

Spis treści

Przedmowa	21
Podziękowania	23
O autorach	23
Redaktorzy techniczni	24
Wprowadzenie	25
Układ książki	26
Dla kogo jest ta książka	27
Co należy przeczytać	27
Grzech I	
Przepelnienie buforów	29
1.1. Omówienie grzechu	30
1.2. Grzeszne języki programowania	31
1.3. Objaśnienie grzechu	31
1.3.1. Grzeszne C/C++	35
1.3.2. Grzechy pokrewne	38
1.4. Wykrywanie grzechu	38
1.5. Wykrywanie grzechu podczas analizy kodu programu	39
1.6. Techniki testowania wykrywające grzech	39
1.7. Przykłady grzechu	40
1.7.1. CVE-1999-0042	40
1.7.2. CVE-2000-0389–CVE-2000-0392	41
1.7.3. CVE-2002-0842, CVE-2003-0095, CAN-2003-0096	41
1.7.4. CAN-2003-0352	42
1.8. Postanowienie poprawy	43
1.8.1. Zastępowanie niebezpiecznych funkcji napisowych	43

1.8.2.	Kontrolowanie operacji przydziału pamięci	43
1.8.3.	Kontrolowanie pętli i odwołań do tablic	43
1.8.4.	Zastępowanie buforów napisowych C napisami C++	44
1.8.5.	Zastępowanie tablic statycznych kontenerami STL	44
1.8.6.	Korzystanie z narzędzi analitycznych	44
1.9.	Specjalne środki ochronne	45
1.9.1.	Ochrona stosu	45
1.9.2.	Sprzętowa ochrona stosu i sterty przed wykonywaniem kodu	46
1.10.	Materiały dodatkowe	46
1.11.	Rachunek sumienia	47

Grzech II

Napisy formatujące	49
2.1. Omówienie grzechu	50
2.2. Grzeszne języki programowania	50
2.3. Objasnienie grzechu	51
2.3.1. Grzeszne C/C++	53
2.3.2. Grzechy pokrewne	54
2.4. Wykrywanie grzechu	54
2.5. Wykrywanie grzechu podczas analizy kodu programu	54
2.6. Techniki testowania wykrywające grzech	55
2.7. Przykłady grzechu	55
2.7.1. CVE-2000-0573	56
2.7.2. CVE-2000-0844	56
2.8. Postanowienie poprawy	56
2.8.1. Poprawa C/C++	57
2.9. Specjalne środki ochronne	57
2.10. Materiały dodatkowe	57
2.11. Rachunek sumienia	58

Grzech III

Nadmiar całkowitoliczbowy	59
3.1. Omówienie grzechu	60
3.2. Grzeszne języki programowania	60
3.3. Objasnienie grzechu	60
3.3.1. Grzeszne C/C++	61

3.3.2.	Grzeszny C#	67
3.3.3.	Grzeszne Visual Basic i Visual Basic .NET	69
3.3.4.	Grzeszna Java	70
3.3.5.	Grzeszny Perl	70
3.4.	Wykrywanie grzechu	72
3.5.	Wykrywanie grzechu podczas analizy kodu programu	72
3.5.1.	C/C++	72
3.5.2.	C#	75
3.5.3.	Java	75
3.5.4.	Visual Basic i Visual Basic .NET	75
3.5.5.	Perl	76
3.6.	Techniki testowania wykrywające grzech	76
3.7.	Przykłady grzechu	76
3.7.1.	Błąd w windowsowym motorze skryptów umożliwiający wykonywanie kodu	76
3.7.2.	Nadmiar całkowitoliczbowy w konstruktorze obiektu SOAPParameter	77
3.7.3.	Przepełnienie sterty procedury obsługi HTR umożliwiające atak na serwer WWW	77
3.8.	Postanowienie poprawy	78
3.9.	Specjalne środki ochronne	80
3.10.	Materiały dodatkowe	80
3.11.	Rachunek sumienia	81

