

Безопасность ASP. NET Core



Кристиан Венц

 MANNING


ИЗДАТЕЛЬСТВО

DOT
NET
.RU

Защитите свои приложения ASP.NET, прежде чем вас взломают!

Приложения ASP.NET Core подвержены риску атак. Существуют конкретные меры, которые помогут избежать взлома.

В книге показаны такие методы защиты веб-приложений ASP.NET Core, как безопасное взаимодействие с браузером, распознавание и предотвращение распространенных угроз, развертывание уникальных API безопасности этого фреймворка. Приводятся способы написания безопасного кода и примеры с аннотациями, а также полное описание встроенных инструментов безопасности ASP.NET Core. Рассматриваются реальные нарушения в системе безопасности, включая мошеннические расширения Firefox и кражу паролей в Adobe.

Вы научитесь:

- использовать инструменты и библиотеки для тестирования и сканирования;
- активировать встроенные механизмы безопасности браузеров из ASP.NET;
- пользоваться преимуществами API безопасности .NET и ASP.NET Core;
- управлять паролями, чтобы свести к минимуму ущерб от утечки данных;
- надежно хранить секретные данные приложения.

Для опытных веб-разработчиков ASP.NET Core.

Кристиан Венц — пионер интернета, консультант и предприниматель.

Интернет-магазин: www.dmkpress.com

Оптовая продажа: КТК «Галактика»
books@aliants-kniga.ru



«Лучшая книга по безопасности ASP.NET, которую я нашел!»

*Том Гет,
Binary Star Technology*

«Ясно и подробно. Эта книга доставляет удовольствие, и я настоятельно рекомендую ее как новичкам, так и продвинутым разработчикам».

Ник Римингтон, Spindogs

«Пишите безопасный код, думая о том, как другие попытаются его взломать».

Марчин Сенк, e-Xim IT

ISBN 978-5-93700-176-4



9 785937 001764 >

Кристиан Венц

Безопасность ASP.NET Core

ASP.NET Core Security

CHRISTIAN WENZ



MANNING
Shelter Island

Безопасность ASP.NET Core

КРИСТИАН ВЕНЦ



Москва, 2023

УДК 004.04
ББК 32.372
В29

Венц К.
В29 Безопасность ASP.NET Core / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2023. – 386 с.: ил.

ISBN 978-5-97060-176-4

В книге рассматриваются методы защиты веб-приложений ASP.NET Core: безопасное взаимодействие с браузером, распознавание и предотвращение распространенных угроз, развертывание уникальных API безопасности этого фреймворка. Приводятся способы написания безопасного кода и примеры с аннотациями, а также полное описание встроенных инструментов безопасности ASP.NET Core. Обсуждаются реальные нарушения в системе безопасности, включая мошеннические расширения Firefox и кражу паролей в Adobe. В универсальных рекомендациях по обеспечению безопасности учтены уникальные потребности приложений ASP.NET Core.

Книга адресована опытным разработчикам ASP.NET Core.

УДК 004.04
ББК 32.372

Copyright © DМК Press 2023. Authorized translation of the English edition © 2022 Manning Publications. This translation is published and sold by permission of Manning Publications, the owner of all rights to publish and sell the same.

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.

ISBN 978-1-6334-3998-6 (англ.)
ISBN 978-5-97060-176-4 (рус.)

© Manning Publications, 2022
© Перевод, оформление, издание, ДМК Пресс, 2023

Оглавление

Часть I ПЕРВЫЕ ШАГИ	20
1 ■ О безопасности веб-приложений.....	21
Часть II НЕЙТРАЛИЗАЦИЯ РАСПРОСТРАНЕННЫХ АТАК	35
2 ■ Межсайтовый скриптинг.....	36
3 ■ Атака на управление сессиями	74
4 ■ Межсайтовая подделка запросов	93
5 ■ Данные, не прошедшие валидацию	121
6 ■ Внедрение SQL-кода (и другие виды внедрений)	142
Часть III БЕЗОПАСНОЕ ХРАНЕНИЕ ДАННЫХ	156
7 ■ Хранение секретных данных.....	157
8 ■ Работа с паролями.....	185
Часть IV КОНФИГУРИРОВАНИЕ	208
9 ■ HTTP-заголовки.....	209
10 ■ Обработка ошибок	224
11 ■ Журналирование и проверка работоспособности	236
Часть V АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ	256
12 ■ Защита веб-приложений с помощью ASP.NET Core Identity	257
13 ■ Защита API и одностраничных приложений.....	291
Часть VI БЕЗОПАСНОСТЬ КАК ПРОЦЕСС	338
14 ■ Безопасные зависимости	339
15 ■ Инструменты аудита	350
16 ■ OWASP Top 10	369

