

Index

COPYRIGHTED MATERIAL

Index

Symbols and Numerics

%00 (null-byte), 138–139
../ (path traversal), 139–140
| (pipe character), 138
<? (script tag), 137–138
%20 (white space), 138
404Print tool, 213, 334

A

A1 – Unvalidated Input, 136–140
A2 – Broken Access Control, 141
A3 – Broken Authentication and Session Management
 authentication, 142–146
 session, 146–154
A4 – Cross-Site Scripting Flaws
 cross-site tracing, 157–158
 overview of, 154–157
A5 – Buffer Overflows
 format string bugs, 160–162
 overview of, 158–160
 shellcode injections, 162–163
A6 – Injection Flaws
 LDAP injection, 163–165
 OS Commanding, 165
 SQL injection, 166–173
 SSI injection, 173
 XPath injection, 173–174
 XXE, 174–175

A7 – Improper Error Handling, 175–176
A8 – Insecure Storage, 176–178
A9 – Denial of Service, 178–180
A10 – Insecure Configuration Management, 181–182
Absinthe, 247–248
Abuse of Functionality, 184–185
access control, broken, 141
accounts, segregating, 438
Active Filter Detection, 81–82
Active Server Pages (ASP), 40–41
ActiveX
 client-side attack and, 271
 description of, 41
 Web server and, 211
administrative Web management, 197
Advanced Package Tool, 457
AES algorithm, 442–443
AJAX (Asynchronous JavaScript and XML), 270, 397–398
ALTER statement (SQL), 475
amap, 97–100
American Registry for Internet Numbers (ARIN), 76–77
analysis in executive summary, 407
analyzing
 error page, 104–106
 threat, 188–189
 Web services, 371–373
ancestor (XML), 485

anti-automation, insufficient, 185

Apache

Axis, 129

HTTPD Web server, threats to, 204–208

applet (Java), 40

application. See also Web application

decomposing and understanding, 187–188

development considerations, 2

honeypot, 458–463

application aspects of Web applications

dynamic technologies, 37–41

state, 35–37

Web-based authentication, 41–42

application fingerprinting

analyze error pages, 104–106

database identification, 102–104

file type probes, 106–107

HTML source sifting, 116–118

overview of, 93–94

port mapping, 94–97

resource enumeration, 107–116

service identification, 97–103

application proxy, 398

application state, 36

Application Vulnerability Description Language (AVDL), 417

AppScan, 306–309

architectural aspects of Web applications

HTTP protocol, 21–25

HTTP proxy, 25–28

overview of, 15–19

SSL/TLS, 28–35

tiers, 19–20

archived data, 177–178

ARIN (American Registry for Internet Numbers), 76–77

ASP (Active Server Pages), 40–41

ASP.NET, 40–41, 440–442

asset, 187

asymmetric key-based algorithm, 45

Asynchronous JavaScript and XML (AJAX), 270, 397–398

Atom, 271

atomic value (XML), 484

attack on system and Web server, 197–201

attack simulation

approval for, 220

golden rule of, 219–220

objectives of, 219

audience, presenting findings to, 423

auditing code, 445–446

auditor, interfacing with, 417

authentication

attacks against

credential discovery, 249–250

overview of, 248–249

password data, 263–266

attacks against mechanism

brute force, 251–259

dictionary, 259–263

infrastructure attack and, 363

insufficient, 183

SSL, TLS, and, 29

Web-based, 41–42

authentication management, broken

HTML form-based, 144–146

HTTP

Basic authentication, 142–143

Digest authentication, 143–144

authorization, infrastructure attack and, 363

automated testing

multi-purpose scanners

Jikto, 302

Nessus, 303–306

ntoinsight, 302–303

Wikto, 294–302

overview of, 273

proxy servers

Paros, 274–280

SPIKE Proxy, 280–285

scanners

E-Or, 289–293

Nikto, 286–289

overview of, 285–286

WSDigger, 390

WSFuzzer, 391–392

wsKnight/WSAudit, 388–390

AVDL (Application Vulnerability Description Language), 417

Axis (Apache), 129

B**Base64 encoding, 48–51****Basic authentication, 41–42****BEA WebLogic, 130–131****best practices**

document section about, 413–416

remediation

input validation, 432–442

session management, 442–445

BiDiBLAH, 311–312**blackbox test, 133****Bochs, 454****BOU tool, 266–267****bound parameter, 437–438****brute force attack**