Grzech IV

Wklucia w SQL	83
4.1. Omowienie grzechu	84
4.2. Grzeszne jazyki programowania	85
4.3. Objasnienie grzechu	85
4.3.1. Grzeszny C#	85
4.3.2. Grzeszny PHP	87
4.3.3. Grzeszne Perl/CGI	87
4.3.4. Grzeszne Java i JDBC	88
4.3.5. Grzeszny SQL	89
4.3.6. Grzechy pokrewne	90
4.4. Wykrywanie grzechu	91

4.5.	Wykrywanie grzechu podczas analizy kodu programu	91
4.6.	Techniki testowania wykrywające grzech	92
4.7.	Przykłady grzechu	94
4.7.1.	CAN-2004-0348	94
4.7.2.	CAN-2005-0554	95
4.8.	Postanowienie poprawy	95
4.8.1.	Weryfikowanie wszystkich danych wejściowych	95
4.8.2.	Bezwzględne niekorzystanie z konkatowania napisów podczas konstruowania instrukcji SQL	95
4.8.3.	Poprawa PHP 5.0 i MySQL 4.1 i nowszych	96
4.8.4.	Poprawa Perl/CGI	97
4.8.5.	Poprawa Javy wykorzystującej JDBC	98
4.8.6.	Poprawa ColdFusion	99
4.8.7.	Poprawa SQL	99
4.9.	Specjalne środki ochronne	100
4.10.	Materiały dodatkowe	100
4.11.	Rachunek sumienia	101

Grzech V

Wklucia w polecenia	103
5.1. Omówienie grzechu	104
5.2. Grzeszne języki programowania	104
5.3. Objasnienie grzechu	104
5.3.1. Grzechy pokrewne	106
5.4. Wykrywanie grzechu	107
5.5. Wykrywanie grzechu podczas analizy kodu programu	107
5.6. Techniki testowania wykrywające grzech	108
5.7. Przykłady grzechu	109
5.7.1. CAN-2001-1187	109
5.7.2. CAN-2002-0652	110
5.8. Postanowienie poprawy	110
5.8.1. Weryfikowanie danych	111
5.8.2. Postępowanie z niepoprawnymi danymi	113
5.9. Specjalne środki ochronne	114
5.10. Materiały dodatkowe	114
5.11. Rachunek sumienia	115

Grzech VI	
Niewłaściwa obsługa błędów	117
6.1. Omówienie grzechu	118
6.2. Grzeszne języki programowania	118
6.3. Objąsnienie grzechu	118
6.3.1. Zwracanie zbyt dużej ilości informacji	119
6.3.2. Ignorowanie błędów	119
6.3.3. Niewłaściwe interpretowanie błędów	120
6.3.4. Bezużyteczne wartości błędne	120
6.3.5. Obsługiwanie niewłaściwych wyjątków	120
6.3.6. Obsługiwanie wszystkich wyjątków	121
6.3.7. Grzeszne C/C++	121
6.3.8. Grzeszne C/C++ w Windows	122
6.3.9. Grzeszny C++	123
6.3.10. Grzeszne C#, VB.NET i Java	123
6.3.11. Grzechy pokrewne	124
6.4. Wykrywanie grzechu	124
6.5. Wykrywanie grzechu podczas analizy kodu programu	124
6.6. Techniki testowania wykrywające grzech	125
6.7. Przykłady grzechu	125
6.7.1. CAN-2004-0077 Linux Kernel do_mremap	125
6.8. Postanowienie poprawy	126
6.8.1. Poprawa C/C++	126
6.8.2. Poprawa C#, VB.NET i Javy	127
6.9. Materiały dodatkowe	127
6.10. Rachunek sumienia	128

Grzech VII	
Skrypty międzyserwisowe	129
7.1. Omówienie grzechu	130
7.2. Grzeszne języki programowania	130
7.3. Objąsnienie grzechu	130
7.3.1. Grzeszne aplikacje lub filtry ISAPI C/C++	131
7.3.2. Grzeszne ASP	132
7.3.3. Grzeszne formularze ASP.NET	132
7.3.4. Grzeszne JSP	132

