

Megalkuvás nélküli biztonsági megoldás a közepes méretű vállalatok webes alkalmazásaihoz

Rational. software

IBM Rational AppScan Express

Legfőbb előnyök

- Megalkuvás nélküli biztonsági megoldás a közepes vállalatok webes alkalmazásaihoz
- Lehetővé teszi, hogy kevés erőforrás felhasználásával átfogóan és rendszeresen teszteljék a webes alkalmazások sérülékeny pontjait
- Rendkívüli mértékben csökkenti a kézzel végzett tesztelést, ezáltal jelentős megtakarítást tesz lehetővé
- Segítségével a sérülékeny pontok felderítéséhez és megértéséhez olyanok is végezhetnek biztonsági ellenőrzéseket, akik nem biztonsági szakértők; az eszköz minden problémáról világos leírást ad
- Szakértői ajánlásokat ad, hogy miként szüntethető meg a sérülékenység kiváltó oka
- Automatikusan ellenőrzi a Web 2.0-s technológiákat (pl. Flash, JavaScript vagy AJAX) használó webes alkalmazásokat
- Az egyedi, integrált webalapú oktatás betekintést nyújt a biztonsági problémák részleteibe
- Egyszerűen telepíthető asztali alkalmazás, amely így gyorsan bevezethető
- Több mint 40 előre definiált jelentést tartalmaz, amelyek megfelelnek az ellenőrzés eredményeit a legfontosabb iparági és hatósági szabványoknak (pl. a bankkártyás fizetésekre vonatkozó PCI DSS szabványnak)

A webes alkalmazások sérülékeny pontjai: kapu az Önök érzékeny adataihoz

Ma már számos alkalmazás webalapú szoftvereket és rendszereket használ az üzleti folyamatok működtetéséhez. Ezek bonyolítják le a tranzakciókat a szállítókkal, és a korábbiaknál sokkal fejlettebb szolgáltatásokat nyújtanak az ügyfelek számára. Igen nagy nyomás nehezedik a vállalatokra, hogy mindig egy lépéssel a vetélytársaik előtt járjanak, ezért sajnos sokszor túl kevés figyelmet fordítanak arra, hogy ezek az alkalmazások ne veszélyeztessék a vállalat egészének biztonságát, miközben a rosszindulatú hackerek a sérülékeny pontokat kihasználva akár a cég bizalmas információihoz vagy az ügyfelek adataihoz is hozzáférhetnek.

Átfogó biztonsági védelem az összetett webes alkalmazásokhoz

Az IBM Rational AppScan Express tesztek és ellenőrzések biztosít a webes alkalmazások számos sérülékeny pontjához, többek között azokhoz, amelyek szerepelnek a fenyegetéseknek a Web Application Security Consortium (WASC) által osztályozott listáján. Az IBM Rational AppScan Express robosztus módon ellenőrzi a legújabb Web 2.0-s technológiákat használó alkalmazásokat. Javítottuk a Flash és a fejlett JavaScript nyelvek támogatását, valamint átfogó támogatást nyújtunk az Ajax-programozásban használt építőkövekhez (többek között kimondottan a JavaScript Object Notation-höz [JSON] és a Web Services paraméterekhez).

Költségmegtakarítás a pontos és automatikus ellenőrzések révén

Az IBM Rational AppScan Express úgy elégíti ki a közepes méretű vállalatok egyedi igényeit, hogy számukra elérhető áron nyújtja az IBM Rational AppScan Standard Edition-ben található magas szintű biztonsági ellenőrzéseket, elérhetővé téve ezáltal a webes alkalmazások átfogó biztonsági tesztelését. Az IBM Rational AppScan Express a sérülékeny pontok kézi ellenőrzéséhez képest jelentősen csökkenti az időráfordítást és a költségeket, hogy Ön a vállalat egyéb informatikai és biztonsági igényeivel foglalkozhasson. Akár házon belül, akár kiszervezve végzik most a sérülékeny pontok kézi ellenőrzését, az IBM Rational AppScan Express drámaian lecsökkenti az alkalmazások teljes biztonsági felméréséhez szükséges időt, ezáltal pedig Önök a negyedéves vagy évenkénti ellenőrzések helyett folyamatosan nyomon követhetik biztonsági helyzetüket. Így sokkal magasabb biztonsági szintet érhetnek el, miközben a költségeik is meredeken csökkennek.