Содержание

<i>Вступительное слово от сообщества</i>	11
<i>Введение</i>	12
<i>Об этой книге</i>	14
<i>Об авторе</i>	18
<i>Об иллюстрации на обложке</i>	19

Часть I ПЕРВЫЕ ШАГИ 20

1	О безопасности веб-приложений	21
1.1	ASP.NET Core: история и фреймворки	22
1.1.1	История версий ASP.NET Core	23
1.1.2	MVC.....	23
1.1.3	Razor Pages	26
1.1.4	Веб-API	27
1.1.5	Blazor.....	29
1.2	Выявление и нейтрализация угроз.....	30
1.2.1	Компоненты веб-приложений.....	30
1.2.2	Эшелонированная защита	32
1.3	API, предназначенные для выполнения функций безопасности.....	33
1.4	Безопасность важна.....	33
	Резюме	34

Часть II НЕЙТРАЛИЗАЦИЯ РАСПРОСТРАНЕННЫХ АТАК 35

2	Межсайтовый скриптинг	36
2.1	Анатомия атаки с использованием межсайтового скриптинга.....	37

2.2	Предотвращение межсайтового скриптинга	44
2.2.1	Правило ограничения домена	44
2.2.2	Экранирование HTML	46
2.2.3	Экранирование в другом контексте.....	50
2.3	Политика безопасности контента.....	53
2.3.1	Пример приложения	54
2.3.2	Как работает CSP	55
2.3.3	Рефакторинг приложений для CSP	57
2.3.4	Рекомендации по CSP	65
2.3.5	Функциональные возможности CSP третьего уровня.....	68
2.4	Дополнительные меры безопасности, предоставляемые браузерами	70
	Резюме	73
3	Атака на управление сессиями	74
3.1	Анатомия атаки	75
3.1.1	Кража сеансовых файлов cookie	77
3.1.2	Файлы cookie и управление сессиями	78
3.2	Файлы cookie и параметры сессий ASP.NET Core	81
3.3	Поддержка протокола HTTPS	85
3.4	Обнаружение перехвата сессий.....	90
	Резюме	91
4	Межсайтовая подделка запросов.....	93
4.1	Анатомия межсайтовой подделки запросов	94
4.2	Меры противодействия для защиты от межсайтовой подделки запросов.....	102
4.2.1	Делаем HTTP-запрос непредсказуемым.....	102
4.2.2	Защита сеансового файла cookie	106
4.3	Кликджекинг	108
4.4	Совместное использование ресурсов между разными источниками.....	112
	Резюме	119
5	Данные, не прошедшие валидацию	121
5.1	Взгляд на HTTP	122
5.2	Валидация в ASP.NET Core	126
5.3	Массовое переназначение параметров	130
5.4	Безопасная десериализация.....	137
	Резюме	141
6	Внедрение SQL-кода (и другие виды внедрений)	142
6.1	Анатомия атаки с использованием внедрения SQL-кода.....	143
6.2	Подготовленные инструкции.....	146
6.3	Entity Framework Core.....	149

6.4	Внешние сущности XML	151
6.5	Другие виды внедрений	153
	Резюме	154

Часть III БЕЗОПАСНОЕ ХРАНЕНИЕ ДАННЫХ 156

7	Хранение секретных данных	157
7.1	О шифровании	158
7.2	Secret Manager	161
7.3	Файл appsettings.json	164
7.4	Хранение секретов в облаке	167
7.4.1	Хранение секретов в Azure	168
7.4.2	Хранение секретов в AWS	172
7.4.3	Хранение секретов в Google Cloud	174
7.5	Использование API, обеспечивающего защиту данных	177
7.6	Локальное хранение секретов с помощью Blazor	181
	Резюме	184

