INDEX

A
Abuse Cases, 452–453
Access Control, 152
Access Levels, 232
Adherence with Information Security, 96–100
Adherence with Software Engineering, 100–101
Advanced Persistent Threats (APTs), 252–253
Agile SDLC, 219
Analyse Attack Scenarios, 461–463, 532, 576–588
Analysis of Attacks, 71–74
Analysis of Attack scenarios, 461–463
Analysing Vulnerabilities and Impacts, 73–76
Anatomy of Account Takeover Fraud, 579
API example, 415
Application Assets, 126–127
Application Containers, 379–381
Application Decomposition & Analysis, 178–182, 393–419, 518–526
Application Design & Development, 24
Application Security Frame, 550
Application Security Goals, 257
Application Service Levels, 226
Application Risk Assessments, 91–92
Application Risk Management, 275–282
Application Walkthrough, 14–15
Architecture Components, 562
Architecture Diagrams, 210
Architecture Risk Analysis, 254
Architectural Analysis with DFDs, 408–415, 524–526
Assess Probability and Impact of Attack Scenarios, 466–469
Assert Completeness of Secure Technical Design, 513–517
Asset, 259
Asset Management, 296
Asset Variables, 182
Assignment of Probabilistic Values for Identified Threats, 547–548
Assurance, 238
Attacks, 45–48, 293
Attack Analysis in Threat Modeling, 130, 571–572

COPYRIGHTED MATERIAL
INDEX

Attack & Countermeasure Analysis, 630
Attack Tree 48, 607
Attack Vector Analysis, 580
Attack Vectors Used by Banking Malware, 595
Attack Vectors Used Against Web Applications, 596
Audit and Compliance, 236
Audit and Risk Management, 236–239
Audit Logs, 429–431
Awareness, 323–324

B
Banking Trojan Attacks, 578–580
Benefits of Threat Modeling, 289
Blind Threat Modeling, 382
Build in Security Maturity Model (BSIMM), 95
Building Security in the SDLC, 195–198
Building Security in Agile Sprints, 222
Business Functionality, 347
Business Impact Estimates, 274
Business Impact, 355–360
Business Impact of Vulnerabilities, 135–136
Business Liabilities, 347
Business Logic Attacks, 257
Business Objectives Mapping to Security Requirements, 348
Business Requirements, 351

C
Capability Maturity Model (CMM), 320
Campaign Against Online Banking Sites, 534
CAPEC Attack Libraries, 464–465
Catching Up With Emerging Threats, 257
CERT, 310
Change Control, 152
Challenges of Securing Software Using Agile SDLC, 220
CISO, 140–142, 246, 282, 310, 331
oversight in threat modeling, 140–142, 331
role in incident response, 310
responsibility, 246
risk management, 282
Conduct Attack Driven Security Tests and Simulations, 470–472
Considerations For Factoring Business Impact, 359
Configuration Management, 153
Common Attack Pattern Enumeration and Classification (CAPEC), 165, 595–600
Compliance as Factor for Information Security Assurance, 257
Compliance as Factor in Risk Reduction, 236–241
Compliance in Risk-Centric Threat Modeling, 331
Compliance Requirements, 350–353
Compliance and Information Risk Management, 290–291
Components in Scope for Threat Modeling (example), 364
Computer Security Incident Handling Guide, 308–309
Contextual Risk Analysis, 454–455
Control Analysis, 298
Control Gap Analysis, 247
Control Requirements, 298
Correlation of Threat Agents to Asset Targets, 546–547
Correlate Vulnerability Data, 443–444
Countermeasures, 627
Cybercrime Gangs, 235
Cyberthreat, 259, 260, 291, 303, 311
alert levels, 311
analysis, 259–260
dissecting, 303
risks, 291
CRUDEntitlements, 37
CVEs Vulnerability Types Exploited by Drive by Download, 595
CVSS Vulnerability Risk Scoring, 623

D
Derive Attack Driven Test Cases to Test Countermeasures, 470
