

SYMBOLS AND NUMERICS

@@version variable (Sybase), 217–218
| | (double pipe) with Windows
Command Interpreter, 43
“ (double quotes) for SQL injection
(Sybase), 220
(hash mark) in #NISR... notation, 12
one-bit patch Trojan (MySQL), 302–303
' (single quote)
CHAR function to bypass quote
filters (Sybase), 219–220
SQL injection using (MySQL), 282
SQL injection using (SQL Server),
359–362
SQL injection using (Sybase), 214–215
three-byte patch backdoor (SQL
Server), 370–373
0x0A leading byte DoS (SQL Server),
357
0x08 leading byte heap overflow (SQL
Server), 356–357

A

accounts (DB2)
enabling lockout, 153–154
on Linux, 109
OS accounts and default passwords,
110

accounts (Informix)
authorization, 163–164
creating highly privileged accounts,
184
discovering server instance name, 160
accounts (MySQL)
columns_priv table, 270, 271
db table, 269–270
hosts table, 270
one-bit patch altering authentication,
302–303
password for root@localhost
account, 322
principle of least privilege, 324
privilege model, 266–272
removing non-root users, 322
renaming root account, 322
restricting by IP address, 323–324
routine audit, 327
tables_priv table, 270–271
user table, 266–269, 272
accounts (Oracle)
changing default passwords, 90
database account authentication, 32
DBA privileged, 33–34, 57–59, 93–95
DBSNMP, 27, 32, 36, 49
default accounts and passwords,
48–49

- accounts (Oracle) (*continued*)
 - default usernames and passwords, 447–469
 - enabling user account lockout, 92
 - for Intelligent Agent, 32
 - MDSYS, 49, 68–70
 - new account creation, 90
 - OS account authentication, 32
 - password policy for, 90–91
 - principle of least privilege, 92
 - roles for user accounts, 91–93
 - security recommendations, 89–91
 - SYS, 33, 48, 69
 - unused, locking and expiring, 90
- accounts (SQL Server)
 - brute-forcing usernames and passwords, 339–340
 - built-in server roles, 348–349
 - common accounts, 348
 - created during installation, 348
 - disabling guest account, 379–380
 - fixed database roles, 349
 - PUBLIC role, 349, 380
 - stored in sysxlogins table, 347
- accounts (Sybase)
 - adding new users, 204
 - enabling lockout, 248
 - running with low-privileged account, 247–248
 - sa account, removing privileges from default, 249
 - sysusers table for, 204
- ACCRDB command (DB2)
 - in code for user authentication, 113–114
 - in packets, 102, 104
- ACCSEC command (DB2)
 - in code for user authentication, 112
 - in packets, 102, 104
- Active Server Pages (ASP), SQL injection in SQL Server and, 358–361
- Adaptive Server Enterprise. *See* Sybase ASE
- ad-hoc queries, disabling (SQL Server), 340, 381–382
- Admin Restrictions for TNS Listener (Oracle), 88
- agentctl utility (Oracle), 27
- Aitel, David (hacker), 6, 333
- ALTER USER command, avoiding for changing passwords, 32
- ALTERAUTH authority (DB2), 121
- Andrews, Chip (SQLPing programmer), 335
- Anley, Chris
 - MySQL issue discovered by, 8
 - Oracle issues discovered by, 6
 - SQL Server issues discovered by, 9, 10
 - three-byte patch attack (SQL Server), 370–373
 - whitepapers, 362, 370
- ANONYMOUS user, resetting password for (Oracle), 61
- APISpy32 utility, 372
- AppDetective scanner (Application Security Inc.), 336
- application roles (SQL Server), 349, 352
- applications, “instrumenting,” 14–15
- arbitrary code execution
 - in intrinsic SQL elements, 9–10, 15
 - in securable SQL elements, 10–11, 15
- ARGUMENT\$ table (Oracle), 51–53
- ARP spoofing (PostgreSQL), 406
- ASCII, mapping EBCDIC to, 105–106
- ASP (Active Server Pages), SQL injection in SQL Server and, 358–361
- @@version variable (Sybase), 217–218
- atoi() function (SQL Server), 357
- attack surface, functionality and, 5, 19, 99
- auditing
 - attacking systems and, 37
 - authenticated users, 7
 - DBA role (Oracle), 93
 - enabling (Informix), 190
 - enabling (Sybase), 250–251
 - evading with sp_password (Sybase), 220
 - listing audited tables (Oracle), 37
 - MySQL routine audit, 319, 326–328

- Oracle, 36, 94
- SQL Server, 379, 383
- AUTH tables (Informix), 162
- authenticated flaws in network protocols, 7
- authentication (DB2)
 - account lockout and, 153–154
 - changing type of, 154
 - code for user authentication, 111–119
 - operating system used for, 109–110
 - OS accounts and default passwords, 110
 - setting server's type, 110
 - types supported, 110
- authentication (Informix)
 - failed, response to, 175
 - operating system used for, 163
 - successful, response to, 174–175
- authentication (MySQL)
 - algorithm flaws, 260, 261–262
 - buffer overflow issues, 262
 - bypassing, 261–262
 - CHANGE_USER command bug
 - prior to 3.23.54, 261
 - check_scramble function, 261–262, 302–303
 - Core-SDI paper on weaknesses, 281
 - cryptographic weakness prior to 4.1, 260
 - default configuration, 258–259
 - hash authentication patch, 307–309
 - one-bit patch altering remote mechanism, 302–303
 - proprietary protocol, 259–260
 - protocol flaws, 8, 260–262, 272
 - protocol for remote authentications, 302
 - snooping, 280–281
- authentication (Oracle)
 - of database accounts, 32, 34–37
 - of OS accounts, 32
 - remote, turning off, 92
- authentication (PostgreSQL)
 - connection types, 392–393
 - crypt method, 394
 - ident method, 393, 395–396
 - krb4 and krb5 methods, 394
 - md5 method, 394
 - pam method, 394
 - password method, 393–394, 396
 - pg_hba.conf file, 392–394, 405, 433
 - process of, 405
 - reject method, 393, 395
 - security considerations for Identification Protocol, 395–396
 - trust method, 393, 394
- authentication protocol flaws, 8
- authentication (SQL Server)
 - deciphering obfuscated passwords, 338–339, 352
 - OPENROWSET re-authentication, 273, 339–340, 367
 - overview, 336–337
 - packet dump of process, 337–338
 - password obfuscation, 337–338
 - secure installation and, 375–377
 - for SQL Server Agent, 351
- authentication (Sybase)
 - default configuration, 203, 211
 - failed, response to, 210
 - logging attempts, 211
 - open authentication protocol support, 198, 203
 - protocol flaws, 8
 - recommendations, 252
 - snooping, 211
- authorization (DB2)
 - authorities, 120
 - DBAUTH view, 120–121
 - PUBLIC and, 121, 122
 - ROUTINEAUTH view, 122
 - TBAUTH view, 121–122
- authorization (Informix)
 - Connect privilege, 163
 - DBAs, 163
 - information in AUTH tables, 162
 - object privileges, 164
 - privileges and creating procedures, 164
 - Resource privilege, 163

- authorization (Oracle), 35
- authorization (SQL Server), 336
- AUTONOMOUS_TRANSACTION
 - pragma (Oracle), 59–60
- Azubel, Agustin (hacker), 8
- B**
- Baseline Security Analyzer (Microsoft), 383
- batched queries. *See* query batching
- BDB storage engine (MySQL), 264, 265
- BINDADDAUTH authority (DB2), 120
- bugtraq id 11399, 10
- bugtraq id 11401, 6
- BugTraq mailing list, 320
- BULK INSERT statement overflow (SQL Server), 10
- Burghate, Nilesh (hacker), 247
- C**
- California Senate Bill No. 1386, 4
- CALL command overflow (DB2), 10, 137
- CAN-1999-0862, 410
- CAN-2000-1081, 10
- CAN-2000-1082, 10
- CAN-2000-1083, 10
- CAN-2000-1084, 10
- CAN-2000-1085, 10
- CAN-2000-1086, 10
- CAN-2000-1087, 10
- CAN-2000-1088, 10
- CAN-2000-1199, 410
- CAN-2001-1255, 292, 304
- CAN-2001-1274, 292
- CAN-2001-1275, 292
- CAN-2002-0641, 10
- CAN-2002-0649, 6
- CAN-2002-0928, 12
- CAN-2002-0969, 292
- CAN-2002-0972, 410
- CAN-2002-1123, 6
- CAN-2002-1373, 292
- CAN-2002-1374, 292, 293
- CAN-2002-1375, 291
- CAN-2002-1376, 291
- CAN-2002-1397, 410
- CAN-2002-1398, 410
- CAN-2002-1399, 410
- CAN-2002-1400, 410
- CAN-2002-1401, 411
- CAN-2002-1402, 411
- CAN-2003-0073, 291
- CAN-2003-0095, 6, 14
- CAN-2003-0150, 13, 288, 291
- CAN-2003-0222, 10
- CAN-2003-0327, 227
- CAN-2003-0634, 6
- CAN-2003-0780, 291
- CAN-2003-0901, 411
- CAN-2004-0381, 290, 304
- CAN-2004-0388, 290, 304
- CAN-2004-0457, 290
- CAN-2004-0547, 411
- CAN-2004-0627, 8, 290, 293–297
- CAN-2004-0628, 290
- CAN-2004-0795, 7
- CAN-2004-0835, 290
- CAN-2004-0836, 290
- CAN-2004-0837, 290
- CAN-2004-0956, 290
- CAN-2004-0977, 411
- CAN-2004-1363, 6
- CAN-2004-1365, 9
- CAN-2004-1370, 11
- CAN-2005-0227, 12
- cash_words() function overflow (PostgreSQL), 413–415
- Cerrudo, Cesar (whitepaper author), 362
- CHANGE_USER command bug (MySQL), 261
- CHAR function to bypass quote filters (Sybase), 219–220
- CheckReg() function with PL/SQL (Oracle), 76
- check_scramble function (MySQL), 261–262, 302–303
- “Choosing an Edition of SQL Server 2000,” 332

