

## Pay Now or Pay Later: Obtaining ROI from Security Solutions

No credit union wants to make headline news for a security breach, so they have invested heavily in traditional security measures such as anti-virus, firewalls, and patching systems. However, attackers have moved up the protocol stack and progressed from simple network-based assaults to more sophisticated web application attacks. The reasons are clear. Eight out of ten websites have a serious vulnerability that is immune to traditional defenses.

Of course traditional security measures still need to be in place, but credit unions must now allocate more resources to secure their online presence and member-facing web applications to avoid becoming victims of these new threats. Many credit unions outsource their online banking and other web applications, and it's important to know the security of those providers as well. The ultimate responsibility and reputation at stake is yours. Every time a website is updated – which is quite frequently in many cases – there is an opportunity to introduce a security issue. Our experience shows that it is more than common; it is actually quite likely to occur.

Unlike networks, all web applications are inherently unique. Each credit union's website contains custom code and many website vulnerabilities cannot be found in an automated manner. Since each website has specialized functionality, the methods to exploit them may be just as specialized. Security expertise, that is often not available in-house, is required.

Assessing your production website is essential. Hackers enter through holes in a live site, not the development or QA environment. Unseen flaws can appear between the time development is completed and production is started. The credit card companies have realized this important distinction. That is why the PCI Data Security Standard mandates scanning all custom web applications in the production environment.

Only a handful of the largest credit unions in the country can afford to keep a web application security specialist on staff to address these issues, which is why it only makes sense to outsource this critical function to WhiteHat Security. In the past, website vulnerability assessment was a time-consuming and often expensive process that was difficult to justify. Our WhiteHat Sentinel service provides continuous vulnerability assessment and management for websites at an affordable price. We provide a quantifiable ROI by minimizing costs, delivering actionable results and offering comprehensive coverage of all vulnerabilities.



All too often security issues boil down to software bugs and those are exactly the issues our technology and team of experts are trained to locate. We identify vulnerabilities that are not just software bugs, but configuration problems, leftover files, poor security settings and much more. There is no hardware or software to install and no drain on your overworked IT staff. We provide continuous assessment that finds the flaws in your website before the hackers do, and arm you with the information you need to protect your organization. By law, credit unions cannot pass liability to a third party – they are ultimately responsible for their members' data. We simplify web application security so that credit unions can rest assured that they are protecting their corporate and member data, complying with government regulations and preserving brand integrity.



**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.