

## Managing Risk and Security Efficiently and Affordably

Due to the recession, many banks are cutting their IT and security budgets, but this is not the time to disregard security issues. Hackers and cyber-criminals are more active today than they have ever been and it is getting easier for novices to join in on these illegal activities. Everyone at the bank - from the CEO on down to the tellers - needs to understand the security implications of their actions.

With malicious and hijacked websites increasing at an alarming rate, some financial institutions have greatly restricted or even eliminated Web access for their employees. Compromised websites can hijack browsers and provide unfettered access into the bank's local area network and their database and file servers. These browser attacks often use sophisticated Java scripts and simply bypass all of the bank's carefully crafted firewall rules.

Bank websites are huge targets for bad actors - and not just their online banking platform. Any time a bank offers a form such as a new account or an online loan application on their website, they can be vulnerable to SQL injection and cross-site scripting attacks. Our research shows exactly how bad the problem has become:

\* 83% of websites have had at least one serious vulnerability\*

\* 64% of websites currently have at least one serious vulnerability\*

Once a form is compromised and personal information gathered, identity theft is almost certain to follow. Even online banking sessions are vulnerable to cross-site request forgery attacks and password thefts. Many people do not realize how easy it is to unencrypt passwords, but it is often a fairly straightforward process.

The ramifications for banks that do not adequately protect and secure their websites are clear: Loss of data, malware infection, loss of customer confidence and failure to meet regulatory requirements. WhiteHat Security is uniquely positioned to help banks mitigate risks because we are at the forefront of website security. Via WhiteHat Sentinel, our SaaS website vulnerability management service, we assess literally thousands of websites per day from a wide range of industries which gives us deep insight into the full range of Web vulnerabilities. More importantly, by keeping our pulse on the latest vulnerabilities, we know how to prevent and stop them. And, we provide this service to our customers on a continuous basis.

Bank IT Departments simply do not have the internal resources to monitor and secure their websites. In response to this dilemma, we have crafted a four-phase Website Risk Management approach built around securing and protecting your website:

1. Asset Identification
2. Vulnerability Management
3. Reporting / Communication
4. Protection

Fortunately, we have also made this an affordable program so that the majority of banks can afford to take part in this solution. We have developed a TCO model that makes sense to come to us for website risk management solutions - the bottom line is that WhiteHat Security offers expert help that can't be duplicated in-house at affordable prices.

\* Data collected in WhiteHat Security Website Security Statistics Report, based on more than 1,500 websites under WhiteHat Security management.



**Anurag Agarwal**  
Director of Education

**Anurag Agarwal** is director of education services at WhiteHat Security. He has more than 14 years of experience designing, developing, managing and securing Web applications at companies including Citigroup, Cisco, HSBC Bank and GE Medical Systems. Mr. Agarwal is also CISSP certified and a Sun Certified Java Developer, and is an active member of the Web application security community, contributing several articles on secure design and coding to industry magazines and frequently speaking at industry events such as Hackerfest, OWASP, and many other regional and national events.