Az IBM Rational AppScan Express szabadalmaztatott ellenőrző algoritmusai nagyon pontos eredményt biztosít és nagymértékben lecsökkenti a téves riasztások számát. A pontosság és hatékonyság növelése érdekében egyedi adaptív tesztelési eljárást használ, amely intelligensen utánozza az emberi viselkedést, hogy alkalmazkodva a leghatékonyabban ellenőrizhesse a különböző alkalmazásokat. Az IBM Rational AppScan Express az egyes paraméterek szintjéig lemenve „megtanulja” használni az alkalmazásokat, és alkalmazkodóképessége révén mindig csak a lényeges teszteket hajtja végre. A legújabb fenyegetések elleni védelem érdekében az IBM Rational AppScan Express minden indításkor letölti az IBM biztonsági szakértőitől származó legfrissebb adatokat.

Az alkalmazás ezenkívül abban is segít a vállalatokat, hogy megfeleljenek a kritikus biztonsági előírásoknak (pl. Card Industry Data Security Standard, PCI DSS), mert lehetővé teszi egy adott biztonsági szint folyamatos fenntartását. Az IBM a Rational AppScan Express alkalmazás révén elismert víruskereső-gyártó (Approved Scanning Vendor, ASV), így az IBM Rational AppScan Express tökéletes választás, ha a cél a PCI DSS által leírt alkalmazás-biztonsági előírásoknak való megfelelés.

Azonnali eredmények, egyedülállóan egyszerű kezelhetőség

Nem mindenki biztonsági szakértő. Az IBM Rational AppScan Express ezért számos egyedülálló felhasználóbarát funkciót tartalmaz, amelyek a „laikusok” számára is megkönnyítik a webes biztonsági ellenőrzést. Az Ellenőrzési beállítások varázsló lépésről lépésre végigvezeti a felhasználót az első ellenőrzés paramétereinek beállításán. Olyan alapvető információkra kérdez rá, mint a kiindulási IP-cím vagy domainnév, a használni kívánt ellenőrzési profil, a szükséges belépési név és jelszó, illetve más egyszerű paraméterek. Az Ellenőrzési szakértő megvizsgálja, hogy helyesek-e a beállítások, majd néhány végső ajánlatot tesz, például a Java-értelmezés bekapcsolását, amennyiben az ellenőrzött rendszer JavaScript-et használ. Amikor a varázsló végzett, az IBM Rational AppScan Express készen áll, hogy megkezdje az ellenőrzést, majd visszaadja a sérülékeny pontok listáját és ajánlatokat tegyen ezek kiküszöbölésére. A vállalat biztonsági ismereteinek bővítése érdekében az IBM a Knowledge On Demand szolgáltatást kínálja. Ez a képzési és oktatási erőforrások olyan egyedi gyűjteményét jelenti, amely webalapú oktatási modulokat is tartalmaz, és mindig igény szerint jeleníti meg a biztonsági kérdésekkel kapcsolatos információkat.

Küszöbölje ki hatékonyabban a problémákat a prioritás szerint rendezett eredmények és megoldási javaslatok segítségével!