8	Работа с паролями	185
8.1	От утечки данных до кражи паролей	186
8.2	Реализация хеширования паролей	190
8.2.1	MD5 (и почему не стоит его использовать)	192
8.2.2	PBKDF2	195
8.2.3	Argon2	199
8.2.4	bcrypt	201
8.2.5	bcrypt	202
8.3	Анализ шаблонов ASP.NET Core	204
	Резюме	207

Часть IV КОНФИГУРИРОВАНИЕ 208

9	HTTP-заголовки	209
9.1	Соккрытие информации о сервере	211
9.2	Заголовки безопасности браузера	213
9.2.1	Заголовок Referrer-Policy	214
9.2.2	Заголовки Feature-Policy и Permissions-Policy	217
9.2.3	Предотвращение сканирования содержимого файла	218
9.2.4	Политики CORS	220
9.2.5	Дополнительные заголовки	221
	Резюме	223

10	Обработка ошибок	224
10.1	Страницы ошибок для веб-приложений	225
10.1.1	Собственные страницы ошибок	227

10.1.2	Страницы ошибок для заданных кодов состояния	230
10.2	Обработка ошибок в API	232
	Резюме	235

11	Журналирование и проверка работоспособности	236
11.1	Проверка работоспособности	237
11.1.1	Настройка проверки работоспособности	237
11.1.2	Расширенная проверка работоспособности	240
11.1.3	Форматирование вывода	242
11.1.4	Пользовательский интерфейс проверки работоспособности	243
11.2	Журналирование	247
11.2.1	Создание записей журнала	248
11.2.2	Уровни сообщения журнала	250
11.2.3	Области журналирования	252
	Резюме	255

Часть V АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ

12	Защита веб-приложений с помощью ASP.NET Core Identity	257
12.1	Настройка ASP.NET Core Identity	258
12.2	Основы ASP.NET Core Identity	262
12.3	Расширенные возможности ASP.NET Core Identity	271
12.3.1	Параметры пароля	272
12.3.2	Параметры файлов cookie	274
12.3.3	Блокировка пользователей	275
12.3.4	Работа с утверждениями	276
12.3.5	Двухфакторная аутентификация	279
12.3.6	Аутентификация с внешними поставщиками	284
	Резюме	289

13	Защита API и одностраничных приложений	291
13.1	Защита API с помощью токенов	292
13.2	OAuth и OpenID Connect	303
13.2.1	OAuth и OpenID Connect	304
13.2.2	Потоки OAuth	305
13.3	Защита приложений	308
13.3.1	Сторонние инструменты	308
13.3.2	Учетные данные клиента	310
13.3.3	Код авторизации + PKCE	317
13.3.4	Одностраничные приложения и паттерн Backend-for-Frontend	325
	Резюме	337

Часть VI БЕЗОПАСНОСТЬ КАК ПРОЦЕСС.....338

14	Безопасные зависимости.....339
14.1	Использование команды npm audit.....340
14.2	Поддержание зависимостей NuGet в актуальном состоянии344
	Резюме349

15	Инструменты аудита.....350
15.1	Поиск уязвимостей351
15.2	OWASP ZAP.....353
15.3	Security Code Scan.....359
15.4	GitHub Advanced Security.....363
	Резюме367

16	OWASP Top 10.....369
16.1	OWASP Top 10370
16.1.1	Процесс создания списка OWASP Top 10370
16.1.2	№ 1: Нарушение контроля доступа.....372
16.1.3	№ 2: Криптографические ошибки373
16.1.4	№ 3: Внедрение.....373
16.1.5	№ 4: Небезопасный дизайн.....374
16.1.6	№ 5: Ошибки настроек безопасности.....374
16.1.7	№ 6: Уязвимые и устаревшие компоненты375
16.1.8	№ 7: Ошибки идентификации и аутентификации.....375
16.1.9	№ 8: Ошибки программного обеспечения и целостности данных.....375
16.1.10	№ 9: Ошибки журналирования и мониторинга.....376
16.1.11	№ 10: Подделка запросов со стороны сервера.....376
16.2	OWASP API Top 10.....378
16.3	Другие списки379
	Резюме381
	Предметный указатель383

Вступительное слово от сообщества

ASP.NET Core – это профессиональный и гибкий инструмент для создания современных веб-приложений, и безопасность – это ключевой аспект, особенно когда речь идет о работе с конфиденциальной информацией. Сам по себе фреймворк ASP.NET Core безопасен благодаря разработкам и стандартам безопасности Microsoft. Однако, несмотря на старания Microsoft, разработчику требуется понимать основы кибербезопасности и уметь выстраивать механизмы защиты.