- chroot
 - running MySQL with — chroot option, 321
 - running Sybase in chroot jail, 248
 - CKPT (Checkpoint) process (Oracle), 26
 - classes of security flaws
 - arbitrary code execution in intrinsic SQL elements, 9–10
 - arbitrary code execution in securable SQL elements, 10–11
 - authenticated flaws in network protocols, 7
 - authentication protocol flaws, 8
 - local privilege elevation issues, 12–13
 - privilege elevation via SQL injection, 11–12
 - unauthenticated access to functionality, 9
 - unauthenticated flaws in network protocols, 6–7
 - clear text. *See* plaintext
 - CLIENT authentication type (DB2), 110
 - clients
 - connecting to remote system (DB2), 107–108
 - implementing your own, 14
 - JSQL TDS client (Sybase), 238–241
 - overflows (SQL Server), 357–358
 - Client-Server applications (Sybase), 199–200
 - code execution, arbitrary
 - in intrinsic SQL elements, 9–10, 15
 - in securable SQL elements, 10–11, 15
 - columns_priv table (MySQL), 270, 271
 - comments, SQL injection using
 - PostgreSQL, 420–421
 - SQL Server, 360–362
 - Sybase, 216
 - Common Vulnerabilities and Exposures database, 409
 - communication protocols, 15
 - Communication Support Module (CSM) in Informix, 167
 - Connect privilege (Informix), 163, 190
 - CONNECT role (Oracle), 91–92
 - CONNECTAUTH authority (DB2), 120
 - CONTROLAUTH authority (DB2), 121
 - COPY command vulnerabilities (PostgreSQL), 425–427
 - CREATE DATABASE LINK statement overflow (Oracle), 10
 - CREATE FUNCTION mechanism (MySQL), 273
 - CREATE LIBRARY system privilege (Oracle), 36
 - CREATE ROLE statement (Oracle), 91
 - CREATE WRAPPER command overflow (DB2), 137
 - CREATE_JOB procedure, running OS commands with (Oracle), 78
 - CREATETABAUTH authority (DB2), 120
 - CSM (Communication Support Module) in Informix, 167
 - CTXSYS account (Oracle), 49
 - current_database function (PostgreSQL), 422
 - current_setting function (PostgreSQL), 421
 - current_time function (PostgreSQL), 422
 - current_timestamp function (PostgreSQL), 422
 - current_user function (PostgreSQL), 421
 - CVE-1999-1188, 293, 304
 - CVE-2000-0045, 293
 - CVE-2000-0148, 8, 293
 - CVE-2000-0981, 8, 293
 - CVE-2001-0407, 292
 - CVE-2001-0524, 9
 - CVE-2002-0567, 9
 - CVE-2002-0624, 9
 - CVE-2002-0802, 410
- D**
- DAS (Database Administration Server) in DB2
 - code for finding servers, 125–128
 - disabling, 155

- DAS (Database Administration Server) in DB2 (*continued*)
 - finding DB2 servers and, 125
 - functions callable remotely, 128–129
 - port listened to, 106, 125
 - querying for information, 128–134
- dasusr1 account, 109
- Data Dictionary Protection (Oracle), 93
- Data Stream Structures. *See* DSS in DB2
- Data Transformation Services (DTS) in SQL Server, 352–353, 380
- Database Administration Server. *See* DAS in DB2
- database links (Oracle), 81–82
- Database Scanner tool (Internet Security Systems), 336
- database security research
 - classes of security flaws, 5–13
 - defined, 5
 - finding flaws in your server, 13–16
 - predictions for, 13
- Database Writer (DBWR) process (Oracle), 26
- databases
 - problems in defining, 4
 - running as low-privileged user, 13
- Datagram proxy (Sybase), 241
- DataRescue (IDA Pro utility), 371
- db table (MySQL), 269–270
- DBA privileged accounts (Informix), 163
- DBA privileged accounts (Oracle)
 - listing accounts, 33–34
 - listing users with DBA role, 57–59
 - security recommendations, 93–95
- dbaccess tool (Informix), 160
- DBADMAUTH authority (DB2), 120
- DBAUTH view (DB2), 120–121
- DBCC CHECKVERIFY overflow (Sybase), 227
- DBMS_DESCRIBE package (Oracle), 52–53
- DBMS_EXPORT_EXTENSION procedure (Oracle), 11, 63–65
- DBMS_SCHEDULER package (Oracle), 78
- DBMS_SQL package (Oracle), 65–68
- DBSNMP account (Oracle)
 - changing passwords for, 32
 - default password, 32, 49
 - finding, 27
 - SELECT ANY DICTIONARY privilege for, 36
- DB2 Universal Database (IBM)
 - ACCRDB command, 102, 104, 113–114
 - ACCSEC command, 102, 104, 112
 - arbitrary code execution in intrinsic SQL elements, 10
 - authenticated flaws in network protocols, 7
 - authentication, 109–119
 - authorization, 120–122
 - buffer overflows in routines, 135–139
 - “call” mechanism buffer overflow, 10
 - code for finding servers, 125–128
 - connecting client to remote system, 107–108
 - DAS, 106
 - deployment scenarios, 100–106
 - disabling peripheral services, 155
 - discovery mode for servers, 128, 154
 - downloading evaluation version, 99
 - EBCDIC used in, 101
 - EXCSAT DDM command, 102
 - file system access through, 142–143
 - finding on the network, 125–128
 - fixpaks, 139, 155
 - getting OS information, 129–134
 - “hiding” servers, 128
 - JDBC Applet Server flaw (DB2), 6, 138–139, 155
 - limiting execute access for routines, 136
 - on Linux, 109
 - LOAD SQL query, 142
 - local attacks against, 143–152
 - logical database layout, 109
 - market share, 100

- packets, 100–106
- physical database layout, 108–109
- ports listened on, 106, 125
- processes, 106–107
- PUBLIC access and, 121, 122, 136, 154–155
- relative security of, 4–5
- Remote Command Server, 139–141, 155
- removing unnecessary components, 155
- response file from installation and, 152
- revoking PUBLIC access, 154–155
- running OS commands through, 141–142
- schemas, 109
- SECCHK command, 102, 104, 112–113
- SECCHK DDM command, 111
- securing the DBMS, 154–155
- securing the network interface, 154
- securing the OS, 153–154
- security alerts published for, 4–5
- Security Check Code (SECCHKCD), 111
- terminology, 106
- unauthenticated flaws in network protocols, 6
- versions, 99
- on Windows, 108–109
- XML* functions, 135–136, 143
- db2admin account, 110
- db2as account, 110
- DB2CTLSV instance, 106, 108
- db2dasdiag.log file, 109
- db2dasfn.dll, 129
- db2dasGetDasLevel function, 129
- DB2DASRRM process, 106–107
- db2diag.log file, 108
- db2fenc1 account, 109, 110, 142
- db2fmp binary, Snosoft advisory for, 152
- DB2FMP process, 106–107
- db2govd binary, Snosoft advisory for, 144
- db2inst1 account, 109, 110, 142
- DB2LPOR environment variable overflow, 149
- DB2RCMD.EXE, 139–141
- DB2REMOSECMD named pipe, 7, 140–141
- db2start binary, Snosoft advisory for, 144
- db2stop binary, Snosoft advisory for, 144
- DB2SYSCS process, 106–107
- DBWR (Database Writer) process (Oracle), 26
- DDM (Distributed Data Management), 102, 104
- debugging to understand your system, 14–15
- decrypting SQL Server procedures, 343
- default databases (Informix), 160
- default password hashing (PostgreSQL), 399
- defaults (DB2)
 - authentication type, 110
 - instances (DB2), 106
 - OS accounts and passwords, 110
 - passwords, eliminating, 154
- defaults (MySQL)
 - system schema, 263
 - test database, removing, 326
 - usernames and passwords, 258–259
- defaults (Oracle)
 - accounts and passwords, 48–49
 - changing for passwords, 90
 - CONNECT role, 91–92
 - CREATE DATABASE LINK privilege, 10
 - Intelligent Agent ports, 27
 - Intelligent Agent user account and password, 32
 - SYS login password, 33, 48
 - SYSTEM account password, 33, 49
 - TNS Listener ports, 21
 - usernames and passwords, 447–469

- defaults (SQL Server)
 - accounts created during installation, 348
 - changing default port, 335
 - UDP Resolution Service port, 6
- defaults (Sybase)
 - authentication configuration, 203, 211
 - configuration passing plaintext passwords, 8
 - mechanisms for enforcing password complexity, 204
 - roles (Sybase), 205
 - sa account, removing privileges from, 249
- DELETE statements, PL/SQL injection (Oracle), 60
- DELETEAUTH authority (DB2), 122
- deployment
 - DB2 scenarios, 100–106
 - MySQL scenarios, 256–257
 - PostgreSQL scenarios, 389
 - secure (PostgreSQL), 387–388, 433–435
 - Sybase scenarios, 199–202
- DESCRIBE_PROCEDURE (Oracle), 52–53
- development environments (Sybase), 201–202
- discovery mode for DB2 servers, 128, 154
- disk init command (Sybase), 205
- Distributed Data Management (DDM), 102, 104
- Distributed Relational Database Architecture (DRDA) protocol
 - DB2 packets and, 101–105
 - open source implementation, 102
- Distributed Transaction Recovery (RECO) process (Oracle), 26
- DLLs
 - nefarious, loading (Informix SPL), 182–184
 - removing for dropped procedures (SQL Server), 441
 - viewing functions exported by (SQL Server), 441–442
- xp_freedll buffer overflow (Sybase), 227–228
- documentation
 - Informix (IBM), 191
 - not believing, 14
- double pipe (| |) with Windows Command Interpreter, 43
- double quotes (“”) for SQL injection (Sybase), 220
- DRDA (Distributed Relational Database Architecture) protocol
 - DB2 packets and, 101–105
 - open source implementation, 102
- DRILOAD.VALIDATE_STMT procedure (Oracle)
 - Oracle Application Server and, 73–74
 - SQL injection flaw, 11, 68
- DROP DATABASE overflow (Sybase), 227
- dSQLSRVD tool, 343
- DSS (Data Stream Structures) in DB2
 - code for user authentication, 111–119
 - DDMID, 104
 - header, 104
 - overview, 102
 - packet example, 102–103
- DTS (Data Transformation Services) in SQL Server, 352–353, 380
- DTS Designer (SQL Server), 353
- dumpbin tool, 441–442
- dumping
 - dumpbin tool (SQL Server), 441–442
 - Intelligent Agent information (Oracle), 27–32
 - packet dump (Informix), 166–167
 - packet dump of authentication process (SQL Server), 337–338
 - reading dump files via SQL queries (Informix), 178–180
 - shared memory dumps upon crashing (Informix), 178–180, 190–191
 - tcpdump packet capture software, 334

