

NUMBERS

- 0x* bytes after Data Flags, 18–19
- 0x044D0000 address, 8
- 0xDEADBEEF, 23
- 10g
 - file header for, 8–9
 - wrapping and unwrapping
 - PL/SQL on, 64
- 10g Application Server, obfuscation of passwords in, 55
- 10g Listener restrictions, bypassing, 32–33
- 403 Forbidden response, 119–120, 122, 126
- 404 File Not Found response, 127
- ' and ' (single quotes), relationship to SQL injection, 67, 70

SYMBOLS

- * (asterisk), significance in Java connections, 151
- : (colon), using with `concat()` function, 70

- @ (at) sign, querying database links with, 152
- || (double pipe) concatenate operator, 71

A

- AASH-AUTHORIA usernames, default passwords for, 153–155
- Accept packet, relationship to TNS header, 17
- `AcceptSecurityContext()` function, 57
- access control, implementing with privileges, 10–11
- ADA language, 60
- ADMIN_RESTRICTIONS option, addition to TNS Listener, 31–32
- Alert 68, 11–12
- ALL_DEPENDENCIES view, displaying called packages with, 66
- ALL_POLICIES view, 112
- ALTER SYSTEM, using to run OS commands, 136

ANO negotiation header, relationship to finding Oracle version number, 23

anonymous PL/SQL, executing block of, 72, 86

ARP, attacks aimed at, 49

asterisk (*), significance in Java connections, 151

at (@) sign, querying database links with, 152

Aurora GIOP server, vulnerability of, 33–38

AUTH_PASSWORD, 47–48

AUTH_SESSKEY, 46–47

authentication process, 43–48

- buffer overflow flaw in, 55
- creating secret number in, 46

AUTHID CURRENT_USER, setting functions to, 71

AUTONOMOUS_TRANSACTION pragma, specifying, 71

B

B2B-BUYMTCH usernames, default passwords for, 155–156

background process, 2

binary files, accessing, 140–142

bind variable, relationship to SQL injection, 68

brute force login attempts, defeating, 55

buffer overflows

- in authentication process, 55
- occurrence with TNS Listener, 32

bug numbers, obtaining list of, 12

bytes

- after Data Flags, 18–19
- in TNS header, 16–17

C

CALC package

- locating, 118
- source for, 117

CAMRON-CZ usernames, default passwords for, 156–158

CELLSPRINT procedure, running arbitrary SELECT queries with, 122

channel method, NUSHU, 145

Checksum SHA function, calling in Checksum package, 54–55

cipher text, creating secret number with, 46–48

classes12.zip resource, 16

clear-text passwords, getting, 48–52, 53

clients, redirecting to connect to other TCP ports, 44–45

code samples, 122

- anonymous PL/SQL block injection, 72
- binary file access, 140–142
- CALC package, 117
- CELLSPRINT procedure, 122
- Checksum SHA function called in Checksum package, 54–55
- cipher text sent to server as AUTH_PASSWORD, 47–48
- clear-text password access, 49–52
- client sending server username in authentication, 45–46
- data exfiltration with DNS queries and UTL_INADDR package, 148
- data exfiltration with UTL_HTTP package, 147
- data exfiltration with UTL_TCP package, 146–147
- database link, 152

- database server converted to TCP port scanner, 150
- DBA privileges obtained from `CREATE ANY TRIGGER`, 100–102
- DBA privileges obtained from `CREATE ANY VIEW`, 102–104
- DBA privileges obtained from `EXECUTE ANY PRIVILEGE`, 105
- `DBMS_CDC_IMPDP` exploit, 82–84
- `DBMS_CDC_SUBSCRIBE` and `DBMS_CDC_ISUBSCRIBE` exploits, 84–89
- `DBMS_EXPORT_EXTENSION` package and PL/SQL injection, 72–74
- `DBMS_RLS` package privileges, 107–108
- directory traversal attack, 132
- file system access using Java, 139
- file system accessed using `UTL_FILE` package, 138
- function injection, 71
- `GET_ENV` procedure, 142–143
- GIOP server vulnerability, 33–38
- invoker rights execution privilege, 62–63
- invoker rights instead of definer rights, 63
- `MDSYS.SDO_CMT_CBK_TRIG` trigger exploit, 96
- `MDSYS.SDO_GEOM_TRIG_INS1` trigger exploit, 93–94
- Oracle process opened by “Everyone” group, 3–7
- OS commands run directly with Job Scheduler, 134–136
- OS commands run through Java, 133
- OS commands run through PL/SQL, 131–132
- OS commands run using `ALTER SYSTEM`, 136
- OS commands run with `DBMS_SCHEDULER`, 134
- packet dump of connection, 43–44
- password logging, 53–54
- PL/SQL execution privileges, 61
- PL/SQL Gateway communication with database server, 121
- PL/SQL Gateway verification with HTTP Server response header, 119
- PL/SQL injection in `SELECT` statements, 68–70
- PL/SQL race conditions, 78–80
- PL/SQL wrapping, 65–66
- redirecting clients to TCP ports, 44–45
- `SDO_GEOM_TRIG_INS1` trigger exploit, 93–94
- `SECRET` orders accessed for VPD, 109
- SQL injection, 67
- SQL injection flaw in `XDB_PITRIG_PKG`, 111
- `SYS.CDC_DROP_CTABLE_BEFORE` trigger exploit, 97
- table for use as VPD, 108–109
- URL class enabling connection to web servers, 151–152
- version number access, 24–30
- VPD (virtual private database), 108
- VPDs defeated with raw file access, 112–114
- XDB (XML database) vulnerability, 33–38