Создание безопасных приложений – это сложный и ответственный процесс, требующий глубоких знаний и опыта в области информационной безопасности. Автор рассказывает о лучших практиках и технологиях работы с секретными данными, векторах атак, защите веб-приложений как с точки зрения создания безопасного кода, так и с точки зрения защиты от попыток получения контроля извне.

Рекомендуем не только прочитать книгу, но и попробовать все практические примеры. Это эффективный способ узнать о том, как именно эксплуатируются наиболее популярные ошибки и уязвимости. Обязательно попробуйте разными способами «взломать» ненадежный магазин соков от OWASP, это увлекательный процесс.

Мы надеемся, что эта книга станет вашим надежным помощником в создании безопасных приложений на платформе .NET и поможет вам защитить свои приложения от различных угроз. Приятного чтения!

Над переводом работали представители сообщества DotNet.Ru:

- Игорь Лабутин;
- Дмитрий Жабин;
- Илья Лазарев;
- Рустам Сафин;
- Радмир Тагиров;
- Сергей Бензенко;
- Андрей Беленцов;
- Андрей Брижак;
- Алексей Ростов;
- Ринат Сафиуллин;
- Анатолий Кулаков.

Введение

Я до сих пор помню, как впервые столкнулся с темой безопасности веб-приложений, хотя в то время и не осознавал ее важности. Где-то в 1997 г., когда я занимался созданием веб-приложений (точнее, сайтов), услуги хостинга были очень дорогими. В случае с одним из моих проектов единственным вариантом, который я мог себе позволить, была возможность создать только одну страницу (!), и для этого мне приходилось использовать инструменты хостинг-провайдера – никакого собственного HTML или CSS. У меня было много свободного места на бесплатном хостинге, но я не мог использовать там собственный домен: у меня было что-то вроде <http://home.someprovider.com/mysite>.

Одной из очень немногих доступных мне функциональных возможностей была настройка ключевых слов страницы (раньше поисковые системы анализировали эту информацию). Если бы я использовал, например, словосочетание *web application security, hacking*, оно было бы преобразовано в следующую HTML-разметку:

```
<meta name="keywords" content="web application security, hacking">
```

Поэкспериментировав, я обнаружил, что могу попробовать такое «ключевое слово»:

```
"><meta http-equiv="refresh" content="0;
    url=http://home.someprovider.com/mysite"><"
```

Оказалось, что провайдер помещал эти данные в тег `<meta>` как есть, что привело к следующему результату (для удобочитаемости код отформатирован, а ввод выделен жирным шрифтом):

```
<meta name="keywords" content="">
<meta http-equiv="refresh" content="0;
    url=http://home.someprovider.com/mysite">
<">
```

Таким образом я внедрил еще один тег `<meta>`, который перенаправлял посетителя на мой настоящий сайт, размещенный на бесплатном хостинге в другом месте.

Потребовалось время, прежде чем я понял значение того, что обнаружил, – на эту страницу можно было внедрить произвольный контент. Моя «атака» была безобидной, но можно было бы добавить и другую, более вредоносную разметку. Это пробудило во мне интерес к изучению безопасности веб-приложений, и с тех пор я не оглядывался назад. Я проверил бесчисленное количество приложений, работал с клиентами до и после аудита, учил разработчиков писать безопасные веб-приложения, выступал на трех континентах на конференциях, посвященных безопасности

веб-приложений, и изо всех сил старался сделать приложения, за которые я отвечал, максимально безопасными. В 2004 г. я впервые получил звание Microsoft MVP по ASP.NET. Я очень внимательно следил за API безопасности, подводными камнями и проблемами в этом фреймворке на протяжении многих лет.

Я думал написать книгу об опыте и знаниях, которые приобрел за последние 25 лет, но не было подходящего времени. В середине 2021 г. оно, наконец, настало, и я отправился в многомесячное путешествие, чтобы изложить все, что я знаю и считаю важным, в книге, которую вы собираетесь прочитать.

