A webes alkalmazások stratégiai védelme
az üzleti célkitűzések támogatására

Rational. software

IBM

IBM Rational AppScan:
növeli a webes alkalmazások biztonságát.

Veszélyben van-e az Ön vállalata a sebezhető alkalmazások miatt?

Sok vállalat használ webalapú szoftvereket az üzleti folyamatok támogatására, a tranzakciók lebonyolítására és arra, hogy egyre kifinomultabb szolgáltatásokat nyújtson ügyfeleinek. A biztonsági kérdéseknek minden online alkalmazás bevezetése során a szoftverfejlesztési folyamat részét kell képezniük. Sajnos azonban a vállalatokra igen nagy nyomás nehezedik, hogy tartsák a határidőket és megőrizzék lépéselőnyüket a versenytársakkal szemben, ezért sokuk nem végzett megfelelő biztonsági tesztelést, és az ebből eredő sebezhető pontok rengeteg lehetőséget jelentenek hackerek számára, hogy jogosulatlanul hozzáférjenek a vállalati vagy személyes adatokhoz, illetve eltulajdonítsák azokat - ez pedig az egész vállalat számára veszélyt jelent.

Az IBM Rational® AppScan szoftvercsomagja piacvezető biztonsági megoldást jelent, amely a teljes szoftverfejlesztési ciklus során használható a láthatóság és ellenőrzés növelésére, így a vállalatok megfelelően kezelhetik az alkalmazásbiztonsággal kapcsolatos kihívásokat. A csomag a következő szoftvereket tartalmazza:

- IBM Rational AppScan Standard Edition
- IBM Rational AppScan Express Edition
- IBM Rational AppScan Tester Edition
- IBM Rational AppScan Developer Edition
- IBM Rational AppScan Build Edition
- IBM Rational AppScan Enterprise Edition
- IBM Rational AppScan SaaS (szoftver mint szolgáltatás) megoldások
- IBM Rational AppScan Reporting Console
- IBM Rational AppScan webalapú oktatási anyagok

Ezen megoldások mindegyike tartalmaz ellenőrző, jelentéskészítő és megoldási javaslattevő funkciókat. Az egyes megoldások különféle felhasználók igényeit elégítik ki, így biztonsági menedzserek, behatolási tesztelők, biztonsági ellenőrök, alkalmazásfejlesztők, build-menedzserek és minőségbiztosítási (QA) csoportok is használhatják őket.

A kritikus webalapú üzleti eszközök védelme

A Rational AppScan szoftvercsomag átfogó biztonsági megoldást jelent az összetett webes alkalmazásokhoz. Képes a webes alkalmazások jellemző sebezhető pontjainak tesztelésére, többek között a Web Application Security Consortium (WASC) osztályozásában szereplő elemek ellenőrzésére. A Rational AppScan összes megoldása tartalmazza ugyanazokat a hatásos és rugalmas alapfunkciókat, amelyek lehetővé teszik a legújabb Web 2.0-s technológiára épülő alkalmazások széles körű ellenőrzését. Ebbe beletartozik az Adobe® Flash technológia és a fejlett JavaScript nyelvek családja csakúgy, mint az aszinkron JavaScript és az XML (AJAX) programozási nyelvek támogatása.

A Rational AppScan alapfunkciói hatékony ellenőrzést biztosítanak és könnyen kezelhetők

- A felhasználói felület részét képezi a nézetválasztó, amelyben faszerkezetben áttekinthetők az alkalmazások és az azonosított, hierarchikusan rendezett biztonsági problémák, illetve a fejlesztők számára tett javaslatok és a részleteket tartalmazó panelek.
- A felhasználók az adaptív tesztelési eljárás segítségével elemezhetik az alkalmazások paramétereit és választhatják csak azon fontos tesztek elvégzését, amelyek nem hátráltatják a fejlesztési folyamatot.
- A rendszer támogatja az összetett hitelesítést, így a többlépéses hitelesítési folyamatok is ellenőrizhetők.