- E**
- EBCDIC (Extended Binary Coded Decimal Interchange Code)
 - character table online, 101
 - DB2 and, 101
 - program for mapping ASCII to, 105–106
 - EFS (Encrypting File System) of Microsoft, 377
 - e-mail stored procedures (SQL Server), 445
 - encryption
 - cracking password hashes (MySQL), 300–301
 - for extended stored procedures (SQL Server), 343
 - for Informix with CSM, 167
 - IPSec or SSH for encrypted tunnels, 8
 - limitations of, 51
 - Microsoft EFS, 377
 - MySQL as password cracking engine, 301
 - MySQL hash authentication patch, 307–309
 - of MySQL passwords, 272, 281, 328
 - for MySQL traffic, 326
 - MySQL weakness prior to 4.1, 260
 - for network traffic (Informix), 189
 - for network traffic (Oracle), 89
 - of passwords for external servers (Sybase), 220–221
 - of passwords (SQL Server), 350–354
 - for PL/SQL procedures and functions, 51
 - Enterprise Manager tool (Oracle), 27
 - environment variables
 - DB2LPORT environment variable, 149
 - expansion and buffer overruns (Oracle), 77–78
 - SQLDEBUG (Informix), 186–187
 - error messages. *See also SQL injection entries*
 - “integer conversion” trick for SQL injection (Sybase), 216–218
 - verbose, absence of, 278
 - Ethereal packet capture software, 334
 - EXCSAT DDM command (DB2), 102
 - exec function, evading filters using (Sybase), 223–224
 - EXECUTE ANY PROCEDURE system privilege (Oracle), 36
 - EXECUTEAUTH authority (DB2), 122
 - Extended Binary Coded Decimal Interchange Code (EBCDIC)
 - character table online, 101
 - DB2 and, 101
 - program for mapping ASCII to, 105–106
 - extended stored procedures (SQL Server)
 - buffer overflow issues, 10
 - buffer overflow vulnerabilities, 342
 - bypassing access controls, 343–344
 - dangerous procedures, 441–446
 - dangers of, 341
 - decrypting, 343
 - dumpbin tool, 441–442
 - e-mail procedures, 445
 - encryption, 343
 - file output using, 342
 - finding security context using, 341
 - global temporary procedures, 345–346
 - MSMQ access using, 342
 - OLE automation procedures, 446
 - overview, 341
 - registry procedures, 442–443
 - removing dlls for dropped procedures, 441
 - retrieving registry values using, 341
 - scripts to drop and restore, 441
 - SQL injection using, 360
 - system procedures, 443–445
 - Trojan procedures, 342–343, 344–346
 - uploading files using, 344
 - viewing functions exported by dlls, 441–442
 - extended stored procedures (Sybase)
 - overview, 206–207
 - SQL injection using custom procedures, 219

- extended stored procedures (Sybase)
 - (*continued*)
 - SQL injection using `xp_cmdshell`, 218–219
- extensions via shared objects (PostgreSQL), 428–429
- external procedures. *See also specific procedures*
- extproc mechanism (Oracle), 6, 9, 12, 21, 77
 - running Oracle OS commands with PL/SQL and, 76–78
 - turning off (Oracle), 89
- EXTERNALROUTINEAUTH
 - authority (DB2), 121, 142
- extproc mechanism (Oracle)
 - flaws in, 6, 9
 - local privilege elevation issues and, 12
 - TNS Listener and, 21
 - unauthenticated access to functionality and, 9, 77

F

- Farmer, Dan (“Improving the Security of Your Site by Breaking into It”), 16
- features, security and number of, 5, 19, 99
- FHasObjPermissions function (SQL Server), 371–372
- file_priv privilege (MySQL), 285–286
- FILETOCLOB function (Informix SPL), 183, 185
- finding. *See also scanning ports*
 - DBSNMP account (Oracle), 27
 - DB2 on the network, 125–128
 - SQL Server servers, 334–336, 340
- finding flaws in your server
 - basic principles and techniques, 14
 - identifying communication protocols, 15
 - implementing your own client, 14
 - not believing the documentation, 14

- understanding arbitrary code
 - execution bugs, 15
 - understanding your system, 14–15
 - writing your own fuzzers, 15–16
- firewalls
 - bypassing with TCP reverse proxy (Sybase), 241
 - for MySQL servers, 320
 - for PostgreSQL, 435
 - Sybase and, 202–203
- fixpaks (DB2), 139, 155
- FreeTDS project, 203, 334
- FROM_TZ function overflow (Oracle), 10
- functionality, attack surface and, 5, 19, 99
- functions (DB2). *See routines (DB2)*
- functions (Informix)
 - buffer overflow vulnerabilities, 176–177
 - code to function mappings, 176–177
 - denial of service attacks using, 176
- functions (Oracle)
 - buffer overflow issues, 10
 - encrypting (wrapping) in PL/SQL, 51
 - procedures versus, in PL/SQL, 50
 - running CheckReg() with PL/SQL, 76
 - in UTL_TCP package, 83
- fuzzers, writing your own, 15–16
- Fyoder’s nMap port scanning tool, 209

G

- GENERATE_DISTFILE overflow (DB2), 136, 137–138
- getDasCfg function (DB2), 129
- get_hash function (MySQL), 308, 309
- getOSInfo function (DB2), 129
- GLBA, 3
- GRANT ANY OBJECT PRIVILEGE
 - system privilege (Oracle), 36
- GRANT ANY PRIVILEGE system privilege (Oracle), 36
- GRANT ANY ROLE system privilege (Oracle), 36

H

hash mark (#) in #NISR... notation, 12
 having/group by clause SQL injection technique, Sybase and, 218
 Heasman, John (hacker), 12
 Hello bug (SQL Server), 6, 333
 HFNetChk tool (SQL Server), 383
 HIPAA, 3
 host (DB2), 106
 hosts table (MySQL), 270
 HTF package (Oracle), 72
 HTP package (Oracle), 72

I

IBM. *See* DB2 Universal Database; Informix

ICAT Metabase, 247, 280, 289, 320

IDA Pro utility (DataRescue), 371

ident spoofing (PostgreSQL), 407–408

identd daemons (PostgreSQL), 408

IDS (Intrusion Detection System), 6–7

IMPLSCHEMAAUTH authority (DB2), 121

“Improving the Security of Your Site by Breaking into It” (Farmer, Dan and Venema, Wietse), 16

INDEXAUTH authority (DB2), 122

inet_client_addr() function (PostgreSQL), 422

inet_client_port() function (PostgreSQL), 422

inet_server_addr() function (PostgreSQL), 422

inet_server_port() function (PostgreSQL), 422

Informix (IBM)

 attacking with SPL, 180–185

 AUTH tables, 162

 authentication, 163, 174–175

 authorization, 163–164

 binaries with setuid bit set, 186

 buffer overflow for long usernames, 174

 code for connecting to arbitrary server, 167–173

 code to function mappings, 176–177

 connecting to remote server, 160

 creating highly privileged accounts, 184

 default databases, 160

 discovering server instance name, 160

 documents, 191

 enabling auditing, 190

 encrypting network traffic, 189

 listing all databases, 161

 listing database tables, 161

 loading a nefarious DLL with SPL, 182–184

 loading arbitrary libraries with SPL, 185

 local attacks on Unix-based platforms, 186–188, 191

 logical database layout, 160–163

 metatables, 161–162

 on the network, 159–160

 packet dump, 166–167

 patches, 189

 ports, 165

 post-authentication attacks, 176–177
 reading and writing arbitrary files, 185

 reading dump files via SQL queries, 178–180

 relative security of, 4–5

 response to failed authentication, 175

 response to successful authentication, 174–175

 restricting language usage, 191

 revoking connect privilege from public, 190

 revoking public execute permissions, 190

 running arbitrary commands with SPL, 181–185

 scanning for servers, 165

 security alerts published for, 4

 SET DEBUG FILE SQL command, 184–185

 shared memory dumps upon crashing, 178–180, 190–191

- Informix (IBM) (*continued*)
 - SPL, 180–185
 - SQL buffer overflows, 185–188
 - usage permission on languages, 164, 180, 191
- injection. *See* PL/SQL injection (Oracle); *SQL injection entries*
- InnoDB storage engine (MySQL), 264, 265
- INSERT statements, PL/SQL injection using (Oracle), 60–62, 70–71
- INSERTAUTH authority (DB2), 122
- installing SQL Server securely
 - authentication, 375–377
 - OS lockdown, 377–378
 - password strength, 377
 - post-installation lockdown, 378–379
- instances (DB2), 106
- “instrumenting” applications, 14–15
- “integer conversion” trick for SQL injection (Sybase), 216–218
- integer overflows (PostgreSQL), 415–416
- Intelligent Agent (Oracle)
 - agentctl utility for, 27
 - DBSNMP account, 27, 32, 36, 49
 - dumping information from, 27–32
 - emagent, 27
 - functions of, 27
 - ports, 27
 - user account and password for RDBMS, 32
- internal_encrypt function (Sybase), 221
- Internet resources. *See also* Microsoft Security Bulletins
 - APISpy32, 372
 - “Choosing an Edition of SQL Server 2000,” 332
 - Common Vulnerabilities and Exposures database, 409
 - Core-SDI paper on MySQL authentication weaknesses, 281
 - DB2 evaluation version, 99
 - for decrypting SQL Server procedures, 343
 - DRDA open source implementation, 102
 - EBCDIC character table, 101
 - Extended Stored Proc Removal and Restore Scripts, 441
 - extracting data using time delays, 288
 - FreeTDS project, 203, 334
 - Fyoder’s nMap port scanning tool, 209
 - HFNetChk tool, 383
 - IBM DDM security mechanisms, 104
 - ICAT Metabase, 247, 280, 289
 - IDA Pro utility, 371
 - identd daemons (PostgreSQL), 408
 - Informix documents, 191
 - killpwd.exe program (SQL Server), 342, 378
 - Metasploit Framework, 333
 - Microsoft EFS, 377
 - multibyte character conversion vulnerability (PostgreSQL), 425
 - MySQL known bugs, 280
 - MySQL security information, 317, 319–320
 - MySQL updates, 317, 320
 - MySQL with SSH information, 257
 - netcat listener, 356
 - Oracle TNS Listener buffer overflow vulnerabilities, 43
 - Oracle TNS protocol information, 20
 - packet capture software, 334
 - patch management solutions, 383
 - PostgreSQL fix information, 435
 - PostgreSQL hardening information, 434
 - PostgreSQL protocol information, 405
 - RegMon utility, 351
 - SQL injection information, 282–283
 - SQL injection whitepapers (SQL Server), 362
 - SQL Server Agent password decryption tool, 352
 - SQL Server Enterprise Manager, 357–358