7.3.5.	Grzeszne PHP	132
7.3.6.	Grzeszny CGI wykorzystujący Perl	133
7.3.7.	Grzeszny mod_perl	133
7.4.	Wykrywanie grzechu	133
7.5.	Wykrywanie grzechu podczas analizy kodu programu	134
7.6.	Techniki testowania wykrywające grzech	135
7.7.	Przykłady grzechu	136
7.7.1.	Zagrożenia skryptów międzyserwisowych i wkląć w HTML IBM Lotus Domino	136
7.7.2.	Błędy weryfikacji danych wejściowych „isqlplus” serwera Oracle HTTP pozwalające na przeprowadzanie ataków skryptów międzyserwisowych	136
7.7.3.	CVE-2002-0840	137
7.8.	Postanowienie poprawy	137
7.8.1.	Poprawa ISAPI C/C++	137
7.8.2.	Poprawa ASP	138
7.8.3.	Poprawa formularzy ASP.NET	139
7.8.4.	Poprawa JSP	139
7.8.5.	Poprawa PHP	142
7.8.6.	Poprawa CGI	142
7.8.7.	Poprawa mod_perla	143
7.8.8.	Uwaga na temat kodowania HTML	143
7.9.	Specjalne środki ochronne	144
7.10.	Materiały dodatkowe	144
7.11.	Rachunek sumienia	145

Grzech VIII

Niewłaściwa ochrona ruchu sieciowego	147
8.1. Omówienie grzechu	148
8.2. Grzeszne języki programowania	148
8.3. Objasnienie grzechu	149
8.3.1. Grzechy pokrewne	151
8.4. Wykrywanie grzechu	151
8.5. Wykrywanie grzechu podczas analizy kodu programu	152
8.6. Techniki testowania wykrywające grzech	155
8.7. Przykłady grzechu	156
8.7.1. TCP/IP	156

8.7.2.	Protokoły pocztowe	156
8.7.3.	E*Trade	157
8.8.	Postanowienie poprawy	157
8.8.1.	Zalecenia niskopoziomowe	158
8.9.	Specjalne środki ochronne	161
8.10.	Materiały dodatkowe	161
8.11.	Rachunek sumienia	161

Grzech IX

Magiczne adresy URL i ukryte pola formularzy	163
9.1. Omówienie grzechu	164
9.2. Grzeszne języki programowania	164
9.3. Objasnienie grzechu	164
9.3.1. Magiczne adresy URL	164
9.3.2. Ukryte pola formularzy	165
9.3.3. Grzechy pokrewne	166
9.4. Wykrywanie grzechu	166
9.5. Wykrywanie grzechu podczas analizy kodu programu	166
9.6. Techniki testowania wykrywające grzech	167
9.7. Przykłady grzechu	168
9.7.1. CAN-2000-1001	168
9.7.2. Modyfikowania ukrytego pola formularza MaxWebPortal	169
9.8. Postanowienie poprawy	169
9.8.1. Napastnicy wyświetlający dane	170
9.8.2. Napastnicy powtarzający dane	170
9.8.3. Napastnicy odgadujący dane	172
9.8.4. Napastnicy zmieniający dane	174
9.9. Specjalne środki ochronne	175
9.10. Materiały dodatkowe	175
9.11. Rachunek sumienia	175

Grzech X

Nieprawidłowe korzystanie z SSL i TLS	177
10.1. Omówienie grzechu	178
10.2. Grzeszne języki programowania	178