against authentication mechanism

Brutus AET2, 253–255

Crowbar, 256–259

ObiWaN, 251–253

overview of, 251

Domino-based WebMail application example and, 326

Session ID and, 147

types of, 145–146

brute-force cracking, 44, 145**Brutus AET2, 253–255****buffer overflow**

attack strings, 498

format string bugs, 160–162

ISAPI, 210

overview of, 158–160

printer, 208–209

shellcode injections, 162–163

testing using BOU, 266–267

XML content attack and, 360

Business Logic Tier, 20**C****CA (Certification Authority), 32, 201, 267****cache poisoning, 203–204****caching system, 177****CANVAS (Immunity), 355–356****categorizing threat, 189–190****CDATA attack, 381–382****CERT (Computer Emergency Readiness Team), 351****Certificate Signing Request (CSR), 30–32****certificate verification, 33****Certification Authority (CA), 32, 201, 267****CGI, 37****CGI checking and Wikto, 300–302****chained SSL certificates, 33****checklist, 220–221****children (XML), 484****chunked encoding overflow, 205****cipher strength identification, 201****client-side attack**

active content, 270–271

cookies, 271–272

example of, 272–273

overview of, 268

XSS, 268–269

client-side session management, 36**code audit, 445–446****coercive parsing, 360****ColdFusion MX (Macromedia), 41****command execution attack, 198****Common Vulnerabilities and Exposures (CVE)****project, 352****compliance issues and documentation, 417–422****Compliance Group, The Guard, 419, 422****Computer Emergency Readiness Team (CERT), 351****configuration management, insecure, 181–182****consent, obtaining, 12****content, default, on Web server, 197****content harvesting, 119****content spoofing, 183****cookie**

client-side attack and, 271–272

description of, 36

managing state via, 150

cookie poisoning attack, 272**cookie-based load balancing, 83****Core Impact, 356****crawling, 107–110****CREATE statement (SQL), 475****creativity, importance of, 6–7****credential discovery attack, 249–250****Critical level, 408****cross-site scripting (XSS) attack, 154–157, 268–269, 435**

cross-site tracing (XST), 157–158

Crowbar, 256–259

cryptanalysis, 44

CSR (Certificate Signing Request), 30–32

custom scripts, 234

CVE (Common Vulnerabilities and Exposures) project, 352

D

data. See also data aspects of Web applications

attacking, 145–146

manual manipulation of, 184–185

Data Access Tier, 20

data aspects of Web applications

encryption and encoding, 42–51

XML, 51–55

data encryption, 43–45

data flow diagram (DFD), 187, 188

Data Tier, 19–20

data type attack strings, 495

database and DoS attack, 180

database identification, 103–104

database technology and state management, 37

decoding, Base64, 50–51

defense strategy, 5

DELETE statement (SQL), 474

Demilitarized Zone (DMZ), 20, 21

Denial of Service (DoS) attack

GET, 207

long HTTP header, 206–207

malformed HTTP request, 209–210

overview of, 178–180

susceptibility to, 197

Web services and, 363

WebDAV XML, 210

XML, 382–383

descendant (XML), 485

DFD (data flow diagram), 187, 188

DHTML (Dynamic HTML), 37

dictionary attack

data generation, 259–262

description of, 145

THC-Hydra, 263

dig utility, 27

DigDug, 75–76

Digest authentication, 41

digging deep within self, 7

directory traversal attack, 211

Discovery of Web services (DISCO), 125–127

Discovery phase

application fingerprinting

analyze error pages, 104–106

database identification, 102–104

file type probes, 106–107

HTML source sifting, 116–118

overview of, 93–94

port mapping, 94–97

resource enumeration, 107–116

service identification, 97–103

information harvesting

content, 119

e-mail addresses, 122

Google, 119–122

job postings, 123–124

overview of, 118–119

search engines, 119

Web statistics, 122–123

logistics

ARIN, 76–77

DNS, 75–76

filter detection, 80–84

SamSpade, 77–80

WHOIS, 72–74

OS fingerprinting

DMitry, 87–89

Netcraft, 85–86

pOf, 86–87

overview of, 71–72

Web server fingerprinting

HTTP headers, 89–92

httpprint, 92–93

Web services

J2EE, 128–131

overview of, 124–125

UDDI and DISCO, 125–127

WSIL, 127–128

Distributed Logic Tier, 20

DMitry, 87–89

DMZ (Demilitarized Zone), 20, 21

dnscan script, 213–214

DNS, 75–76

DNS Round-Robin load distribution, 27**Document Type Definition (DTD), 52, 54****documentation**

- best practices section, 413–416
- compliance factors, 417–422
- executive summary, 406–407
- final summary, 416
- overview of, 401
- reproducing work and, 317
- results verification, 402–406
- risk matrix, 408–413
- rolling, 9
- security of, 416–417
- structure of, 406
- Web services and, 392–394