- SQL Server patches, 383
 - SQL Server security scanners, 336
 - SQLPing utility, 335
 - SQLShield tool, 343
 - Stunnel application, 434
 - Sybase manuals, 246
 - Sybase security information, 246–247
 - Sybase update page, 246
 - “Violating Database-Enforced Security Mechanisms,” 370
 - vulnerability databases, 247, 280, 317, 320
 - WindDbg debugger, 372
 - Windows Update, 383
 - Internet Security Systems’ Database Scanner tool, 336
 - Intrusion Detection System (IDS), 6–7
 - IPS (Intrusion Prevention System), 7
 - IPSec
 - encrypted tunnel using, 8
 - filtering rule set for MySQL, 320
 - IPTables for MySQL security in Linux, 320
 - ISAM storage engine (MySQL), 264, 265
- J**
- Java
 - disabling in Sybase, 251
 - information leakage (PostgreSQL), 409
 - JSQL (Java in SQL) with Sybase, 196–197, 237–242
 - name collisions with Transact-SQL, 197
 - Oracle file system access with, 80–81
 - running Oracle OS commands with, 78–79
 - Servlet example (Sybase), 212–214
 - JDBC Applet Server flaw (DB2), 6, 138–139, 155
 - Jimmers (Rakhmanoff, Martin), 9, 351–352
 - JSQL (Java in SQL) with Sybase
 - advantages for hackers, 237–238
 - overview, 196–197
 - scanning ports with, 237, 238
 - TCP reverse proxy, 241–242
 - TDS client, 238–241
- K**
- Kargieman, Emiliano (hacker), 8
 - KERBEROS authentication type (DB2), 110
 - KERBEROS_ENCRYPT authentication type (DB2), 110
 - killpwd.exe program (SQL Server), 342, 378
 - Kornbrust, Alexander (hacker), 11
- L**
- LC_TYPE overflow (DB2), 7
 - LDAP, scanning for Sybase and, 210
 - legislative burdens for security, 3–4
 - LGWR (Log Writer) process (Oracle), 26
 - libpq library (PostgreSQL), 425
 - library privileges (Oracle), 36
 - linked servers, weakly encrypted passwords for (Sybase), 220–221
 - Linux platforms. *See also* Unix-based platforms
 - DB2 on, 109
 - default Informix databases, 160
 - host-based firewalls, 202–203, 320
 - OS accounts and default passwords (DB2), 110
 - PostgreSQL hardening information, 434
 - running external programs with MySQL UDFs, 309–311
 - running OS commands through DB2, 141–142
 - Listener Control Utility (lsnrctl) in Oracle
 - described, 21
 - error if password has been set, 41
 - querying for services and status information, 21–22
 - services command, 41
 - setting Listener to connect to, 40

- Listener Control Utility (lsnrctl) in
 - Oracle (*continued*)
 - status command, 42
 - version command, 40–41
 - Litchfield, David
 - DB2 issues discovered by, 6, 7
 - Oracle issues discovered by, 6, 9, 10, 11, 14
 - SQL Server issues discovered by, 6, 12, 333
 - Litchfield, Mark
 - Oracle issues discovered by, 6, 10, 48
 - SQL Server issue discovered by, 10
 - LOAD command overflow (DB2), 136–137
 - LOAD command vulnerabilities (PostgreSQL), 429–432
 - LOAD DATA INFILE statement (MySQL)
 - disabling, 325
 - SQL injection using, 287
 - LOAD SQL query (DB2), 142
 - LOADAUTH authority (DB2), 121, 142
 - LOAD_FILE function, SQL injection using (MySQL), 285–287
 - local attacks against DB2
 - binaries with setuid bit set, 143–144
 - buffer overflow in shared object, 149–152
 - *nix platforms and, 143
 - setuid bit and, 143
 - Snosoft advisory, 144
 - unsafe call to printf() example, 145–149
 - local attacks against Informix, 186–188, 191
 - local attacks against MySQL, 304–305
 - local privilege elevation issues, 12–13.
 - See also* PL/SQL injection (Oracle);
SQL injection entries
 - lockout for accounts
 - authentication and (DB2), 153–154
 - enabling (DB2), 153–154
 - enabling (Oracle), 92
 - enabling (Sybase), 248
 - unused accounts, locking and expiring (Oracle), 90
 - log file poisoning with TNS Listener (Oracle), 43–44
 - Log Writer (LGWR) process (Oracle), 26
 - logging
 - audit information (Oracle), 36–37
 - authentication attempts (Sybase), 211
 - checking logs (MySQL), 326–327
 - enabling query log (MySQL), 324–325
 - LOTOFILE function (Informix SPL), 183, 185
 - lsnrctl utility. *See* Listener Control Utility in Oracle
- M**
- magic_quotes_gpc setting (PHP), 283
 - mailing lists, 320, 435
 - man-in-the-middle attacks (Sybase), 211
 - MDSYS account (Oracle)
 - default password, 49
 - PL/SQL injection and triggers, 68–70
 - Memory storage engine (MySQL), 264
 - Merge storage engine (MySQL), 264
 - Metasploit Framework, 333
 - metatables (Informix), 161–162
 - Microsoft Baseline Security Analyzer, 383
 - Microsoft Data Engine (MSDE), 4, 332, 333
 - Microsoft EFS (Encrypting File System), 377
 - Microsoft Message Queue Server (MSMQ), 342
 - Microsoft Query Analyzer, 370
 - Microsoft Security Bulletins
 - MS00-035, 378
 - MS00-048, 346
 - MS02-043, 367
 - MS02-056, 333
 - MS03-031, 366
 - MS03-033, 358
 - MS99-059, 334

- Microsoft SQL Server. *See* SQL Server
- MSDE (Microsoft Data Engine), 4, 332, 333
- MSMQ (Microsoft Message Queue Server), 342
- multibyte character conversion
 - vulnerability (PostgreSQL), 425
- my.ini file (MySQL), 258
- MyISAM storage engine (MySQL)
 - referential integrity not supported by, 276–277
 - security features and properties, 264
- MyLUA UDF (MySQL), 303
- MyPHP UDF (MySQL), 303
- MySQL
 - access control system flaws, 276
 - authentication, 8, 258–262, 272, 280–281, 302–303, 307–309
 - binary packages available, 255–256
 - clearing .mysql_history file, 322
 - columns_priv table, 270, 271
 - configuration security, 319, 324–326
 - db table, 269–270
 - default system schema, 263
 - default usernames and passwords, 258–259
 - deployment scenarios, 256–257
 - disabling TCP/IP connections (if local only), 325
 - disabling unnecessary services or daemons, 322
 - disallowing symbolic links, 325–326
 - encrypting traffic, 326
 - exploit code for CAN-2004-0627, 293–297
 - exploiting architectural design flaws, 272–278
 - extracting data using time delays, 288–289
 - file-per-table approach, 263–264
 - file_priv privilege, 285–286
 - filesystem layout, 265, 305
 - finding targets, 279–281
 - firewalls, 320
 - getting to root account, 258–259
 - hosts table, 270
 - known bugs and fixes, 289–297
 - licensing, 255
 - limiting file access, 321
 - LOAD DATA INFILE statement, 287, 325
 - local attacks against, 304–305
 - local privilege elevation issues, 12, 13
 - logging, 324–325, 326–327
 - logical database architecture, 263–272
 - mailing lists, 320
 - missing features that improve security, 278
 - missing features with security impact, 276–278
 - one-bit patch (Trojan), 302–303
 - OS security, 318, 320–322
 - packet format, 259–260
 - as password cracking engine, 301
 - physical database architecture, 255–262
 - plaintext credentials, 258, 321–322
 - platforms supported, 255–256
 - popularity of, 255
 - ports, 279
 - principle of least privilege, 324
 - privilege model, 266–272
 - proprietary protocol, 259–260
 - query batching, 265–266
 - querying invalid users, 298–300
 - referential integrity not enforced in, 276–277
 - relative security of, 4–5
 - removing non-root users, 322
 - renaming root account, 322
 - REQUIRE SSL for remote connections, 323
 - restricting users by IP address, 323–324
 - root account protection, 259
 - routine audit, 319, 326–328
 - running external programs on Linux, 309–311
 - running external programs on Windows, 311–315

MySQL (*continued*)
 running with — chroot option, 321
 running with low-privileged account, 321
 scanning for servers, 279–280
 security alerts published for, 4
 security checklist, 317–319
 security information online, 317, 319–320
 separate users for web applications, 323
 simplicity of, 273–274
 snooping authentication, 280–281
 SQL injection, 282–289
 SSH server with, 257
 storage engines, 264–265, 276–277
 subqueries not supported prior to 4.1, 278
 symbolic link syntax, 265
 tables_priv table, 270–271
 test database, removing, 326
 transactional support not default in, 277–278
 Trojanning, 297–303
 UNION statement lacking prior to 4.0, 278
 update page, 317, 320
 user and group accounts, 266–272
 User Defined Functions (UDFs), 266, 273–276, 303, 309–315, 325
 user security, 318–319, 322–324
 user table, 266–269, 272, 324
 verbose error messages missing from, 278
 version numbers, 256–257, 280
 web applications, 257
 WinMySQLAdmin tool, 257–258
 W32.Spybot.IVQ worm or W32/Sdbot.worm.gen.j worm, 259, 309
mysqlbug script, 304
mysqld_multi script, 304
.mysql_history file, clearing, 322

N

National Institute of Standards and Technology (NIST), 247, 280
netcat listener, 356
netlibs (SQL Server), 334, 379
Network Intelligence India, 247
network protocol flaws, 6–7
network sniffing (PostgreSQL), 406
NGSSQuirreL scanner (Next Generation Security Software), 336
NIST (National Institute of Standards and Technology), 247, 280
*nix platforms. *See* Unix-based platforms
nMap port scanning tool (Fyoder), 209
NOFENCEAUTH authority (DB2), 120
NUMTOSTDINTERVAL function overflow (Oracle), 10
NUMTOYMINTERVAL function overflow (Oracle), 10

O

object privileges (Informix), 164
object privileges (Oracle), 35
ODBC (Open Database Connectivity) in Client-Server applications (Sybase), 199
 driver overflow (PostgreSQL), 416–417
 OPENROWSET re-authentication (SQL Server), 339–340
 password obfuscation algorithm, 352
 scanning for Sybase and, 210
OLE automation stored procedures (SQL Server), 446
one-bit patch Trojan (MySQL), 302–303
Open Database Connectivity. *See* ODBC
OPEN_CONNECTION function (Oracle), 83
OPENROWSET re-authentication (SQL Server)
 brute-forcing usernames and passwords, 339–340

