

Highlights

Independent Expert Review: Veracode is a recognized application security expert with experience in PCI guidelines

Rapid Results: Perform analysis and receive results generally within 24 hours

Rapid Time to Compliance: Provides actionable advice for faster remediation by developers

Automated & Integrated: Automated application penetration testing with seamless integration into software development lifecycle

Streamline Costs: Subscription model provides consistent testing costs regardless of application testing frequency

Automated Risk Ranking: Assigns risk severity rankings based on CWE & CVSS to meet auditing standards

PCI training: Several online courses fulfill PCI training program requirements.

Benchmarking: Compare your state of PCI compliance against that of industry peers

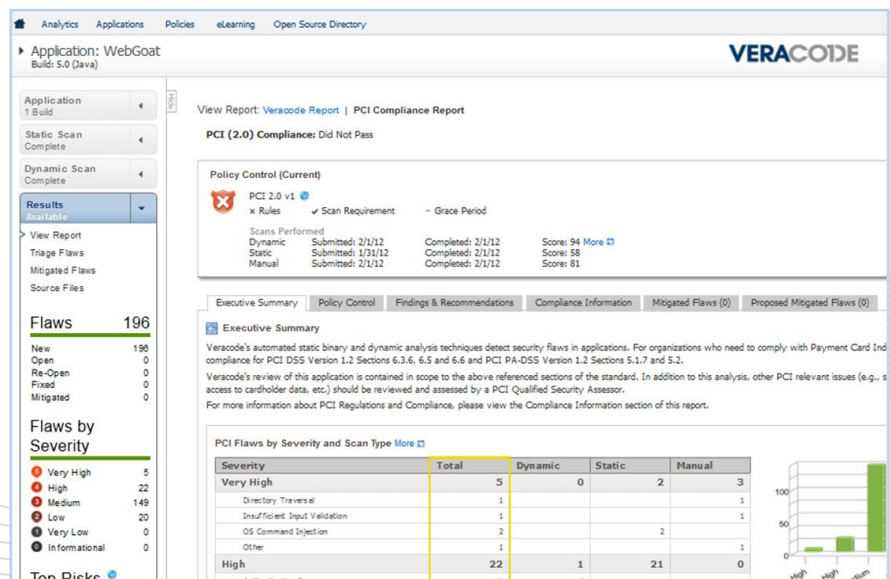
PCI Compliance Simplified

An on-going application security program is a cornerstone of PCI-DSS compliance. Veracode's approach to application security is the simplest approach to PCI compliance for enterprises.

Customers can simply assign Veracode's predefined policy for PCI compliance to the appropriate applications and then request automated application scans. The platform does the rest – it automates the testing and analysis, assigns risk severity rankings based on industry standards, populates the appropriate dashboards and reports for at-a-glance compliance status based on actual scan results, and provides detailed actionable findings for rapid remediation. Veracode is also the only application vulnerability assessment solution supporting iOS, Android, Blackberry and Windows Mobile applications, which is a must for companies considering mobile payment applications.

Customers can also retest applications to track actual remediation against planned timelines. This allows enterprises to evaluate their program's effectiveness, which is key to minimizing the on-going business risks that PCI is ultimately meant to address. The Veracode platform also provides QSA-ready proof that PCI related applications are tested, remediations are implemented and eLearning courses are completed. The reports can be sent directly to QSAs or other auditing teams.

Continuous improvement is also built into the platform. As a cloud provider we test thousands of applications and in the process we improve our ability to find high risk vulnerabilities. We deliver this new knowledge to customers with automatic updates. In addition, as OWASP or CWE top vulnerabilities lists change over time, our scans and predefined PCI compliance policies are automatically updated. Veracode simplifies the effort required to get compliant and stay compliant.



Application Security Requirements for PCI-DSS

PCI DSS Requirements	The Veracode Advantage
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	<ul style="list-style-type: none"> ☑ Standards-Based Risk Ratings – Veracode combines MITRE’s Common Weakness Enumeration (CWE) and FIRST’s Common Vulnerability Scoring System (CVSS) to classify and assess application security and risk and provide practical guidance for risk management. ☑ Policy Manager – Once you select the PCI policy in policy manager – the platform is automatically updated to match changes in the OWASP and SANS top vulnerabilities as they change year to year.
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	<ul style="list-style-type: none"> ☑ Deploy Rapidly & Globally – Provides a single web portal for teams to centrally collaborate on projects with executive rollup dashboards to gauge overall compliance status. ☑ No Source? No Problem – For companies that do not have access to the original application source code about to be released into production, Veracode is the only vendor that provides binary code analysis without requiring access to source code.
6.4 Follow change control processes and procedures, including verification that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	<ul style="list-style-type: none"> ☑ Subscription Service – Allows frequent compliance testing throughout the software development lifecycle at a fixed annual cost and without requiring manual code reviews by external consultants. ☑ SDLC integration – Plugin and API integration with SDLC makes it easy for every application build to be tested and vulnerability and remediation advice are delivered directly to developer IDE’s and QA bug tracking systems. ☑ Analytics – Consolidate all the test data in one place it is possible to track compliance improvements over time.
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes	<ul style="list-style-type: none"> ☑ Actionable remediation guidance – Developers can learn secure coding best practices as they remediate vulnerabilities. ☑ Comprehensive Knowledgebase – Searchable content and specific guidance for development or security team members. ☑ Integrated eLearning Service – Contains over 65 hrs of online courses for developers and security. Participation is automatically tracked for compliance purposes. ☑ Analytics – Enables CISOs to target eLearning curriculum at specific teams or reoccurring vulnerabilities.
6.6 Verify that public-facing web applications are protected against attacks	<ul style="list-style-type: none"> ☑ Web Application Testing at Scale – Leverages elastic cloud infrastructure to scan thousands of websites within days. ☑ Test Web 2.0 Applications – Next generation website crawling enables us to automatically test Web 2.0 applications. ☑ Test Mobile Applications – Support for iOS, Android, Blackberry and Windows Mobile applications.
11.3.2 Application-layer penetration tests after any significant application upgrade or modification. The tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.	<ul style="list-style-type: none"> ☑ Automate Penetration Tests – Penetration testers’ first step becomes automated scanning for routine vulnerabilities to get immediate results for enterprise developers. Results from penetration tests may also be imported to the platform so there is a single dashboard for viewing all results ☑ SDLC Integration – Makes it easy to perform automated penetration tests on every application upgrade or modification