Az IBM Rational AppScan biztonsági tanácsadó nézete

- A fejlett munkamenet- (session-) kezelés automatikusan újra bejelentkezik, amikor az szükséges.
- Az eredmények valós időben jelennek meg, így a teljes ellenőrzés befejezése előtt is lehet reagálni a felismert problémákra.
- A beépített mintaillesztési szabályok leegyszerűsítik a hitelkártya-számokkal, társadalombiztosítási számokkal ill. egyéb numerikus sorozatokkal kapcsolatos tesztelési feladatokat.

A Rational AppScan testreszabást és irányítást támogató alapfunkciói

- Az IBM Rational AppScan eXtensions Framework segítségével a felhasználók a tesztelési lehetőségeket kibővítő modulokat hozhatnak létre, oszthatnak meg és tölthetnek be.
- A Pyscan egyesíti a Rational AppScan-t a Python parancsfájlok képességeivel, lehetővé teszi, hogy kibővítsük a tesztelést a felhasználói felület korlátozása nélkül.
- A Rational AppScan szoftverfejlesztő csomagja (SDK-ja) lehetővé teszi, hogy a rendszer funkcióit programkódból is elérjék, legyen szó egy hosszú ellenőrzés lefuttatásáról vagy egy egyedi teszt megkezdéséről. Az SDK-ban található interfészek leegyszerűsítik az integrációt, támogatják az ellenőrzőmotor egyedi felhasználását és hozzáférést biztosítanak a Rational AppScan eXtensions Framework-höz és a Pyscan funkcióihoz is.

A Rational AppScan alapfunkciói a sebezhető pontok azonosítására

- A globális validálás elemzi a nem szándékosan kiváltott problémákra adott teszt-válaszokat, az SSL-tanúsítványok ellenőrzését és a szájtok közötti hívások hamisíthatóságát (CSRF-tesztelés).
- A hacker-szimulációk segítenek a létező, ismert sebezhető pontok megtalálásában.
- A Rational AppScan alkalmazás induláskor automatikusan értesíti a felhasználókat a legújabb fenyegetésekről.
- A szoftverrel együtt járó alkalmazáscsomag segíti a behatolási tesztelőket és biztonsági tanácsadókat a webes alkalmazások fejlesztésében és tesztelésében, valamint a hibakeresés során.

A Rational AppScan jelentéskészítő és problémamegoldó alapfunkciói

- A szoftver több mint 40 előírással és szabvánnyal kapcsolatban tartalmaz teszteket.
- A kiemelési funkció rámutat azokra a HTML-kódhelyekre, amelyek sebezhető pontot jelentenek, leírást ad a problémáról, és javaslatot tesz, hogy milyen módosított HTML-kóddal küszöbölhető ki a veszélyforrás.
- A megoldási jelentések javaslatot tesznek a PHP-kód javítására és listát készítenek a fejlesztői feladatokról. Ezekben a jelentésekben a felhasználók áttekinthetik az alkalmazásokkal, az infrastruktúrával, illetve mindkettővel kapcsolatos problémákat, és kitörölhetnek vagy ártalmatlannak minősíthetnek egyes változatokat a későbbi ellenőrzések számára.
- A gyanús tartalomra vonatkozó részletes jelentések olyan problémákra mutatnak rá, mint a HTML-megjegyzésekben szereplő érzékeny adatok vagy a gyanús tartalmak körül tapasztalható HTTP-tevékenység.
- A tesztek leírásai kiterjednek a gyakran előforduló sebezhető pontok és támadási felületek azonosítására az IBM által karbantartott adatbázis alapján.
- A szoftver képes arra, hogy a belsejében használt böngészőből képernyőképeket másoljon a jelentésekbe, illetve hogy az egyes tesztekben szereplő információkat összegyűjtse, tömörítse és titkosítsa, hogy e-mailben el lehessen azokat küldeni.
- A szoftver a téves riasztásokról (vagy tévedésből nem észlelt problémákról) jelentést küld az IBM Rational AppScan biztonsági kutatócsoportjának, hozzájárulva a termék folyamatos továbbfejlesztéséhez.