- described, 339
- finding servers using, 340
- port scanning using, 273, 367
- reading files using, 340
- OpenSSL vulnerabilities (PostgreSQL), 417–418
- Oracle
 - account security, 89–91
 - arbitrary code execution in intrinsic SQL elements, 10
 - arbitrary code execution in securable SQL elements, 10
 - auditing, 36, 94
 - authorization, 35
 - buffer overflow for wrapped procedures, 53
 - creating new database, 95
 - database account authentication, 32, 34–37
 - database links, 81–82
 - DBA privileged accounts, 33–34, 57–59, 93–95
 - default accounts and passwords, 48–49
 - default usernames and passwords, 447–469
 - executing user-supplied queries with DBMS_SQL, 65–68
 - file system access, 79–81
 - functionality, risks from, 19
 - injecting into anonymous PL/SQL blocks, 62–65
 - injecting into DELETE statements, 60
 - injecting into INSERT statements, 60–62
 - injecting into UPDATE statements, 60, 62
 - installing new database, 95
 - Intelligent Agent, 27–32
 - Java and, 78–79, 80–81
 - learning SIDs for services, 41, 42, 43
 - listing DBA privileged accounts, 33–34
 - network access, 81–82
 - object privileges, 35
 - OS account authentication, 32
 - passwords stored in SYS.USER\$ table, 33
 - patching, 94
 - PL/SQL and Oracle Application Server, 71–74
 - PL/SQL injection, 53–60, 68–71
 - PL/SQL overview, 49–53
 - PL/SQL security recommendations, 93–94
 - PlsqlExclusionList, 72–73
 - popularity of, 19
 - ports for common processes, 39–40
 - privilege elevation via SQL injection, 11
 - querying services information, 21–22, 41
 - querying status information, 21–22, 42
 - querying version information, 23–25, 40–41, 42
 - RDBMS processes, 26
 - relative security of, 4–5
 - revoking unnecessary permissions, 93
 - roles, 91–93
 - running OS commands, 75–79
 - scanning for servers, 39–49
 - security alerts published for, 4
 - security audits, 94
 - security recommendations, 87–94
 - sending arbitrary packets over TNS, 44–48
 - shells on servers, avoiding, 9
 - SQL92 Security parameter, 92–93
 - SYS account, 32–33, 48
 - system privileges, 35–36
 - TCP port scanner, 83–84
 - TNS Listener, 9, 20–25, 40–49, 87–89
 - unauthenticated access to functionality, 9
 - unauthenticated flaws in network protocols, 6
 - on Windows versus UNIX-based platforms, 26

- ORACLE account password (Oracle), 49
- Oracle Application Server, PL/SQL and, 71–74
- oracle.exe process, 26
- oracleorasidsol process, 26
- Osql command-line tool (SQL Server), 335
- OWA_UTIL package (Oracle), 72–73

P

- packet capture software, 334
- packet dump (Informix), 166–167
- packet format (MySQL), 259–260
- packets (DB2)
 - commands, 102–103, 104
 - datatypes, 104–105
 - DRDA protocol for, 101–105
 - DSS (Data Stream Structures), 102–103, 104
 - DSS header, 104
 - EBCDIC used in, 101
 - IP Header, 100–101
 - TCP Header, 101
- parameterized queries (PostgreSQL), 435
- passwords (DB2)
 - EBCDIC used in, 101
 - eliminating defaults, 154
 - OS accounts and default passwords, 110
 - policy for, 153
 - response file from installation and, 152
- passwords (in general)
 - authenticated flaws in network protocols and, 7
 - changing with ALTER USER command, avoiding, 32
 - MySQL as password cracking engine, 301
- passwords (Informix)
 - clear text in packet dump, 167
 - encryption with CSM, 167
 - extracting from shared memory dump, 178–180
- passwords (MySQL)
 - access control system flaws, 276
 - checking hashes, 328
 - cracking password hashes, 300–301
 - default configuration, 258–259
 - encryption, 272, 281, 328
 - file_priv privilege and, 286
 - hash authentication patch, 307–309
 - MySQL as password cracking engine, 301
 - plaintext storage by
 - WinMySQLAdmin tool, 258
 - root account protection, 259
 - for root@localhost account, 322
 - in user table, 268, 272
- passwords (Oracle)
 - changing defaults, 90
 - default accounts and passwords, 48–49
 - default usernames and passwords, 447–469
 - for highly privileged roles, 92
 - for Intelligent Agent, 32
 - obtaining for SYS account, 69
 - obtaining from SYS.USER\$ table, 54–56, 57–58
 - one-bit patch altering authentication, 302–303
 - policy for, 90–91
 - resetting for ANONYMOUS user, 61
 - setting for TNS Listener, 87–88
 - stored in SYS.USER\$ table, 33
 - for SYS account, 33, 48
 - for SYSTEM account, 33, 49
 - for TNS Listener, 9, 21, 41, 43, 87–88
- passwords (PostgreSQL)
 - default hashing (md5), 399
 - storing in plaintext, 399–400
- passwords (SQL Server)
 - brute-forcing accounts, 339–340
 - buffer overflow issues, 9
 - deciphering obfuscated passwords, 338–339, 352
 - DTS package passwords, 352–353
 - encryption, 350–354
 - killpwd.exe program, 342, 378

- obfuscation, 337–338
- pwdencrypt function, 9, 350
- replication passwords, 353–354
- role passwords, 352
- saved in plaintext, 342, 378
- secure installation and, 377
- SQL Server Agent password, 351–352
- time-based salting for hash, 350–351
- viewing sa user’s hash, 350
- passwords (Sybase)
 - enforcing complexity, 204, 248–249
 - for linked servers, weak encryption of, 220–221
 - specifying expiration, 204
 - transmitted in clear text, 203, 211
- patches
 - for arbitrary code execution in intrinsic SQL elements, 10
 - for arbitrary code execution in securable SQL elements, 11
 - for authentication protocol flaws, 8
 - fixpaks (DB2), 139, 155
 - for Informix, 189
 - MySQL hash authentication patch, 307–309
 - MySQL one-bit patch (Trojan), 302–303
 - for Oracle, 94
 - for PostgreSQL, 435
 - for privilege elevation via SQL injection, 12
 - for SQL Server, 333, 383
 - for Sybase, 199, 202, 217
- Patchlink Update tool, 383
- Performance Manager (Oracle), 27
- pgAdmin (PostgreSQL), 408
- pg_class catalog (PostgreSQL), 396, 397–398
- pg_database catalog (PostgreSQL), 396, 397
- pg_group catalog (PostgreSQL), 397, 399
- pg_hba.conf file (PostgreSQL)
 - authentication method token, 393–394
 - connection type tokens, 392–393
 - database token, 393
 - record forms, 392
 - secure deployment, 433
 - startup packet and, 405
 - username token, 393
- pg_language catalog (PostgreSQL), 397, 398, 400
- pg_largeobject catalog (PostgreSQL), 397, 398, 427–428
- pg_proc catalog (PostgreSQL), 397, 398, 400–401
- pg_shadow catalog (PostgreSQL), 397, 398, 399
- pg_trigger catalog (PostgreSQL), 397, 398
- PHP
 - magic_quotes_gpc setting, 283
 - MyPHP UDF (MySQL), 303
 - SQL injection example (PostgreSQL), 418–420
- plaintext
 - authentication mechanisms, 8
 - Informix password issues, 167, 203, 211
 - MySQL credentials, 258, 321–322
 - SQL Server passwords saved in, 342, 378
 - storing PostgreSQL passwords in, 399–400
- PL/SQL (Procedural Language/SQL)
 - in Oracle. *See also* PL/SQL injection (Oracle)
 - buffer overflow for wrapped procedures, 53
 - described, 49
 - encrypting (wrapping) procedures and functions, 51
 - executing procedures over the web, 71–74
 - executing procedures with definer rights, 51
 - executing procedures with invoker rights, 51
 - extending with external procedures, 50
 - external procedures and, 21

- PL/SQL (Procedural Language/SQL)
 - in Oracle (*continued*)
 - file system access, 79–80
 - “Hello, world!” program example, 49–50
 - listing available procedures and functions and their parameters, 51–53
 - network access, 81, 82–85
 - Oracle Application Server and, 71–74
 - overview, 49–53
 - PlsqlExclusionList, 72–73
 - procedures versus functions, 50
 - running OS commands with, 76–78
 - security recommendations, 93–94
 - TCP port scanner, 83–84
 - Toolkit for web applications, 72
 - UTL_FILE package, 79–80
 - UTL_HTTP package, 84
 - UTL_SMTP package, 85
 - UTL_TCP package, 82–84
- PL/SQL injection (Oracle). *See also* PL/SQL (Procedural Language/SQL) in Oracle
 - into anonymous PL/SQL blocks, 62–65
 - of attacker-defined functions to overcome barriers, 55–59
 - dangers of, 51
 - database triggers and, 68–71, 94
 - into DBMS_EXPORT_EXTENSION procedure, 11, 63–65
 - into DELETE statements, 60
 - into DRILOAD.VALIDATE_STMT procedure, 11, 68
 - inheriting SYS privileges, 56
 - into INSERT statements, 60–62, 70–71
 - listing users with DBA role, 57–59
 - output buffering and, 58–59
 - privilege elevation via, 53–54
 - into SELECT statements, 54–60
 - into UPDATE statements, 60, 62
 - of user-supplied queries with DBMS_SQL, 65–68
 - using AUTONOMOUS_TRANSACTION pragma, 59–60
 - into WK_ACL.STORE_ACL procedure, 11, 61–62
 - into WK_ADM.COMPLETE_ACL_SNAPSHOT procedure, 11, 62
- PlsqlExclusionList (Oracle), 72–73
- PMON (Process Monitor) process (Oracle), 26
- ports
 - changing default for SQL Server, 335
 - for common Oracle processes, 39–40
 - for DAS listening (DB2), 106, 125
 - for DB2 instances, 106
 - for Informix processes, 165
 - for Intelligent Agent (Oracle), 27
 - scanning for DB2 servers, 125
 - scanning for Informix servers, 165
 - scanning for MySQL servers, 279
 - scanning for Oracle servers, 39
 - scanning for SQL Server servers, 334–336
 - scanning for Sybase servers, 209–210
 - for SQL Server processes, 334–336
 - starting listeners (Sybase), 207
 - for Sybase services, 202
 - TCP port scanner (Oracle), 83–84
 - for TNS Listener (Oracle), 20–21, 39, 40
- PostgreSQL
 - ARP spoofing, 406
 - authentication, 392–396
 - cash_words() function overflow, 413–415
 - code execution vulnerabilities, 412–416
 - commercial versions, 388
 - Common Vulnerabilities and Exposures database, 409
 - component vulnerabilities, 416–418
 - configuration vulnerabilities, 411–412
 - COPY command vulnerabilities, 425–427
 - dangerous functions, 435
 - deployment scenarios, 389

