platform for in-depth security scans. Qualys Vulnerability Management allowed the firm to automatically scan its development infrastructures and place the scan results in the same backlog with vulnerability reports on the company’s code. It also provided the firm with a 360-degree view of vulnerabilities on its network that trickled down to individual devices.

“We now have a comprehensive map of all 4,000 servers and 6,000 clients across our global IT infrastructure and an accurate view of all the vulnerabilities and their severity,” says Hans Petter Holen, CISO, Visma.

“We can perform scans in the background, even when a device is offline, and deliver the results as soon as it is reconnected to the network. When we detect a vulnerability, we deliver the findings to whoever is responsible for the machine — either via email to the local IT department or via Jira to the developer who owns the device.”

**Industry:** IT services

**Vulnerability scanning provider:** Qualys

**Outcomes:**

* Vulnerability detection across more than 10,000 connected devices
* Functions on minimal external management
* Quarterly patching cycles accelerated up to 80%

## **3. California Polytechnic State University**

[California Polytechnic (Cal Poly) State University](https://portswigger.net/customers/california-polytechnic) in San Luis Obisbo, California serves over 21,000 students.

Cal Poly was looking for a vulnerability scanning solution to address vulnerabilities existing across its web portfolio. The tools used previously were quite expensive and didn’t meet the university’s security requirements. Cal Poly needed a scanning solution that could not only run frequent penetration tests, but also provide faster feedback to its security team.  
PortSwigger’s Burp Suite Enterprise Edition helped the application security team automate security scanning. Moreover, the vulnerability solution gave Cal Poly full visibility of its entire web portfolio at a single glance with its dashboard and scan summary reports. It lends greater flexibility in security testing, because of Burp Suite’s customizable scan configurations.

“A vulnerability scanner, like Burp Suite, frees our AppSec team to spend their time where it’s most valuable,” says a Cal Poly rep.

**Industry:** Higher education

**Vulnerability scanning provider:** Burp Suite Enterprise Edition by PortSwigger

**Outcomes:**

* Reduced workload, resource optimization, and a faster feedback loop
* Reduced risk and increased security coverage across its web portfolio
* Security integration into the software development life cycle

**See more:**[Why Vulnerability Scanning is Important](https://www.datamation.com/security/importance-of-vulnerability-scanning/)

## **4. Bitbrains**

[Bitbrains](https://www.tenable.com/case-studies/bitbrains) builds native and hybrid phone apps for Android and iOS platforms. The firm is now on its third-generation cloud and has a complex IT environment: with about 3,000 virtual machines (VMs), 300 blades, and numerous network devices, with three network operations centers to manage the customer cloud.

Bitbrains’ cloud environment posed a cybersecurity challenge for the team, which needed a way to manage its baseline vulnerability checks for regulatory compliance while also keeping up with the threat environment. One of Bitbrains’ customers also requested daily vulnerability scans. Since the process wasn’t automated, the whole exercise was labor-intensive and took more than a week to complete.

After hearing about Tenable SecurityCenter’s Continuous View, the company decided to try it out. For the next three months, Bitbrains worked with a Tenable sales engineer and an outside consultant on the deployment of SecurityCenter CV. With SecurityCenter CV, Bitbrains could perform continuous monitoring, providing a comprehensive view of network health across different assets.

Moreover, Bitbrains’ professionals could now easily verify the status of antivirus across systems, update progress, and firewalls installed as well as check for functionally redundant network components.

“Security-wise, we have much better insight into what our current state is, what threats exist, and what solutions are available,” says Giray Devlet, chief security officer, Bit brains.

“It also provides us insight with service customers, where we can see they did something wrong and are vulnerable to attacks, and when certain patches are not installed or missing.”

**Industry:** Mobile app development

**Vulnerability scanning provider:** Tenable SecurityCenter Continuous View

**Outcomes:**

* Automated scanning of external-facing sites in 24 hours
* Easy identification of weak spots in the cloud environment
* Insight into mistakes made by service customers that could lead to potential vulnerabilities

## **5. Hill & Smith**

With a net revenue of $858.21 million, [Hill & Smith](https://www.intruder.io/success-stories/how-hill-smith-holdings-plc-achieved-comprehensive-vulnerability-management-with-intruder-vanguard) is known for creating sustainable and resilient infrastructure throughout the U.K., U.S., India, Sweden, and Australia. The company has a diverse portfolio, ranging from roads and transportation to utilities, engineered composite solutions, and galvanizing services.

Hill & Smith previously deployed limited resources in protecting its internet-facing assets. The issue gave rise to a foundational hurdle in creating attack-resilient structure: The company did not have enough time to attend to every threat.

Moreover, Hill & Smith was also struggling with the lack of visibility. The security tools used by the team could only perform searches on classified assets only. Hill & Smith faced challenges in tracking all of the potential risks stemming from new system updates. The process made the organization’s operations vulnerable to attacks.

Shifting to Intruder Vanguard provided the company with much more than automated vulnerability scanning. Vanguard sent users manual reviews done by security experts, flagged detected vulnerabilities, and offered remedies to create durable infrastructure. Hill & Smith then tackled its visibility issues by seeking out extra assets that might be in use and creating a 360-degree profile of all vulnerabilities in place.

“When we needed to go way beyond the usual programmatical scans, a specialized vulnerability scanner really let us enumerate the services behind IPs and find vulnerabilities and weaknesses that were previously hidden,” says Sam Ainscow, group CISO, Hill & Smith.

“Going in, we simply wanted to get an understanding of the organizational risks associated with the services we made available online. The open-source intelligence we received with Intruder Vanguard dramatically broadened our threat awareness.”

**Industry:** Infrastructure and construction

**Vulnerability scanning provider:** Intruder Vanguard

**Outcomes:**

* Proactive bug hunting and reduced response time
* Expert-informed human sights and limited occurrence of false positives
* Early stage identification of vulnerabilities that could potentially turn lethal
* Automated detection combined by manual reviews to dig deeper into system weaknesses

**See more:**[Simple Guide to Vulnerability Scanning Best Practices](https://www.datamation.com/security/vulnerability-scanning-best-practices/)

## **Bottom Line**

These case studies show examples of how vulnerability scanning software is being used in various industries: IT; telecommunications; higher education; mobile app development; infrastructure; and construction.

Clients selected a range of providers in the vulnerability scanning market for implementations: Invicti; Qualys; PortSwigger; Tenable; and Intruder.

Together, the organizations’ vulnerability scanning solutions improved numerous aspects of their networks:

* Automated reporting of identified vulnerabilities
* Drastically reduced workload for security professionals
* Vulnerability detection across thousands of connected devices
* Reduced workload, resource optimization, and faster feedback loop
* Reduced risk and increased security coverage across web portfolio
* Identification of weak spots in cloud environment