

УДК 004.4
ББК 32.973.26-018.2
Х68

А

Ховард, Майкл.

Х68 Уязвимости в программном коде и борьба с ними / М. Ховард, Д. Лебланк, Дж. Виега ; пер. с англ. А. А. Слинкина. — 2-е изд., эл. — 1 файл pdf : 289 с. — Москва : ДМК Пресс, 2023. — Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10". — Текст : электронный.

ISBN 978-5-89818-460-5

Эта книга необходима всем разработчикам программного обеспечения, независимо от платформы, языка или вида приложений.

Рассмотрены уязвимости на языках C/C++, C#, Java, Visual Basic, Visual Basic .NET, Perl, Python в операционных системах Windows, Unix, Linux, Mac OS, Novell Netware. Авторы издания, Майкл Ховард и Дэвид Лебланк, обучают программистов как писать безопасный код в компании Microsoft. На различных примерах продемонстрированы как сами ошибки, так и способы их исправления и защиты от них.

Если вы — программист, то вам просто необходимо прочесть эту книгу.

УДК 004.4
ББК 32.973.26-018.2

Электронное издание на основе печатного издания: Уязвимости в программном коде и борьба с ними / М. Ховард, Д. Лебланк, Дж. Виега ; пер. с англ. А. А. Слинкина. — Москва : ДМК Пресс, 2011. — 288 с. — ISBN 978-5-94074-240-1. — Текст : непосредственный.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

В соответствии со ст. 1299 и 1301 ГК РФ при устранении ограничений, установленных техническими средствами защиты авторских прав, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации.

ISBN 978-5-89818-460-5

© Перевод на русский язык, оформление,
издание, ДМК Пресс, 2011

А

Содержание

Об авторах	18
О научных редакторах	19
Предисловие	20
Благодарности	22
Введение	23
Структура книги	24
Кому предназначена эта книга	25
Какие главы следует прочитать	25
Грех 1. Переполнение буфера	26
В чем состоит грех	26
Подверженные греху языки	27
Как происходит грехопадение	27
Греховность C/C++	31
Родственные грехи	33
Где искать ошибку	33
Выявление ошибки на этапе анализа кода	33
Тестирование	34
Примеры из реальной жизни	35
CVE-1999-0042	35
CVE-2000-0389 – CVE-2000-0392	35
CVE-2002-0842, CVE-2003-0095, CAN-2003-0096	35
CAN-2003-0352	36
Искупление греха	37
Замена опасных функций работы со строками	37
Следите за выделениями памяти	37
Проверьте циклы и доступ к массивам	37
Пользуйтесь строками в стиле C++, а не C	37
Пользуйтесь STL-контейнерами вместо статических массивов	38

Пользуйтесь инструментами анализа	38
Дополнительные защитные меры	38
Защита стека	39
Запрет исполнения в стеке и куче	39
Другие ресурсы	39
Резюме	40
Грех 2. Ошибки, связанные с форматной строкой	42
В чем состоит грех	42
Подверженные греху языки	42
Как происходит грехопадение	43
Греховность C/C++	45
Родственные грехи	45
Где искать ошибку	46
Выявление ошибки на этапе анализа кода	46
Тестирование	46
Примеры из реальной жизни	47
CVE-2000-0573	47
CVE-2000-0844	47
Искупление греха	47
Искупление греха в C/C++	48
Дополнительные защитные меры	48
Другие ресурсы	48
Резюме	48
Грех 3. Переполнение целых чисел	49
В чем состоит грех	49
Подверженные греху языки	49
Как происходит грехопадение	49
Греховность C и C++	50
Поразрядные операции	55
Греховность C#	55
Греховность Visual Basic и Visual Basic .NET	56
Греховность Java	57
Греховность Perl	58
Где искать ошибку	59
Выявление ошибки на этапе анализа кода	59
C/C++	59
C#	61
Java	62
Visual Basic и Visual Basic .NET	62