- disabling unnecessary services, 434
- enabling SSL, 433–434
- extensions via shared objects, 428–429
- file structure, 389–391
- filesystem attacks, 425–432
- finding targets, 403–404
- firewalls, 435
- hardening the server and environment, 434–435
- ident spoofing, 407–408
- identd daemons, 408
- information leakage from compromised resources, 408–409
- integer overflows, 415–416
- known bugs, 409–418
- LOAD command vulnerabilities, 429–432
- local privilege elevation issues, 12
- mailing list, 435
- network sniffing, 406
- network-based attacks against, 406–408
- obtaining group information, 399
- ODBC driver overflow, 416–417
- OpenSSL vulnerabilities, 417–418
- parameterized queries, 435
- patches, 435
- pg_hba.conf file, 392–394, 405, 433
- physical database architecture, 387–389
- platforms supported, 387–388
- protocols, 391–392, 395–396, 404–405
- relative security of, 4–5
- running on single user system, 434
- secure deployment, 387–388, 433–435
- as “secure out of the box,” 388
- security alerts published for, 4
- Sir Mordred advisories, 412
- socket creation options, 392
- SQL injection, 418–425
- stored procedures, 400–401, 423–424
- system catalogs, 396–398
- TCP Hijacking, 406, 407
- template databases, 391
- terminology, 389
- TZ environmental variable overflow, 412–413
- users and groups, 399–400
- version numbers, 404–405
- principle of least privilege, 92, 324
- privilege elevation. *See also* PL/SQL injection (Oracle); *SQL injection entries*
- local privilege elevation issues, 12–13
- by SQL injection, 11–12
- privilege model
- MySQL, 266–272
- Sybase, 203–204
- Procedural Language/SQL. *See* PL/SQL in Oracle
- procedures. *See also* extended stored procedures (SQL Server); PL/SQL in Oracle; stored procedures; *specific procedures*
- creating in Informix, privileges and, 164
- extended stored (Sybase), 206–207, 218–219
- external (Oracle), 76–78, 89
- extproc mechanism (Oracle), 6, 9, 12, 21, 77
- routines (DB2), 135–138, 143
- Process Monitor (PMON) process (Oracle), 26
- ProFTPD (PostgreSQL), 424–425
- protocols. *See also* TNS Listener (Oracle); *specific protocols*
- DRDA protocol (DB2), 101–105
- flaws (DB2), 6, 7
- flaws in network protocols, authenticated, 7
- flaws in network protocols, unauthenticated, 6–7
- flaws (MySQL), 8, 260–262, 272
- flaws (Oracle), 6
- flaws (Sybase), 8
- Identification Protocol (PostgreSQL), 395–396

- protocols (*continued*)
 - identifying communication
 - protocols, 15
 - open authentication protocol
 - support (Sybase), 198, 203
 - PostgreSQL protocols, 391–392, 395–396, 404–405
 - proprietary (MySQL), 259–260
 - for remote authentications (MySQL), 302
 - TDS protocol (SQL Server), 333–334
 - TDS protocol (Sybase), 203, 238–241
 - Proxy Table support (Sybase)
 - disabling, 251
 - enabling, 224
 - psql PostgreSQL client, 408
 - pwdencrypt function (SQL Server), 9, 350
- Q**
- Query Analyzer (Microsoft), 370
 - query batching
 - MySQL, 265–266
 - SQL Server, 368
 - Sybase, 215, 218
 - query log (MySQL), 324–325
 - QUIESCECONNECTAUTH authority (DB2), 121
 - quotation marks
 - CHAR function to bypass quote filters (Sybase), 219–220
 - SQL injection using double quotes (Sybase), 220
 - SQL injection using single quote (MySQL), 282
 - SQL injection using single quote (SQL Server), 359–362
 - SQL injection using single quote (Sybase), 214–215
- R**
- race conditions (MySQL), 304
 - RAISERROR format string bug (SQL Server), 9
 - Rakhmanoff, Martin (hacker), 9, 351–352
 - raw disk partitions, Sybase support for, 198
 - READ_RAW function (Oracle), 83
 - READ_TEXT function (Oracle), 83
 - RECO (Distributed Transaction Recovery) process (Oracle), 26
 - REC2XML routine (DB2), 135
 - REFAUTH authority (DB2), 122
 - referential integrity, not enforced in MySQL, 276–277
 - registry (SQL Server)
 - dangerous stored procedures, 442–443
 - RegMon utility for monitoring, 351
 - retrieving values using xp_regread, 341
 - SQL injection using keys, 364
 - RegMon utility, 351
 - Remote Command Server (DB2), 139–141, 155
 - replication passwords (SQL Server), 353–354
 - REQUIRE SSL for remote connections (MySQL), 323
 - Resource privilege (Informix), 163
 - Richarte, Gerardo (hacker), 8
 - roles (SQL Server)
 - application roles, 349, 352
 - built-in server roles, 348–349
 - fixed database roles, 349
 - passwords, 352
 - PUBLIC role, 349, 380
 - User-Defined Roles, 349
 - roles (Sybase), 205, 243, 248
 - ROUTINEAUTH view (DB2), 122
 - routines (DB2)
 - CALL command overflow, 137
 - CREATE WRAPPER command overflow, 137
 - defined, 135
 - GENERATE_DISTFILE overflow, 136, 137–138
 - known buffer overflow vulnerabilities, 135–136
 - limiting execute access for, 136

- LOAD command overflow, 136–137
 - SET LOCALE LCTYPE overflow, 138
 - XML* functions, 135–136, 143
 - running external programs with UDFs (MySQL)
 - on Linux, 309–311
 - on Windows, 311–315
 - running OS commands (Oracle)
 - authorization for, 75
 - with DBMS_SCHEDULER, 78
 - with Java, 78–79
 - with PL/SQL, 76–78
 - running OS commands with SPL (Informix), 181–185
- S**
- sa_role, granting to users (Sybase), 243
 - Sarraute, Carlos (hacker), 8
 - Satellite control database (stctldb) in DB2, 106
 - SatEncrypt routine (DB2), 136
 - scanning for MySQL, 279–280
 - scanning ports
 - for DB2 servers, 125
 - for Informix servers, 165
 - for MySQL servers, 279
 - for Oracle servers, 39–49
 - SQL injection for (SQL Server), 367
 - for SQL Server servers, 334–336
 - for Sybase servers, 209–210
 - TCP port scanner (Oracle), 83–84
 - sc.exe tool (SQL Server), 336
 - schemas (DB2), 109, 122
 - SECCHK command (DB2)
 - in code for user authentication, 112–113
 - in packets, 102, 104
 - SECCHK DDM command (DB2), 111
 - SECCHKCD (Security Check Code) in DB2, 111
 - security alerts, 4. *See also specific alerts*
 - security audits. *See auditing*
 - Security Focus site, 43, 247, 320
 - SELECT ANY DICTIONARY system privilege (Oracle), 36, 93
 - SELECT statements, injecting into (Oracle PL/SQL), 54–60
 - SELECT statements, UNION. *See* UNION SELECT statements
 - SELECTAUTH authority (DB2), 122
 - SELECT...INTO OUTFILE statement, SQL injection using (MySQL), 287–288
 - SERVER authentication type (DB2), 110, 154
 - Server Network Utility (SQL Server), 334–335
 - SERVER_ENCRYPT authentication type (DB2), 110, 154
 - services
 - Data Transformation Services (SQL Server), 352–353, 380
 - disabling peripheral services (DB2), 155
 - disabling unnecessary services (PostgreSQL), 434
 - getting information (Oracle), 21–22, 41
 - learning SIDs for (Oracle), 41, 42, 43
 - ports for Sybase services, 202
 - removing unnecessary features and services (SQL Server), 381–382
 - service interaction (Sybase), 206–207
 - session_user function (PostgreSQL), 421
 - SET DEBUG FILE SQL command (Informix), 184–185
 - SET LOCALE LCTYPE overflow (DB2), 138
 - setuid bit
 - local attacks against DB2 and, 143
 - local attacks against Informix and, 186–188
 - SHA1 hash, cracking with MySQL, 301
 - shared memory (Informix), 190
 - dumped upon crashing, 178
 - preventing dumping, 178, 190–191
 - reading dump files, 178–180
 - The Shellcoder's Handbook* (Wiley publication), 15

- shells, avoiding on Oracle servers, 9
- SHUTDOWN command, SQL injection using (Sybase), 220
- SIDs, learning for Oracle services, 41, 42, 43
- single quote (')
 - CHAR function to bypass quote filters (Sybase), 219–220
 - SQL injection using (MySQL), 282
 - SQL injection using (SQL Server), 359–362
 - SQL injection using (Sybase), 214–215
- Sir Mordred advisories (PostgreSQL), 412
- Slammer worm (SQL Server), 4, 6, 332, 356
- SMON (System Monitor) process (Oracle), 26
- snmp_ro.ora file (Oracle), 32
- snmp_rw.ora file (Oracle), 32
- snooping authentication
 - MySQL, 280–281
 - Sybase, 211
- SOX, 3
- sp_addexternlogin procedure (Sybase), 221
- sp_addlogin procedure (Sybase), 248
- sp_configure procedure (Sybase)
 - allowing updates to system tables, 243
 - disabling Java, 251
 - disabling Proxy Table support, 251
 - enabling auditing, 251
 - enabling Proxy Table support, 224
 - enforcing password complexity, 204, 248–249
 - setting account lockout, 248
- sp_decrypt_7.sql tool, 343
- sp_dropextendedproc procedure (Sybase), 251
- sp_enum_dtspackages procedure (SQL Server), 353
- sp_get_dtspackage procedure (SQL Server), 353
- sp_get_SQLagent_properties procedure (SQL Server), 351, 352, 380
- sp_helpdevice procedure (Sybase), 205
- SPL (Stored Procedural Language) in Informix
 - creating highly privileged accounts, 184
 - FILETOCLOB function, 183, 185
 - loading a nefarious DLL, 182–184
 - loading arbitrary libraries, 185
 - LOTOFILE function, 183, 185
 - reading and writing arbitrary files, 185
 - running arbitrary commands, 181–185
 - start_onupload procedure, 181–182
 - SYSTEM function, 181
 - usage permission on languages and, 180
- sp_listener procedure (Sybase), 207
- sp_modifylogin procedure (Sybase), 204, 249
- sp_MSscopyscript procedure (SQL Server), 12
- sp_MSscopyscriptfile procedure (SQL Server), 367
- sp_MSdropretry procedure (SQL Server), 365–366
- sp_password procedure (Sybase), 220
- SQL Agent (SQL Server), 12
- SQL injection (in general)
 - arbitrary code execution in intrinsic SQL elements and, 9
 - background information online, 282–283
 - code for SQL injection harness, 437–440
 - defense against, 12
 - discovered flaws, 11–12
 - privilege elevation via, 11–12
- SQL injection (MySQL)
 - background information online, 282–283
 - file_priv privilege and, 285–286
 - as initial attack vector, 282