colon (:), using with `concat ()` function, 70

`comps.xml` file, incorrect information in, 12

`concat ()` function, relationship to SQL injection, 70

connection, packet dump of, 43–44

control files, contents of, 9

CORBA applications, accessing, 33

CPU (critical patch update), release of, 12

`CREATE ANY TRIGGER`, getting DBA privilege from, 99–102

`CREATE ANY VIEW`, getting DBA privilege from, 102–104

`CREATE PROCEDURE`, getting DBA privilege from, 105

`CREATE_SUBSCRIPTION` procedure, vulnerability of, 87

`CREATERLSPOLICY` procedure, 114

critical patch update (CPU), release of, 12

crypto aspects, attacks against, 48–52

cursors, examining for SQL injection, 81

D

DACL (Discretionary Access Control List), relationship to Oracle process, 7–8

data

- encrypting prior to exfiltrating, 149
- selecting based on condition, 61–62
- storage in tablespaces, 8

data blocks in file system, block numbers in, 9

data exfiltration

- with DNS queries and `UTL_INADDR` package, 147–149
- overview, 145–146
- with `UTL_HTTP` package, 147
- with `UTL_TCP` package, 146–147

Data Flags, relationship to Data packets, 18

Data packets, 18

- bug associated with, 18

data type representation exchange, indicating for packets, 18

database links, 152

database objects

- listing, 10
- support for, 10

database server. *See also* servers communication with PL/SQL Gateway, 120–121

- converting to TCP port scanner, 150–151

database triggers, 91. *See also* SQL injection

- creating in DBA schema, 100
- creating on `MYTABLE`, 91–93
- executing `INSERT` statement with, 93
- `MDSYS.SDO_CMT_CBK_TRIG`, 94–96
- `MDSYS.SDO_DROP_USER_BEFORE`, 97–98
- `MDSYS.SDO_GEOM_TRIG_INS1`, 93–94
- `SDO_GEOM_TRIG_INS1`, 93–94
- `SYS.CDC_DROP_CTABLE_BEFORE`, 96–97
- vulnerability of, 93

