



**Hadarics Kálmán - H. Dudás Nóra - Dr. Leitold Ferenc:**

**SQL injekción alapuló sérülékenységek vizsgálata**

Napjainkban rengeteg különféle adatot kell nyilvántartani és rendszerezni az élet minden területén. Ezen adatok jellemzően adatbázisokban, adattárházakban vannak tárolva, melyekhez különböző technológiákkal, megfelelő interfészeken keresztül férhetünk hozzá. Az egyes adatbázis kezelő rendszerekben az adatmanipuláció jellemzően SQL (Structured Query Language) parancsok segítségével történik.

Az adatbázisban tárolt adatok megjelenítése, manipulációja különböző platformokon történhet. A hagyományos számítógép alapú kliensek mellett egyre fontosabb szerepet töltenek be a web alapú és mobil eszközökön futó kliens alkalmazások. Ezek általában dinamikusan szerkesztett SQL utasításokkal végzik az adatbázis műveleteket.

Az SQL injekción alapuló sérülékenységek lehetővé teszik „kártékony kód” végrehajtását, amely segítségével egy támadó képes lehet a teljes adatbázis tartalmához való hozzáférésre, vagy jogosulatlan adat beszúrára vagy módosításra. A SQL injekción alapuló fenyegetések jellemzően programozási hibákhoz (pl.: ellenőrzés elmulasztása) kapcsolódnak.

Jelen előadásban megvizsgáljuk az utóbbi évek SQL injekción alapuló sérülékenységeit, az aktuális trendeket ezen a területen, elemezzük azon biztonsági hiányosságokat, melyek révén, egy SQL injekción alapuló támadás megvalósulhat.