10.3.	Objaśnienie grzechu	179
10.3.1.	Grzechy pokrewne	182
10.4.	Wykrywanie grzechu	183
10.5.	Wykrywanie grzechu podczas analizy kodu programu	183
10.6.	Techniki testowania wykrywające grzech	185
10.7.	Przykłady grzechu	186
10.7.1.	Klienty poczty elektronicznej	186
10.7.2.	Przeglądarka Safari	186
10.7.3.	Proxy SSL Stunnel	187
10.8.	Postanowienie poprawy	188
10.8.1.	Wybieranie wersji protokołów	188
10.8.2.	Wybieranie pakietów szyfrujących	189
10.8.3.	Zapewnianie weryfikacji certyfikatów	190
10.8.4.	Weryfikowanie nazw hostów	192
10.8.5.	Sprawdzanie unieważnień certyfikatów	193
10.9.	Specjalne środki ochronne	195
10.10.	Materiały dodatkowe	196
10.11.	Rachunek sumienia	196

Grzech XI

Słabości systemów chronionych hasłami.....	197
11.1. Omówienie grzechu	198
11.2. Grzeszne języki programowania	198
11.3. Objasnienie grzechu	198
11.3.1. Grzechy pokrewne	201
11.4. Wykrywanie grzechu	201
11.5. Wykrywanie grzechu podczas analizy kodu programu	201
11.5.1. Założenia systemowe dotyczące treści hasel	201
11.5.2. Zmienianie i reinicjalizowanie hasel	202
11.5.3. Protokoły obsługi hasel	202
11.5.4. Przetwarzanie i przechowywanie hasel	203
11.6. Techniki testowania wykrywające grzech	204
11.7. Przykłady grzechu	204
11.7.1. CVE-2005-1505	205
11.7.2. CVE-2005-0432	205
11.7.3. Błąd TENEX-a	205
11.7.4. Włamanie do telefonu Paris Hilton	206

11.8.	Postanowienie poprawy	207
11.8.1.	Różne metody uwierzytelnienia	207
11.8.2.	Przechowywanie i sprawdzanie haseł	207
11.8.3.	Wskazówki dotyczące wyboru protokołów	211
11.8.4.	Wskazówki dotyczące reinicjalizowania haseł	212
11.8.5.	Wskazówki dotyczące wyboru haseł	213
11.8.6.	Inne wskazówki	214
11.9.	Specjalne środki ochronne	214
11.10.	Materiały dodatkowe	215
11.11.	Rachunek sumienia	215

Grzech XII

Niewłaściwa ochrona przechowywanych danych	217
12.1. Omówienie grzechu	218
12.2. Grzeszne języki programowania	218
12.3. Objasnienie grzechu	218
12.3.1. Słaba kontrola dostępu „chroniąca” poufne dane	218
12.3.2. Grzeszna kontrola dostępu	220
12.3.3. Osadzanie tajnych danych w kodzie	223
12.3.4. Grzechy pokrewne	223
12.4. Wykrywanie grzechu	224
12.5. Wykrywanie grzechu podczas analizy kodu programu	224
12.6. Techniki testowania wykrywające grzech	226
12.7. Przykłady grzechu	228
12.7.1. CVE-2000-0100	228
12.7.2. CAN-2002-1590	229
12.7.3. CVE-1999-0886	229
12.7.4. CAN-2004-0311	229
12.7.5. CAN-2004-0391	229
12.8. Postanowienie poprawy	230
12.8.1. Korzystanie z zabezpieczeń systemów operacyjnych	231
12.8.2. Poprawa C/C++ w Windows 2000 i nowszych	231
12.8.3. Poprawa ASP.NET 1.1 i nowszych	233
12.8.4. Poprawa C# w .NET Framework 2.0	233
12.8.5. Poprawa C/C++ w Mac OS X v10.2 i nowszych	234

12.8.6.	Poprawa bez korzystania z mechanizmów systemów operacyjnych (czyli bezpieczne przechowywanie poufnych danych)	235
12.8.7.	Uwaga na temat Javy i klasy KeyStore	238
12.9.	Specjalne środki ochronne	239
12.10.	Materiały dodatkowe	240
12.11.	Rachunek sumienia	241

