Hogyan törjünk fel webhelyeket

Avagy hogyan ne írjuk webalkalmazásokat

Cím: Hogyan törjünk fel webhelyeket
Szerzők: James A. Whittaker, Mike Andrews
Kiadó: Kiskapu (Addison-Wesley)
Oldalszám: 256
Ár: 3980 Ft

Az utóbbi években az internet rohamos terjedésének köszönhetően a programfejlesztés is új irányt vett. Míg 10-12 évvel ezelőtt csupán statikus weblapok voltak jelen a hálón, a programok nagyobb része pedig helyben futott a számítógépen, addig ma már szinte minden áthelyeződött a világhálóra. Legyen szó valamilyen rendelésről (könyv, virág, pizza, aszpirin, viagra stb.), banki műveletről, aukciós oldalról, közösségi webhelyről vagy bármi másról, nyitjuk a böngészőt, és a világ legtermészetesebb módján használjuk, amit a webfejlesztő elénk rakott.
Az oldalak dinamikussá válásával azonban képbe került egy új probléma is: hogyan írjunk olyan webalkalmazásokat, amelyekkel mind a felhasználó, mind az üzemeltető biztonságban lehet anélkül, hogy az túlzottan megbonyolítaná a napi ügymenetet.
Manapság már számtalan nagyon jónak mondható webprogramozásról szóló könyv kapható itthon is.
A probléma az, hogy ezekből – akárcsak a többi, klasszikus programozási tankönyvből (*C*, *C++* stb.) – gyakran kifelejtettek egy fontos részt a szerzők.
A programozás elméletének és szintaxisának, meg az alkalmazási területeknek a bemutatásával sajnos nem érhet véget egy tankönyv. Nem csak a világos oldalt kell megvizsgálni ugyanis, amikor a felhasználó a tankönyvi példa szerint viselkedik, hanem a sötétet is, amikor – akár szándékosan, akár véletlenül – megpróbálja kihozni az alkalmazásból azt, amit mi egyáltalán nem terveztünk bele.
E tekintetben ***Whittaker*** és ***Andrews*** könyvét amolyan hiánypótló műnek tekinthetjük, hiszen a két szerző – tapasztalt biztonságtechnikai szakemberek – 24 lehetséges feltörési módszer tárgyal hét logikai részre tagolva. Minden betörési módszernél részletes leírást kapunk magáról a támadásról – mi is valójában és mikor kell rá odafigyelni –, a támadás végrehajtásáról és persze a támadás elleni védekezésről.
A három további fejezetben a web természetéről, az adatvédelemről és a webszolgáltatásokról kapunk áttekintést. A függelékben helyet kapott ezen kívül egy rövid – tíz oldalas – összefoglaló a szoftverfejlesztés történetéről a kezdetektől napjainkig, valamint a könyvben bemutatott virágboltos weboldal hibáinak rövid összefoglalása.
Apropó virágbolt... A könyvhöz tartozik egy ***CD*** melléklet is, melyen a könyvben említett segédprogramok és egy „állatorvosi ló” gyanánt használható webhely forrása található. Az eszközök elsősorban windowsosak, de számos alkalmazás – mint például az ***Ethereal*** – megtalálható a legtöbb ***Linux*** terjesztésben is. Emellett három, a témával kapcsolatos ***Firefox*** bővítmény is helyet kapott a lemezen.
A legfontosabb tanács talán az, hogy hibát követünk el, ha a felhasználót alapból jóindulatúnak tekintjük. Ha ezerből csak egy van, aki kihasználja az általunk ottfelejtett biztonsági rést, az eset már akkor is romba döntheti a cégünket. Anyagilag és erkölcsileg egyaránt.
Teljes védelem persze szintén nincs, mint ahogy örökké tartó sem. Újra és újra felül kell vizsgálnunk a kész alkalmazásokat is. A könyv ehhez és további támadási módok kigondolásához is segítséget nyújt.
A hátsó borítón ugyan „Haladó” szint van megjelölve, én azért mégis ajánlanám ezt a művet bárkinek, aki valamilyen szinten webprogramozással foglalkozik, akár a szerver akár a kliens oldalán. A hibás programozói magatartást ugyanis sokkal nehezebb levetkőzni, mint körültekintően programozni már a kezdetektől fogva.

Medve Zoltán
e-medve@e-medve.hu