

# ShopVisible™

## *Enlightened Ecommerce and Vulnerability Management: PCI Reqs., WAFs, and the SDLC*

For many engaged Ecommerce enthusiasts, PCI requirement 6 is an esoteric exercise in critical data security. Primarily focused on cardholder data environment (CDE) breaches, access point (AP) attacks and suspect SQL injections, PCI 6.6 regulates web application input scenarios and offers direction for how to comprehensively inspect and safeguard the Ecommerce production data environment that may or may not store sensitive cardholder information. While PCI auditors may recommend utilizing a 3<sup>rd</sup> party web application firewall (WAF), it is not imperative. ShopVisible has employed internally wrought measures to address PCI requirement 6 and in doing so has again proven its innovative spirit in the midst of increasingly stringent global credit card protection aims.

ShopVisible realizes that maliciously driven attacks on web applications have grown all too common in the modern Ecommerce software arena. Protected environments have become open to public Internet spaces giving hackers and other thieves wiggle room to devise and employ breach strategies often ahead of Ecommerce and PCI best practices. ShopVisible strives to function ahead of the curve. Our organizational methodology and level of commitment to Ecommerce security is robust and growing, commensurately with the PCI standards. Heightened online payment safety is crucial and for Ecommerce solution providers, should be priority number one with regards to increasing client ROI and ensuring quality and security for online shoppers.

### PCI DATA SECURITY STANDARD

#### PRINCIPLES AND REQUIREMENTS

##### Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

##### Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

##### Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

##### Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

##### Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

##### Maintain an Information Security Policy

12. Maintain a policy that addresses information security

While the inherent objective of PCI requirement 6.6 is to “prevent exploitation of common vulnerabilities” there are multiple routes to deal with this process. When dealing with either a manual or an automated process, considerations must be dynamic and pro-active. One or more of the following alternative processes can be utilized in order to address PCI requirement 6. This can supply the minimum level of PCI harmony by *1. Manually reviewing applications source code, 2. Properly using an automated source code analyzer/scanning tool, 3. Manually assessing the web application security vulnerabilities and 4. Properly using an automated web application security vulnerability assessment tool.* It is helpful here to distinguish between vulnerability assessments as an identification tool of general susceptibilities and penetration testing as an attempted exploitation of these vulnerabilities, determining whether or not unwanted access and malicious intent is possible.



# ShopVisible™

One way to better prepare for a PCI audit review and consolidate security initiatives is to build upwards from your software development life cycle (SDLC) and extend policy into the WAF. With regards to manual code reviews and assessments, PCI states that these may be performed by qualified internal resources or third party certified reviewers. Analogously, those using automated tools “must have the skills and knowledge to properly configure the tool and test environment, use the tool and, evaluate the results.” A key component here related to internal versus external testing resources is that for the former, “they should be organizationally separate from the management of the application being tested.” In other words, the technical team developing the code should not also be the team that tests and verifies its vulnerabilities.”

It is a PCI best practice to handle a separation of environments and have perhaps one team of developers produce the code and another technical support group unfamiliar with the SDLC then assess it strengths and weakness concerning breach gaps and intrinsic vulnerabilities. In the ShopVisible Ecommerce eco-system for instance, while the Director of Development and the CTO employ industry best practices in the SDLC, the review will ultimately be managed by a Director of Technical Services to ensure code protocol is not corrupted by those who designed it, malicious intent present or not...

PCI shows two ways in which code reviews can be performed to function in accord with application firewall protection. One features the company’s SDLC being scrutinized by an independent security review testing its application source code. Here common and standardized web application vulnerabilities are addressed. They can be either manual or automated process. The other option commonly utilized for requirement 6 is to undergo a test to investigate manual processes and specialized tools to test for the “presence of exposed vulnerabilities and defects in an executing web application.” Here, attacks are simulated via the creation of malicious input. Input responses are then examined “for indications that the application may be vulnerable to certain attacks.” As a safety imperative, here the safeguard should be retested after any breach, simulated or not, to verify that the application is thoroughly constructed and no longer vulnerable Internet insurgency.



Prior to web application deployment into the production arena, all reviews and tests should first be incorporated into the organizational SDLC. Per PCI requirement 6.3, all this should include the company’s information security throughout it. Possible relevant ISP content here may include but is not limited to the following: internal and external security procedures, organizational and system configurations protocols, HR rules etc... Change control processes must be documented clearly here to enforce developers’ inability to bypass code review assessments and engage with the production environment directly. As mentioned earlier, if vulnerabilities are detected in the eco-system then pre-production correction and a retesting must first take place before production implementation.

PCI requirement 6.6 defines application firewalls as WAFs or the “web application firewall which is a security policy enforcement point positioned between a web application and the client end point.” It can be implemented in either software or hardware form and can run in an application device or in a standard OS as a stand-alone piece or component integrator. Normally the firewalls are constructed



# ShopVisible<sup>TM</sup>

along the perimeter of a network or between network conjoining zones or intersections; these act as what PCI deems the “first line of defense” in securing the CDE. ShopVisible’s WAF is built from the ground up in order to provide layered security initiatives. The tiered environment consists of data, business and presentation layers transitioning from the SQL servers through the front-end API and onto the production arena. In Ecommerce, security begins with development and extends through the customer credit card information insertion into the site. Incrementally sound procedures provide the framework for a comprehensive transaction arena and must be solidified before a hacker ever has the ability to maliciously enter the environment.

The WAF is ultimately designed to inspect the application layer contents of the IP packet. PCI 6.6 however “is not meant to introduce redundant controls.” If the IP packet is investigated at some level by the firewall, proxy, or other component then it does not have to be re-inspected by the WAF. It is valuable to understand what the application layer is with regards to the application firewall. PCI defines it as “the layer containing the content that is processed by the application” in a layered or tiered model for the IP packet. WAF technology is “integrated into solutions that include other functions such as packet filtering, proxying, SSL termination, load balancing, object caching” and more. Ultimately, while implementing a WAF is one route to meet PCI requirement 6.6, it does not reduce the imperative importance of crafting a secure SDLC to address PCI requirement 6.3.



#### *PCI's Recommended WAF Capabilities:*

-A PCI commensurate WAF must be able to:

- Meet all PCI requirements related to CDE protection and react accordingly to threats of vulnerability as identified at a minimum in the OWASP TopTen and/or PCI requirement 6.5
- Inspect web application input and respond in a manner set in the organizational ISP with associated log maintenance
- Prevent data leakage: inspect web application output and respond based on active policy rules and log actions
- Enforce positive and negative security models alike: a positive model (white list) here will inform acceptable, permissible behaviors for input and data ranges while denying everything else; the negative model (or black list) defines what is not permissible in scope such as blocked signatures or non-permissible traffic
- Inspect webpage content including HTML, DHTML and CSS; also verify content delivery systems for protocols like HTTP and HTTPS and SSL
- Inspect web services messages if they are exposed to the public Internet, including SOAP and XML
- Inspect any protocol or data construct which is used to transmit data to or from any web application if not otherwise inspected at an alternative access point in the message system flow

**Summary article written by ShopVisible Marketing Manager, Vijay Mahoney; citations and quotations derived from PCI Information Supplement: Req. 6.6 Code Reviews and Application Firewalls, 4/15/2008.**

