

# VERACODE

CASE STUDY



“Veracode was a quick win for Barclays, for our customers, and also for our third-party vendors,” adds Rhonda MacLean.

“Their SecurityReview product has helped Barclays and its software suppliers deal with the difficult task of scanning code in large volumes in a very efficient manner.”

#### RHONDA MACLEAN

Global Security Officer for Barclays  
Global Retail and Commercial Bank

## Barclays Application Security Assurance Project

Veracode Inc., the world’s leader for on-demand application security testing solutions, won the award for Information Security Project of the Year in The Banker Technology Awards for its work on the Application Security Assurance Project with Barclays.

### Background

As threats within the corporate information security landscape intensify, this award is geared to recognizing excellence in IT security projects within the financial sector. Veracode Security Review, a subscription-based application security testing solution, underpins Barclay’s implementation of secure procurement practices and enables them to manage both their own and their customers’ risk profile. Security Review is the only on-demand service available to test internally developed applications, commercial off-the-shelf software and applications developed offshore for potential software vulnerabilities.

### Business Challenge

As one of the leading global financial services institutions, Barclays, like many of its peers, relies heavily on a number of third-party commercial software and outsourcing providers to help drive its core banking systems. Application vulnerabilities and security breaches are very steadily on the rise. According to Gartner, 75% of new attacks target the application layer, and software vulnerabilities have reached an all-time high—with 7,000 new vulnerabilities discovered over the last year. Against this backdrop, Barclays was justifiably concerned about potential security issues arising from these third-party providers and decided to take a proactive approach to software assurance.

### Project Goals

The bank decided to seek an application security solution that could help create security thresholds for vendors supplying commercial off-the shelf applications and outsourced code to Barclays. In addition to implementing a security best practice approach for any new application purchases, Barclays also was determined to establish security guidelines for existing relationships, even in those cases where existing contracts did not clearly define the scope of security best practices as a mandate. In these cases, the challenge for Barclays was to build a joint business case that would demonstrate a win-win for all parties involved. As the bank did not want to take on potential liability issues of analyzing and reviewing third-party source code, Barclays needed to find a solution that could be deployed without such limitations and could be rolled out quickly, consistently and globally, based on international standards across its broader ecosystem.



“Veracode’s rating system and remediation roadmaps provide extremely meaningful data that help our software suppliers to fix not just the obvious defects, but also the root cause of problems. The net result for Barclays is a rapid cycle of improvement in the security of applications, which is a clear benefit to our customers”

**RHONDA MACLEAN**

Global Security Officer for Barclays  
Global Retail and Commercial Bank

“Rather than trying to change processes within both the bank and our vendors, Veracode’s software-as-a-service model gave us rapid execution and results with minimal resources. Together we have delivered measurable value to our business and our customers, addressing the challenges of a growing and rapidly changing threat environment.”

**RHONDA MACLEAN**

Global Security Officer for Barclays  
Global Retail and Commercial Bank



Veracode, Inc.  
4 Van de Graaff Drive  
Burlington, MA 01803  
Tel +1.781.425.6040  
Fax +1.781.425.6039  
www.veracode.com

© 2010 Veracode, Inc.  
All rights reserved.

## Project Team

Barclays chose Veracode SecurityReview, an on-demand application security service that helps test internally developed applications, commercial-off-the-shelf software, offshore code and open source applications for potential software vulnerabilities. This is the only service on the market to offer code reviews on a software-as-a-service subscription basis. The initial project scope involved Veracode providing fully automated tests and security audits for 20 third-party vendors. The on-demand service requires no hardware, no software, no training and no maintenance, so Barclays was able to undertake the entire project with minimal resources.

## Solution and Results

To initiate the project Barclays quickly identified one of their strategic suppliers of financial services software applications as the pilot vendor for the program. Since Veracode is the only provider that can inspect software executables (binary code), the external supplier was able to upload its code to Veracode’s on-demand code assurance platform without exposing any of its intellectual property in the form of source code. This is an absolute breakthrough. Veracode performed its fully automated analysis within 72 hours and assigned a security rating for each application in the form of a letter grade from A (best) to F (worst) to determine the security level of the supplier’s applications. Veracode’s ratings are based on internally established industry standards such as the Common Weakness Enumeration (CWE), the Common Vulnerability Scoring System (CVSS) and the National Institute of Standards and Technology (NIST). These three standards help provide context around the vulnerability type, the score and the business criticality of each application.

A key benefit for Barclays and all vendors that are being assessed is that Veracode’s rating system provides a common and consistent benchmark that can be used to clearly determine security risk levels and thresholds as well as tracking progress over time. In the case of Barclays, the bank determined that third-party applications had to achieve a pre-defined minimum rating to meet software acceptance criteria by Barclays.

In addition to providing high-level security ratings, Veracode delivered very detailed remediation roadmaps back to the software vendors to help outline a path of achieving software assurance. This remediation roadmap is based on a prioritized list of software vulnerabilities that are ranked depending on ease of remediation and level of severity. Based on this roadmap, the pilot vendor fixed the flaws that were found in the initial analysis within two weeks of receiving the initial report, re-submitted the applications for another scan, and received a score that was well within Barclay’s range of code acceptance.

Given the success of the initial project, Barclays is now rolling out the program to dozens of third-party vendors and outsourcing providers with plans to expand further. Additionally, Barclays will now turn to Veracode SecurityReview to perform security audits on internally developed software, allowing the bank to obtain a holistic view of the security posture of all applications, regardless of whether they were developed internally, offshore or purchased off-the-shelf. No other service is able to scan the entire code base and, therefore, provide such breadth of vision backed by clear, independent metrics.

## ABOUT VERACODE

Veracode is the world’s leader in cloud-based application risk management. Veracode SecurityReview is the industry’s first solution to use patented binary code analysis, dynamic web assessments, and partner or Veracode delivered manual penetration testing, combined with developer e-learning and access to open source security ratings to independently assess and manage application risk across internally developed applications and third-party software without exposing a company’s source code. Delivered as a cloud-based service, Veracode provides the simplest, most complete, and most accurate way to implement security best practices, reduce operational cost and comply with internal security policies or external standards such as OWASP Top 10, CWE/SANS Top 25 and PCI.