IBM Kundenreferenz
Digitale Medien

Rational. software

OEV Online Dienste: Objektiv getestete Sicherheit von Web-Anwendungen durch AppScan.

Überblick

- ***Die Aufgabe***
  Ergänzung von externen Security Audits in der Anwendungsentwicklung durch rasch einsetzbares Sicherheitswerkzeug im eigenen Haus
- ***Die Lösung***
  IBM Rational AppScan Standard Edition für das automatisierte Scannen von Web-Anwendungen und für die Erstellung von Berichten
- ***Die Vorteile***
  Hohe Zeitersparnis durch automatisch generierte Sicherheitsberichte mit Korrekturempfehlungen für verschiedene Zielgruppen; objektive, aktuelle Ergebnisse; Optimierung der Qualitätssicherung im Anwendungsentwicklungsprozess

Web-Anwendungen: Spagat zwischen Offenheit und Sicherheit.
Zielgruppenspezifische Inhalte, interaktive Elemente, leichte Kontaktaufnahme, Abschluss online: Öffentliche Versicherer sind mit ihren Web-Auftritten und -Strategien im Wettbewerb ganz vorne dabei. Was für den Besucher wie ein spielerisch-informativer Spaziergang erscheint, ist das Ergebnis präziser Projektarbeit. Dafür haben die öffentlichen Versicherer und Sparkassen einen speziellen Partner: die OEV Online Dienste GmbH in Düsseldorf. Der Experte für digitale Medien und medienübergreifende Vertriebskonzepte wurde 2001 gegründet und beschäftigt heute 30 Spezialisten in den drei Bereichen Projekt- und Prozessmanagement, Marketing und Kommunikation sowie Support.

„Digitaler Vertrieb ist oft eine Gratwanderung für den Anbieter“, sagt Finn Axt, im Team Projekt- und Prozessmanagement für die Anwendungsentwicklung von Vertriebskomponenten und für Internet-Auftritte verantwortlich. „Auf der einen Seite will man es dem Kunden so einfach wie möglich machen, zum Beispiel durch Web-Formulare oder Tarifrechner. Auf der anderen Seite geht man im Versicherungsbereich mit sensiblen persönlichen Daten um, die besonderen Schutz und Sicherheit benötigen. Dafür müssen letztlich wir geradestehen.“

AppScan ergänzt Security Audits und bringt objektive Ergebnisse.
Verwundbar sind Web-Seiten zum Beispiel durch Cross-Site Scripting (XSS), bei dem eine URL oder Formulareingabe von außen manipuliert wird, um Adressen auszuspionieren. Über manipulierte Hyperlinks könnten Cookies, Passwörter oder Formularinhalte in unbefugte Hände gelangen und schädlicher Programm-Code in die Web-Seite einfließen, auch wenn die Seite selbst hundertprozentig vertrauenswürdig ist. „Man braucht viel Wissen und Erfahrung, um Web-Anwendungen sicher zu machen“, so Finn Axt. „Die Anwendungen lassen wir von externen Entwicklungspartnern erstellen, und wir konzentrieren uns auf die technischen Spezifikationen, Qualitätssicherung und die Auftragsabwicklung mit den Kunden.“ Die Entwicklungspartner der OEV sind gehalten, regelmäßig Security Audits auf Anwendungsseite und auf Netzwerkseite durchzuführen.

„Ein sehr großer Vorteil von AppScan ist, dass das Programm die Ergebnisse sofort bewertet und einordnet, einschließlich Vorschlägen für Korrekturen."

Finn Axt, Team Projekt- und Prozessmanagement, OEV Online Dienste GmbH, Düsseldorf

Mit IBM Rational AppScan verfügt die OEV über ein zusätzliches Werkzeug, um die Qualität der Anwendungsentwicklungsarbeit objektiv nachvollziehen zu können. In erster Linie setzt die OEV AppScan für automatisierte Sicherheitstests schon während der Entwicklungsphase ein. So weisen die produktiven Anwendungen von Anfang an einen sehr hohen Sicherheitsstandard auf und werden später eher routinemäßig in einzelnen Bereichen gezielt geprüft. „Mit AppScan testen wir die Sicherheit von Anwendungen, noch bevor wir sie unseren Kunden zur Verfügung stellen", unterstreicht Finn Axt. „Ein sehr großer Vorteil von AppScan ist, dass das Programm die Ergebnisse sofort bewertet und einordnet, einschließlich Vorschlägen für Korrekturen. Mit AppScan können wir selbst nachvollziehen, ob eine Schwachstelle für eine bestimmte Anwendung besonders kritisch ist, und ob die Lücke geschlossen wurde, nachdem wir den Auftrag dazu an die Entwickler zurückgegeben haben."

Präzise Auswertungen je nach Zielgruppe sehr einfach möglich.

IBM stellte AppScan 2007 als neu in die Rational Produktpalette aufgenommene Lösung bei der OEV vor, und man war sofort interessiert an diesem Werkzeug. Es ergänzt bei der OEV den Functional Tester und Performance Tester von IBM Rational. „Wir haben auf dem europäischen Markt keine Lösung zur Identifizierung von Schwachstellen gefunden, die annähernd vergleichbar ist", meint Finn Axt. „IBM steht für kontinuierliche Weiterentwicklung und kann uns einen verlässlichen Support bieten, und zwar zu den Zeiten, die für uns am wichtigsten sind. Das sind die Öffnungszeiten der Sparkassen und Versicherungsagenturen." Die OEV war der erste Anwender von IBM Rational AppScan innerhalb der Sparkassen-Finanzgruppe in Deutschland. Finn Axt: „Unsere Architektur ist relativ komplex, und wir haben festgestellt, dass wir mit dem Werkzeug leicht gewisse Netzwerkeinstellungen vor dem Scannen vornehmen können. Wir gewinnen Zeit, weil wir selbst schnell einen Testlauf durchführen können, wenn irgendwo ein Verdacht auf eine Schwachstelle besteht. Und wir können unseren Kunden anhand der grafischen Präsentationen schnell sagen, wo gehandelt werden muss, oder ihm die notwendigen Informationen für die eigene Abwägung zur Verfügung stellen." AppScan erlaubt es der OEV, sehr einfach Auswertungen je nach Zielgruppen zu erstellen: umfangreiche technische Berichte für die Entwickler, Zusammenfassungen für Projektleiter oder Überblicksschaubilder für die Kunden.

Intuitive Bedienoberfläche für den schnellen Start.

IBM Rational AppScan läuft bei der OEV in der Standard Edition auf einem handelsüblichen PC mit Breitband-Internet-Anbindung. Die Grundfunktionalität ist selbsterklärend, lobt die OEV. Man könne AppScan intuitiv nutzen und mit Hilfe von Assistenten rasch die richtigen Eingaben machen. Und fürs gezielte Testen einzelner Anwendungsbereiche gibt es eine Vielzahl von detaillierten Einstellmöglichkeiten. Präzision ist alles: Ein jüngst durchgeführtes externes Security Audit für eine Anwendung brachte vergleichbare Ergebnisse wie der Test mit AppScan.

OEV
ONLINE DIENSTE

IBM

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM Form GK12-4390-00 (02/2009)