По моему опыту, недостаточно просто знать контрмеры, применяемые против определенных угроз. Разработчики должны понимать, как работают атаки, поскольку легче защититься от вещей, с которыми вы уже сталкивались. Вот почему во многих главах сначала будет продемонстрирована сама атака, а затем я объясню, как ее предотвратить. Помимо того что это облегчает восприятие материала, это еще и весело: мы видим, как что-то можно сломать, и называем это работой!

Как следует из названия, центральная тема книги – ASP.NET Core, куда входят Razor Pages и ASP.NET Core MVC. Также там, где это возможно, в ней рассматривается Blazor – еще один фреймворк для создания веб-приложений от компании Microsoft. Во всех примерах используется язык C#, а в качестве основы для них была выбрана платформа .NET 6 (в надежде, что они по-прежнему будут работать и со многими последующими версиями).

Благодарности

Многие, кто принимал участие в подготовке этой книги, упомянуты на обороте титульного листа (и это правильно!), и кроме них есть еще большое количество людей, которые помогли мне и внесли свой вклад.

Я в долгу как перед рецензентами, которые предоставляли полезные комментарии на различных этапах подготовки книги, так и перед читателями издания, которое было доступно по программе Manning Early Access Program (MEAP): Аль Пезевски, Билли Мигель Ванегас, Даниэль Васкес, Даррен Гиллис, Дэвид Пакку, Деннис Хейс Джордже, Дмитрий Сергеевич Дорогой, Дойл Тернер, Эммануил Шардалас, Гай Лэнгстон, Гарри Полдер, Джедиджа Буржуа, Джо Куэвас, Хосе Луис Перес, Марчин Сенк, Марек Петак, Маркус Вольф, Мэттью Харвелл, Майкл Холмс, Милош Тодорович, Ник МакГиннесс, Ник Римингтон, Онофри Джордж, Пол Браун, Ричард Вон, Рон Лиз, Сэмюэл Бош, Стэнли Анози, Сумит К. Сингх, Том Гет, Вьорель-Мариан Муазе и Уэйн Мэтер – спасибо за ваш вклад и помощь в улучшении книги.

Некоторые из моих близких друзей и коллег также оставили неопенимые отзывы и сделали книгу намного лучше. Спасибо всем вам за ваши идеи и поддержку!

Особая благодарность редактору по развитию Дагу Раддеру, который не только занимался поддержкой этого проекта, но и ловил меня каждый раз, когда я пытался «схалтурить».

Об этой книге

Название книги говорит само за себя: в ней рассказывается о безопасности приложений, созданных с использованием ASP.NET Core, поэтому здесь подробно описываются различные угрозы и риски для веб-приложений, основанных на технологии .NET. Я верю в принцип «показывай, а не рассказывай», поэтому вы увидите не только API и меры противодействия, но и то, как происходит атака. Основой для многих глав служат реальные инциденты.

Кому адресована эта книга?

Вы должны понимать основы .NET и владеть хотя бы одним из фреймворков ASP.NET Core (Razor Pages или MVC/Web API). Еще лучше, если вы хорошо разбираетесь в HTML и CSS («я понимаю это, когда вижу»). По крайней мере, в некоторых главах будет полезен поверхностный опыт работы с JavaScript. В качестве предпочтительного языка здесь используется C#, поэтому это еще одно необходимое условие, чтобы получить максимальную отдачу от прочтения книги.

Структура книги

Книга разбита на пять частей, которые содержат 16 глав. В первой части закладывается основа для последующих тем:

- в главе 1 обсуждается, почему важна безопасность веб-приложений и какие существуют параметры ASP.NET Core, а также то, как они могут быть затронуты. Вы получите краткую информацию о настройках проекта, которые предоставляет ASP.NET Core.