Biztonsági auditok és működés közbeni ellenőrzés a Rational AppScan Standard Edition segítségével

A webes alkalmazás-tesztelési folyamatok automatizálása segíti a biztonsági ellenőröket és a behatolási tesztelőket, hogy gyorsan és hatékonyan végezhessék munkájukat. Ehhez azonban fejlett és intelligens ellenőrzési technológiára van szükség. A hagyományos alkalmazásként és menedzselt (SaaS) szolgáltatásként is rendelkezésre álló Rational AppScan Standard Edition a közepes és professzionális felhasználók számára nyújt funkciókat. A következő funkciók állnak rendelkezésre:

- Az Ellenőrzési szakértő egy olyan varázsló, amely a legjobb gyakorlatra vonatkozó tanácsokkal segít az ellenőrzések létrehozásában és beállításában, beleértve a további eszközök használatát is. A felhasználók végrehajthatnak egy előzetes ellenőrzést, amely felméri a célalkalmazást és ajánlatokat tesz a sikeres ellenőrzéshez szükséges teendőkről.
- Az állapotkövető segítségével ellenőrizhetők és tesztelhetők az összetett üzleti folyamatok (pl. többlépcsős, kosaras online vásárlás vagy a megrendelések nyomon követése). Ez az eszköz a teljes folyamat során megőrzi a paraméterek értékeit és a cookie-kat.
- Az előre definiált ellenőrzési sablonokkal a felhasználók gyorsan kiválaszthatják a beállításokat és elindíthatják az ellenőrzést.
- A gyors ellenőrzés-beállítási varázsló végigvezeti a felhasználókat a legfontosabb beállításokon, a proxy/platform-hitelesítés feltételes lépésein és a munkamenet-detektálási adatok kitöltésén.
- Az új kérés/válasz füleken a szöveg a szintaxist tükröző színkiemeléssel jelenik meg, követhetők a kérések és válaszok, elrejthetők vagy kinyithatók az egyes részek, a gépeléssel egy időben kereshető a szöveg, és az úszómenüből egyéb lehetőségek is elérhetők.
- A Microsoft® Word sablonjaira épülő jelentések készíthetők.
- A beépített webalapú oktatási modulok leírást adnak a problémákról és bemutatják a támadási módokat.

Az IBM Rational AppScan biztonsági problémák nézete

Az IBM Rational AppScan probléma-megoldási nézete

Az IBM Rational AppScan Express Edition által nyújtott robosztus webes alkalmazás-biztonsági funkciók

A biztonsági tesztelést azoknál a vállalatoknál is be kell építeni a fejlesztési ciklusba, amelyek csak kicsi vagy korlátozott alkalmazásfejlesztő csapatot engedhetnek meg maguknak. Ezek a vállalatok azonban gyakran arra kényszerülnek, hogy a költséghatékonyság oltárán feláldozzanak egyes funkciókat. A 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 tesztelési funkciókat. Az IBM Rational AppScan Express könnyen telepíthető és jelentősen csökkenti a sebezhető pontok kézi ellenőrzéséhez szükséges időt és költségeket, hogy az Ön fejlesztői a vállalat egyéb informatikai és biztonsági igényeivel foglalkozhassanak.

A biztonsági tesztelés beépítése a minőségbiztosítási programba a Rational AppScan Tester Edition segítségével

A Rational AppScan Tester Edition asztali (desktop) alkalmazásként érhető el, és lehetővé teszi, hogy a minőségbiztosítással foglalkozó csoportok a biztonsági tesztelést beépítsék meglevő minőségbiztosítási folyamataikba, csökkentve ezzel a biztonsági szakértők terhelését. Mivel a Rational AppScan Tester Edition integrálható a vezető tesztelési rendszerekkel, a minőségbiztosítási szakemberek a rendelkezésre álló funkciókat tesztelési parancsfájlokból is elérhetik és a megszokott tesztkörnyezeten belül végezhetnek biztonsági ellenőrzéseket. Ez leegyszerűsíti a biztonsági tesztelés bevezetését a funkcionális és teljesítmény-tesztelés mellett.

