Guide: **Selecting Sentinel Dynamic for PCI Compliance**

WhiteHat Sentinel exceeds the requirements of PCI DSS for application security by providing ongoing, verified vulnerability assessment for both internal and public websites. We support over 50 vulnerabilities, covering every risk in the OWASP Top 10 and PCI DSS 3.1 application security requirements. With a combination of our manual and automated assessments, business logic and penetration testing, integration with WAFs and CBT offerings, you can be confident that WhiteHat Sentinel has you PCI DSS 3.1 compliant.

Sentinel PE - Premium Edition is for mission critical permanent websites with multi-step forms and rigorous compliance requirements. It includes all SE features and business logic testing.

Sentinel SE - Standard Edition is for permanent websites, that are not necessarily mission critical. It includes all BE features and tests for issues involving multi-step forms and logins.

Sentinel BE - Baseline Edition is the foundational solution for basic, less critical websites. BE Enterprise is massively scalable, "best value" solution for any environment.

Business Logic Flaws	PE	SE	BE	OWASP Top 10	PCI DSS v3.2 Section 6.5
Abuse of Functionality	✓	✓	✓		6.5.1 Injection Flaws
Brute Force	✓				6.5.10 Broken Authentication and Session Management
Session Prediction	✓			A2 Broken Authentication and Session Management	6.5.3 Insecure Cryptographic Storage
Cross-Site Request Forgery	✓	✓	✓	A8 Cross-Site Request Forgery (CSRF)	6.5.9 Cross Site Request Forgery
Clickjacking	✓				
Denial of Service	✓				
Insecure Indexing	✓			A6 Sensitive Data Exposure	6.5.8 Improper Access Control
Insufficient Anti-automation	✓				
Insufficient Authentication	✓			A2 Broken Authentication and Session Management A4 Insecure Direct Object References	6.5.10 Broken Authentication and Session Management
Insufficient Authorization	✓			A4 Insecure Direct Object References A7 Missing Function Level Access Control	6.5.8 Improper Access Control
Insufficient Password Recovery	✓			A7 Missing Function Level Access Control	6.5.8 Improper Access Control
Insufficient Process Validation	✓			A7 Missing Function Level Access Control	6.5.8 Improper Access Control
Insufficient Password Policy Implementation	✓				
Insufficient Session Expiration	✓			A2 Broken Authentication and Session Management	6.5.10 Broken Authentication and Session Management
Session Fixation	✓			A2 Broken Authentication and Session Management	6.5.10 Broken Authentication and Session Management
Technical Vulnerabilities	**PE**	**SE**	**BE**	**OWASP Top 10**	**PCI DSS v3.2 Section 6.5**
Application Misconfiguration	✓	✓	✓	A5 Security Misconfiguration	6.5.5 Improper Error Handling
Buffer Overflow	✓			A1 Injection	6.5.2 Buffer Overflow
Content Spoofing	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
Cross-Site Scripting	✓	✓	✓	A3 Cross-Site Scripting (XSS)	6.5.7 Cross Site Scripting
Directory Indexing	✓	✓	✓	A5 Security Misconfiguration	6.5.8 Improper Access Control
Fingerprinting	✓	✓	✓	A5 Security Misconfiguration	6.5.5 Improper Error Handling
HTTP Response Splitting	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
Improper Input Handling	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
Information Leakage	✓	✓	✓	A6 Sensitive Data Exposure	6.5.5 Improper Error Handling
Insufficient Transport Layer Protection	✓	✓	✓	A6 Sensitive Data Exposure	6.5.4 Insecure Communications
LDAP Injection	✓			A1 Injection	6.5.1 Injection Flaws
Mail Command Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
OS Command Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
Path Traversal	✓	✓	✓	A4 Insecure Direct Object References	6.5.8 Improper Access Control
Predictable Resource Location	✓	✓	✓	A5 Security Misconfiguration	6.5.8 Improper Access Control
Remote File Inclusion (RFI)	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
Server Misconfiguration	✓	✓	✓	A5 Security Misconfiguration	6.5.5 Improper Error Handling
SQL Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
SSI Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
URL Redirector Abuse	✓	✓	✓	A10 Unvalidated Redirects and Forwards	6.5.1 Injection Flaws
XML External Entities	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
XML Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
XPath Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
XQuery Injection	✓	✓	✓	A1 Injection	6.5.1 Injection Flaws
Informational Findings - upon request	**PE**	**SE**	**BE**	**OWASP Top 10**	**PCI DSS v3.2 Section 6.5**
Autocomplete Attribute	✓				6.5.3 Insecure Cryptographic Storage
Non-HttpOnly Session Cookie	✓			A6 Sensitive Data Exposure	6.5.10 Broken Authentication and Session Management
Cacheable Sensitive Response	✓			A6 Sensitive Data Exposure	
Insufficient Cookie Access Control	✓			A6 Sensitive Data Exposure	
Persistent Session Cookie	✓			A2 Broken Authentication and Session Management	6.5.10 Broken Authentication and Session Management
Frameable Resource	✓			A5 Security Misconfiguration	
Insufficient Cross-domain Configuration	✓			A5 Security Misconfiguration	
Improper HTTP Method Usage	✓			A2 Broken Authentication and Session Management A6 Sensitive Data Exposure	
Personally Identifiable Information	✓			A6 Sensitive Data Exposure	
Unsecured Session Cookie	✓			A6 Sensitive Data Exposure	6.5.10 Broken Authentication and Session Management

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com