Security Myth Busters Part 1

Posted At : July 29, 2005 5:01 PM | Posted By : Mark Kruger
Related Categories: Security

When it comes to security and the web there are a number of myths held by casual users. In the next several posts we are going to plow through them together and see if we can come to some conclusions on how best to advise our clients. The first, and perhaps the most ubiquitous myth, has to do with the efficacy of simply having a secure site.

(this blog is a follow up to **Why the padlock is your friend**)

Myth I - Shopping on a Secure Site Keeps me Safe

Many users (maybe most users) think that simply shopping on a site with the little SSL padlock on it makes it safe. That is *not* the case. The little padlock in the corner means that the data you exchange with the server is encrypted. That's *all* it means. It's rather like the white stone path that leads among the land mines in Afghanistan. It provides safe passage *from land mines*. It doesn't keep a sniper from shooting you. It doesn't keep mortar shells from landing on your head. It doesn't keep a rottweiler from ripping out the seat of your pants. It simply guarantees that if you stay on the path you won't step on a land mine. In the same way, using SSL secures the data as it is transmitted through the SSL layer. It doesn't keep your data safe once it arrives. It doesn't ensure that something on the client end (some virus or spyware) isn't logging your data and sending it away on another request. It *just* guarantees that your data will be encrypted from point A to point B.

In the early days of my career we would take virtually any assignment as we were building our business. I remember on 2 separate but equally scary incidents that serve as a reminder to me every time I go onto an unknown site.

Email and Credit Card Numbers - a Bad Combination

First, there was the customer with a "shopping cart" that wanted some modifications. The customer had purchased a very cheap hosting plan with no database. The "shopping cart" was nothing more than a single form that the user will fill out and click submit. Was it secure? Well, it was using SSL if that's what you mean. But without a database the site owner had no way of getting at the data to fill the order. The solution? A simple PHP script collected the form fields and emailed them all to the site owner. The customer of course assumed that through the "magic" of SSL the data was protected and locked away in the technological equivalent of a bank vault. The reality was that they just put their credit card and contact information into the probably the least secure of the internet protocols.

Putting the database online - I mean *really* on line

I once had a customer who's shopping cart worked with access. This is not a great idea... not really even a good idea. But I *am* on occasion willing to work with access. I walked through his routine with him. He showed me how he took the database file and made changes and processed orders - ok fine. He did it once a day and then uploaded the file via FTP. Still nothing really terrible - but I warned him about data synchronization. What happens if someone orders something and you put the file up and overwrite the order. "Oh," he informed me, "I always copy down the latest file

before I overwrite - just so I can check it. Here, let me show you." And with that, he proceeded to open a browser and hit a bookmark. The bookmark was a URL that pointed to his live access file, which was apparently stored under the root of his web site in a folder cleverly named "db". In other words, a Jr. High School student could have easily figured out how to access his Access. When I explained to him why this was a bad idea he assured me it was ok. "Look," he said pointing to the URL, "It's a secure URL!".