Seeker®

Agile Software Security

PRODUCT BRIEF

Chaque build, Chaque version, Chaque application, Sécurisés

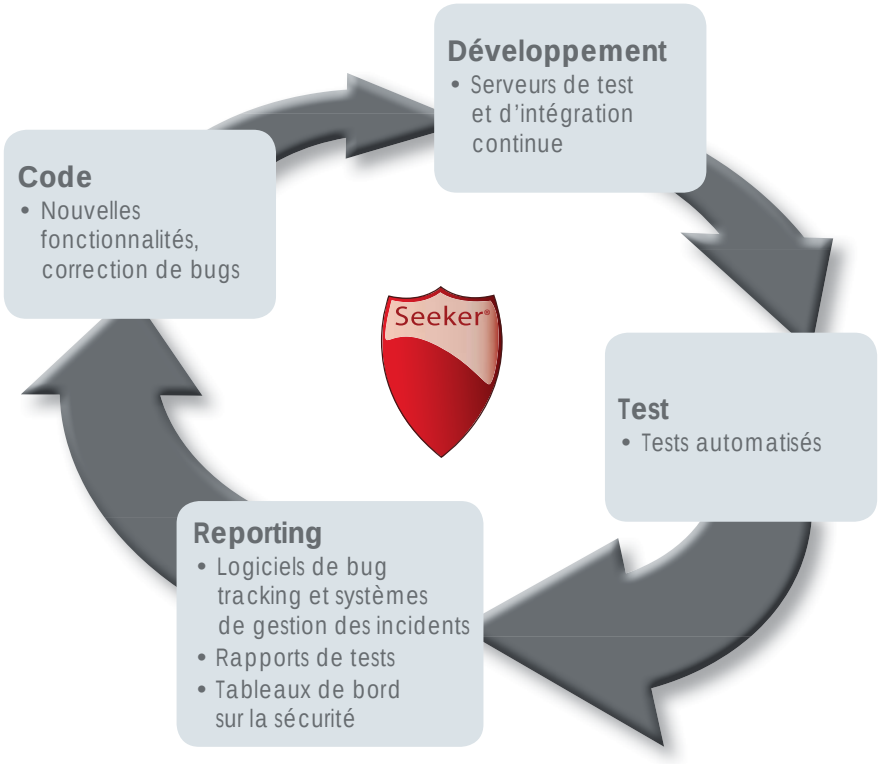
Seeker est une solution IAST (Interactive Application Security Testing) qui permet aux entreprises de développer des logiciels sécurisés.

Seeker détecte avec une grande précision les vulnérabilités lors des processus de développement et de test. À l'aide d'une technologie unique, il analyse le code et les flux de données pendant l'exécution de l'application afin de mieux comprendre le contexte dans lequel se trouvent les vulnérabilités.

Seeker évalue l'impact de l'exploitation du code vulnérable et fournit une explication claire des risques. Seeker élimine totalement les faux positifs. Cette approche permet de confirmer ou d'infirmer l'exploitabilité et la criticité des vulnérabilités détectées sans intervention humaine.

Seeker fournit une vision claire du niveau de sécurité des applications en fonction des critères de conformité. Il met à la disposition des développeurs toutes les informations nécessaires pour sécuriser le code.

Seeker permet un processus d'automatisation des tests de sécurité dans le SDLC :



"SEEKER A ÉTÉ CONÇU POUR ÊTRE PLEINEMENT INTÉGRÉ DANS LE PROCESSUS DE DÉVELOPPEMENT AGILE, PERMETTANT A TOUS LES ACTEURS DE TRAVAILLER ENSEMBLE POUR CRÉER DES LOGICIELS SÉCURISÉS"

