FORTINET

SOLUTION GUIDE

FortiWeb Web Application Firewall

Ensuring Compliance for PCI DSS requirement 6.6

Overview

Web applications and the elements surrounding them have not only become a key part of every company's core business infrastructure, they also provide a high profile target for malicious activity. This malicious activity ranges from simple defacement attacks, denial of service attacks to more damaging data harvesting resulting in damage to customer confidence, loyalty, brand reputation, and corporate credibility.

In response to major breaches, data theft and e-commerce security the major five credit card companies (Visa, MasterCard, American Express, Discover and JCB) aligned their individual policies and released the Payment Card Industry Data Security Standard (PCI DSS). The standard's intention is to create an additional level of protection for card issuers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data.

The Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized. The PCI DSS outlines 12 requirements that are put in six categories.

Build and Maintain a Secure Network and Systems

R1: Install and maintain a firewall configuration to protect cardholder data.

R2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

R3: Protect stored cardholder data.

R4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

R5: Protect all systems against malware and regularly update anti-virus software or programs.

R6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

R7: Restrict access to cardholder data by business need-to-know.

R8: Identify and authenticate access to system components.

R9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

R10: Track and monitor all access to network resources and cardholder data.

R11: Regularly test security systems and processes.

Maintain an Information Security Policy

R12: Maintain a policy that addresses information security for all personnel.

PCI Compliance for Web Applications

Of the 12 requirements outlined in the PCI DSS, web applications present some of the biggest challenges as they are usually high performance production systems which provide business driving revenue. These are usually complex applications such as e-commerce, web mail, online retail stores, social web sites, online auctions and B2B applications that quickly change, are updated regularly, and constantly evolve. Web applications use complex Web 2.0 technologies that create major security challenges. Addressing these for web applications to meet PCI DSS regulations creates design, policy, architecture, and human resource implications.

According to the Web Application Security Consortium (WASC) 13% of web sites can be compromised completely using automatic tools. 49% of web sites contain high risk vulnerabilities prone to automatic tools while 80-96% of web applications contain high risk items that can be exploited using standard hacking methods. The most common vulnerabilities are Cross Site Scripting and SQL injection.

While Fortinet provides solutions for all 12 of the PCI DSS requirements, this paper discusses those strategic to web applications.

Requirement 6.6 mandates that all web applications must either undergo extensive vulnerability assessments or implement a web application firewall.

R6.6. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

Although not specifically addressed by FortiWeb, Requirement 6.5 is an important guideline for building web applications to ensure they meet the OWASP Top 10 guidelines. FortiWeb can protect your applications from the OWASP Top 10 Threats and can help uncover vulnerabilities with its built-in scanner.

R6.5: Develop web applications securely based on the OWASP Top 10 guidelines. Implementing a secure coding practice as part of the development life cycle is an important part of every application development project. Web application security needs to be an essential part of any successful project. Guidelines recommended by OWASP and with requirement 6.5 help users build a more secure and trusted application, reducing the number of exploits throughout the application life cycle.

Solely relying on secure development practices is very important. However it is not enough in today's threat environment. The three major challenges to this are:

- **Web 2.0 technologies.** Modern web applications use complex Web 2.0 technologies such as Web Services, AJAX, JavaScript, Adobe Flex and others. Most developers do not have the right knowledge and expertise to fully implement the security measures needed during development cycles.
- **Business needs trump security procedures.** Tight timeframe requirements driven by business demands sometimes cause new software updates to bypass secure coding practices potentially creating vulnerabilities with new releases.

- **Legacy software.** Older applications, applications inherited through mergers and acquisitions, and those developed by third-parties make it nearly impossible for developers to understand and correct security flaws.

Meeting PCI 6.6 Compliance

In order to satisfy requirement 6.6, two options are provided by the PCI standard:

- **Web application scanning.** Applications should be reviewed with manual or automated application vulnerability assessment tools to find existing vulnerabilities.
- **Web Application Firewall (WAF)**. Installing an automated solution such as a web application firewall in front of web-facing applications. A WAF allows an organization to block application layer attacks that might compromise credit card information.

The first option can be achieved by conducting a manual assessment or using automated tools. In either case, the assessments need to be performed by a qualified internal resource or third party who has the proper skills and experience to understand the web application, know how to evaluate it for vulnerabilities, and understand the findings.

There are 4 main drawbacks of web application scanning:

1. Some vulnerabilities are closely tied to the operating system and web/application server configurations which are typically outside of the software developer's expertise and responsibilities.
2. To fix the broken code or application, the application/service needs to be removed from live production which can introduce significant costs and delays in remediation exposure.
3. It is costly to acquire and maintain proper tools for vulnerability assessments, and hire and train personnel capable of performing the tests.
4. It is time consuming and tedious to conduct tests that cover common vulnerability areas for each application and every time it is updated.