Perl	62
Тестирование	62
Примеры из реальной жизни	62
Ошибка в интерпретаторе Windows Script позволяет выполнить произвольный код	63
Переполнение целого в конструкторе объекта SOAPParameter	63
Переполнение кучи в HTR-документе, передаваемом поблочно, может скомпрометировать Web-сервер	63
Искупление греха	64
Дополнительные защитные меры	66
Другие ресурсы	66
Резюме	66
Не рекомендуется	66
Грех 4. Внедрение SQL-команд	67
В чем состоит грех	67
Подверженные греху языки	67
Как происходит грехопадение	68
Греховность C#	68
Греховность PHP	69
Греховность Perl/CGI	69
Греховность Java	70
Греховность SQL	71
Родственные грехи	72
Где искать ошибку	72
Выявление ошибки на этапе анализа кода	72
Тестирование	73
Примеры из реальной жизни	75
CAN-2004-0348	75
CAN-2002-0554	75
Искупление греха	75
Проверяйте все входные данные	76
Никогда не применяйте конкатенацию для построения SQL-предложений	76
Дополнительные защитные меры	79
Другие ресурсы	79
Резюме	80
Грех 5. Внедрение команд	82
В чем состоит грех	82

Подверженные греху языки	82
Как происходит грехопадение	82
Родственные грехи	84
Где искать ошибку	84
Выявление ошибки на этапе анализа кода	84
Тестирование	86
Примеры из реальной жизни	86
CAN-2001-1187	86
CAN-2002-0652	87
Искупление греха	87
Контроль данных	87
Если проверка не проходит	90
Дополнительные защитные меры	90
Другие ресурсы	91
Резюме	91
Грех 6. Пренебрежение обработкой ошибок	92
В чем состоит грех	92
Подверженные греху языки	92
Как происходит грехопадение	92
Раскрытие излишней информации	92
Игнорирование ошибок	93
Неправильная интерпретация ошибок	93
Бесполезные возвращаемые значения	94
Обработка не тех исключений, что нужно	94
Обработка всех исключений	94
Греховность C/C++	94
Греховность C/C++ в Windows	95
Греховность C++	96
Греховность C#, VB.NET и Java	96
Родственные грехи	97
Где искать ошибку	97
Выявление ошибки на этапе анализа кода	97
Тестирование	97
Примеры из реальной жизни	98
CAN-2004-0077 do_mremap в ядре Linux	98
Искупление греха	98
Искупление греха в C/C++	98
Искупление греха в C#, VB.NET и Java	99
Другие ресурсы	99
Резюме	100

Грех 7. Кросс-сайтовые сценарии	101
В чем состоит грех	101
Подверженные греху языки	101
Как происходит грехопадение	101
Греховное ISAPI-расширение или фильтр на C/C++	102
Греховность ASP	103
Греховность форм ASP.NET	103
Греховность JSP	103
Греховность PHP	103
Греховность Perl-модуля CGI.pm	103
Греховность mod-perl	104
Где искать ошибку	104
Выявление ошибки на этапе анализа кода	104
Тестирование	105
Примеры из реальной жизни	106
Уязвимость IBM Lotus Domino для атаки с кросс-сайтовым сценарием и внедрением HTML	106
Ошибка при контроле входных данных в сценарии isqlplus, входящем в состав Oracle HTTP Server, позволяет удаленному пользователю провести атаку с кросс-сайтовым сценарием	106
CVE-2002-0840	107
Искупление греха	107
Искупление греха в ISAPI-расширениях и фильтрах на C/C++	107
Искупление греха в ASP	108
Искупление греха в ASP.NET	108
Искупление греха в JSP	108
Искупление греха в PHP	110
Искупление греха в Perl/CGI	110
Искупление греха в mod-perl	111
Замечание по поводу HTML-кодирования	111
Дополнительные защитные меры	112
Другие ресурсы	112
Резюме	113
Грех 8. Пренебрежение защитой сетевого трафика	114
В чем состоит грех	114
Подверженные греху языки	114
Как происходит грехопадение	115
Родственные грехи	117

Где искать ошибку	117
Выявление ошибки на этапе анализа кода	118
Тестирование	121
Примеры из реальной жизни	121
TCP/IP	121
Протоколы электронной почты	122
Протокол E*Trade	122
Искупление греха	122
Рекомендации низкого уровня	123
Дополнительные защитные меры	126
Другие ресурсы	126
Резюме	126