Domino-based WebMail application, as target, 317–326**DoS. See Denial of Service attack****DREAD model, 190****DROP statement (SQL), 475****DTD (Document Type Definition), 52, 54****Dynamic HTML (DHTML), 37****dynamic server-side technology**

- ActiveX, 41
- ASP/ASPnet, 40–41
- CGI, 37
- ColdFusion MX, 41
- DHTML, 37
- Java, 39–40
- overview of, 37
- Perl, 39
- PHP, 38–39
- Python, 39
- Ruby, 39
- SSI, 38
- XHTML, 38
- XML, 37

E**Eclipse Web Services Explorer, 127****edge security models, limitations of, 2****edge-level protection**

- description of, 425
- Web Application Firewalls, 426–430
- Web services, 430–432

eEye, 351**e-mail address**

- HTML source sifting and, 117–118
- information harvesting and, 122

encoding

- Base64, 48–51
- description of, 42
- SOAP, 61
- URL, 45–48

encryption

- AES algorithm, 442–443
- data-level, 43–45
- description of, 42
- free software packages, 416–417
- Lotus Domino and, 324–325
- one-way hashing, 42–43
- salted hashing, 51
- socket-level, 358
- SSL and TLS, 28–29
- WSS, 378–379

enumeration

- information, 363
- resource
 - approach 1 (crawling), 107–110
 - approach 2, 110–115
 - HTTrack, 115
 - wget, 115–116
- Web services and, 368–371

E-Or, 248, 289–293**error handling**

- best practices for, 415–416
- improper, 175–176
- XML content attack and, 361

error page, analyzing, 104–106**escape input characters, 436–437****ethereal, 465****executive summary, 406–407****expectations, setting, 13****experience and pen testing, 3****exploit research Web sites, 315–317****eXtensible Access Control Markup Language (XACML), 398****eXtensible Markup Language (XML)**

- attributes, 54
- Declaration, 53
- Document Type Definition, 52

eXtensible Markup Language (XML) (continued)

- namespace, 55–56
- overview of, 37, 51–52
- tags and elements, 53–54
- terminology, 483–485
- well-formed versus valid document, 54

external entity, 360

external test, 11

F

false positives, 402–406

file type probe, 106

filter detection

- Active Filter Detection, 81–82
- load balancing, 82–83
- Nmap, 80–81
- SSL/TLS, 84

fingerprinting. See application fingerprinting; OS fingerprinting; Web server fingerprinting

firewall and Web services, 358

FLWOR expression (XQuery), 491

footprinting of Web services, 364–368

format string bugs, 160–162

Foundstone SSLDigger, 201, 202

404Print tool, 213, 334

framework

- description of, 67–68
- for pen testing Web apps, 244–246

FrontPage extensions, 203

function (XQuery), 491

fuzzing, 373. See also injection attack dictionary

FuzzTest service, 368–369, 370, 371, 373

G

general attack strings, 495–498

global server load balancing, 28

goals of pen tester, 8

golden rule, 219–220

Google

- example of search results from, 318–320
- information harvesting and, 119–122
- phonebook: directive, 121

The Guard (Compliance Group), 419, 422

H

hacker, motivations for, 7

HackersCenter (HSC), 349–351

Hacme Bank/Hacme Books, 463

hardware for lab, 450

hardware load balancing, 28

hash data type, 235

hashencodes program (Shu), 46–48

header-based load balancing, 83

Health Insurance Portability and Accountability Act (HIPAA), 419–421

hidden field, 36, 149

high availability, 26

High level, 408

hijacking, of session, 146–147

honeypot application

- Hacme Bank/Hacme Books, 463
- WebGoat, 458–460
- WebMaven, 460–462

HSC (HackersCenter), 349–351

HTML source sifting

- application server imprints, 118
- client-side logic, 116–117
- e-mail addresses and user data, 117–118
- hidden HTML forms, 118
- HTML comments, 117
- hyperlinks, 118
- legacy code, 118

HTTP

- authentication and, 41
- Basic authentication, 142–143, 374
- Digest authentication, 143–144
- Log hyperlink, 393–394
- POST method, 24–25
- Proxy
 - load balancing, 26–27
 - overview of, 25–26
 - Reverse Proxy server, 26
- request smuggling, 200–201
- Requests and Responses, documenting, 317
- Response headers, 89–92
- Response Splitting, 198–200, 435
- as stateless, 35
- status codes, 22–23

structure of transactions, 21–22

verbs, 23–24, 196

HTTPD Web server (Apache), threats to, 204–208

httpprint, 92–93

HTTPS, 29

HTTrack, 115, 246–247

Hypertext Pre-processor (PHP), 38–39

I

IAM method, 193

IBM WebSphere, 130

identifying mitigation strategy, 190–193

IDS (Intrusion Detection System), 4

IIS (Internet Information Server)