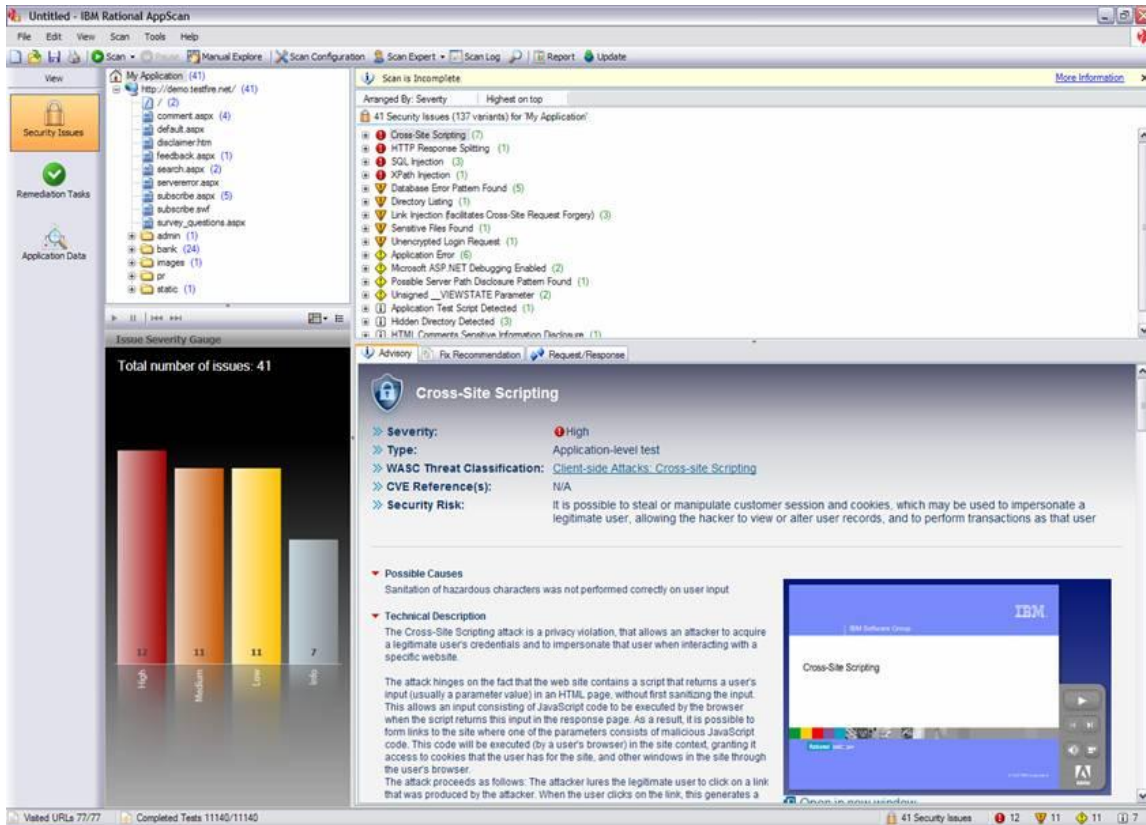
A webes alkalmazások sérülékeny pontjainak kiküszöbölése kapcsán az egyik leginkább kritikus kérdés, hogy milyen gyorsan orvosoljuk az egyes problémákat. Az IBM Rational AppScan Express minden egyes lefuttatott ellenőrzés után prioritás szerint rendezett listát ad vissza a talált sérülékeny pontokról. Ez lehetővé teszi, hogy először a legmagasabb prioritású problémákat oldjuk meg, így a vállalat a biztonsági szempontból legfontosabb kérdésekre összpontosíthat. Minden sérülékeny ponthoz leírás tartozik annak hátteréről és a lehetséges következményekről. Az egyedülálló, integrált webalapú oktatási modulok közvetlenül a felhasználói felületről érhetőek

el. Az IBM Rational AppScan Express megoldási képernyője ezután leírja, hogy milyen lépéseket kell tenni a probléma kiküszöbölésére, és példákat is mutat a biztonságos és nem biztonságos programkódra.

Az integrált jelentések betekintést nyújtanak a biztonsággal és az előírásokkal kapcsolatos legfontosabb kérdésekbe

Az IBM Rational AppScan Express képes testreszabott biztonsági jelentéseket készíteni; többek között az is megadható, hogy melyik adatpontok melyik jelentésekben szerepeljenek. A felhasználók ezen kívül több mint 40 előre definiált jelentés közül is választhatnak, amelyek megfeleltek az ellenőrzés eredményeit a legfontosabb iparági és hatósági szabványoknak. Ezek közé tartoznak a következők: National Institute of Standards and Technology Special Publication (NIST SP) 800-53 és az OWASP Top 10, Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA), Freedom of Information and Protection of Privacy Act (FIPPA), valamint a Payment Application Best Practices (PABP).

