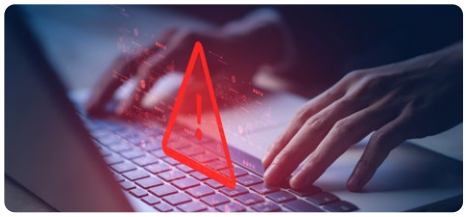
Vulnerability Scans & Approved Scanning Vendors

A Resource Guide from PCI Security Standards Council

What is a Vulnerability Scan?

A process for identifying security weaknesses and flaws in systems and software. New vulnerabilities, security holes, and bugs are being discovered daily. Test your systems regularly to identify weaknesses and address them as soon as possible.

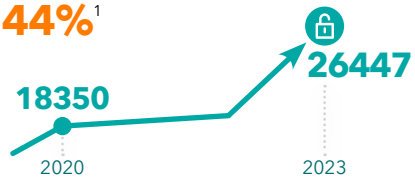


Why are vulnerability scans important?

In 2023, **25%** of high-risk vulnerabilities were exploited on the day of disclosure.[1]

Another **50%** of these high-risk vulnerabilities were exploited within 19 days.[1]

Between 2020 and 2023, the number of disclosed vulnerabilities increased by **44%**[1]



One of the main ways attackers access an organization is by **exploiting vulnerabilities**[2]

Sources:
1: Qualys 2023 Threat Landscape Year in Review: If Everything Is Critical, Nothing Is
2: 2023 Verizon Data Breach Investigation Report

Regular vulnerability scans help an organization identify and address vulnerabilities promptly, which reduces the likelihood of an attacker exploiting a vulnerability and potentially compromising the organization and all its payment account data.

What is an Approved Scanning Vendor (ASV)?

ASVs are qualified by PCI SSC to provide security services and tools (the "ASV scan solution") for external vulnerability scans. PCI DSS Requirement 11.3.2 requires evidence of passing external vulnerability scans, performed by an ASV, at least once every three months.

PCI SSC maintains a list of Approved Scanning Vendors (ASVs) on our website.

Which systems need to be included in an ASV scan?

ASV scans apply to Internet-facing systems (like webservers) – these systems are the most vulnerable because they can be easily accessed and exploited by criminals. Once in, the criminals compromise systems that allow them to steal payment account data where it is stored or while it is being entered and processed by customers.

Want more info about scoping your scan? Review section 5.5 in the ASV Program Guide.

Which organizations need to perform ASV scans?

Your organization may be asked by a merchant bank or payment brand to show evidence of PCI DSS compliance by completing a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ). Talk to the entity that is requesting this evidence to understand if you are being asked to complete a ROC or an SAQ. If it is an SAQ, ask them which SAQ is correct for your organization.

Which SAQs include ASV scans?

For merchants, ASV scans are included for SAQs A, A-EP, B-IP, C, and D. SAQ D for Service Providers also includes ASV scans.

Will I need evidence of four passing scans for my first assessment against PCI DSS Requirement 11.3.2?

No. Read FAQ 1485 "What is the meaning of 'initial PCI DSS assessment'?"

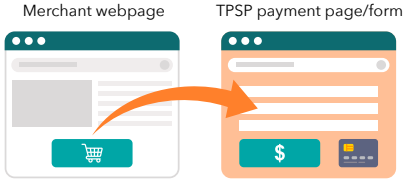
Why were ASV scans added to SAQ A for PCI DSS v4?

SAQ A for PCI DSS v4 adds security controls to address common breaches that target SAQ A merchant environments at alarming rates, including two requirements for external vulnerability scans performed by an ASV.

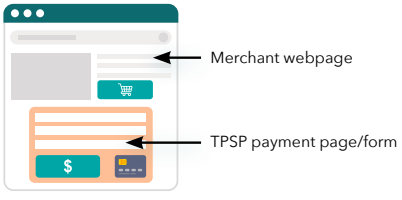
Do ASV scans apply to all SAQ A merchants?

No, ASV scan requirements in SAQ A only apply to e-commerce merchant system(s) that hosts the webpage that either 1) redirects payment transactions to a PCI DSS compliant TPSP or 2) includes an embedded payment page/form from a PCI DSS compliant TPSP. The intent is for merchants to minimize the risk of compromise by scanning for and resolving identified vulnerabilities that could potentially expose their link to the TPSP's payment page.

Redirect to PCI DSS compliant TPSP (for example, URL redirect)



Merchant webpage with a PCI DSS compliant TPSP's embedded payment page/form (for example, one or more iframes)



My merchant website is hosted by a PCI DSS compliant TPSP – is the TPSP responsible for the ASV scans?

It is essential to confirm with your TPSP who is responsible for ASV scans. Ask your hosting TPSP for documentation that confirms 1) they are PCI DSS compliant for their hosting services and 2) your website is included in their ASV scans, including the external IP address, domain name, or URL of the webserver that hosts your website. If your website is not included in the TPSP's ASV scans, coordinate with your TPSP about the best way to get that website scanned at least once every three months.

Should I perform scans more often than once every three months?

Yes! Performing scans more often is recommended. Performing scans more frequently provides organizations with earlier awareness of vulnerabilities that need to be addressed, and more time to fix those vulnerabilities to achieve a passing ASV scan within the three-month window.

Are all vulnerability scans from an ASV automatically considered ASV scans?

No. ASVs may offer a variety of services, including various scan products and penetration testing. To meet PCI DSS Requirement 11.3.2, make sure your external vulnerability scans are performed with an ASV's PCI approved scan solution.

What is a "passing" ASV scan result?

It means the ASV report contains no vulnerabilities ranked as "medium" or "high". It's important to ask your ASV for an Attestation of Scan Compliance with every passing scan.

Review sections 6 and 7 of the ASV Program Guide for details.

Are vulnerability scans and penetration tests the same thing?

No. Penetration testing (or pen testing) is an active, mostly manual, process where the tester attempts to exploit vulnerabilities to gain access to a system or environment. Vulnerability scans are a passive process to identify, but not exploit, security weaknesses. Vulnerability scans can be likened to turning a doorknob to see if it is locked or an alarm sounds, whereas pen testing is more like attempting to pick the lock or disable the alarm to gain access to the building.

What if I fail, or my TPSP fails, an ASV scan for my website?

It means you have vulnerabilities to address! Next steps? Fix the vulnerabilities and perform rescans with the ASV tool until you achieve a passing scan. If your TPSP's scan for your website fails, coordinate with your TPSP to fix those vulnerabilities.

Do you need help fixing vulnerabilities?

The ASV scan report includes remediation recommendations for each vulnerability. If you need help, ask your ASV, a PCI Qualified Security Assessor (QSA), your TPSP, or other technical resource you work with.

Quick tips for getting started with an ASV

Get Advice
Ask your acquiring bank about any partnerships they may have with PCI ASVs.

Talk to a PCI ASV
See PCI SSC website for the list of PCI ASVs.

Select an ASV
Contact several PCI ASVs and select a suitable program.

Address Vulnerabilities
Ask your PCI ASV for help correcting issues found by scanning.

Additional Resources

PCI ASV List

PCI DSS v4.0 Quick Refence Guide

PCI DSS v4.0 Resource Hub

SAQ Instructions and Guidelines

ASV Program Guide