

Finding a Balance between Security and Convenience

In the rush to comply with the FFIEC guidelines, many banks may actually be making their online banking channel less secure. The addition of challenge questions is especially troubling. Most customers, myself included, do not want to provide even more personal information just to login to online banking. Challenge questions are inherently weak and troublesome, and do not even represent a true "second factor" for authentication.

Unfortunately, in many ways we are fighting a losing battle. If the customer cannot trust the website that they are signing into, then authentication efforts are wasted. Cyber criminals adjust rapidly and are constantly looking for new exploits. If the 'front door' is locked, they will simply try another method. That is why it is necessary to focus more on transactions than authentication - stronger processes must be built around fraud control at the back end.

To guard their reputations and critical customer data, banks need to protect both their information or "brochureware" websites as well as their online banking sites. At WhiteHat Security, we accomplish this by offering banks the industry's only continuous vulnerability assessment and management service for Web sites. Our Sentinel 3.0 solution provides an ongoing service that delivers up-to-date and comprehensive identification of the vulnerabilities that are putting online customers and organizational data at risk.

Every time a bank updates its website or its third party online banking vendor makes even the slightest change to its software, there is the potential for a new vulnerability to be introduced. For example, cross-site scripting vulnerabilities are very common and troublesome, enabling access to online accounts and even intranet devices. Also it is surprisingly easy for criminals to simply setup an account legitimately at the bank, then after logging into their online banking accounts, use hacking techniques to switch over to another user account.

That is why it is so critical for banks to stay on top of Web site updates, and identify and quickly mitigate new vulnerabilities that may have been inadvertently introduced. Using a combination of expert analysis and proprietary scanning technologies, the WhiteHat Sentinel Service performs scanning, verification and custom testing to identify those vulnerabilities. This kind of ongoing vigilance is needed to protect bank Web sites from emerging threats and vulnerabilities.

While bank IT Departments may have tools to run automated scans against their sites, all too often this approach produces far too many false positives, misses potentially dangerous vulnerabilities and is difficult to repeat as often is required. We have learned from years of experience that a two-pronged, combined approach is necessary: scanning and expert analysis. The vast majority of bank IT employees do not have the time or technical expertise to effectively assess their Web sites. That is where Sentinel 3.0 comes in: it makes the entire process of managing website security much easier and more convenient by providing all the information necessary to quickly and efficiently find and remediate web application vulnerabilities.



Jeremiah Grossman
CTO

Jeremiah Grossman is Chief Technology Officer at WhiteHat Security. Mr. Grossman founded WhiteHat Security in 2001. Prior to WhiteHat, Mr. Grossman was an information security officer at Yahoo! responsible for performing security reviews on the company's hundreds of web applications. Mr. Grossman is a world-renowned leader in web security and frequent speaker at the Blackhat Briefings, NASA, Air Force and Technology Conference, Washington Software Alliance, ISSA, ISACA and Defcon. Mr. Grossman is also a founder of the Web Application Security Consortium (WASC) and the Open Web Application Security Project, as well as a contributing member of the Center for Internet Security Apache Benchmark Group.