- LOAD DATA INFILE statement for, 287
- LOAD_FILE function for, 285–287
 - major danger areas, 283
 - “missing features” and, 278
 - PHP magic_quotes_gpc setting and, 283
 - PHP script for examples, 284
- SELECT...INTO OUTFILE statement for, 287–288
 - seriousness of, 282
 - single quote for, 282
 - time delays for, 288–289
- UNION SELECT statements for, 284–285
- SQL injection (Oracle). *See* PL/SQL injection (Oracle)
- SQL injection (PostgreSQL), 417–418
 - built-in functions for, 421–422
 - comments for, 420–421
 - in libpq library, 425
 - multibyte character conversion and, 425
 - in other applications, 424–425
 - PHP example, 418–420
 - in ProFTPD, 424–425
 - stored procedures for, 423–424
 - time delays for, 422–423
- UNION SELECT statements for, 420–421
- SQL injection (SQL Server)
 - alternative attack vectors, 363–364
 - ASP script and, 358–361
 - batched queries for, 368
 - comments for, 360–362
 - as common attack vector, 358
 - defending against attacks, 368–370
 - port scanning, 367
 - single quote for, 359–362
 - stored procedures for, 365–367
 - system-level attacks, 362–363
 - temporary tables for, 363
 - time delays for, 364–365
 - whitepapers, 362
 - xp_cmdshell procedure for, 362–363
- SQL injection (Sybase)
 - audit evasion with sp_password, 220
 - basics, 212–215
 - batch injection, 215, 218
 - CHAR function to bypass quote filters, 219–220
 - comments for, 216
 - exec function for, 223–224
 - extended stored procedures for, 218–219
 - getting usernames from syslogins table, 214–215
 - having/group by clause technique and, 218
 - “integer conversion” trick, 216–218
 - Microsoft “ancestral” code and, 211
 - MS SQL Server techniques, 215–224
 - obtaining list of databases on server, 216–217
 - querying external servers and, 220–221
 - seriousness of, 212, 215
 - SHUTDOWN command for, 220
 - single quote for, 214–215
 - truncating queries with comments, 216
 - UNION SELECT statements for, 216
 - using JSQL, 237–238
 - using time delays as communications channel, 221–223
 - using Transact-SQL query batching, 215, 218
 - VARBINARY literal for, 224
 - web application for examples, 212–214
 - web applications and, 200
 - xp_cmdshell for privilege elevation, 218–219
- SQL Monitor port (SQL Server), 335
- SQL Server (Microsoft). *See also* extended stored procedures (SQL Server)
 - arbitrary code execution in intrinsic SQL elements, 9

- SQL Server (Microsoft) (*continued*)
 - arbitrary code execution in securable SQL elements, 10
 - auditing, 379, 383
 - authentication and authorization, 336–340
 - authentication protocol flaws, 8
 - background, 331–332
 - basic security measures, 369–370
 - bypassing access controls, 343–344
 - changing default port, 335
 - “Choosing an Edition of SQL Server 2000,” 332
 - client overflows, 357–358
 - configuration security, 379–383
 - confined to Windows platforms, 333
 - covering attacker tracks, 370–373
 - denial of service vulnerabilities, 347, 355, 356–357
 - disabling ad-hoc queries, 340, 381–382
 - disabling “allow updates” option, 381
 - disabling remote access, 381
 - DTS packages, 352–353, 380
 - exploiting design flaws, 355–358
 - Extended Stored Proc Removal and Restore Scripts, 441
 - finding servers, 334–336, 340
 - getting server information, 335
 - guest account, disabling, 379–380
 - Hello bug, 6, 333
 - history, 331–332
 - local privilege elevation issues, 12
 - locking down privileges, 379–380
 - logical architecture, 341–347
 - market share, 331
 - Microsoft Baseline Security Analyzer, 383
 - MSDE and, 4, 332, 333
 - network libraries, 334, 379
 - network protocols supported, 334
 - OPENROWSET re-authentication, 273, 339–340, 367
 - Osql command-line tool, 335
 - password encryption, 350–354
 - patches, 333, 383
 - physical architecture, 333–340
 - ports, 334–336
 - privilege elevation via SQL injection, 12
 - processes, 334–335
 - PUBLIC role, 349, 380
 - querying remote servers, 272–273
 - relative security of, 4–5
 - removing unnecessary features and services, 381–382
 - roles, 348–349
 - sample databases, removing, 379
 - secure installation, 375–379
 - security alerts published for, 4
 - security scanners, 336
 - Slammer worm and, 4, 6, 332, 356
 - SQL injection, 358–370
 - SQL injection techniques in Sybase, 215–224
 - start-up procedure Trojanning, 373
 - stored procedures, 341–346, 382–383
 - Sybase and, 196, 211
 - TDS protocol, 333–334
 - three-byte patch backdoor, 370–373
 - triggers, 346–347
 - UDP Resolution Service, 4
 - unauthenticated flaws in network protocols, 6
 - users and groups, 347–354
 - versions (editions), 332
 - Windows Server Controller tool, 336
 - xstatus backdoor, 373
 - 0x0A leading byte DoS, 357
 - 0x08 leading byte heap overflow, 356–357
- SQL Server Agent
 - decrypting password hashes, 351–352
 - described, 351
 - retrieving information, 351
- SQL Server Enterprise Manager, 357–358
- SQL Server Monitor, 381
- SQLDEBUG environment variable (Informix), 186–187

- SQL92 Security parameter (Oracle), 92–93
- SQLPing utility, 335, 336, 355
- SQLShield tool, 343
- SSH
 - deploying with MySQL, 257
 - encrypted tunnel using, 8
- SSL
 - authentication (MySQL), 8
 - OpenSSL vulnerabilities (PostgreSQL), 417–418
 - REQUIRE SSL for remote connections (MySQL), 323
- sso_role, granting to users (Sybase), 243
- start_onupload procedure (Informix SPL), 181–182
- start-up procedure Trojanning (SQL Server), 373
- status information, getting from Oracle, 21–22, 42
- stctldb (Satellite control database) in DB2, 106
- storage engines (MySQL)
 - referential integrity not supported by, 276–277
 - security features and properties, 264–265
- Stored Procedural Language. *See* SPL in Informix
- stored procedures. *See also* extended stored procedures (SQL Server); *specific procedures*
 - dangerous (SQL Server), 341
 - extended (Sybase), 206–207, 218–219
 - local privilege elevation issues, 12
 - PostgreSQL, 400–401
 - removing (SQL Server), 382–383
 - scheduled for MySQL 5.1, 266
 - security issues, 341
 - SQL injection risks, 11–12
 - SQL injection using (PostgreSQL), 423–424
 - SQL injection using (SQL Server), 360, 365–367
 - strtok() function (SQL Server), 357
 - Stunnel application, 434
 - subqueries, MySQL and, 278
 - Sybase ASE (Adaptive Server Enterprise). *See also* SQL injection (Sybase)
 - accessing system tables, 243–244
 - accessing the network, 235–236
 - arbitrary code execution in intrinsic SQL elements, 10
 - authentication, 198, 203, 210–211, 252
 - background, 195–196
 - Client-Server applications, 199–200
 - communicating with Sybase, 203
 - configuration security, 246, 250–252
 - connecting to other servers with, 236–237
 - creating arbitrary binary files, 225–226
 - cross-platform support, 198
 - defending against attacks, 226
 - deployment scenarios, 199–202
 - development environments, 201–202
 - disabling Java, 251
 - disabling Proxy Table support, 251
 - disabling xp_cmdshell, 251
 - enabling auditing, 250–251
 - enabling lockout, 248
 - enabling Proxy Table support, 224
 - extended stored procedures, 206–207, 218–219
 - external filesystem access, 224–226
 - extracting data using time delays, 222–223
 - FAQ page, 247
 - file layout, 205–206
 - firewall implications, 202–203
 - granting sa_role or sso_role to users, 243
 - history, 196
 - JSQL (Java in SQL), 196–197, 237–242
 - listing explicit permissions, 243–244
 - local privilege elevation issues, 12
 - login account basics, 204
 - man-in-the-middle attacks, 211

- Sybase ASE (Adaptive Server Enterprise) (*continued*)
 - manuals online, 246
 - Microsoft “ancestral” code and, 196, 211
 - older known security bugs, 226–228
 - open authentication protocols support, 198
 - OS security, 245–246, 247–248
 - packet filters, 247
 - passwords and password complexity, 204, 248–249
 - patches, 199, 202, 217
 - ports for services, 202
 - privilege elevation via SQL injection and, 12
 - privilege model, 203–204
 - querying external servers, 220–221
 - raw disk partitions support, 198
 - relative security of, 4–5
 - restricting filesystem access, 248
 - restricting Sybase directory access, 248
 - roles, 205, 243, 248
 - running in chroot jail, 248
 - running with low-privileged account, 247–248
 - scanning for servers, 209–210
 - security alerts published for, 4
 - security checklist, 245–246
 - security evaluations, 203–204
 - security information online, 246–247
 - service interaction, 206–207
 - starting new listeners, 207
 - Sybase ASA versus, 195
 - TDS communication protocol, 203
 - Transact-SQL interoperability, 196–197
 - Trojanning, 243–244
 - update page, 246
 - user security, 246, 248–249
 - variable declarations and buffer overflow, 10
 - version numbers, 195, 210–211, 217
 - version-grabbing tool, 228–233
 - web applications, 200–201
 - XML support, 197–198
- symlink vulnerability (PostgreSQL), 411–412
- SYS account (Oracle)
 - default password, 33, 48
 - obtaining password for, 69
- SYSADM authority (DB2), 120
- SYSCAT schema (DB2)
 - authorities information in, 120
 - DBAUTH view, 120–121
 - described, 109
 - ROUTINEAUTH view, 122
 - TABAUTH view, 121–122
- sysdatabases table (Informix), 160–161
- SYSFUN schema (DB2)
 - described, 109
 - limiting execute access for routines and, 136
 - PUBLIC authority and, 122
- SYSIBM schema (DB2)
 - described, 109
 - limiting execute access for routines and, 136
 - PUBLIC authority and, 122
- syslangauth table (Informix), 164, 180
- SYS.LINK\$ table (Oracle), 82, 93
- syslogins table, getting usernames from (Sybase), 214–215
- sysmaster database (Informix), 160–161
- SYSPROC schema (DB2), 109
- sysroutinelangs table (Informix), 164
- SYSTEM account password (Oracle), 33, 49
- system catalogs (PostgreSQL)
 - complete list of, 396–397
 - overview, 396
 - pg_class, 396, 397–398
 - pg_database, 396, 397
 - pg_group, 397, 399
 - pg_language, 397, 398, 400
 - pg_largeobject, 397, 398, 427–428
 - pg_proc, 397, 398, 400–401
 - pg_shadow, 397, 398, 399
 - pg_trigger, 397, 398