Quotium

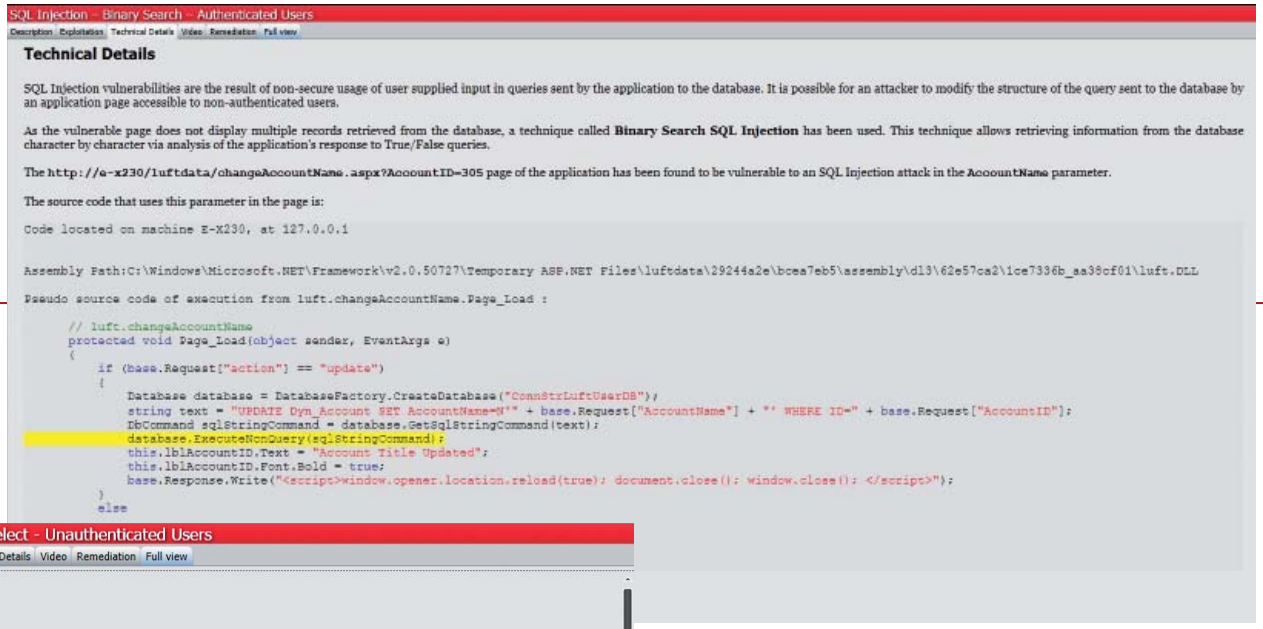
TOUTES LES INFORMATIONS NÉCESSAIRES POUR SÉCURISER LE CODE

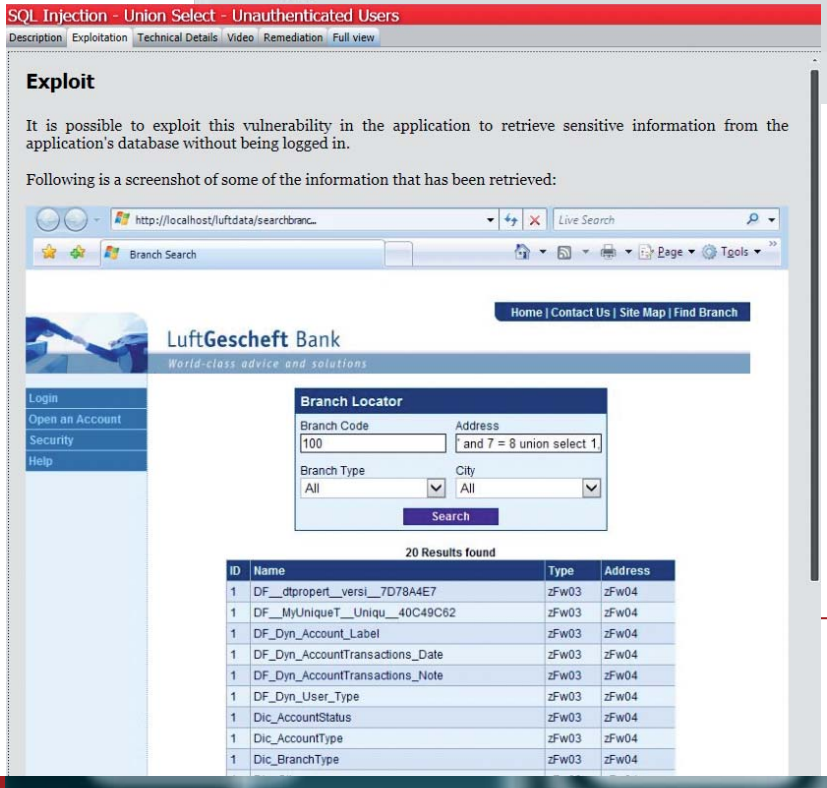
Les lignes de code vulnérables

Seeker fournit des informations détaillées sur l'emplacement exact de la vulnérabilité dans le code applicatif, le niveau auquel est déployé le code et le chemin qu'a suivi le code à risque à partir du moment où il est apparu jusqu'à la vulnérabilité créée.