Grzech XIII

Wpływ informacji	243
13.1. Omówienie grzechu	244
13.2. Grzeszne języki programowania	244
13.3. Objasnienie grzechu	245
13.3.1. Kanały wypływu	245
13.3.2. Zbyt wiele informacji	246
13.3.3. Model zabezpieczeń przepływu informacji	249
13.3.4. Grzeszny C# (i dowolny inny język)	251
13.3.5. Grzechy pokrewne	251
13.4. Wykrywanie grzechu	252
13.5. Wykrywanie grzechu podczas analizy kodu programu	252
13.6. Techniki testowania wykrywające grzech	253
13.6.1. Skradzione komputery przenośne	254
13.7. Przykłady grzechu	254
13.7.1. Atak czasowy Dana Bernsteina na algorytm AES	254
13.7.2. CAN-2005-1411	255
13.7.3. CAN-2005-1133	255
13.8. Postanowienie poprawy	256
13.8.1. Poprawa C# (i innych języków)	257
13.8.2. Poprawa rozgłaszania informacji w sieci	257
13.9. Specjalne środki ochronne	258
13.10. Materiały dodatkowe	258
13.11. Rachunek sumienia	258

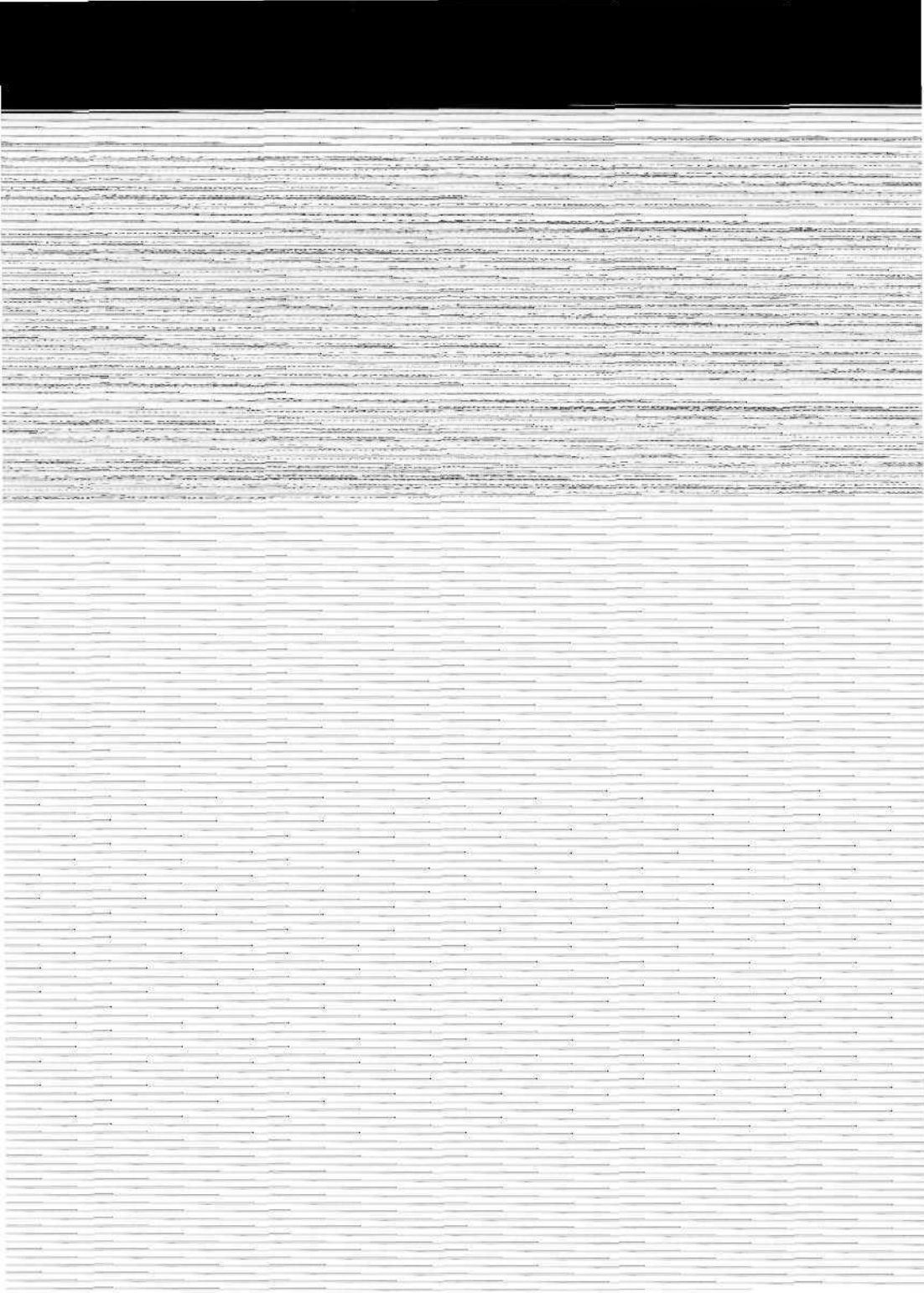
Grzech XIV

Nieprawidłowy dostęp do plików	261
14.1. Omówienie grzechu	262
14.2. Grzeszne języki programowania	262

14.3.	Objaśnienie grzechu	263
14.3.1.	Grzeszne C/C++ w Windows	263
14.3.2.	Grzeszne C/C++	264
14.3.3.	Grzeszny Perl	264
14.3.4.	Grzeszny Python	264
14.3.5.	Grzechy pokrewne	265
14.4.	Wykrywanie grzechu	265
14.5.	Wykrywanie grzechu podczas analizy kodu programu	265
14.6.	Techniki testowania wykrywające grzech	266
14.7.	Przykłady grzechu	267
14.7.1.	CAN-2005-0004	267
14.7.2.	CAN-2005-0799	267
14.7.3.	CAN-2004-0452 i CAN-2004-0448	268
14.7.4.	CVE-2004-0115 – Microsoft Virtual PC dla komputerów Macintosh	268
14.8.	Postanowienie poprawy	268
14.8.1.	Poprawa Perla	269
14.8.2.	Poprawa C/C++ w systemach unixowych	269
14.8.3.	Poprawa C/C++ w Windows	270