as target, 326–338

threats to, 208–214

Immunity CANVAS, 355–356

Info level, 409

information enumeration, 363

information harvesting

content, 119

e-mail addresses, 122

Google, 119–122

job postings, 123–124

overview of, 118–119

search engines, 119

Web statistics, 122–123, 124

Information Leakage, 184

infrastructure attack, 362–364

injection attack, 360–361

injection attack dictionary

buffer overflows, 498

data type attack strings, 495

general attack strings, 495–498

LDAP injection, 502

meta-characters, 498–500

SQL injection, 500–502

XML content attack strings, 503

XPath injection, 502

XSS attack strings, 500

injection flaws

LDAP injection, 163–165

OS Commanding, 165

SQL injection, 166–173

SSI injection, 173

XPath injection, 173–174

XXE, 174–175

input, unvalidated, 136–140

input validation

attack on, 360–361

best practices for, 432–442

INSERT statement (SQL), 474

Insufficient Anti-Automation, 185

Insufficient Authentication, 183

Insufficient Process Validation, 185

integration models

overview of, 56

portals, 66–67

SOAP, 56–65

XML-RPC, 65–66

integrity services, 29

interfacing with auditor, 417

Internet Information Server (IIS)

as target, 326–338

threats to, 208–214

Intrusion Detection System (IDS), 4

Intrusion Prevention System (IPS), 4

item (XML), 484

J

Java

frameworks and, 68

overview of, 39–40

Stinger and, 439

Java Server Pages (JSP), 40

Java Web Service (JWS), 129

JBoss, 129–130

Jikto, 302

job postings, 123–124

J2EE, 128–131

JME specification, 70

Juno (Sorcerer), 198

K

knowledge and pen testing, 3, 7

known exploits

manual examples

Domino WebMail, 317–326

IIS, 326–338

known exploits (continued)

- MetaSploit, 338–347
- overview of, 315–317
- sources
 - CERT, 351
 - CVE, 352
 - eEye, 351
 - HSC, 349–351
 - OSVDB, 351
 - Secunia, 351
 - SecurityFocus, 347–349
- warning, 352–355

L

lab

- hardware for, 450
- importance of, 449
- software for
 - client tools, 451–452
 - honeypot applications, 458–463
 - server OS installations, 452–457
 - Web applications, 457–458, 465–468
 - Web services, 463–465
 - webAppHoneyPot, 468–469

Lcrack, 263–264, 325–326

LDAP injection

- attack strings, 502
- characters and, 435–436
- types of, 163–165

LDAP (Lightweight Directory Access Protocol)

- attributes, 478–479
- Base Search DN, 480
- entries, 478
- Filter, 481
- operations, 479–482
- overview of, 477
- Scope, 481–482
- structure of, 477–478

leakage, 44, 184

liability, 13

LibWhisker

- code, 239–244
- “crawl” library, 107
- Nikto and, 286

- overview of, 234–235
- using, 235–239

Lightweight Directory Access Protocol. See LDAP

Lingua::31337, 262

Linux

- Apache MySQL PHP/Perl/Python architecture, 16
- OS virtualization, 454–455

live data sources, 177

load balancing

- DNS Round-Robin load distribution, 27
- filter detection and, 82–83
- global server, 28
- hardware, 28
- overview of, 26–27
- software, 28

logistics

- ARIN, 76–77
- DNS, 75–76
- filter detection, 80–84
- SamSpade, 77–80
- WHOIS, 72–74

long-slash directory listing, 205–206

Lotus Domino-based WebMail application, as target, 317–326

Low level, 409

L33T Speak, 262

M

Macromedia ColdFusion MX, 41

Man-in-the-Middle attack, 363

manipulation of input

- meta-characters and, 137–140
- overview of, 136–137

manual testing

- authentication
 - brute force attacks, 251–259
 - credential discovery, 249–250
 - dictionary attacks, 259–263
 - overview of, 248–249
 - password data, attacks on, 263–266
- buffer overflow, 266–267
- CDATA attack, 381–382
- client-side attack
 - active content, 270–271
 - cookies, 271–272