Data Flow Analysis, 398–408
Data Flow Diagrams (DFDs), 110, 212, 232, 403, 405, 407, 408
security centric DFDs for distributed attacks, 159
revisiting DFDs in architectural analysis, 451
symbols, 156
syntax, 402
Data Breach Incidents, 235, 242–243, 235–259
economic impact, 242
cost estimates, 242–243
lesson for risk management, 235–259
notification laws (SB 1386), 255
Data Sinks & Sources, 369–376
Defence in Depth, 295
Define Activities, 349–369
Define Participants, 364–366
Define Roles 366–367
Define Business Requirements, 349–350, 492
Define Business Impact (example), 497–498
Define Security Requirements (example), 490, 495–497
Defining the “who”, “what”, “when”, “where”, 176
Defining Participants, 386–390
Denial of Service Attacks, 163, 257
Derivation of Test Cases for Testing Countermeasures, 608–617
Design For Resilience, 200
Design Flaws, 104–118
eXamples, 107–108
identification, 104–118
remediation, 113–118
root cause analysis, 114–115
Detection and Analysis, 311
Determine the Risk Profile (example), 499–501
Difference Between Top Vulnerabilities and Top Exploits, 567–568
Distributed Denial of Service Attacks (DDoS) Risk Analysis Examples, 265–269, 313, 532–535
Document business requirements (example), 489
Documenting DFDs in a threat model (example), 522–523
Dynamic Application Security Testing Tools (DAST), 105
Dynamic Analysis, 229
DREAD Threat Risk Calculation, 624
E
Effectiveness of Security Controls, 247
Elicitation of Security Requirements, 206–207
Embedding Threat Modeling in the SDLC, 197
Emerging Threats, 67, 244–245
Empirical Risk Calculation Formulas, 265, 267, 268, 439, 459, 631–633
End-to-End View of Security Controls, 215
Engineering for Attacks, 600
Enumeration of Use Cases, 395–398
Enumeration of Software Components (example), 509–510
Enumeration of System-Level Services (example), 511–512
Enumeration of Technical Scope, 177
Enumeration of Third Party Infrastructure Components (example), 512–513
Estimates of Business Impacts of Data Breach Incidents, 257
Exposure to Vulnerabilities as Factor for Risk, 263–264
Executive Sponsorship, 139
Exploring Stages and Activates of PASTA Threat Modeling, 345–480
Expected Outputs of Stage I of PASTA Threat Modeling, 339–343
F
Factors Influencing Attack Probability, 128–129
FAIR, 296
False Negatives & Positives, 105
False Sense of Security, 257
Final Security Review, 225
Financial Impact Estimates, 269, 357
Functional Requirements, 399–400
Functional Analysis and Trust Boundaries, 408–416
Fuzz Testing Process, 226
G
Governance Risk Control (GRC), 331
<table>
<thead>
<tr>
<th>INDEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRC Cross Section of Threat Modeling Team, 331</td>
</tr>
<tr>
<td>GRC Artefacts, 353–355</td>
</tr>
<tr>
<td><strong>H</strong></td>
</tr>
<tr>
<td>Hardening Guidelines For Inherent Risk Mitigation, 383–385</td>
</tr>
<tr>
<td>High Level View of Threats-Attacks-Vulnerabilities-Countermeasures, 629</td>
</tr>
<tr>
<td>Hybrid Software Security Assessments, 229–232</td>
</tr>
<tr>
<td><strong>I</strong></td>
</tr>
<tr>
<td>Identify Actors And Data Interfaces (example), 510–511</td>
</tr>
<tr>
<td>Identify Weak Design Patterns in The Application Architecture, 557–560</td>
</tr>
<tr>
<td>Identify the Attack Surface, 465–466</td>
</tr>
<tr>
<td>Identify Weak Design Patterns in Architecture, 444–452</td>
</tr>
<tr>
<td>Initial Risk Profile, 301–302</td>
</tr>
<tr>
<td>Integrating Threat Modeling in Agile, 219–222</td>
</tr>
<tr>
<td>Integrating Threat Modeling in the SDLC, 196–233</td>