Achieving PCI compliance through option 2, a Web Application Firewall, also requires hiring and training of proper personnel, purchasing the WAF, and creating and maintaining security policies. However, there are many benefits that both lower the cost of compliance and provide better levels of security and accountability. Additionally, it is much easier to master the management and policy development on a WAF than perform application reviews necessary in the first option.

Choosing only one of these two technologies will still leave gaps in the security posture of an organization and most likely will create cost inefficiencies in addressing them. The best solution is a hybrid approach that not only scans and reports on application vulnerabilities but also protects the web application in real time with a variety of out-of-the-box security policies.

PCI DSS 6.5: Protecting Against the OWASP Top 10 with FortiWeb

FortiWeb-4000E

One of the most important requirements is PCI DSS Section 6.5. It focuses organizations on the specific web application threats as defined by the Open Web Application Security Project (OWASP) with relation to code development. The OWASP Top 10 Web Application Security Risks are the de-facto standard of the most critical web application security flaws.

Although FortiWeb doesn't provide code analysis and development, it can play a crucial role behind your development efforts. It can block new zero-day threats, patch vulnerabilities in legacy applications, and give your organization additional time to repair applications once threats are detected and mitigated by FortiWeb.

FortiWeb Web Application Firewalls specifically address each of the OWASP Top 10 threats as documented in the PCI DSS 6.5 requirements. The following is the OWASP Top 10 and the way the FortiWeb solution protects against each of the attacks:

A1 - Injection

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

FortiWeb A1 Protection

Auto-Learn profiling automatically builds an allowed baseline to provide comprehensive request validation capability to enforce strict URL and parameter control. Enhanced application signature detection engine updated regularly by the FortiGuard Labs team adds a secondary layer for abnormal characters and known injection strings.

A2 - Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

FortiWeb A2 Protection

FortiWeb enforces session management with strict cookie control by tracking all sessions and cookies. Any attempt to compromise cookies is mitigated. Additionally various Authentication Offload capabilities (supporting Local, LDAP and NTLM) are included to offer additional security layer.

A3 - Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

FortiWeb A3 Protection

FortiWeb's application signature layer engine includes various XSS signatures to protect against the most sophisticated XSS attacks. Additionally, FortiWeb's Auto-Learn builds a comprehensive baseline of normal behavior such as URLs and parameters. Any attempt to inject illegal and unknown characters to arguments can be immediately blocked.

A4 - Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

FortiWeb A4 Protection

Auto-Learn profiling builds a comprehensive profile of allowed elements within the application. Any attempt to manipulate a parameter will trigger an alert and immediately be blocked. Hidden Fields Rules detect and block any attempt by the client to alter a hidden parameter value.

A5 - Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.

FortiWeb A5 Protection

FortiWeb provides multiple ways to counter misconfigurations. Using Auto-Learn FortiWeb will block any attempt made by an attacker to exploit a misconfigured web application. Also, monitoring application responses allows FortiWeb to identify any application failure. Lastly, FortiWeb's unique Vulnerability Scanner feature provides the ability to scan the protected applications, find inherent misconfigurations, and quickly turn these to security rules.

A6 – Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

FortiWeb A6 Protection

FortiWeb protects against attacks that lead to sensitive data exposure such as SQL Injection and other injection types. Additionally, FortiWeb inspects all web server outgoing traffic for sensitive data such as Social Security numbers, credit card numbers and other predefined or custom based sensitive data. When identified, FortiWeb can either mask the data or block it from reaching the client all together.

A7 - Missing Function Level Access Control

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization

FortiWeb A7 Protection

Authentication Offload allows organizations to use FortiWeb to authenticate different URLs in different Realms. Administrators can define URL groups that require specific authentication while leaving other URLs open to the public. Using FortiWeb's local, RADIUS or LDAP authentication capabilities ensure correct URL access rights are enforced.

A8 - Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

FortiWeb A8 Protection

Strict reference page enforcing provides protection against sophisticated CSRF attacks. Also, page access rules allow customers to define URL order. Common CSRF attacks attempt to submit a specific crafted request. For example, in a payment order FortiWeb enforces a page order sequence that will block the request if it doesn't go through the proper payment order sequence.

A9 - Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

FortiWeb A9 Protection

FortiWeb protects against known vulnerabilities in third party components using multiple layers of defenses that include both negative and positive security models. Signatures (updated regularly via the FortiGuard Labs network) and Protocol Constraints, together with a robust correlation layer protect against attempts that exploit these known vulnerabilities. Additionally, Auto-Learn creates a positive "normal" user behavior profile that protects against zero day attacks by blocking suspicious activity outside of normal parameters.