A biztonsági tesztelés tökéletes integrálása a meglevő fejlesztési környezetbe a Rational AppScan Developer Edition segítségével

Az alkalmazások biztonsági hibáit úgy lehet a lehető leghatékonyabban megelőzni, ha a szoftvert már a kezdetektől fogva a biztonsági szempontok figyelembevételével tervezik meg. A fő kihívást az jelenti, hogy a fejlesztők többsége nem biztonsági szakember, és gyakran nem a biztonságos kód a fő szempont a számukra. A legkönnyebben ezért úgy lehet a fejlesztőket bevonni az alkalmazások biztonságával foglalkozó folyamatba, ha a saját környezetükben működő eszközöket adunk a kezükbe, amelyek számukra is érthető nyelven közlik az eredményeket.

A Rational AppScan Developer Edition segítségével a fejlesztők már a kezdet kezdetétől saját fejlesztői környezetükből hívhatják meg a webes alkalmazások biztonsági tesztelésére szolgáló funkciókat. Így a fejlesztési részleg kézben tarthatja a kódot fenyegető nagyszámú biztonsági problémát, leegyszerűsítheti a fejlesztési ciklushoz kötődő munkafolyamatot és kiküszöbölheti a költséges biztonsági tesztelés szűk keresztmetszeteit, amelyek a fejlesztési ciklus végén merülhetnek fel.

A Rational AppScan Developer Edition számos elemzési technikát alkalmaz, amelyek pontosan beazonosítják a webes alkalmazások biztonsági problémáit. A használt módszerek közé tartozik a statikus kódelemzés, a dinamikus elemzés, a futási időben végzett elemzés és a string-elemzés, amelyre az IBM szabadalmi kérelmet adott be.

A biztonsági tesztelés automatizálása a Rational AppScan Build Edition segítségével

A Rational AppScan Build Edition a szoftverfejlesztési ciklus fordítási fázisánál (build stage) támogatja az automatikus biztonsági tesztelést. Az eszköz az ütemezett buildek biztonsági teszteléséről gondoskodik és több build-menedzselési szoftverrel is integrálódik, többek között az IBM Rational Build Forge® alkalmazásával. Az eredményeket vissza is juttatja a fejlesztőkhöz, vagy a hibakövető rendszeren keresztül (pl. IBM Rational ClearQuest®), vagy egy biztonsági jelentéskészítő rendszer segítségével (pl. Rational AppScan Enterprise Edition vagy Rational AppScan Reporting Console).

A Rational AppScan Build Edition ugyanazokat az elemzési technikákat használja, mint a Rational AppScan Developer Edition. Igen pontos eredményeket szolgáltat és számon tartja, hogy mely kódrészletek tesztelését végezte el.

Az alkalmazások biztonsági tesztelésének teljes vállalatra kiterjedő skálázhatósága a Rational AppScan Enterprise Edition segítségével

A Rational AppScan Enterprise Edition webalapú architektúrájának köszönhetően lehetővé teszi, hogy a vállalatok több érintett között megosszák a biztonsági tesztelés felelősségét. A szoftver SaaS modellben, szolgáltatásként is igénybe vehető. Ekkor könnyen felvehetők új felhasználók és egyszerűbb kézben tartani a költségeket.

A központosított, könnyen bővíthető adminisztráció kényelmén túl a Rational AppScan Enterprise Edition a következő funkciókat biztosítja:

- Egyszerre ellenőrizhető és tesztelhető egy összetett webhely akár több ezer alkalmazása; a tesztelés a változások követésére gyakran megismételhető.
- A gyors ellenőrzést végző tesztelési eszköz telepítés vagy konfigurálás nélkül képes végrehajtani a rendszergazdák által definiált ellenőrzési sablonokat a fejlesztők és más nem biztonsági szakértő emberek számára.
- A központi adattárház automatikusan tárolja és összesíti a teszteredményeket, így azok a vállalat bármely pontjáról, többféle nézetben is elérhetők.
- A webalapú jelentéskészítő konzol szerepeken alapuló hozzáférést nyújt a biztonsági jelentésekhez és leegyszerűsíti a vállalati kommunikációt.
- A vezetői áttekintő képernyők és különbségképző elemzések megmutatják a két ellenőrzés közötti eltéréseket, beleértve a kijavított, folyamatban levő és új biztonsági problémákat.
- A vállalat összes webes alkalmazásának biztonsági tesztelése központi helyről követhető és irányítható.
- A beépített webalapú oktatási modulok leírást adnak a problémákról és bemutatják a támadási módokat.