14.8.4.	Uzyskiwanie informacji o lokalnym folderze tymczasowym użytkownika	270
14.8.5.	Poprawa kodu .NET	270
14.9.	Specjalne środki ochronne	271
14.10.	Materiały dodatkowe	271
14.11.	Rachunek sumienia	272

Grzech XV

Ufanie rozstrzygnięciu nazw sieciowych	273
15.1. Omówienie grzechu	274
15.2. Grzeszne języki programowania	274
15.3. Objasnienie grzechu	275
15.3.1. Grzeszne aplikacje	277
15.3.2. Grzechy pokrewne	278
15.4. Wykrywanie grzechu	278
15.5. Wykrywanie grzechu podczas analizy kodu programu	279
15.6. Techniki testowania wykrywające grzech	279



17.7.2.	CAN-2004-0155	302
17.8.	Postanowienie poprawy	303
17.9.	Specjalne środki ochronne	303
17.10.	Materiały dodatkowe	304
17.11.	Rachunek sumienia	304

Grzech XVIII

Silnie kryptograficzne liczby losowe	305
18.1. Omówienie grzechu	306
18.2. Grzeszne języki programowania	306
18.3. Objasnienie grzechu	306
18.3.1. Grzeszne generatory niekryptograficzne liczb pseudolosowych	307
18.3.2. Grzeszne generatory kryptograficzne liczb pseudolosowych	308
18.3.3. Grzeszne generatory liczb losowych	309
18.3.4. Grzechy pokrewne	309
18.4. Wykrywanie grzechu	310
18.5. Wykrywanie grzechu podczas analizy kodu programu	310
18.5.1. Określanie potrzeby używania liczb losowych	310
18.5.2. Znajdowanie źródeł liczb pseudolosowych	310
18.5.3. Kontrolowanie poprawnego inicjalizowania generatorów kryptograficznych	311
18.6. Techniki testowania wykrywające grzech	312
18.7. Przykłady grzechu	313
18.7.1. Przeglądarka Netscape	313
18.7.2. Problemy OpenSSL-a	313
18.8. Postanowienie poprawy	314
18.8.1. Windows	314
18.8.2. Kod .NET	314
18.8.3. Unix	315
18.8.4. Java	316
18.8.5. Powtarzanie ciągów liczb	317
18.9. Specjalne środki ochronne	317
18.10. Materiały dodatkowe	317
18.11. Rachunek sumienia	318

