

## Vulnerability assessment service pays off for Debt Exchange

By Colleen Frye, News Writer  
14 Aug 2006  
SearchAppSecurity.com

When you deal with some of the biggest banks in the world, it goes without saying that security is an overarching concern. That's why The Debt Exchange Inc., a full-service loan sale advisor for commercial, consumer and specialty finance debt, continues to raise the security bar for its online marketplace, which enables financial professionals to collaborate in buying and selling debt and loans.

The latest defense tactic in its arsenal is the addition of automated application vulnerability assessment and penetration testing through ClickToSecure, a software-as-a-service (SaaS) offering from Cenzic Inc. in Santa Clara, Calif.

The Boston-based Debt Exchange launched in 2000 and is one of the largest online exchanges of its kind, according to Kevin Jarnot, chief technology officer. The exchange enables the selling banks to have information posted about the loans they want to sell, and the buying institutions can do their full due diligence online, he explained. Behind this online execution platform is a large service component to the business that happens offline, with The Debt Exchange's seasoned staff of ex-bankers and underwriters providing a loan sale advisory service, helping banks determine which loans they want to sell and how to price them, as well as determining which documents should be scanned and placed online.

Testing applications for security vulnerabilities is an emerging concern among The Debt Exchange's clients, Jarnot said. "We go through quite a few security audits. [Clients] want us to do every type of security audit out there. Application testing has only come up recently in discussions. It's more on their radar now."

Penetration testing was on The Debt Exchange's radar, and Cenzic's managed service for doing so was a good fit for the company, Jarnot said. The ClickToSecure service offered the cost efficiency and the functionality required, he said.

The Debt Exchange also has a limited IT staff -- another reason to look to a third-party service. "We wanted it done as a service," Jarnot said. "We didn't want to purchase software and have to train someone to do the testing."

According to Jarnot, the company has used third parties to test other parts of the site, such as the network perimeter, in several different ways. And The Debt Exchange does its own testing as it develops and releases new pieces of code. However, the company wanted to find a third party to test the application itself.

"We know there are so many ways [to attack an application], like SQL injection and cross-site scripting. It's always better to get a third party. If you know the code too well, it's better to have somebody else do the testing for you," Jarnot said. "Cenzic's testing is completely different from the other types of testing we do. It's our first external application testing."

With ClickToSecure, Cenzic tests the application remotely using its Hailstorm automated penetration testing product. It then provides a vulnerabilities report and analysis, along with remediation steps to correct any problems.

Together, Cenzic and The Debt Exchange came up with a test plan to test the two different parts of the Web site, the administrative side and the user side. Jarnot said his company put a copy of its Web site on a specialized staging server and gave Cenzic access to it. The entire process took roughly two weeks.

Jarnot said the testing was "pretty much flawless in execution. Cenzic did a great job keeping me in the loop, checking in at all hours."

So far, The Debt Exchange has done one scanning with ClickToSecure, and Jarnot said the company is contemplating the frequency of using the service. "It's so cost-effective it can be done several times a year," he said.

While Jarnot said it's hard to quantify the ROI of security investments, "every little bit you do security-wise pays off."