- example of, 272–273
- overview of, 268
- XSS, 268–269
- custom scripts, LibWhisker, 234–244
- frameworks, 244–246
- proxy server, WebScarab, 222–234
- SQL injection
 - Absinthe, 247–248
 - mieliekoek, 246–247
 - other tools, 248
 - overview of, 380–381
- WebScarab, 386, 387
- WSDigger, 386, 387
- wsKnight/WSProxy, 384–385
- XML DoS attack, 382–383
- XML infection, 381
- XML parser overload, 384
- XML signature attack, 382
- XPath injection, 381
- MD5 online cracker, 265**
- mechanism, attacking, 145**
- Medium level, 409**
- meta-characters, 137–140, 434, 498–500**
- MetaSploit**
 - description of, 316, 338
 - exploit module, 339
 - modes of operation, 340
 - updating, 340–341
 - using, 341–347
- Microsoft**
 - Internet Information Server (IIS)
 - as target, 326–338
 - threats to, 208–214
 - Windows, 449, 457
- Midlet, 70**
- mieliekoek, 246–247**
- milw0rm site, 330–332, 333, 339, 340**
- mindset**
 - creativity and, 6–7
 - digging deep and, 7
 - overview of, 6
- mitigation strategy, identifying, 190–193**
- Model-View-Controller model and frameworks, 67–68**
- ModSecurity software, 426–428, 430–431**

- Monkey Shell, 463–464**
- multi-purpose scanner and automated testing**
 - Jikto, 302
 - Nessus, 303–306
 - ntoinsight, 302–303
 - Wikto, 294–302
- MultiView functionality (HTTPD), 207**

N

- Nessus, 214–215, 248, 303–306**
- .NET Framework, 457**
- Netcraft, 85–86**
- netkill.pl script, 197–198**
- Network Attached Storage (NAS), 450**
- Network layer, 363**
- networking, 450**
- Nikto, 248, 286–289, 402–403**
- Nmap, 80–81, 95–97**
- node (XML), 484**
- Non Disclosure Agreement, 13**
- N-Stealth, 215–216**
- N-Tier architecture, 19–20**
- ntoinsight tool, 302–303**
- NTOMax, 267**
- null-byte character (%00), 138–139**

O

- ObiWaN, 251–253**
- objectivity, 10**
- OCTAVE method, 193**
- on-demand JavaScript, 398**
- one-way hashing**
 - description of, 42–43
 - protecting, 263
- Open Protocol Resource Project (OPRP), 100–103**
- Open Source Security Testing Methodology Manual, 8**
- Open Source Vulnerability DataBase (OSVDB), 351**
- Open Web Application Security Project (OWASP), 4, 134–135**
- OpenSSL, 32, 33, 417**
- Oracle Web service model, 131**
- OS Command attack, 165**

OS fingerprinting

- DMitry, 87–89
- Netcraft, 85–86
- pOf, 86–87

OS virtualization

- Bochs, 454
- Linux, 454–455
- overview of, 449, 452
- package managers, 456–457
- ReactOS, 457
- VMware Player, 454
- VMware Workstation, 452–454
- Windows, 457

OSVDB (Open Source Vulnerability DataBase), 351

oversized payload, 362

OWASP (Open Web Application Security Project), 4, 134–135

OWASP Validation Project, 416, 434

P

package manager, 456–457

parameter tampering, 360

parent (XML), 484

Paros Proxy, 248, 274–280

parser overload, XML, 384

passive OS fingerprinting (pOf), 86–87

password cracker, 251–259

password data, attack on

- Lcrack, 263–264
- MD5 online cracker, 265
- overview of, 263
- Rainbow Crack, 265–266

password recovery validation, 183

path expression (XQuery), 491

path traversal attack, 198, 211, 434–435

path traversal character (../), 139–140

pen (penetration) testing

- bottom line and, 5
- as business, 10–13
- case for, 3
- goals of, 8
- industry preparedness and, 3–5
- methodology of, 4–5, 8–9
- reproducing work and, 317

Perl

- hash data type, 235
- overview of, 39

permissions, limiting, 438

persistent cookie, 272

PHPFilters, 440

pipe character (|), 138

pOf (passive OS fingerprinting), 86–87

port mapping

- nmap, 95–97
- unicornscan, 94–95

port scanning, 196

portal, 66–67

predicate (XQuery), 491

Presentation Logic Tier, 20

presentation of findings, 423

private key, 30–31

privilege boundary, 188

process validation, insufficient, 185

production system, 12–13

programming community, focus of, 3

proxy, definition of, 20

proxy server

- automated testing
 - Paros, 274–280
 - SPIKE Proxy, 280–285
- manual testing with WebScarab
 - Analysis tab, 231
 - feature set, 222–223
 - Fragments section, 227–229
 - Fuzzer section, 225, 226–227
 - Manual Request section, 229–230
 - spider the tree options, 224
 - starting point, 223
 - Transcoder tool, 233–234
 - Visualization tab, 231–232