Központosított hozzáférés a webes alkalmazások sebezhető pontjairól készült jelentésekhez az IBM Rational AppScan Reporting Console segítségével

Az IBM Rational AppScan Reporting Console egy hatékony webalapú menedzsment- és jelentéskészítő eszköz, amely teljes mértékben integrálódik a Rational AppScan Standard Edition alkalmazással. Nagyvállalati szintű adatbázisra épül, amely konszolidálja a több Rational AppScan kliensből érkező teszteredményeket, központosított adattárházat hozva létre az alkalmazások sebezhető pontjairól. Az ellenőrzési eredmények könnyen eljuttathatók a minőségbiztosítási és fejlesztési csoportokhoz, méghozzá további munkaállomáshoz kötött licencek telepítése nélkül. Ez leegyszerűsíti a hibajavítási folyamatot és lehetővé teszi a biztonsági elemzés beépítését a teljes szoftverfejlesztési ciklusba. A Rational AppScan Reporting Console alkalmazásban a különböző felhasználók számára eltérő áttekintő képernyők hozhatók létre, így az emberek a biztonsági adatokat alkalmazás, üzleti egység vagy külső szállító szerinti bontásban vizsgálhatják.

A Rational AppScan Standard Edition és a Rational AppScan Enterprise Edition lehetőségei SaaS modellben is rendelkezésre állnak

Ha a Rational AppScan lehetőségeit menedzselt szolgáltatásként veszi igénybe, anélkül élvezheti a termék előnyeit, hogy további alkalmazottakra vagy hardverre kellene költenie.

Első vonalbeli biztonsági tesztelési környezet

A szolgáltatások célja az Önök működési környezetének védelme; ennek érdekében fejlett biztonsági eszközökre és technikákra épülnek.

Az IBM szakértői segítséget nyújtanak a biztonsági előírásoknak való megfeleléshez

A Rational AppScan Standard Edition és a Rational AppScan Enterprise Edition SaaS-felhasználói igénybe vehetik az IBM biztonsági elemzőjének szolgáltatásait, aki segítséget nyújt a következőkhöz:

- Az ellenőrzések konfigurálása és finomhangolása, hogy azok minden alkalmazáshoz a lehető leginkább átfogó védelmet biztosítsák.
- Az eredmények áttekintése és elemzése, hogy kiszűrjék a téves riasztásokat, felismerjék a szabályszerűségeket, prioritizálják a problémákat és rámutassanak a megoldáshoz szükséges feladatokra.
- A megoldási folyamat nyomon követése a folyamatokra vonatkozó adatok karbantartásával, a javítások ellenőrzésről ellenőrzésre terjedő követésével és a hibajavítás hatékonyságára vonatkozó jelentésekkel.

Az IBM Rational AppScan Enterprise Edition áttekintő képernyője

A biztonsággal és az előírásoknak való megfeleléssel kapcsolatos problémák megelőzése a webalapú oktatás segítségével

Az IBM webalapú képzést nyújt az alkalmazások biztonságával kapcsolatban. Ez online érhető el, 15 perces időközönként. A képzési szolgáltatás a termékekkel kapcsolatos alapvető útmutatáson túl célzott tanácsokat tartalmaz a fejlesztők, minőségbiztosítási csoportok és biztonsági szakértők számára.

A képzési folyamat során online tesztek is elérhetők a termékkel kapcsolatos ismeretek három különböző szintjének tanúsítására, a vezetők pedig a számukra készült, szintén online elérhető áttekintő képernyőn követhetik az alkalmazottak fejlődését a Rational AppScan Enterprise Edition alkalmazáson belül.

További információk

Az IBM Rational AppScan termékekről további információt kaphat az IBM képviselőjétől vagy az IBM Üzleti Partnerétől, illetve az alábbi weblapon:

ibm.com/software/rational/offerings/testing/webapplicationsecurity

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Készült az Amerikai Egyesült Államokban
2008. augusztus

RAB14001-USEN-01