Грех 9. Применение загадочных URL и скрытых полей форм

В чем состоит грех	128
Подверженные греху языки	128
Как происходит грехопадение	128
Загадочные URL	128
Скрытые поля формы	129
Родственные грехи	129
Где искать ошибку	130
Выявление ошибки на этапе анализа кода	130
Тестирование	131
Примеры из реальной жизни	131
CAN-2000-1001	132
Модификация скрытого поля формы в программе MaxWebPortal	132
Искупление греха	132
Противник просматривает данные	132
Противник воспроизводит данные	133
Противник предсказывает данные	135
Противник изменяет данные	136
Дополнительные защитные меры	137
Другие ресурсы	137
Резюме	137

Грех 10. Неправильное применение SSL и TLS

В чем состоит грех	138
Подверженные греху языки	138
Как происходит грехопадение	139

Родственные грехи	142
Где искать ошибку	142
Выявление ошибки на этапе анализа кода	143
Тестирование	144
Примеры из реальной жизни	145
Почтовые клиенты	145
Web-браузер Safari	146
SSL-прокси Stunnel	146
Искупление греха	147
Выбор версии протокола	147
Выбор семейства шифров	148
Проверка сертификата	149
Проверка имени хоста	150
Проверка отзыва сертификата	151
Дополнительные защитные меры	153
Другие ресурсы	153
Резюме	154

Грех 11. Использование слабых систем

на основе паролей	155
В чем состоит грех	155
Подверженные греху языки	155
Как происходит грехопадение	155
Родственные грехи	158
Где искать ошибку	158
Выявление ошибки на этапе анализа кода	158
Политика управления сложностью пароля	158
Смена и переустановка пароля	159
Протоколы проверки паролей	159
Ввод и хранение паролей	160
Тестирование	160
Примеры из реальной жизни	161
CVE-2005-1505	161
CVE-2005-0432	162
Ошибка в TENEX	162
Кража у Пэрис Хилтон	163
Искупление греха	163
Многофакторная аутентификация	163
Хранение и проверка паролей	164
Рекомендации по выбору протокола	167
Рекомендации по переустановке паролей	168

Рекомендации по выбору пароля	169
Прочие рекомендации	170
Дополнительные защитные меры	170
Другие ресурсы	170
Резюме	170
Не рекомендуется	171
Стоит подумать	171

Грех 12. Пренебрежение безопасным хранением

и защитой данных	172
В чем состоит грех	172
Подверженные греху языки	172
Как происходит грехопадение	172
Слабый контроль доступа к секретным данным	172
Греховность элементов управления доступом	174
Встраивание секретных данных в код	176
Родственные грехи	177
Где искать ошибку	177
Выявление ошибки на этапе анализа кода	178
Тестирование	178
Примеры из реальной жизни	181
CVE-2000-0100	181
CAN-2002-1590	181
CVE-1999-0886	181
CAN-2004-0311	182
CAN-2004-0391	182
Искупление греха	182
Использование технологий защиты, предоставляемых операционной системой	183
Искупление греха в C/C++ для Windows 2000 и последующих версий	183
Искупление греха в ASP.NET версии 1.1 и старше	185
Искупление греха в C# на платформе .NET Framework 2.0 ...	185
Искупление греха в C/C++ для Mac OS X версии v10.2 и старше	186
Искупление греха без помощи операционной системы (или «храните секреты от греха подальше»)	186
Замечание по поводу Java и Java KeyStore	188
Дополнительные защитные меры	189
Другие ресурсы	190
Резюме	191

Грех 13. Утечка информации	192
В чем состоит грех	192
Подверженные греху языки	192
Как происходит грехопадение	193
Побочные каналы	193
Слишком много информации!	194
Модель безопасности информационного потока	196
Греховность C# (и других языков)	198
Родственные грехи	198
Где искать ошибку	199
Выявление ошибки на этапе анализа кода	199
Тестирование	200
Имитация кражи ноутбука	200
Примеры из реальной жизни	200
Атака с хронометражем Дэна Бернстайна на шифр AES	201
CAN-2005-1411	201
CAN-2005-1133	201
Искупление греха	202
Искупление греха в C# (и других языках)	203
Учет локальности	203
Дополнительные защитные меры	203
Другие ресурсы	204
Резюме	204
Грех 14. Некорректный доступ к файлам	206
В чем состоит грех	206
Подверженные греху языки	206
Как происходит грехопадение	207
Греховность C/C++ в Windows	207
Греховность C/C++	208
Греховность Perl	208
Греховность Python	208
Родственные грехи	209
Где искать ошибку	209
Выявление ошибки на этапе анализа кода	209
Тестирование	210
Примеры из реальной жизни	210
CAN-2005-0004	210
CAN-2005-0799	211
CAN-2004-0452 и CAN-2004-0448	211
CVE-2004-0115 Microsoft Virtual PC для Macintosh	211