DAVIDMORGAN-DVP1 user-names, default passwords for, 158–160

- DBA privileges. *See also* privileges
 - getting from CREATE ANY TRIGGER, 99–102
 - getting from CREATE ANY VIEW, 102–104
 - getting from CREATE PROCEDURE, 105
 - getting from EXECUTE ANY PROCEDURE, 105
 - DBA_DEPENDENCIES table, querying, 75–77
 - DBAs, creating triggers in schema for, 100
 - .dbf file extension, 8
 - DBMS_ASSERT package, validating user input with, 81–82
 - DBMS_ASSERT.QUALIFIED_SQL_NAME function, 103
 - DBMS_CDC_IMPDP, exploiting, 82–84
 - DBMS_CDC_ISUBSCRIBE, exploiting, 84–89
 - DBMS_CDC_SUBSCRIBE, exploiting, 84–89
 - DBMS_CRYPTO package, 149
 - DBMS_EXPORT_EXTENSION package, flaws in, 72–73, 75–77
 - DBMS_FGA package, creating VPDs with, 107–108
 - DBMS_JAVA.GRANT_PERMISSION, 139
 - DBMS_OBFUSCATION_TOOLKIT package, 149
 - DBMS_RLS package, creating VPDs with, 107–108
 - DBMS_SCHEDULER, running OS commands with, 133–134
 - DBMS_SQL calls, examining for SQL injection, 80–81
 - DBMS_SYS_SQL calls, examining for SQL injection, 81
 - DBSNMP default password, 52, 54
 - DDL statements, executing arbitrarily, 128
 - DEFINER procedure, obtaining details about, 63
 - definer rights execution privilege, 60. *See also* privileges
 - strength and weakness of, 62
 - using invoker rights instead of, 63
 - DES key scheduling, performing with `kzsrenp()` function, 47
 - DIANA, design objectives of, 64–65
 - directory traversal attack, 132
 - Discretionary Access Control List (DACL), relationship to Oracle process, 7–8
 - DML statements, executing arbitrarily, 128
 - DNS queries and UTL_INADDR package, exfiltrating data with, 147–149
 - double pipe (`| |`) concatenate operator, 71
- E**
- EAA-EXS4 usernames, default passwords for, 160–161
 - emoms file, contents of, 53
 - encryption, implementing prior to exfiltration, 149
 - environment variables, returning values of, 142–143
 - errors
 - ORA-01756, 67
 - ORA-31007, 111
 - PLS-00103, 125

“Everyone” group, security flaw related to, 2–7

EXECUTE ANY PROCEDURE, getting DBA privilege from, 105

EXECUTE ANY system privileges, examples of, 11

execute immediate :1, executing arbitrary SQL with, 128

EXECUTE IMMEDIATE calls, examining for SQL injection, 80

execution privileges in PL/SQL, types of, 60–63. *See also* privileges

EXEMPT ACCESS POLICY system privilege, 114

exfiltrating data
with DNS queries and UTL_INADDR package, 147–149

overview, 145–146

with UTL_HTTP package, 147

with UTL_TCP package, 146–147

EXPACT\$ table, inserting into, 76

exploit, running relative to Oracle process, 8

EXTEND_WINDOW_LIST function, vulnerability of, 87

extjob external process, implementing Job Scheduler with, 134–136

EXTPROC, requesting access to, 132

extproc program, 2

F

FA-FVP1 usernames, default passwords for, 161

Figures
calling out from PL/SQL to C functions or Java methods, 60

DBA privileges granted, 104

hash fed into Oracle password cracker, 96

Oracle PL/SQL Gateway, 115

OSI networking model, 16

file header for Oracle 10g, description of, 8–9

file system
accessing with Java, 139–140

accessing with UTL_FILE package, 137–138

overview, 8–9

file types, control files and redo logs, 9

FINDRICSET procedure in LT package, vulnerability of, 84

flaws, investigating, 74–77

functions, injecting into SQL, 71–72

G

GALLEN-GUEST usernames, default passwords for, 161–163

gateway. *See* Oracle PL/SQL Gateway

General Inter-Orb Protocol (GIOP), relationship to IIOP, 33

GET_DOMAIN_INDEX_METADATA function, problem with, 73

GET_ENV procedure, 142–143

GIOP (General Inter-Orb Protocol), relationship to IIOP, 33

GIOP server, vulnerability in, 33–38

H

hashes, feeding into Oracle password cracker, 95–96

HCC-HXT usernames, default passwords for, 163

hostnames, looking up, 147–149
 HTTP Server response header, verifying PL/SQL Gateway with, 118–120

I

IA-ITG usernames, default passwords for, 163–164
 IIOP (Internet Inter-Orb Protocol) server, installation of, 33
 init<SID>.ora file, location of, 9
 INSERT statement, executing with trigger, 93
 Internet Inter-Orb Protocol (IIOP) server, installation of, 33
 INVOKER procedure, obtaining details about, 63
 invoker rights execution privilege, 60. *See also* privileges
 example, 62–63
 using instead of definer rights, 63
 IP addresses, looking up, 147–149

J

JA-JUSTOSHUM usernames, default passwords for, 164–165
 Java
 accessing file system with, 139–140
 connecting to networks with, 151–152
 running OS commands through, 132–133
 java.net.SocketPermission, 151
 Job Scheduler, running OS commands directly with, 134–136

K

KELLYJONES-KPN usernames, default passwords for, 165
 kzsrddec() function, getting clear-text passwords with, 49–52
 kzsrddep() function, getting clear-text passwords with, 49–52
 kzsrenc() function, using with secret number, 46–47

