

Spis treści

	O autorce	11
	O korektorach merytorycznych	12
	Podziękowania	13
	Przedmowa	15
	Wstęp	17
Część I	Co trzeba wiedzieć, by pisać kod na tyle bezpieczny, żeby można go było umieścić w internecie	21
Rozdział 1.	Podstawy bezpieczeństwa	23
	Zadania w zakresie bezpieczeństwa — triada CIA	23
	Poufność	24
	Integralność	25
	Dostępność	25
	Założ, że dojdzie do naruszenia bezpieczeństwa	26
	Zagrożenia wewnętrzne	27
	Dogłębna ochrona	29
	Najmniejsze uprzywilejowanie	30
	Zabezpieczanie łańcucha dostaw	31
	Zabezpieczanie przez niejawność	33
	Ograniczanie powierzchni ataku	33
	Trwałe kodowanie	34
	Nigdy nie ufaj, zawsze sprawdzaj	34

Użyteczność zabezpieczeń	36
Składniki uwierzytelniania	37
Ćwiczenia	38
Rozdział 2. Wymagania związane z bezpieczeństwem	40
Wymagania	41
Szyfrowanie	42
Nigdy nie ufaj danym wejściowym systemu	43
Kodowanie i stosowanie znaków ucieczki	47
Komponenty innych podmiotów	48
Nagłówki bezpieczeństwa — pasy bezpieczeństwa dla aplikacji sieciowych	50
Zabezpieczanie ciasteczek	60
Hasła, przechowywanie danych i inne ważne ustalenia	64
Tworzenie kopii zapasowych i przywracanie danych	71
Funkcje bezpieczeństwa na platformach programistycznych	71
Dług techniczny = dług bezpieczeństwa	71
Przekazywanie plików	72
Błędy i rejestrowanie zdarzeń	73
Weryfikowanie i oczyszczanie danych wejściowych	74
Autoryzacja i uwierzytelnianie	75
Zapytania parametryczne	75
Najmniejsze uprzywilejowanie	76
Lista kontrolna wymagań	77
Ćwiczenia	79
Rozdział 3. Projektowanie pod kątem bezpieczeństwa	80
Wada projektowa a usterka bezpieczeństwa	81
Późne wykrycie wady	81
Zepchnięcie w lewo	82
Koncepcje projektowania pod kątem bezpieczeństwa	83
Ochrona poufnych danych	83
Nigdy nie ufaj, zawsze sprawdzaj/zero zaufania/załóż, że dojdzie do naruszenia zabezpieczeń	85
Kopie zapasowe i przywracanie danych	86
Sprawdzanie bezpieczeństwa danych po stronie serwera	87
Funkcje bezpieczeństwa platformy programistycznej	88
Izolowanie funkcji bezpieczeństwa	88
Partycjonowanie aplikacji	89
Zarządzanie wpisami tajnymi	89
Powtórne uwierzytelnianie transakcji (unikanie ataków CSRF)	90
Odizolowanie danych środowiska produkcyjnego	91
Ochrona kodu źródłowego	91
Modelowanie zagrożeń	92
Ćwiczenia	95

Rozdział 4.	Bezpieczny kod	96
	Wybór platformy i języka programowania	96
	Reguła wyboru języka i platformy programistycznej	99
	Niezaufane dane	100
	Zlecenia HTTP	102
	Tożsamość	103
	Zarządzanie sesjami	103
	Sprawdzanie zakresu	105
	Uwierzytelnianie (AuthN)	106
	Autoryzacja (AuthZ)	108
	Obsługa błędów, rejestrowanie zdarzeń i monitorowanie	110
	Zasady obsługi błędów	111
	Rejestrowanie zdarzeń	112
	Monitorowanie	113
	Ćwiczenia	115
Rozdział 5.	Często spotykane pułapki	116
	OWASP	116
	Środki obrony przed zagrożeniami nieopisanymi wcześniej	120
	Fałszowanie żądań między witrynami	120
	Fałszowanie żądań po stronie serwera	123
	Deserializacja	125
	Sytuacje wyścigu	126
	Uwagi końcowe	127
	Ćwiczenia	127
Część II	Co należy robić, by powstał bardzo dobry kod	129
Rozdział 6.	Testowanie i wdrażanie	131
	Testowanie kodu	131
	Inspekcja kodu	132
	Statyczne testowanie bezpieczeństwa aplikacji (SAST)	133
	Analiza składu oprogramowania (SCA)	135
	Testy jednostkowe	136
	Infrastruktura jako kod (IaC) i bezpieczeństwo jako kod (SaC)	138
	Testowanie aplikacji	139
	Testowanie manualne	141
	Testowanie infrastruktury	150
	Testowanie baz danych	151
	Testowanie interfejsów API i usług sieciowych	152
	Testowanie integracji	153
	Testowanie sieci	154