- SYSTEM function (Informix SPL), 181
 - System Monitor (SMON) process (Oracle), 26
 - system privileges (Oracle), 35–36
 - system tables, granting access to (Sybase), 243–244
 - SYS.USER\$ table (Oracle)
 - listing password hashes, 54–55, 57–58
 - listing usernames and password hashes, 55–56
 - passwords stored in, 33
 - sysusers database (Informix), 160, 163
 - sysusers table (Sybase), 204
 - sysutils database (Informix), 160
- T**
- TABAUTH view (DB2), 121–122
 - tables_priv table (MySQL), 270–271
 - Tabular Data Stream protocol. *See* TDS protocol
 - TCP Hijacking (PostgreSQL), 406, 407
 - TCP port scanner (Oracle), 83–84
 - TCP ports. *See* ports
 - TCP reverse proxy (Sybase), 241–242
 - TCP valid node checking for TNS
 - Listener (Oracle), 88–89
 - tcpdump packet capture software, 334
 - TDS (Tabular Data Stream) protocol
 - JSQL TDS client (Sybase), 238–241
 - open source version (FreeTDS), 203, 334
 - SQL Server, 333–334
 - Sybase, 203
 - testing, fuzzers for, 16
 - three-byte patch backdoor (SQL Server), 370–373
 - time delays
 - code for SQL injection harness, 437–440
 - extracting MySQL data, 288–289
 - extracting Sybase data, 222–223
 - SQL injection using (PostgreSQL), 422–423
 - SQL injection using (SQL Server), 364–365
 - TIME_ZONE session parameter
 - overflow (Oracle), 10
 - TNS (Transparent Network Substrate)
 - Listener (Oracle). *See also* extproc mechanism (Oracle)
 - Admin Restrictions, 88
 - attacking Oracle and, 40–49
 - buffer overflow vulnerabilities, 43
 - commands, 20
 - defined, 20
 - encrypting network traffic, 89
 - functions of, 20–21
 - Listener Control Utility (lsnrctl), 21–22, 40–42
 - log file poisoning via, 43–44
 - password error message, 41
 - password needed for, 9, 21, 43
 - PL/SQL and external procedures and, 21
 - ports, 20–21, 39, 40
 - remote administration dangers for, 21
 - reply to invalid TNS packet by, 22–23
 - security recommendations, 87–89
 - sending arbitrary packets over, 44–48
 - services information from, 41
 - setting password for, 87–88
 - status information from, 42
 - TCP valid node checking, 88–89
 - TNS protocol information online, 20
 - turning off external procedures, 89
 - turning off XML Database (XDB), 89
 - unauthenticated access to functionality and, 9
 - version information from, 40–41, 42
 - tnsnames.ora file (Oracle), 49
 - tools database (toolsdb) in DB2, 106
 - Transact-SQL (Sybase). *See also* JSQL with Sybase
 - audit evasion with sp_password, 220
 - interoperability, 196–197
 - mixing Java statements with, 237
 - name collisions with Java, 197
 - SQL injection using query batching, 215, 218
 - stored procedures, 206

- Transparent Network Substrate
 - Listener. *See* TNS Listener (Oracle)
 - triggers
 - PL/SQL injection and (Oracle), 68–71, 94
 - SQL Server, 346–347
 - Trojanning MySQL
 - adding administrative user, 298–300
 - cracking password hashes, 300–301
 - methods for achieving, 297
 - modifying existing user's privileges, 300
 - one-bit patch, 302–303
 - Trojan defined, 297
 - UDFs, 303
 - Trojanning SQL Server
 - extended stored procedures for, 342–343, 344–346
 - start-up procedure for, 373
 - Trojanning Sybase, 243–244
 - TZ environmental variable overflow (PostgreSQL), 412–413
- U**
- UDFs (User Defined Functions) in MySQL
 - adding to MySQL, 274
 - calling functions, 275
 - calling Windows ExitProcess function as, 275
 - CREATE FUNCTION mechanism for, 273
 - defined, 266
 - locking user's workstation with, 275
 - MyLUA, 303
 - MyPHP, 303
 - mysql.func table, 274–275
 - removing unused UDFs, 325
 - running external programs on Linux, 309–311
 - running external programs on Windows, 311–315
 - security issues, 273, 275–276
 - Trojanning using, 303
 - UDF library source code example, 273–274
 - W32.Spybot.IVQ worm or W32/Sdbot.worm.gen.j worm, 259, 309
 - UDP ports. *See* ports
 - UDP Resolution Service (SQL Server), Slammer worm and, 4, 6, 356
 - unauthenticated access to functionality, 9
 - unauthenticated flaws in network protocols, 6–7
 - UNION SELECT statements
 - lacking in MySQL prior to 4.0, 278
 - for SQL injection (MySQL), 284–285
 - for SQL injection (Oracle), 54–55
 - for SQL injection (PostgreSQL), 420–421
 - for SQL injection (Sybase), 216
 - Unix-based platforms. *See also* Linux platforms
 - Informix binaries with setuid bit set, 186
 - local attacks against Informix, 186–188, 191
 - Oracle on Windows versus, 26
 - OS accounts and default passwords (DB2), 110
 - PostgreSQL support for, 387–388
 - race conditions (MySQL), 304
 - Sybase file layout, 205–206
 - UPDATE statements, PL/SQL
 - injection using (Oracle), 60, 62
 - UPDATEAUTH authority (DB2), 122
 - UpdateExpert tool, 383
 - User Defined Functions. *See* UDFs in MySQL
 - user table (MySQL)
 - default users lacking in, 272
 - described, 266–268
 - host field, 268
 - password field, 268
 - purpose of, 266
 - restricting access to, 324

- system privilege values, 268–269
 - user field, 268
 - User-Defined Roles (SQL Server), 349
 - usernames (Informix)
 - buffer overflow issues, 174
 - extracting from shared memory dump, 178–180
 - stored in sysusers table, 163
 - usernames (MySQL)
 - access control system flaws, 276
 - adding administrative user, 298–300
 - default configuration, 258–259
 - modifying existing user's privileges, 300
 - plaintext storage by
 - WinMySQLAdmin tool, 258
 - usernames (Oracle)
 - default usernames and passwords, 447–468
 - listing usernames and password hashes, 55–56
 - usernames (PostgreSQL), token in
 - pg_hba.conf file, 393
 - usernames (SQL Server), brute-forcing, 339–340
 - usernames (Sybase), getting from
 - syslogins table, 214–215
 - UTL_FILE package (Oracle), 79–80
 - UTL_HTTP package (Oracle), 84
 - UTL_SMTP package (Oracle), 85
 - UTL_TCP package (Oracle), 82–84
- V**
- van der Meulen, Robert (MySQL issue discoverer), 8
 - VARBINARY literal (Sybase), 224
 - Venema, Wietse (“Improving the Security of Your Site by Breaking into It”), 16
 - version() function (PostgreSQL), 421–422
 - version information
 - getting from MySQL, 256–257, 280
 - getting from Oracle, 23–25, 40–41, 42
 - getting from PostgreSQL, 404–405
 - getting from Sybase, 210–211, 217, 228–233
 - usefulness for attacks, 41
 - @@version variable (Sybase), 217–218
 - “Violating Database-Enforced Security Mechanisms” (Anley, Chris), 370
 - vulnerability databases, 247, 280, 317, 320
 - VulnWatch mailing list, 320
- W**
- Waissbein, Ariel (hacker), 8
 - waitfor command, SQL injection using
 - SQL Server, 364–365
 - Sybase, 221–223
 - web application environment, 3.
 - See also SQL injection entries*
 - web applications (MySQL)
 - backend deployment, 257
 - running MySQL server on same host, 257
 - separate user for each application, 323
 - web applications (SQL Server), 368–369
 - web applications (Sybase)
 - backend deployment, 200
 - configuration problems, 201
 - Java Servlet example, 212–214
 - legacy systems and, 201
 - slave connections and credentials, 200
 - SQL injection and, 200, 212–215
 - trusted paths and, 200
 - using separate users for, 249
 - Web sites. *See* Internet resources
 - WindDbg debugger, 372
 - Windows Ident Server identd
 - daemon, 408
 - Windows platforms
 - calling ExitProcess function as UDF (MySQL), 275
 - DB2 on, 108–109

- Windows platforms (*continued*)
 - double pipe (| |) with Command Interpreter, 43
 - host-based firewalls, 202, 320
 - information leakage (PostgreSQL), 409
 - Informix dbaccess tool on, 160
 - Oracle on UNIX versus, 26
 - PostgreSQL hardening information, 434
 - PostgreSQL support for, 388
 - running external programs with MySQL UDFs, 311–315
 - running OS commands through DB2, 141
 - SQL Server confined to, 333
 - Sybase file layout, 205
 - version-grabbing tool for Sybase, 228–233
- Windows Server Controller tool (SQL Server), 336
- Windows Update (SQL Server), 383
- WinMySQLAdmin tool, 257–258
- WK_ACL.DELETE_ACLS_WITH_STATEMENT procedure (Oracle), 11
- WK_ACL.GET_ACL procedure (Oracle), 11
- WK_ACL.STORE_ACL procedure (Oracle), 11, 61–62
- WK_ADM.COMPLETE_ACL_SNAPSHOT procedure (Oracle), 11, 62
- WRITE_RAW function (Oracle), 83
- WRITE_TEXT function (Oracle), 83
- W32.Spybot.IVQ worm or W32/Sdbot.worm.gen.j worm, 259, 309
- X**
 - XDB (XML Database) of Oracle, turning off, 89
 - XML, Sybase support for, 197–198
 - XMLClobFromFile routine (DB2), 135, 136, 143
 - XMLFileFromClob routine (DB2), 136, 143
 - XMLFileFromVarchar routine (DB2), 136, 143
 - XMLVarcharFromFile routine (DB2), 135, 136, 143
 - XP Server process (Sybase), 206–207
 - xp_cmdshell procedure (SQL Server), 341, 344, 346, 362–363
 - xp_cmdshell procedure (Sybase), 218–219, 251
 - xp_execresultset procedure (SQL Server), 344
 - xp_freedll buffer overflow (Sybase), 227–228
 - xp_instanceregread procedure (SQL Server), 341
 - xp_instanceregwrite procedure (SQL Server), 341
 - xp_msver procedure Trojan (SQL Server), 344–345
 - xp_peakqueue procedure (SQL Server), 342
 - xp_readerrorlog procedure (SQL Server), 342
 - xp_regread procedure (SQL Server), 341
 - xp_regread procedure (Sybase), 219
 - xp_regwrite procedure (SQL Server), 341
 - xp_repl_help_connect procedure (SQL Server), 354
 - xstatus backdoor (SQL Server), 373
- Z**
 - 0x0A leading byte DoS (SQL Server), 357
 - 0x08 leading byte heap overflow (SQL Server), 356–357