PCI DSS v4.0 Fulfillment Table

Learn about the changes in the new version of PCI and how Reflectiz can assist your organization in meeting the requirements of each section:

Item	Requirement	Fulfillment
PCI 6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be high-risk or critical to the environment. • Vulnerabilities for bespoke, custom, and third-party software (for example operating systems and databases) are covered	Reflectiz continually scans the website for malicious scripts, domains, vulnerabilities, and known CVEs. We use the VirusTotal service, the CVE database, the Whois service, and the internal Reflectiz database of vulnerabilities, malicious scripts, and domains. And since the NIST methodology doesn't cover all the relevant aspects of risk assessment, Reflectiz also uses its own risk assessment mechanism.
PCI 6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	An inventory of all scripts (bespoke and third-party) is available via the Inventory report. In addition, Reflectiz provides an important subset of this inventory—a log of all scripts that touch sensitive data, an explanation of why each of them is necessary for the business, a notice of any changes, identification of malicious code, and the action taken to prevent or remove it.
PCI 6.4.1	Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities. Common assessment tools include specialized web scanners that perform automatic analysis of web application protection.	Reflectiz continually scans the website for malicious scripts and domains, vulnerabilities, and known CVEs. If found, the system raises an alert, assigning each one an appropriate severity according to a risk assessment mechanism.

Item	Requirement	Fulfillment
PCI 6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of publicfacing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs • Configured to either block web-based attacks or generate an alert that is immediately investigated.	Reflectiz raises a high-severity alert when it detects each of these: • Script change that looks malicious • Application behavior change, for example, an application starts collecting sensitive data • An application starts sending data to a malicious domain • A new application (script) is added and it looks malicious • A new application version is added to the known vulnerabilities database and it is part of the web application
PCI 6.4.3	PCI 6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed.	This section extends the above requirement to all scripts loaded to sensitive pages, whether they access sensitive data or not.
PCI 11.6.1	Unauthorized changes on payment pages are detected and responded to.	Identify changes in sensitive page headers and prevent or remove any malicious additions to them.

Get access tou your PCI Dashboard

Free PCI Compliance Sacn

Try it now **More aboue PCI DSS v4.0**

reflectiz