Grzech XIX

Czynnik ludzki	319
19.1. Omówienie grzechu	320
19.2. Grzeszne języki programowania	320
19.3. Objaśnienie grzechu	320
19.3.1. Określanie potrzeb użytkowników	321
19.3.2. Pole minowe – informowanie użytkowników o zabezpieczeniach systemu	322
19.3.3. Grzechy pokrewne	323
19.4. Wykrywanie grzechu	323
19.5. Wykrywanie grzechu podczas analizy kodu programu	323
19.6. Techniki testowania wykrywające grzech	324
19.7. Przykłady grzechu	324
19.7.1. Uwierzytelnianie certyfikatów SSL/TLS	325
19.7.2. Instalowanie certyfikatu głównego w przeglądarce Internet Explorer 4.0	325
19.8. Postanowienie poprawy	326
19.8.1. Upraszczenie interfejsu użytkownika	326
19.8.2. Podejmowanie decyzji za użytkowników	327
19.8.3. Ułatwianie wybiórczego rezygnowania z niektórych mechanizmów zabezpieczeń	328
19.8.4. Precyzyjne informowanie o konsekwencjach	329
19.8.5. Umożliwianie wykonywania czynności	332
19.8.6. Zapewnianie centralnego zarządzania	332
19.9. Materiały dodatkowe	332
19.10. Rachunek sumienia	333

Dodatek A

19 grzechów śmiertelnych a klasyfikacja OWASP	335
--	------------

Dodatek B

Rachunek sumienia	337
B.1. Rachunek sumienia dla grzechu przepełnienia buforów	338
B.2. Rachunek sumienia dla grzechu napisów formatujących	338
B.3. Rachunek sumienia dla grzechu nadmiaru całkowitoliczbowego	339
B.4. Rachunek sumienia dla grzechu wkuć w SQL	339
B.5. Rachunek sumienia dla grzechu wkuć w polecenia	340

B.6.	Rachunek sumienia dla grzechu niewłaściwej obsługi błędów	340
B.7.	Rachunek sumienia dla grzechu skryptów międzyserwisowych	341
B.8.	Rachunek sumienia dla grzechu niewłaściwej ochrony ruchu sieciowego	341
B.9.	Rachunek sumienia dla grzechu magicznych adresów URL i ukrytych pól formularzy	342
B.10.	Rachunek sumienia dla grzechu nieprawidłowego korzystania z SSL i TLS	342
B.11.	Rachunek sumienia dla grzechu słabości systemów chronionych hasłami	343
B.12.	Rachunek sumienia dla grzechu niewłaściwej ochrony przechowywanych danych	344
B.13.	Rachunek sumienia dla grzechu wpływu informacji	345
B.14.	Rachunek sumienia dla grzechu nieprawidłowego dostępu do plików	345
B.15.	Rachunek sumienia dla grzechu ufania rozstrzyganiu nazw sieciowych	346
B.16.	Rachunek sumienia dla grzechu problemów ze współbieżnością	346
B.17.	Rachunek sumienia dla grzechu niewierzytelnionej wymiany kluczy	346
B.18.	Rachunek sumienia dla grzechu silnie kryptograficznych liczb losowych	347
B.19.	Rachunek sumienia dla grzechu czynnika ludzkiego	347

Skorowidz	349
------------------------	------------