Des instructions de correction contextualisées

Seeker utilise les informations sur l'application, le langage de programmation, le cadre utilisé, les composants et les bases de données pour fournir des explications claires du problème et la correction la plus rapide et efficace. Seeker n'a pas besoin du code source pour effectuer son analyse. Cela permet d'effectuer des tests de sécurité de n'importe quel code tiers intégré dans l'application, comme les bibliothèques open source, les composants développés par d'autres éditeurs ou des solutions du commerce. Seeker peut également proposer des corrections pour sécuriser les interfaces, même si le code source n'est pas disponible.





Explication des exploitations

Seeker fournit une explication pas à pas de la manière dont un pirate peut exploiter la vulnérabilité et propose une vidéo illustrant le déroulement de l'attaque sur l'application testée.

Il permet aux développeurs, aux testeurs et aux managers de simuler à nouveau l'attaque et de comprendre les conséquences du code vulnérable.

UNE VUE D'ENSEMBLE CLAIRE DE LA SÉCURITÉ ET DE LA CONFORMITÉ DE L'APPLICATION

Rapports sur les vulnérabilités

Les rapports sur les tests Seeker offrent une vue d'ensemble immédiate du niveau de risque auquel est exposée l'application en fonction de critères de conformité. Celle-ci peut être établie selon les classifications standards ou selon des besoins sur mesure.

Tableaux de bord Seeker pour la gestion de la sécurité

Le référentiel de données centralisé stocke les informations sur tous les projets et tests de l'entreprise. Les utilisateurs autorisés peuvent ainsi surveiller le niveau de risque général, les tendances de vulnérabilités, l'état de conformité des applications, les équipes chargées du développement et les projets au sein de l'entreprise. Seeker permet aux managers de repérer les systèmes vulnérables et les équipes qui ont besoin de davantage d'attention.

TECHNOLOGIES PRISES EN CHARGE

➔ **Systèmes d'exploitation**
Windows XP/2003 ou version supérieure (32/64 bits)
Linux (ex : RedHat, CentOS, Debian, SUSE)
Unix (ex : Solaris, HP-UX, AIX)

➔ **Technologies applicatives**
JAVA, .NET, PHP

➔ **Serveurs d'application**
.NET – IIS
Java – Tomcat, WebSphere, WebLogic, Glassfish, JBoss ou tout serveur J2EE
PHP – Apache/IIS

➔ **Bases de données**
Oracle, MS SQL Server, MySQL, PostGreSQL, DB2

➔ **Procédures stockées**
PL-SQL (Oracle), T-SQL (SQL Server)

INTERFACES

Les utilitaires incorporés dans Seeker permettent une intégration transparente aux outils et processus de développement logiciels.

➔ **Cadres de test automatisés**
Selenium, IBM Rational Functional Tester ou tout autre cadre

➔ **Serveurs de test en intégration continue**
Microsoft TFS, HP Quality Center, Hudson, Jenkins et toute autre plateforme après activation par la ligne de commande Seeker

➔ **Logiciels de bug tracking et systèmes de gestion des incidents**
IBM Clear Quest, HP QC, Jira, Bugzilla, Microsoft TFS, etc...

À PROPOS DE QUOTIUM

Quotium est un éditeur français spécialisé dans le développement de solutions logicielles innovantes pour des applications métiers sécurisées et robustes tout au long de leur cycle de vie. Avec sa solution logicielle de sécurité applicative, Quotium est le pionner du développement de la technologie d'analyse du code applicatif pendant son exécution (IAST - Interactive Application Security Testing).

NEW YORK
575 Madison Avenue, 25th fl. New-York, NY 10022, USA
Tél. : +1-212-935-9760 - Fax : +1-212-755-6385

LONDRES
4 Park Place, London SW1A 1LP, Royaume-Uni
Tél. : +44 (0) 203 178 3681 - Fax : +44 (0) 207 898 9101

PARIS
84/88 bd de la Mission Marchand 92411 Courbevoie Cedex
Tél. : +33 (0)1 49 04 70 00 - Fax : +33 (0)1 49 04 71 66

Contact : sales@quotium.com

Suivez-nous sur Twitter @quotium

www.quotium.com

Quotium