L

LADAMS-LSA usernames, default passwords for, 165
 libc, registering to run OS commands through PL/SQL, 131–132
 libraries, restricting location of external libraries, 132
 Linux
 exploit techniques on, 56–57
 exploiting UNLOCK overflow running on, 33–38
 LIST_LIBRARIES procedure, using | | concatenate operator with, 71
 Listener. *See* TNS Listener
 lncupw() function, creating copy of password hask with, 47
 LOCAL SYSTEM, running commands as, 134–136
 log files, examining, 9
 LT package, exploiting, 84
 LZ_COMPRESS function, 149

M

MDDATA-MWA usernames, default passwords for, 165–166
 MDSYS SDO_CMT_CBK_TRIG trigger, exploiting, 94–96

MDSYS.SDO_DROP_USER_
 BEFORE trigger
 execution of, 100
 exploiting, 97–98
MDSYS.SDO_GEOM_TRIG_INS1
 trigger, exploiting, 93–94
msvcrt.dll, registering to run
 OS commands through
 PL/SQL, 131–132
MYTABLE, creating for use with
 trigger, 91–93
MYTABLE_LONG, creating for use
 with trigger, 91–93

N

named pipes
 accessing, 9
 orcljsex<SID>, 134
 relationship to Oracle process, 7
NEILKATSU username, default
 password for, 166
Net8/Net9, 15
NGSSQuirreL program, determin-
 ing server vulnerability with,
 12–13
*nix platforms, background
 processes on, 2
NTLM SSPI AcceptSecurity-
 Context() function, 57
NULL, verifying PL/SQL Gateway
 with, 119
NUSHU channel method, 145

O

OBJ7333-OZS usernames, default
 passwords for, 166–168
object privileges, examples of,
 10–11. *See also* privileges

opatch utility, installing Oracle
 patches with, 12
ORA-01756 error, 67
ORA-31007 error, preventing rela-
 tive to VPD, 111
Oracle
 configuring to listen on TCP
 sockets, 9
 installation on Windows XP, 57
Oracle 9i and earlier, wrapping
 and unwrapping PL/SQL on,
 64–66
Oracle 10g
 file header for, 8–9
 wrapping and unwrapping
 PL/SQL on, 64
Oracle database server, converting
 to TCP port scanner, 150–151
Oracle datafiles, accessing directly,
 141–142
Oracle Home directory, 8
Oracle password cracker, feeding
 hash into, 95–96
Oracle PL/SQL Gateway, 115
 attacking, 122–129
 communication with database
 server, 120–121
 and Oracle Portal application, 118
 URLs for, 116–118
 verifying existence of, 118–121
 weakness of, 118
Oracle Portal application, 118
Oracle process, security flaw
 related to, 2–7
Oracle servers, connecting with
 database links, 152
Oracle version number
 obtaining with TNS error text, 22
 obtaining with TNS protocol,
 20–21

- obtaining with TNS version TTC function, 23
 - obtaining with `version` and `status` commands, 20
 - obtaining with XML databases, 21–22
 - `$ORACLE_HOME` environment variable, 8
 - `oracle.exe` process, 2
 - `ORAEXEC` procedure, 132
 - `orcljsex<SID>` named pipe, 134
 - OS commands
 - running directly with Job Scheduler, 134–136
 - running through Java, 132–133
 - running through PL/SQL, 131–132
 - running using `ALTER SYSTEM`, 136
 - running using
 - `DBMS_SCHEDULER`, 133–134
 - OS environment variables, returning values of, 142–143
 - OSI networking model, 16
 - `owa_util`, gaining access to, 128
 - `OWA_UTIL.SIGNATURE`, requesting for PL/SQL Gateway, 119–120
- P**
- packages, scheduling execution of, 133–134
 - packet dump of connection, 43–44
 - packet type, indicating in TNS header, 16–17
 - packets, WORDs in, 18
 - PA-PY9 usernames, default passwords for, 168–171
 - password cracker, feeding hash into, 95–96
 - password hashes
 - creating copy of, 47
 - gaining access to, 70
 - passwords
 - defaults for, 52–55
 - defaults for usernames, 153–176
 - logging, 53–54
 - looking in files for, 53–55
 - obfuscation in 10g Application Server, 55
 - vulnerability of, 9
 - patchset, release of, 11–13
 - PL (Procedural Language), 59
 - PLS-00103 error, 125
 - PL/SQL
 - encrypting, 64–66
 - execution privileges, 60–63
 - overview, 59–60
 - running OS commands through, 131–132
 - working without source, 66
 - wrapping and unwrapping, 64–66
 - PL/SQL code
 - auditing for SQL injection vulnerabilities, 80–81
 - checksumming, 12
 - PL/SQL Gateway. *See* Oracle PL/SQL Gateway
 - PL/SQL injection
 - into anonymous PL/SQL blocks, 72
 - of functions, 71–72
 - overview, 66–68
 - into `SELECT` statements to get more data, 68–70