Искупление греха	211
Искупление греха в Perl	212
Искупление греха в C/C++ для Unix	212
Искупление греха в C/C++ для Windows	213
Получение места нахождения временного каталога пользователя	213
Искупление греха в .NET	213
Дополнительные защитные меры	214
Другие ресурсы	214
Резюме	214

Грех 15. Излишнее доверие к системе разрешения

сетевых имен	215
В чем состоит грех	215
Подверженные греху языки	215
Как происходит грехопадение	215
Греховные приложения	218
Родственные грехи	218
Где искать ошибку	219
Выявление ошибки на этапе анализа кода	219
Тестирование	220
Примеры из реальной жизни	220
CVE-2002-0676	220
CVE-1999-0024	221
Искупление греха	221
Другие ресурсы	222
Резюме	223

Грех 16. Гонки

В чем состоит грех	224
Подверженные греху языки	224
Как происходит грехопадение	224
Греховность кода	226
Родственные грехи	227
Где искать ошибку	227
Выявление ошибки на этапе анализа кода	228
Тестирование	229
Примеры из реальной жизни	229
CVE-2001-1349	229
CAN-2003-1073	230
CVE-2004-0849	230

Искупление греха	230
Дополнительные защитные меры	232
Другие ресурсы	232
Резюме	233
Грех 17. Неаутентифицированный обмен ключами	234
В чем состоит грех	234
Подверженные греху языки	234
Как происходит грехопадение	234
Родственные грехи	236
Где искать ошибку	236
Выявление ошибки на этапе анализа кода	236
Тестирование	237
Примеры из реальной жизни	237
Атака с «человеком посередине» на Novell Netware	237
CAN-2004-0155	238
Искупление греха	238
Дополнительные защитные меры	239
Другие ресурсы	239
Резюме	239
Грех 18. Случайные числа криптографического качества	240
В чем состоит грех	240
Подверженные греху языки	240
Как происходит грехопадение	240
Греховность некриптографических генераторов	241
Греховность криптографических генераторов	242
Греховность генераторов истинно случайных чисел	242
Родственные грехи	243
Где искать ошибку	243
Выявление ошибки на этапе анализа кода	244
Когда следует использовать случайные числа	244
Выявление мест, где применяются PRNG-генераторы	244
Правильно ли затравлен CRNG-генератор	245
Тестирование	245
Примеры из реальной жизни	246
Браузер Netscape	246
Проблемы в OpenSSL	246
Искупление греха	247



Windows	247
Код для .NET	248
Unix	248
Java	249
Повторное воспроизведение потока случайных чисел	250
Дополнительные защитные меры	250
Другие ресурсы	250
Резюме	251
Стоит подумать	251
Грех 19. Неудобный интерфейс	252
В чем состоит грех	252
Подверженные греху языки	252
Как происходит грехопадение	252
Каков круг ваших пользователей?	253
Минное поле: показ пользователям информации о безопасности	254
Родственные грехи	254
Где искать ошибку	255
Выявление ошибки на этапе анализа кода	255
Тестирование	255
Примеры из реальной жизни	256
Аутентификация сертификата в протоколе SSL/TLS	256
Установка корневого сертификата в Internet Explorer 4.0	257
Искупление греха	257
Делайте интерфейс пользователя простым и понятным	258
Принимайте за пользователей решения, касающиеся безопасности	258
Упрощайте избирательное ослабление политики безопасности	259
Ясно описывайте последствия	260
Помогайте пользователю предпринять действия	262
Предусматривайте централизованное управление	263
Другие ресурсы	263
Резюме	264
Приложение А. Соответствие между 19 смертными грехами и «10 ошибками» OWASP	265
Приложение В. Сводка рекомендаций	266
Предметный указатель	276