</tr>
<tr>
<td>Impact Analysis, 297</td>
</tr>
<tr>
<td>Impact of Procurement, 390–392</td>
</tr>
<tr>
<td>Inputs and Outputs of PASTA Process, 324–325</td>
</tr>
<tr>
<td>Information Security Reviews, 88–89</td>
</tr>
<tr>
<td>Information Security Risk Defined, 292</td>
</tr>
<tr>
<td>Information Security &amp; Risk Management, 289–301</td>
</tr>
<tr>
<td>Information Security Assurance, 290</td>
</tr>
<tr>
<td>Information Sharing and Analysis Centers (ISACs), 255, 310</td>
</tr>
<tr>
<td>Inherent Risk, 362–363</td>
</tr>
<tr>
<td>Inherent Risk Profile by Application Type, 363</td>
</tr>
<tr>
<td>Inherent Challenges to Threat Modeling, 320</td>
</tr>
<tr>
<td>ISAC Alert Levels, 311–312</td>
</tr>
<tr>
<td>ISO/IEC 27001, 294–296, 488</td>
</tr>
<tr>
<td><strong>J</strong></td>
</tr>
<tr>
<td>Judging by Motives, 12</td>
</tr>
<tr>
<td>Justification for Investing in Security, 295</td>
</tr>
<tr>
<td><strong>K</strong></td>
</tr>
<tr>
<td>Kill-chain Attack Modeling, 542–544</td>
</tr>
<tr>
<td>Kill-chain Analysis of Banking Malware Attacks, 581–584</td>
</tr>
<tr>
<td>Kill-chain Analysis of DDoS Attacks, 584–588</td>
</tr>
<tr>
<td><strong>L</strong></td>
</tr>
<tr>
<td>Labelling Threats &amp; Application Components, 458</td>
</tr>
<tr>
<td>Lesson Learnt from Security Incidents, 249–250–251</td>
</tr>
<tr>
<td>List of Insecure Architecture Gaps, 444–451</td>
</tr>
<tr>
<td>Logical Flow Considering Threats to Assets, 456</td>
</tr>
<tr>
<td>Low Hanging Fruits (LHF), 105</td>
</tr>
<tr>
<td><strong>M</strong></td>
</tr>
<tr>
<td>Malware Threats, 251–252</td>
</tr>
<tr>
<td>Man-in the Middle (MiTM) Attacks 216, 251, 253, 607</td>
</tr>
<tr>
<td>Man-in the Browser (MiTB) Attacks, 257, 304</td>
</tr>
<tr>
<td>Mapping Threats To Vulnerabilities, 452, 565</td>
</tr>
<tr>
<td>Mapping Threat Modeling Activities, 299</td>
</tr>
<tr>
<td>Mapping Test Cases to Vulnerabilities, 132–133</td>
</tr>
<tr>
<td>Maturity, 323</td>
</tr>
<tr>
<td>Microsoft SDL, 222–229</td>
</tr>
<tr>
<td>Minimal Threat Modeling Requirements, 225</td>
</tr>
<tr>
<td>Misconfigurations, 217</td>
</tr>
<tr>
<td>Missing Architectural Countermeasures, 451</td>
</tr>
<tr>
<td>MITRE Corp Security Content, 189</td>
</tr>
<tr>
<td>Mobile Web Application Example, 180, 414</td>
</tr>
<tr>
<td>Modeling and Simulation, 459–473</td>
</tr>
<tr>
<td>Multi Factor Authentication (MFA), 252</td>
</tr>
<tr>
<td><strong>N</strong></td>
</tr>
<tr>
<td>NIST Risk Terminology 635–653</td>
</tr>
<tr>
<td>NIST Risk Assessment Methodology, 297–298</td>
</tr>
<tr>
<td>Number of Attacks Observed, 567–568</td>
</tr>
<tr>
<td><strong>O</strong></td>
</tr>
<tr>
<td>OCTAVE, 296</td>
</tr>
<tr>
<td>OWASP Guide for Building Secure applications, 116</td>
</tr>
<tr>
<td>OWASP Mapping to WASC, 567</td>
</tr>
<tr>
<td>OWASP Top Ten, 240, 241, 292</td>
</tr>
<tr>
<td>Out of Band Authentication (OOBA), 253</td>
</tr>
</tbody>
</table>
INDEX

P
PASTA Risk–Centric Threat Modeling in the Details, 345–480
PASTA Risk-Centric Threat Modeling Use Case, 481–633
Patch Management, 153
Performing the DFD exercise, 398–408
PCI-DSS, 216, 236–238, 240
PCI-DSS Audits & Data Breaches, 240
PCI-DSS Fines, 241
PCI-DSS Effectiveness, 247–249
Phishing, 257
Post-Mortem Incident Analysis, 249–250
Proactive Risk Mitigation Strategy, 277
Privacy Testing, 225
Privacy Requirements, 352
Probability of Attacks, 466–469, 605–608
Process IDs, 374–375
Process Areas For Threat Modeling, 139
Process and People, 334–335
