Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Biztonsági metrikák automatikus kiértékelése

Strott András (HGI0IJ), BSc mérnök inf. szakos hallgató
Konzulens: Gönczy László, MIT
Informatikai Technológiák szakirány / Rendszertervezés ágazat
Önálló laboratórium 2 összefoglaló
2009/10. II. félév

Az önálló labor tantárgy keretein belül a feladatom a következő volt: az informatikai biztonság egy jelentős területének, a web biztonságnak a vizsgálata, a biztonsági metrikákhoz kapcsolódó irodalom áttanulmányozása, egy automatizált tesztelő eszköz, az IBM Rational AppScan alkalmazása egy előre kiépített mintainfrastruktúrán, és a szoftver működésének tanulmányozása.

Áttekintettem a webalkalmazások ellen indított gyakoribb támadásokat, és ezekre példákat hoztam fel. Tanulmányoztam a biztonsági metrikák irodalmát, azt, hogy hogyan definiáljuk, osztályozzuk őket, példákat hoztam fel. Megismertem a CVSS (Common Vulnerability Scoring System) metrikadefiníciós módszereit, valamint a Web Application Security Consortium web biztonsági scannerekre vonatkozó követelményrendszerét. Példákat hoztam sérülékenység scannerekre. A továbbiakban a Rational AppScan szoftverét tanulmányoztam.

A BME MIT tanszék virtualizációs szerverén létrehoztunk virtuális gépeket, külön a tesztelő szoftvernek, külön a tesztelendő mintaalkalmazásoknak. Ezek Java EE és .NET platformra épülő Pet Store alkalmazások voltak, forráskódból felépítve, a szükséges adatbáziskezelő rendszerekkel. A feladat során sok, debug jellegű probléma merült fel, de ezeket a tanszék munkatársaival közösen sikeresen megoldottuk. A terv végül nem valósult meg véglegesen, mert nem sikerült az AppScan szoftverhez a megfelelő licenszet beszerezni. Amennyiben ez megtörténik, a mintaalkalmazásokat leteszteljük, és az AppScan javaslatai alapján kísérletet teszünk a talált sérülékenységek közül néhány kijavítására.

Az AppScan működését ennek ellenére demonstrálni tudtam egy ilyen célokra létrehozott tesztoldalon, a *demo.testfire.net*-en. Ennek során megismertem a szoftver konfigurációs lehetőségeit, a kapott eredmények alapján pedig a kiértékelést tanulmányoztam. Egy konkrét példa alapján elemeztem a sérülékenység megtalálásának módszerét.

Meghatároztam a jövőben (feltehetőleg szakdolgozat keretei között) elvégzendő vizsgálódások tárgykörét.