Proxy Tier, 20

Python, 39

Q

query, 471

query string, 36

R

Rainbow Crack, 265–266
Rainbow Tables, 145–146
ranking threat, 189–190
RATS (Rough Auditing Tool for Security), 446
ReactOS, 457
recursive payload, 362
Redhat Package Manager, 456
RegEx, 434
remediation
 best practices
 input validation, 432–442
 overview of, 426
 session management, 442–445
 description of, 425
 edge-level protective steps
 overview of, 425
 Web Application Firewalls, 426–430
 Web services, 430–432
Representational State Transfer (REST), 398
reproducing work, 317
requirements, gathering and clarifying, 11
resource enumeration
 approach 1 (crawling), 107–110
 approach 2, 110–115
 HTTrack, 115
 wget, 115–116
resources. See sources of information; tools
results verification, 402–406
Reverse Engineering, 185–186
Reverse Proxy server, 26, 426
risk matrix section of document
 elements of, 409–410
 examples, 410–413
 overview of, 408
 severity levels, 408–409
robots.txt file, 115
rolling documentation, 9
Rough Auditing Tool for Security (RATS), 446
routing detour, 364
RSS, 271
Ruby, 39
rules of engagement, 11–12

S

salted hashing, 51
SAML (Security Assertions Markup Language), 375
SamSpade, 77–80
scalability, 26
scanner and automated testing. See also multi-purpose scanner and automated testing
 E-Or, 289–293
 Nikto, 286–289
 overview of, 285–286
schema poisoning, 362
screamingCSS tool, 268–269
script tag character (<?), 137–138
search engines, 119
Secunia, 351
secure services
 HTTP Basic Authentication, 374
 overview of, 373–374
 SAML, 375
 SSL client authentication, 374
 WSS encryption, 378–379
 WSS signature, 377–378
 WSS username token, 376–377
Secure Sockets Layer (SSL)
 application protocol, 35
 chained certificates, 33
 client authentication, 374
 configuration, analyzing, 201–202
 filter detection and, 84
 Handshake Protocol, 33–35
 misconceptions about, 29
 overview of, 28–33
Security Assertions Markup Language (SAML), 375
security community, focus of, 3
security industry weaknesses
 application development considerations, 2
 limitations of edge security models, 2
 overview of, 1
security of results document, 416–417
security threat modeling. See threat modeling
SecurityFocus, 347–349
SELECT statement (SQL), 472–474
self protection, 12–13
server. See proxy server; Web server

server for lab, 450

server OS installations, virtualization

- Bochs, 454
- Linux, 454–455
- overview of, 452
- package managers, 456–457
- ReactOS, 457
- VMware Player, 454
- VMware Workstation, 452–454
- Windows, 457

Server Side Includes (SSI), 38

Server Side Includes (SSI) injection, 173

server-side session management, 36–37

service identification

- amap, 97–100
- Open Protocol Resource Project (OPRP), 100–103

session expiration, 153

session fixation attack, 153–154

Session ID

- brute forcing, 150–154
- length, 152–153
- overview of, 147–148
- randomness, 151–152
- URL-based, 148–149

session management, best practices for, 442–445

session management, broken

- hijacking, 146–147
- management of
 - brute forcing Session ID, 150–154
 - cookie, 150
 - hidden HTML field, 149
 - overview of, 147–148
 - URL-based Session ID, 148–149
- overview of, 146

session state, 37

severity levels, 408–409

shellcode injections, 162–163

Shu, David, hashencodes program, 46–48

sibling (XML), 484

Simple Object Access Protocol (SOAP)

- Distributed Logic Tier and, 20
- encoding, 61
- Envelope, 58–59
- Fault element, 59–61
- Header element, 59
- overview of, 56–58

social engineering, 5

Software Development Life Cycle, 5

software load balancing, 28

Sorcerer Juno, 198

source disclosure, 210

sources of information

- for building network, 450
- CERT, 351
- CVE, 352
- eEye, 351
- for error handling, 416
- HSC, 349–351
- injection attack dictionaries, 495
- Network Attached Storage, 450
- OSVDB, 351
- overview of, 347
- Secunia, 351
- SecurityFocus, 347–349
- Windows, 457
- XPath, 485, 493
- XQuery, 493

SPIKE Proxy, 248, 280–285

SQL

- command modifiers, 473
- commands, 472–475
- overview of, 471
- SELECT statement, 472–474
- special characters, 475–476

SQL injection

- attack strings, 500–502
- best practices for, 436
- DB actions, 171–173
- overview of, 166–168
- for pen testing Web apps, 246–248
- schema discovery, 169
- table names, 170
- user data, 171
- Web services and, 380–381

SSI (Server Side Includes), 38

SSI (Server Side Includes) injection, 173

SSL (Secure Sockets Layer)

- application protocol, 35
- chained certificates, 33
- client authentication, 374
- configuration, analyzing, 201–202
- filter detection and, 84