Process for Attack Simulation and Threat Analysis (PASTA), 171–194
Provide Context Risk Analysis, 566
Q
Qualified Security Assessors (QSA), 236–239
Quantitative Risk Analysis, 272–275, 625–626
R
Rational Unified Process, 217–218
Reducing the Attack Surface, 604–605
Reasons For Security Failure, 20
Relationship Among Assets, Use Cases and Actors, 181
Regulatory Compliance, 360
and business impact, 361
Review and correlate vulnerabilities, 556
Remote Access Tools (RATs), 253
Requirement Scope Creeps, 348–349
Resilience to Attacks, 200–201
Residual Risk Analysis and Management, 62, 270–272, 473–480
calculate residual risk, 62, 270–272, 473, 476–478
identify countermeasures, 474–475
recommend strategy to manage risks, 478–480
Risk Analysis, 261–275, 297
Risk Analysis and Management, 305–307, 617–633
Risk Analysis with Threat Models, 60–62
Risk Assessors, 331
Risk Based Threat Modeling, 167–168, 284, 282–289
Risk Based Security Requirements, 207
Risk Calculations, 265–275
factoring likelihood and impact, 265
reference scale, 266
Risk Centric Threat Modeling, 319–344
preparedness, 321
team selection, 325–326
supporting personnel, 327–328
security operations, 329–330
mapping to security processes, 336–338
Risk Characterization, 259, 262–263
Risk Culture, 281
Risk Determination, 298
Risk DREAD, 116, 168–170
Risk Heat Maps, 266, 268, 294, 626
Risk Management, 275–278, 297
Risk Mitigation, 631–633
Risk Profile, 363, 502
Risk Reporting, 298
Risk Terminology, 259 also see Glossary, 635–653
Roles and Benefits of Threat Modeling, 69
Root Cause Analysis, 115
in application security reviews, 230
after security incidents, 316–317
S
Security Analysis, 9–17
Secure Architecture Design Reviews, 201–202
Secure Architecture Design Guidelines, 561
Secure By Design, 84–88, 222
Security Centric Threat Modeling, 156–157
Security Content Automation Protocol (SCAP), 188
bank sys admin case study, 157–158
for complex attacks, 158
Secure Coding and Threat Modeling, 213
Security Development Lifecycle (SDL), 222–229
agile SDL, 225–226
Security Development Lifecycle (SDL) (Continued)
line of business SDL, 226
phases, 227
security principles incorporated in the SDL, 224
design flaw identification, 108–109
Security Enhanced SDLC, 222–229
Security Functional Analysis, 524–526
Security Functional Transactional Analysis, 527
Security In the Software Development Life-Cycle, 92–104
adopting it, 102–104
Security Incident Response, 283–317
assessment, 313–315
escalation procedures, 315
containment and eradication, 315–316
response, 307–317
preparation, 308
event monitoring, 303
course of action, 283–284
handling process, 310
root cause analysis, 316–317
Security Improvements with Threat Modeling, 82–92
Security Measures For Mitigating Risk, 80–82
derived using kill-chain attack analysis, 590–592
Security Objectives in Support of Business Objectives, 175
Security Operation Centre (SOC), 426–428
Security Operations, 55–57
Security Requirements, 82–84
Security Requirements, 199–200
engineering, 206
for conducting a threat model in SDL, 228
Security Risk Assessment, 223
Security Risk Management, 57
risk components, 58
Security Test Case, 470–472, 611
Security Testing 202–203
Security Testing Tools, 54
effectiveness of automated tools, 105–108
coverage, 106
Source Code Analysis & Threat Modeling, 231
Software Components, 369
enumeration, 371–374
Software Development, 149
expertise leveraged for threat modeling, 149–151
System and Network Administration, 151–152
Software Assurance Maturity Model (SAMM), 95
Software Enumeration, 377