Hogy a jelentések még hozzáférhetőbbek legyenek, a vállalatok a jelentéskészítésre szolgáló IBM Rational AppScan Reporting Console-t hozzáadhatják meglévő IBM Rational Standard Edition rendszerükhöz. Az Rational AppScan Reporting Console skálázható vállalati architektúrára épül, amely szerepeken alapuló hozzáférést biztosít a jelentésekhez, és képes összesíteni a több IBM Rational AppScan Express példányból származó adatokat. A részletekbe menő, ám könnyen érthető áttekintő képernyőknek és a rugalmas jelentéskészítési nézeteknek köszönhetően az IBM Rational AppScan Reporting Console az egész vállalatra kiterjedően betekintést nyújt a kockázatokba és segítségével folyamatosan nyomon követhető az ezek kiküszöbölésére irányuló erőfeszítés.



Az IBM Rational AppScan Express Biztonsági tanácsadó nézete segítségével a felhasználók egyszerűen azonosíthatják, értelmezhetik és kiküszöbölhetik a webes alkalmazások legfontosabb sérülékeny pontjait.

Hatékonyabb irányítás az ellenőrzések teste szabásával és kibővítésével

Az IBM Rational AppScan Express különlegesen hatékony testreszabási lehetőségeinek köszönhetően az Önök cége hatékonyabban irányíthatja a webes alkalmazások sérülékeny pontjainak ellenőrzését.

Az **IBM Rational AppScan Express** egy hatékony interfész, amely lehetővé teszi, hogy a naplózott ellenőrzés végrehajtásától kezdve egyedi tesztek elindításáig az IBM Rational AppScan Express minden egyes funkcióját egyedi módon meghívják. A platform révén az alkalmazás egyszerűen integrálható már létező rendszerekbe. Ezenkívül támogatja a Rational AppScan Express ellenőrzőmotorjának speciális, egyedi felhasználását; erre épül a Rational AppScan eXtensions Framework és a Pyscan is.

A **Rational AppScan eXtensions Framework (AXF)** egy rugalmas keretrendszer, amelynek segítségével a felhasználók az IBM Rational AppScan Express funkcióinak kiegészítésére egyedi modulokat tölthetnek be. A Rational AppScan eXtensions programozási hozzáférést biztosít az IBM Rational AppScan Express-hez, így a felhasználók teste szabhatják és kibővíthetik a meglévő funkciókat, hogy azok illeszkedjenek saját folyamataikhoz, valamint automatizálhatják a házon belüli tevékenységeket és letöltés után kihasználhatják a Rational AppScan eXtensions

közösségi portálon (<http://axf.watchfire.com>) rendelkezésre álló számos nyílt forráskódú modul funkcióit.

A **Pyscan** a Rational AppScan-re és a Pythonra épülő platform, amely a webes alkalmazások biztonsági tesztelésére szolgál. A Pyscan segítségével az ellenőrök a kézi audit elvégzése során is támaszkodhatnak a Rational AppScan Standard Edition által nyújtott funkciókra. A platformon keresztül könnyen elérhetők az olyan szolgáltatások, mint az AppScan Standard Edition-be épített, belépési állapot megőrzésére szolgáló fejlett session-kezelés, az ellenőrzött alkalmazásokra vonatkozó adatok tárháza és a hatékony jelentéskészítési funkciók. A Pyscan rendkívüli mértékben megnöveli az audit kézzel végzett feladatainak a hatékonyságát, s mindeközben nem kell lemondani az ellenőr pótolhatatlan szaktudásáról.

Az IBM Rational AppScan Express rendszerkövetelményei

Processzor: Pentium P4, 1,5 GHz (2,4GHz ajánlott)

Memória: 512 MB RAM (1 GB ajánlott a nagy weblapok ellenőrzéséhez)

Szabad lemezterület: 1 GB (10 GB ajánlott a nagy weblapok ellenőrzéséhez)

Hálózat: 1 NIC 10 MBPS a TCP/IP-vel konfigurált hálózati kommunikációhoz (100 Mbps ajánlott)

Operációs rendszer: Windows XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista

Microsoft Internet Explorer 5.5 vagy annál magasabb verzió (IE 6.0 vagy magasabb verzió ajánlott)

Microsoft .Net keretrendszer 2.0 vagy annál magasabb verzió

JRE 5.0 (csak a HTTP proxy-hoz)