Handshake Protocol, 33–35
 misconceptions about, 29
 overview of, 28–33

SSLDigger (Foundstone), 201, 202

state, management of, 35–37

statistics, presenting, 406–407

storage

insecure, 176–178
 for lab, 450

stored procedure, 438

STRIDE model, 189

Stringer, 439

symmetric key-based algorithm, 45

T

testing. See automated testing; manual testing; pen testing

THCDBFP utility, 103

THC-Hydra, 263

THCSSLCheck utility, 84

threat modeling

analysis of threats, 188–189
 categorization and ranking of threats, 189–190
 decompose and understand application, 187–188
 identification of mitigation strategies, 190–193
 overview of, 186–187
 pen test, 193

Threat Tree, 190, 191, 192

tiers, 19–20

Tiger Team, 5

time frame, 13

TLS. See Transport Layer Security

tools. See also specific tools

for attacking Domino hashes, 325
 for auditing Web server, 214–216
 for automated exploit testing, 355–356
 DB related, 313
 for threat modeling, 193
 Web Application Firewall, 429–430
 Web application related, 306–313
 for Web services security, 431–432
 for Web services testing, 394–396

Transport Layer Security (TLS)

configuration, analyzing, 201–202
 filter detection and, 84

misconceptions about, 29
 overview of, 28–33
 session initiation, 33–35

TRIKE method, 193

Twill, 244–246

U

unicode-encoded attack, 211–212

unicornscaN, 94–95

UNION statement (SQL), 474–475

Universal Description, Discovery, and Integration (UDDI), 124–127

UPDATE statement (SQL), 474

URL encoding, 45–48

URL-based Session ID, 148–149

UrlScan, 428–429

user and DoS attack, 180

user directory harvesting, 208

username, credential discovery of, 249–250

V

validation

overview of, 136
 password recovery, 183
 process, 185

“variant”, 259

verification, manual, 380–387

VMware Player, 454

VMware Workstation, 452–454

vulnerability analysis

A1 – unvalidated input, 136–140
 A2 – broken access control, 141
 A3 – broken authentication
 authentication, 142–146
 session, 146–154
 A4 – cross-site scripting flaws, 154–158
 A5 – buffer overflows, 158–163
 A6 – injection flaws
 LDAP injection, 163–165
 OS Commanding, 165
 SQL injection, 166–173
 SSI injection, 173
 XPath injection, 173–174
 XXE, 174–175

vulnerability analysis (continued)

- A7 – improper error handling, 175–176
- A8 – insecure storage, 176–178
- A9 – Denial of Service, 178–180
- A10 – insecure configuration management, 181–182
- abuse of functionality, 184–185
- content spoofing, 183
- information leakage, 184
- insufficient anti-automation, 185
- insufficient authentication, 183
- insufficient process validation, 185
- overview of, 133–134
- OWASP and top ten threats, 134
- reverse engineering, 185–186
- threat modeling
 - analysis of threats, 188–189
 - categorization and ranking of threats, 189–190
 - decompose and understand application, 187–188
 - identification of mitigation strategies, 190–193
 - overview of, 186–187
 - pen test, 193
- WASC, 134–135
- weak password recovery validation, 183

W

WAF (Web Application Firewall), 4, 426–430

WAP (Wireless Access Protocol), 69–70

warning regarding exploit discovery, 352–355

WASC (Web Application Security Consortium), 4, 134–135

WASP (Web Application Security Project), 467–468

Weak Password Recovery Validation, 183

Web application

- application aspects of
 - dynamic technologies, 37–41
 - state, 35–37
 - Web-based authentication, 41–42
- architectural aspects of
 - HTTP protocol, 21–25
 - HTTP proxy, 25–28
 - overview of, 15–19
 - SSL/TLS, 28–35
 - tiers, 19–20

- data aspects of
 - encryption and encoding, 42–51
 - XML, 51–55
- emerging models
 - frameworks, 67–68
 - integration, 56–67
 - wireless, 68–70
- honeypot
 - Hacme Bank/Hacme Books, 463
 - WebGoat, 458–460
 - WebMaven, 460–462
- overview of, 15–19
- testing against, 465
- WASP (Web Application Security Project), 467–468
- Xoops, 466–467

Web Application Firewall Evaluation Criteria, 426

Web Application Firewall (WAF), 4, 426–430

Web Application Security Consortium (WASC), 4, 134–135

Web Application Security Project (WASP), 467–468

Web harvesting. See information harvesting

Web proxy, 398

Web server

- DoS attack and, 179–180
- logging mechanisms and, 2
- overview of, 195–196
- threats to
 - attacks on system, 197–201
 - configurations, 201–204
 - default content and settings, 196–197
 - product specific, 204–214
 - tools for auditing, 214–216
 - vulnerabilities of, 363