Sprinits (Agile), 219
Stages of PASTA methodology (in summary), 173
Static Application Security Testing (SAST), 105
Static Analysis, 229
STRIIDE, 39, 160–165
categorization table, 164
classification model, 166
per element example, 548
threat list, 549
Structured Threat Information Expression (STIX), 434, 538–542
data breach incidents, 235
risk mitigation strategy, 255
impact estimates, 274–275
remediation options, 307
SQL-CAPEC, 598–599
System Characterization, 298
System Level Services, 376
T
Targeted Vulnerability Testing, 455–459, 569–570
Taxonomy of Attacks, 46
Technical Scope Definition, 369–371
Technical Design, 379
assertion of completeness, 379–382
Testing with threat models, 214–217
test case derivation, 214–215
prioritization, 215
Test Cases, 470, 612–616
Test Techniques, 261
Threat Modeling in the SDLC, 224
Threat Modeling Activity Integration, 218–219
Third Party Infrastructures, 369
<table>
<thead>
<tr>
<th>Threats</th>
<th>42, 118–123, 131–132, 259, 625</th>
</tr>
</thead>
<tbody>
<tr>
<td>classification</td>
<td>42</td>
</tr>
<tr>
<td>analysis of countermeasures</td>
<td>118–123</td>
</tr>
<tr>
<td>mapping to vulnerabilities</td>
<td>131–132</td>
</tr>
<tr>
<td>risk</td>
<td>259</td>
</tr>
<tr>
<td>and risk dashboard</td>
<td>625</td>
</tr>
<tr>
<td>Threat actors</td>
<td>260</td>
</tr>
<tr>
<td>Threat Analysis</td>
<td>68–71, 182–185, 296, 302–304, 419–441, 526–549</td>
</tr>
<tr>
<td>agents to asset mapping</td>
<td>437</td>
</tr>
<tr>
<td>assignment of probability</td>
<td>437–439</td>
</tr>
<tr>
<td>frequency</td>
<td>17</td>
</tr>
<tr>
<td>sources of info gathering</td>
<td>18</td>
</tr>
<tr>
<td>and risk management</td>
<td>64–65, 259–282</td>
</tr>
<tr>
<td>effectiveness</td>
<td>258</td>
</tr>
<tr>
<td>factors influencing attacks</td>
<td>183</td>
</tr>
<tr>
<td>threat re-examination</td>
<td>419–420</td>
</tr>
<tr>
<td>key roles</td>
<td>440–441</td>
</tr>
<tr>
<td>objectives</td>
<td>421</td>
</tr>
<tr>
<td>threat scenario analysis</td>
<td>422–427</td>
</tr>
<tr>
<td>threat intelligence gathering</td>
<td>427–431</td>
</tr>
<tr>
<td>threat possibilities per industry</td>
<td>425</td>
</tr>
<tr>
<td>threat library updates</td>
<td>436</td>
</tr>
<tr>
<td>Threat Agents</td>
<td>124–125</td>
</tr>
<tr>
<td>Threat Anatomy</td>
<td>33–48</td>
</tr>
<tr>
<td>Threat Attributes</td>
<td>259–260</td>
</tr>
<tr>
<td>Threat Driven Test Cases</td>
<td>613–615</td>
</tr>
<tr>
<td>Threat Factors</td>
<td>10–16</td>
</tr>
<tr>
<td>Threat Intelligence</td>
<td>65–66</td>
</tr>
<tr>
<td>Threat Intelligence Gathering</td>
<td>427–436</td>
</tr>
<tr>
<td>internal sources</td>
<td>427–431</td>
</tr>
<tr>
<td>external sources</td>
<td>431–436</td>
</tr>
<tr>
<td>Threat Libraries</td>
<td>111–113, 545</td>
</tr>
<tr>
<td>using STRIDE</td>
<td>11</td>
</tr>
<tr>
<td>updates</td>
<td>436–437</td>
</tr>
<tr>
<td>Threat Management Dashboard</td>
<td>551, 637</td>
</tr>
<tr>
<td>Threat Methodologies</td>
<td>138–194</td>
</tr>
<tr>
<td>Threat Modeling</td>
<td>1, 35–36, 210–211</td>
</tr>
<tr>
<td>approaches</td>
<td>154–155</td>
</tr>
<tr>
<td>areas of collaboration</td>
<td>141</td>
</tr>
<tr>
<td>art of espionage</td>
<td>7</td>
</tr>
<tr>
<td>baseline</td>
<td>225</td>
</tr>
<tr>
<td>benefits for various roles</td>
<td>27–29</td>
</tr>
<tr>
<td>business case</td>
<td>21–24</td>
</tr>
<tr>
<td>classification</td>
<td>37</td>
</tr>
<tr>
<td>collaboration among stakeholders</td>
<td>48–53</td>
</tr>
<tr>
<td>criteria for defining scope</td>