PL/SQL objects, vulnerability to
 race conditions, 77–80

PL/SQL package, conceptualizing,
 117

PL/SQL procedures
 executing, 120
 gaining access to, 122

PLSQLExclusionList, bypassing,
 122–129

policies
 dropping, 107–112
 getting names of, 112

postDBCreation.log file, log-
 ging password in, 53

predicate, setting up for VPD,
 109–110

PREPARE_UNBOUNDED_VIEW pro-
 cedure, vulnerability of, 89

privileges, 114
See also DBA privileges
See also execution privileges in
 PL/SQL
See also invoker rights execution
 privilege
See also object privileges
See also SYS privileges
 determining, 11
 implementing access control
 with, 10–11

processes
 security flaw related to, 2–7
 types of, 2

protocol negotiation, indicating for
 packets, 18

PUBLIC
 assigning to execute privilege on
 procedure, 61–62
 granting EXECUTE permission
 to, 61

Q

QA-QS_WS usernames, default
 passwords for, 171–172

queries
 escaping from, 67
 modifying, 68

R

race conditions, vulnerability of
 PL/SQL objects to, 77–80

Redirect packet, relationship to
 TNS header, 17

redo logs, contents of, 9

Refuse packets, relationship to
 TNS header, 17–18

RENE-RWA1 usernames, default
 passwords for, 172

RLMGR_TRUNCATE_MAINT trigger,
 execution of, 79–80

RLS policies, manipulating, 108

S

SALLYH-SYSTEM usernames,
 default passwords for, 172–174

scheduling. *See*
 DBMS_SCHEDULER; Job
 Scheduler

schema
 creating trigger in, 100
 definition of, 10

SDO_GEOM_TRIG_INS1 trigger,
 exploiting, 93–94

second-order SQL injection, 82, 88

SECRECY policy
 dropping from VPDTESTTABLE,
 111
 enforcing for VPD, 110

secret number, creating in authen-
 tication process, 46–47

- SECRET orders, accessing for VPD, 109, 111
- SELECT queries, running arbitrarily, 122
- SELECT statements, injecting into, 68–70
- server process, 2
- servers. *See also* database server; web servers
- connecting with database links, 152
- determining vulnerability of, 12–13
- sending usernames to in authentication, 45–46
- TCP port associated with, 9
- SGA (System Global Area), relationship to processes, 2
- shadow process, 2
- shared pool, contents of, 2
- shell scripts, scheduling execution of, 133–134
- SID (System Identifier), 1
- in `$ORACLE_HOME` directory, 8
- single quotes (' and '), relationship to SQL injection, 67, 70
- sleeping thread, reactivating relative to Oracle process, 8
- `slgdt()` function, calling to create secret number, 46
- `spfile<SID>.ora` file, location of, 9
- SQL
- executing arbitrarily, 68, 87, 128
- executing directly, 77
- SQL injection, 66–67. *See also* triggers
- flaw in `XDB_PITRIG_PKG`, 110–111
- of functions, 71–72
- second-order injection, 82, 88
- vulnerability to, 69–70
- statements, executing SQL arbitrarily with, 68
- status command, obtaining Oracle version number with, 20
- SUBSCRIBE procedure, vulnerability of, 86
- SYS, recovering password for, 54
- SYS privileges, gaining, 76–77. *See also* privileges
- SYS user, importance of, 10
- `SYS.CDC_DROP_CTABLE_BEFORE` trigger, exploiting, 96–97
- SYSMAN
- password for, 53
- recovering password for, 54
- SYSTEM, recovering password for, 54
- `system()` function, calling to run OS commands through PL/SQL, 131–132
- System Global Area (SGA), relationship to processes, 2
- System Identifier (SID), 1
- in `$ORACLE_HOME` directory, 8
- system privileges, obtaining list of, 11
- SYSTEM user, importance of, 10
- T**
- TABACT function, relationship to `DBMS_EXPORT_EXTENSION` package, 75
- tables, setting up for use as VPD, 108–109
- tablespaces, storage of data in, 8
- TCP port 2100, obtaining version information with, 21–22