Web server fingerprinting

- HTTP headers, 89–92
- httpprint, 92–93

Web Service Description Language (WSDL), 61–65, 125, 126

Web Service Description Language (WSDL) scanning, 362

Web services

- AJAX, 397–398
- commercial tools, 394–396
- edge security and, 358–359, 430–432
- infrastructure attacks, 362–364

- J2EE, 128–131
 - Monkey Shell, 463–464
 - overview of, 124–125, 357–358
 - simulating attack
 - analysis, 371–373
 - automated probing or fuzzing, 388–392
 - documentation, 392–394
 - enumeration phase, 368–371
 - footprinting, 364–368
 - manual testing, 380–387
 - post security/no security, 379
 - secure services, 373–379
 - threats to, 359
 - UDDI and DISCO, 125–127
 - Web service attacks, 362
 - WSDigger_WS, 463
 - WSID4ID, 396–397
 - WSIL, 127–128
 - XML content attacks, 359–362
 - Web services for Remote Portals (WSRP), 67**
 - Web Services Inspection Language (WSIL), 127–128**
 - Web statistics, 122–123, 124**
 - webAppHoneyPot, 468–469**
 - WebDAV, 202, 210**
 - WebGoat, 458–460**
 - WebInspect**
 - Web application testing and, 309–311
 - Web service testing and, 394–396
 - WebLogic (BEA), 130–131**
 - WebMaven, 460–462**
 - WebScarab**
 - Analysis tab, 231
 - feature set, 222–223
 - Fragments section, 227–229
 - Fuzzer section, 225, 226–227
 - Manual Request section, 233
 - pop-up functionality, 225
 - SessionID Analysis section, 229–230
 - spider the tree options, 224
 - starting point, 223
 - Transcoder tool, 233–234
 - Visualization tab, 231–232
 - Web services and, 386, 387
 - WebSphere (IBM), 130**
 - wget, 115–116**
 - white space character (%20), 138**
 - whitebox test, 133, 317**
 - WHOIS, 72–74**
 - Wikto**
 - BackEnd tab, 298–300
 - GoogleHacks tab, 297–298
 - Googler tool, 296
 - Mirror & Fingerprint tab, 297
 - overview of, 248, 294
 - SystemConfig tab, 294–295
 - Wikto tab, 300–302
 - Windows (Microsoft), 449, 457**
 - Wireless Access Protocol (WAP), 69–70**
 - wireless models, 68–70**
 - WSAudit, 388–390**
 - WSDigger**
 - automated testing, 390
 - documentation and, 392–393
 - enumeration and, 371
 - footprinting and, 367
 - manual testing, 386, 387
 - WSDigger_WS, 463**
 - WSDL (Web Service Description Language), 61–65, 125, 126**
 - WSDL (Web Service Description Language) scanning, 362**
 - WSFuzzer, 391–392, 393**
 - WSID4ID, 396–397**
 - WSIL (Web Services Inspection Language), 127–128**
 - wsKnight, 370, 384, 388–390**
 - WSMap, 367–368**
 - wsPawn, 366**
 - WSPProxy, 384**
 - wsRook, 431**
 - WSRP (Web services for Remote Portals), 67**
 - WSS encryption, 378–379**
 - WSS signature, 377–378**
 - WSS username token, 376–377**
- ## X
- XACML (eXtensible Access Control Markup Language), 398**
 - XCBF (XML Common Biometric Format), 398**
 - XHTML, 38**

XML content attack, 359–362

XML content attack strings, 503

XML DoS attack, 382–383

XML (eXtensible Markup Language)

attributes, 54

Declaration, 53

Document Type Definition, 52

namespace, 55–56

overview of, 37, 51–52

tags and elements, 53–54

terminology, 483–485

well-formed versus valid document, 54

XML External Entity (XXE) attack, 174–175

XML injection and Web services, 381

XML parser overload, 384

XML signature attack, 381–382

XML-RPC

description of, 65–66

Distributed Logic Tier and, 20

Xoops, 402, 404, 466–467

XPath

overview of, 485–486

resources on, 493

syntax, 486–490

XML and, 483–485

XPath Explorer, 485

XPath injection

attack strings, 502

best practices for, 438–439

overview of, 173–174

Web services and, 381

XML content attack and, 361–362

XQEngine, 492

XQuery

basic syntax rules, 491–493

elements of, 491

overview of, 490

resources on, 493

XML and, 483–485

XML content attacks and, 361–362

XSS attack strings, 500

**XSS (cross-site scripting) attack, 154–157,
268–269, 435**

XST (cross-site tracing), 157–158

XXE (XML External Entity) attack, 174–175

Y

Yellowdog Updater Modified, 456–457