<td>92</td>
</tr>
<tr>
<td>criteria for updating it</td>
<td>94</td>
</tr>
<tr>
<td>definition</td>
<td>1–3</td>
</tr>
<tr>
<td>development metrics</td>
<td>25</td>
</tr>
<tr>
<td>elements of risk</td>
<td>59–60</td>
</tr>
<tr>
<td>expertise</td>
<td>146, 148–149</td>
</tr>
<tr>
<td>in military strategy</td>
<td>3–9</td>
</tr>
<tr>
<td>mapping to security processes</td>
<td>143–145</td>
</tr>
<tr>
<td>origin and use</td>
<td>3–7</td>
</tr>
<tr>
<td>preventive risk management</td>
<td>30–31</td>
</tr>
<tr>
<td>rationale for integration in SDLC</td>
<td>94–96</td>
</tr>
<tr>
<td>scalability factors</td>
<td>25–26</td>
</tr>
<tr>
<td>security benefits</td>
<td>29</td>
</tr>
<tr>
<td>software security assessments and</td>
<td>202</td>
</tr>
<tr>
<td>software risks management</td>
<td>204</td>
</tr>
<tr>
<td>time commitments</td>
<td>153</td>
</tr>
<tr>
<td>Threat Modeling Tools</td>
<td>170–171, 228, 333–334</td>
</tr>
<tr>
<td>Threat Risk Rating Table Example</td>
<td>169</td>
</tr>
<tr>
<td>Threat Risk Factors</td>
<td>551</td>
</tr>
<tr>
<td>Threat Scenarios</td>
<td>125</td>
</tr>
<tr>
<td>analysis</td>
<td>125–126, 422–427</td>
</tr>
<tr>
<td>affecting financial IT systems and applications</td>
<td>536–537</td>
</tr>
<tr>
<td>Threat Scenario of Financial IT Systems and Applications</td>
<td>536</td>
</tr>
<tr>
<td>Threat Sources to Consider</td>
<td>433</td>
</tr>
<tr>
<td>Threat Targets</td>
<td>127</td>
</tr>
<tr>
<td>Threat Tree</td>
<td>203, 213</td>
</tr>
<tr>
<td>Tools, Techniques and Procedures (TTPs)</td>
<td>571</td>
</tr>
<tr>
<td>Total Cost of Ownership (TCO)</td>
<td>295</td>
</tr>
<tr>
<td>TJ Maxx Data Breach Incident</td>
<td>235–238</td>
</tr>
<tr>
<td>Training and Awareness</td>
<td>202</td>
</tr>
<tr>
<td>Trusted Automated exchange of Indicator Information (TAXII)</td>
<td>434</td>
</tr>
<tr>
<td>Trust Boundaries</td>
<td>408</td>
</tr>
<tr>
<td>U</td>
<td>Unlawful Compliance Risks</td>
</tr>
<tr>
<td>Update Attack Libraries</td>
<td>463–465, 545</td>
</tr>
<tr>
<td>Update Control Frameworks</td>
<td>463–465, 546</td>
</tr>
<tr>
<td>Update Attack libraries and Control Frameworks</td>
<td>463–464</td>
</tr>
<tr>
<td>Use and Abuse Cases</td>
<td>207–208, 610</td>
</tr>
<tr>
<td>Use Case Diagrams</td>
<td>85</td>
</tr>
<tr>
<td>Use Cases Derived From Business Objectives</td>
<td>350</td>
</tr>
<tr>
<td>Use Cases Derived From Functional Requirements</td>
<td>401</td>
</tr>
</tbody>
</table>
Use Cases Enumeration, 395–398
Use Cases Visualization Example, 521
Using Containers to Organize DFDs, 404–451

V
Verizon Enterprise Risk Incident Sharing (VERIS), 434–435
Vulnerability, 259
analysis, 304–305
characterization with threats and assets, 262
exposure, 292
mapping to attacks, 41–42
risks and impacts, 76–80, 261
Vulnerability Assessments, 296
and integration with threat modeling, 147
Vulnerability CVSS Risk Severity Calculations, 116, 134, 278
Vulnerability Data Sources, 454
Vulnerability Management, 89–90
Vulnerability Risk Management, 290
Vulnerability Testing, 455–459

W
Walk-Through Use Case of PASTA Risk Centric Threat Modeling, 481–633
Waterfall SDLC, 205
Weakness & Vulnerability Analysis, 185–197, 441–459, 549–570
Weak Design Patterns in Architecture, 444–452
Web Application, 278
security risks, 278–282
characterization, 300–302
use cases, 302
user roles, 302
trust boundaries, 302
targeted vulnerability testing, 457–459
Web Application Firewall, 313
Web Hacking Incident Database (WHID), 544, 601

X
XSS vulnerabilities, 233, 304–305