- TCP port scanner, converting Oracle database server into, 150–151
 - TCP ports
 - creating outbound connections on, 146–147
 - redirecting clients to, 44–45
 - TCP sockets, configuring Oracle to listen on, 9
 - TDEMARCO-TWILLIAMS usernames, default passwords for, 174–175
 - TESTPRIV table, creating, 61
 - threads, relationship to Oracle process, 7
 - TNS (Transparent Network Substrate) protocol, task of, 15
 - TNS header, 16–18
 - TNS Listener, 17
 - attacking, 31–33
 - buffer overflows associated with, 32
 - connecting to, 33
 - description of, 2
 - role in processes, 2
 - vulnerability related to GIOP server, 33
 - TNS protocol, 19
 - obtaining Oracle version with, 20–21
 - tnsver.c, obtaining Oracle version number with, 24–30
 - TOCTOU race condition, vulnerability of PL/SQL objects to, 77–80
 - Transparent Network Substrate (TNS) protocol, task of, 15
 - transport protocols, support for, 15
 - triggers, 91. *See also* SQL injection
 - creating in DBA schema, 100
 - creating on MYTABLE, 91–93
 - executing INSERT statement with, 93
 - MDSYS.SDO_CMT_CBK_TRIG, 94–96
 - MDSYS.SDO_DROP_USER_BEFORE, 97–98
 - MDSYS.SDO_GEOM_TRIG_INS1, 93–94
 - SDO_GEOM_TRIG_INS1, 93–94
 - SYS.CDC_DROP_CTABLE_BEFORE, 96–97
 - vulnerability of, 93
 - TTC (Two-Task Common), 15
 - TTI (Two-Task Interface) function call, indicating for packets, 18–19
 - TYPE_SCHEMA, checking validity of, 73–74
- ## U
- UDDISYS username, default password for, 175
 - UNION SELECT statement, injecting, 69–70
 - UNLOCK overflow, exploiting on XDB, 33–38
 - URL class, connecting to web servers with, 151–152
 - URLs, recognizing for PL/SQL web applications, 116–118
 - user input, validating with DBMS_ASSERT package, 81–82
 - usernames
 - default passwords for, 153–176
 - defaults for, 52–55
 - sending to server in authentication, 45–46
 - users
 - authentication of, 10
 - determining privileges of, 11

UTL_ENCODE package, 149
 UTL_FILE package, using to
 access file system, 137–138
 UTL_HTTP package, exfiltrating
 data with, 147
 UTL_INADDR package and DNS
 queries, exfiltrating data with,
 147–149
 UTL_TCP, connecting to TNS Lis-
 tener with, 33
 UTL_TCP package, exfiltrating
 data with, 146–147, 149–151

V

VALIDATE_IMPORT procedure,
 vulnerability of, 83
 VALIDATE_STMT procedure, flaw
 related to, 77
 VEA-VP6 usernames, default pass-
 words for, 175
 version command, obtaining
 Oracle version number with, 20
 version information
 obtaining with TNS error text, 22
 obtaining with TNS protocol,
 20–21
 obtaining with TNS version TTC
 function, 23
 obtaining with version and
 status commands, 20
 obtaining with XML databases,
 21–22
 VPDs (virtual private databases)
 creating, 107–110
 defeating with raw file access,
 112–114
 VSNNUM, converting decimal num-
 ber in, 22
 VTEST.VPROC procedure, inject-
 ing into, 103–104

W

WAA1-WSM usernames, default
 passwords for, 175–176
 web resources
 exploit techniques on Linux ver-
 sus Windows, 57
 local execution of commands, 32
 unwrapping PL/SQL, 65
 web servers. *See also* servers
 making out-of-band requests to,
 147
 using URL class for connection
 to, 151–152
 where clause, setting up for VPD,
 109–110
 whoami, running relative to Oracle
 process, 8
 Windows
 background processes on, 2
 exploit techniques on, 56–57
 Windows XP, installation of Oracle
 on, 57
 WORD bytes in TNS header, 16–17
 WORD in TNS connect packet,
 specifying Oracle version with,
 20–21

X

X_INSIDE, executing, 63
 XDB (XML database), vulnerability
 of, 33–38
 XDB_PITRIG_PKG package, SQL
 injection flaw in, 110–111
 XDB-XTR usernames, default pass-
 words for, 176
 XML database
 obtaining Oracle version number
 with, 21–22
 overflows in, 55

Y

YCAMPOS-YSANCHEZ user-
names, default passwords for,
176

Z

ZFA-ZSA usernames, default pass-
words for, 176