Wdrożenie	154
Edytowanie kodu działającego na serwerze	155
Publikowanie ze środowiska IDE	156
Systemy wdrażania „domowej roboty”	156
Podręczniki procedur	157
Ciągła integracja/ciągłe dostarczanie/ciągłe wdrażanie	157
Ćwiczenia	159
Rozdział 7. Program bezpieczeństwa aplikacji	160
Cele programu bezpieczeństwa aplikacji	161
Utworzenie i prowadzenie ewidencji aplikacji	162
Możliwość znajdowania podatności w treści kodu, po jego uruchomieniu i w kodzie innych podmiotów	162
Wiedza i zasoby potrzebne do naprawy podatności	163
Edukacja i materiały informacyjne	164
Zapewnienie programistom narzędzi bezpieczeństwa	164
Wykonywanie jednego lub kilku działań w zakresie bezpieczeństwa w każdej fazie procesu SDLC	165
Wdrożenie przydatnych i efektywnych narzędzi	166
Zespół reagowania na incydenty, który wie, kiedy wzywać na pomoc	166
Stale ulepszaj program, opierając się na wskaźnikach, eksperymentowaniu i informacjach zwrotnych	168
Specjalna uwaga na temat metodyk DevOps i Agile	171
Działania zabezpieczające aplikacje	171
Narzędzia zabezpieczające aplikacje	173
Twój program bezpieczeństwa aplikacji	175
Ćwiczenia	175
Rozdział 8. Zabezpieczanie nowoczesnych aplikacji i systemów	176
Interfejsy API i mikrousługi	177
Internetowa przestrzeń dyskowa	180
Kontenery i orkiestracja	181
Przetwarzanie bezserwerowe	182
Infrastruktura jako kod (IaC)	184
Zabezpieczenia jako kod (SaC)	186
Platforma jako usługa (PaaS)	187
Infrastruktura jako usługa (IaaS)	188
Ciągła integracja/dostarczanie/wdrażanie	188
Dev(Sec)Ops	189
DevSecOps	190
Chmura	191
Przetwarzanie w chmurze	191
Rozwiązania natywne dla chmury	192
Zabezpieczenia natywne dla chmury	193

Przepływy pracy w chmurze	194
Nowoczesne narzędzia	194
Interaktywne testowanie bezpieczeństwa aplikacji	194
Samoochrona aplikacji w czasie wykonania	195
Monitorowanie integralności plików	195
Narzędzia kontroli aplikacji (listy zatwierdzonego oprogramowania)	196
Narzędzia bezpieczeństwa przeznaczone dla potoków DevOps	196
Narzędzia inwentaryzacji aplikacji	196
Automatyzacja ograniczania uprawnień i innych zasad	197
Nowoczesne taktyki	197
Podsumowanie	198
Ćwiczenia	199
Część III	
Przydatne informacje o tym, jak nadal tworzy bardzo dobry kod	201
Rozdział 9. Dobre nawyki	203
Zarządzanie hasłami	204
Usuń reguły złożoności hasel	204
Korzystaj z menedżera hasel	205
Wyrażenia hasłowe	205
Nie używaj wielokrotnie tych samych hasel	206
Nie zmuszaj do okresowej zmiany hasel	206
Uwierzytelnianie wieloskładnikowe	207
Reagowanie na incydenty	208
Ćwiczenia przeciwpożarowe	208
Ciągłe skanowanie	210
Dług techniczny	210
Ewidencja	210
Inne dobre nawyki	211
Zasady	211
Pobieranie plików i korzystanie z urządzeń	212
Blokuj swój komputer	212
Prywatność	212
Podsumowanie	213
Ćwiczenia	214
Rozdział 10. Ciągłe uczenie się	215
Czego się uczyć	216
Ofensywa != defensywa	216
Nie zapominaj o umiejętnościach miękkich	216
Przywództwo != zarządzanie	217

	Możliwości nauki	217
	Odpowiedzialność	221
	Utwórz swój plan	221
	Podjmij działanie	222
	Ćwiczenia	222
	Plan nauki	224
Rozdział 11.	Uwagi końcowe	225
	Wciąż powracające pytania	226
	Kiedy uznać własne działania za wystarczające?	226
	Jak uzyskać poparcie kierownictwa?	228
	Jak zaangażować programistów?	229
	Od czego zacząć?	230
	Gdzie szukać pomocy?	231
	Zakończenie	231
Dodatek A	Przypisy	233
Dodatek B	Klucz odpowiedzi	239