

Slovenská Technická Univerzita
Fakulta Informatiky a Informačných Technológií

Bezpečnosť v Oracle a SQL databázach

Matej Kubík

Vedúci projektu: doc. Ladislav Hudec

Predmet: Bezpečnosť počítačových systémov

Úvod

Tento dokument bol vytvorený v rámci semestrálneho projektu z predmetu Bezpečnosť počítačových systémov. Obsahuje stručný obsah pripravovaného dokumentu o bezpečnosti databázy Oracle a SQL databáz všeobecne.

Analyzované oblasti

Analýzou SQL databáz som identifikoval tieto oblasti, ktoré sú z bezpečnostného hľadiska zaujímavé:

- 1) Bezpečnostné vlastnosti databázy; medzi ne patria najmä spôsoby identifikácie a autentifikácie používateľov, ďalej autorizácia používateľov na rozličné operácie (v databáze Oracle predstavovaná užívateľskými privilégiami a rolami), a v neposlednom rade zabezpečenie neodškriepiteľnosti.
- 2) Inherentné bezpečnostné problémy databázy, ktoré súvisia s:
 - 2.1) štandardnými užívateľskými účtami,
 - 2.2) nedostatočnou ochranou dôležitých informácií na úrovni OS,
 - 2.3) chybami v programových komponentoch samotnej databázy, ktoré umožňujú eskaláciu privilégií.
- 3) Bezpečnostné problémy aplikácií používajúcich databázu; tieto sa týkajú jednak SQL injection (vkladania kódu SQL) a bezpečnosti na aplikačnej úrovni. Druhej časti témy sa dotknem skôr okrajovo, pretože je veľmi obsiahla a mnohokrát je aplikácia modifikovateľná tak, aby bolo možné autentifikáciu alebo autorizáciu používateľov aspoň čiastočne presunúť z aplikácie do databázy.

Bezpečnostné vlastnosti databázy

- 1) V stati o autentifikácii používateľov sa zameriam na spôsoby autentifikácie do databázy a ochranu pred krádežou identity.
- 2) Pri autorizácii zhrniem, aké operácie môžu užívatelia vykonávať a spôsoby zjednodušenia pridelovania privilégií.
- 3) Zabezpečenie neodškriepiteľnosti súvisí s auditom operácií, čo všetko sa dá auditovať atď.

Inherentné bezpečnostné problémy databáz

- 1) Štandardné užívateľské účty sa vyskytujú v každej databáze po jej inštalácii. Prečo sú nebezpečné, bude pojednávať táto časť dokumentu.
- 2) Každý databázový stroj beží na určitom OS a iní užívatelia (okrem administrátorov) tohoto OS môžu (ale nemusia) mať zvýšené prístupové práva k programovým, dátovým a konfiguračným súborom databázy. Bude opísané, aké informácie môžu týmto spôsobom uniknúť a ako sa proti tomuto nebezpečenstvu brániť.
- 3) Hovorí sa, že v každom programe je aspoň jedna chyba. Databázové stroje sú programy veľmi rozsiahle a zložité. Dozvieme sa, aké riziká môže vzdialený prístup do databázy priniesť a aké špecifické problémy má databáza Oracle.

Bezpečnostné problémy aplikácií využívajúcich SQL

- 1) SQL injection je spôsobená nedostatočnou kontrolou vstupných dát v aplikácii, jedná sa však o natoľko rozšírený problém, že mnohé databázy vrátane Oracle obsahujú viac či menej dokonalé nástroje na odchyťovanie pokusov o ňu. Táto kapitola bude pojednávať práve o nich.
- 2) Bezpečnosť na aplikačnej úrovni je téma na väčšiu prácu, v tejto časti sa však stručne dotknem toho, ako môže databáza tejto bezpečnosti napomôcť. Skôr než nové informácie však bude zhrňať veci z predchádzajúcich kapitol so zameraním na aplikačnú bezpečnosť.

Očakávané zmeny v špecifikácii výslednej dokumentácie

Vzhľadom na potenciálny rozsah tretej časti dokumentácie očakávam najväčšie zmeny v tejto časti.

Použitá literatúra

- [1] Finnigan, Pete: SQL Injection and Oracle, <http://online.securityfocus.com/infocus/1644>
- [2] Finnigan, Pete: Exploiting and Protecting Oracle,
<http://downloads.securityfocus.com/library/oracle-security.pdf>
- [3] Newman, Aaron: Protecting Oracle Databases,
http://www.appsecinc.com/presentations/Protecting_Oracle_Databases_White_Paper.pdf
- [4] Nevalis, Richard D.: Database Security 101,
<http://www.geocities.com/ckempster/wpapers/oracle/databasesecurity101.pdf>
- [5] Hanzel, Lorraina: An overview of Oracle database security features,
<http://www.sans.org/rr/appsec/oracle.php>
- [6] Naude, Frank: Oracle Security FAQ, <http://www.orafaq.com/faqdbase.htm>