A10 - Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

FortiWeb A10 Protection

Auto-Learn profiling identifies when parameters are used in a different manner then they are supposed to. Validation enforcement makes sure characters that are often associated with redirects and forwards are not allowed as part of normal application usage.

FortiWeb Web Application Firewall Ensures Compliance with PCI 6.6

FortiWeb is the only WAF that provides a Vulnerability Scanner module within the web application firewall that completes a comprehensive solution for PCI DSS requirement 6.6 allowing organizations to scan their applications, find existing vulnerabilities and protect them in real time from the same platform. The following is a list of features provided by FortiWeb to help achieve PCI 6.6 compliance:

Features	Benefits
Auto-Learn Security Profiling	Automatically and dynamically builds a security model of protected applications by continuously monitoring real time user activity. Access outside the baseline can then be alerted or blocked.
Application Layer Vulnerability Protection	Automatically Scans and analyzes the protected web applications and detects security weaknesses, potential application known and unknown vulnerabilities to complete a comprehensive solution for PCI DSS.
Web Application Vulnerability Assessments	Automatically Scans and analyzes the protected web applications and detects security weaknesses, potential application known and unknown vulnerabilities and provides reporting on issues that need to be addressed.
Data Leak Prevention	Extended monitoring and protection for credit card leakage and application information disclosure by tightly monitoring all outbound traffic.
Anti Web Defacement	Unique capabilities for monitoring protected applications for any defacement and ability to automatically and quickly revert to stored version.
Multiple Deployment Options	FortiWeb provides a flexible solution that can be easily introduced to any environment introduce FortiWeb in to any existing network implementations.
High Performance and Availability	With ASIC-based technology FortiWeb is able to process tens of thousands of web transactions and provide hardware accelerated SSL offload capabilities and advanced load balancing capabilities. The high availability mode provides configuration synchronization, and allows for a network level failover in the event unexpected potential outage events.
Logging and Reporting	With extensive and accurate logging capability, the web application administrators can pinpoint the specific details when an attack happens. Hundreds of out-of-the-box report types allow administrators or auditors to analyze attacks, events, and traffics for regulatory compliance purposes.

Mapping Fortinet Solutions to PCI Requirements

While FortiWeb helps specifically address PCI DSS requirement 6.6, Fortinet products provide a complete solution for all 12 PCI DSS requirements. The following is a table outlining the requirements and the solutions Fortinet delivers to help address them:

PCI Data Security Standard	Description	Fortinet Solution
Build and Maintain a Secure Network and systems	▪ R1: Install and maintain a firewall configuration to protect cardholder data ▪ R2: Do not use vendor-supplied defaults for system passwords and other security parameters	▪ FortiGate integrated firewall functionality ▪ FortiDB vulnerability assessment and auditing ▪ FortiGate OS vulnerability mgmt
Protect Cardholder Data	▪ R3: Protect stored data ▪ R4: Encrypt transmission of cardholder data and sensitive information across public networks	▪ FortiDB vulnerability assessment and monitoring ▪ FortiWeb web application security ▪ FortiGate IPSec VPN
Maintain a Vulnerability Management Program	▪ R5: Protect all systems against malware and regularly update anti-virus software or programs ▪ R6: Develop and maintain secure systems and applications	▪ FortiGate integrated AV ▪ FortiClient integrated AV ▪ FortiDB vulnerability assessment, auditing and monitoring ▪ FortiWeb web application security ▪ FortiGate OS vulnerability mgmt
Implement Strong Access Control Measures	▪ R7: Restrict access to data by ▪ R8: business need-to-know Identify and authenticate access to system components ▪ R9: Restrict physical access to cardholder data	▪ FortiDB vulnerability assessment, auditing and monitoring ▪ FortiGate integrated database or hooks to Active Directory
Regularly Monitor and Test Networks	▪ R10. Track and monitor all access to network resources and cardholder data ▪ R11. Regularly test security systems and processes	▪ FortiDB auditing and monitoring ▪ FortiAnalyzer event reporting ▪ FortiDB vulnerability assessment ▪ FortiGate OS vulnerability mgmt
Maintain and Information Security Policy	▪ R12: Maintain a policy that addresses information security for all personal	▪ FortiManager security policy management appliance ▪ FortiGate OS vulnerability mgmt

Summary

Achieving PCI DSS 6.6 compliance requires deploying a web application firewall or periodic application vulnerability scanning. FortiWeb helps customers achieve PCI DSS compliance, mitigate application attack threats, and secure their business by providing a unique solution that incorporates both a web application firewall with a vulnerability assessment module.

For more information about the FortiWeb solution and other Fortinet platforms please visit www.fortinet.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Aug 10, 2015