Handling Credit Card Data and PCI Compliance

Posted At : November 3, 2006 11:07 AM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

> *Muse Reader Asks:*
> "I thought I would ask your opinion on how to use CF as a front-end to SQL database with CC information and still be compliment with PCI standard 10.2 and 10.3. We are going to have an appliance to capture and store the information needed by the auditors. But I can't have everything showing up as the CF service."

I asked my good friend Brian Harvey from **Studio Cart** to answer this question. He has been a good resource for us on the pitfalls of working with Credit Card data and PCI compliance. His response is quite informative.

Last year I received PCI certification from a third party compliance authority, **Trustkeeper.net**, and am actually in the process of getting re-certified this month. If you are planning to be compliant with the PCI standard I would highly recommend getting certified by a third party. The cost is not that great in relation to the total expense of compliance, and they can actually save you in some cases by providing a framework to follow. I am a level 4 merchant so the complexity of my systems is far less than that of a large corporation.

10.2 and 10.3 deal with providing logs and audit trails for all of your systems that allow access to cardholder data. Being a single owner operator this is a straight forward process for me and includes keeping logs on the following: VPN access to the internal network, Windows logins, database logins, and all web logs.

How you will use Coldfusion to "access credit card data" in your system makes a big difference. In the case of a standard real time shopping cart solution you would simply use CF to interact with a merchant gateway such as authorize.net over an SSL connection. If this is the case you really do not need to store the credit card data. Once you post to the merchant gateway and get a response you can purge the credit card data. Note that if you need to persist the credit card data in your application before you post it to a merchant gateway it should be held as a session variable and not a cookie. However, If your business model requires you to store the card data in a database it needs to be in an encrypted state (Strong encryption available natively in MX7 like Trip-DES or Blowfish) and not be directly accessible by the internet:

(Internet -- Firewall (NAT) -- DMZ -- Firewall (NAT) -- Database)

Also be aware that it is against the PCI standard to store the CVV (Card Verification Value) which is the three or four digit code found on the back of the credit card.

There are not really many cases I can think of in which a credit card number needs to be shown in the clear. In my systems where it is necessary to show credit card data 99% of the time it is masked (Master Card - xxxxxxxxxxxx9200 - Exp. 10/09) like in the event that a user needs to update their account information. In cases where you do need to show all of the credit card data onscreen you can isolate the functionality within a cfc and log the IP, user, date and time, and credit card record ID to a file or a DB when the cfc is invoked. From my understanding that, along with your other logs would meet the requirements.