Во второй части показаны наиболее распространенные атаки на веб-приложения и способы защиты от них:

- в главе 2 рассматривается межсайтовый скриптинг (XSS) – очень распространенная атака, обычно основанная на внедрении вредоносного кода JavaScript. Пример с внедрением HTML, описанный во введении, также попадает в эту категорию;
- в главе 3 обсуждаются способы атаки на управление сессиями и как сделать сессии более безопасными. Сюда входят функциональные возможности, предоставляемые современными веб-браузерами;
- в главе 4 рассматривается межсайтовая подделка запросов (CSRF) – очень опасная атака, которую можно нейтрализовать

с помощью встроенных функций ASP.NET Core и механизмов защиты, которые есть в последних версиях браузеров;

- в главе 5 описываются потенциальные последствия использования данных, не прошедших валидацию, и как в этом может помочь ASP.NET Core. Сюда входит удобное и мощное средство: валидация модели;
- глава 6 посвящена внедрению SQL-кода, очень старой атаке, редко встречающейся в мире ASP.NET Core благодаря простым в использовании мерам противодействия и появлению инструментов объектно-реляционного отображения, в частности Entity Framework Core.

Третья часть посвящена безопасному хранению данных:

- в главе 7 рассказывается о том, как хранить секретные данные, в частности токены. Один из вариантов – использовать шифрование; другой – использовать предложения облачных провайдеров;
- в главе 8 обсуждается работа с паролями и способы их безопасного хранения. На самом деле пароли вообще не стоит хранить, в отличие от их хешей.

В четвертой части рассматриваются различные параметры конфигурации, связанные с безопасностью:

- в главе 9 подробно описаны HTTP-заголовки, поддерживаемые современными веб-браузерами, которые добавляют в приложение дополнительный уровень безопасности, а также рассказывается, как предотвратить отправку заголовков, отображающих скрытую информацию, клиенту;
- глава 10 знакомит вас с обработкой ошибок в приложениях ASP.NET Core с использованием передовых практик;
- в главе 11 рассматриваются две темы, которые отличаются друг от друга, но тем не менее в какой-то степени они связаны: журналирование может обеспечить сохранение диагностической информации о сайте для последующего ее извлечения, а проверка работоспособности обеспечивает механизм наблюдения за доступностью сайта и его сервисов.

Пятая часть посвящена проверке подлинности и авторизации в приложениях ASP.NET Core:

- в главе 12 вы познакомитесь с системой ASP.NET Core Identity, благодаря которой управлять пользователями и выполнять аутентификацию на сайте становится проще;
- в главе 13 описывается защита API и одностраничных приложений с помощью решения на основе токенов, а также рассматриваются протоколы OAuth и OpenID Connect с точки зрения ASP.NET Core.

Шестая часть охватывает ряд аспектов, являющихся частью процесса обеспечения безопасности:

- в главе 14 обсуждается, как обеспечить безопасность зависимостей, включая различные инструменты аудита;
- в главе 15 основное внимание уделяется инструментам аудита, которые могут помочь обнаружить уязвимости в веб-приложениях;
- в главе 16 рассматривается OWASP Top 10, регулярно обновляемый список десяти главных уязвимостей в веб-приложениях и то, как они описаны в этой книге.

Большинство глав не зависят друг от друга, но при необходимости приводятся соответствующие ссылки.

О коде

В этой книге содержится большое количество примеров исходного кода. Часть из них представляет собой пронумерованные листинги, а часть встречается в самом тексте. В обоих случаях исходный код отформатирован соответствующим шрифтом фиксированной ширины, чтобы отделить его от обычного текста. В некоторых случаях исходный код был переформатирован. Я добавил разделители строк и переделал отступы, чтобы уместить их по ширине книжных страниц. В редких случаях, когда этого оказалось недостаточно, в листинги были добавлены символы продолжения строки (⇒). Также из многих листингов, описываемых в тексте, были убраны комментарии. Некоторые листинги сопровождают аннотации, выделяющие важные понятия.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если

вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Manning Publications очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Об авторе

Кристиан Венц – пионер Интернета, специалист по информационным технологиям и предприниматель. С 1999 г. он написал около 150 книг, посвященных веб-технологиям и смежным темам, которые были переведены на десять языков. На своей основной работе он занимается консультацией предприятий по вопросам цифровизации и Индустрии 4.0, или Четвертой промышленной революции. Будучи неизменным участником международных конференций для разработчиков, он выступал на трех континентах. С 2004 г. Кристиан носит звание MVP для ASP.NET, является ведущим автором официальной сертификации по PHP и время от времени участвует в проектах по разработке программного обеспечения с открытым исходным кодом. У него высшее образование в области компьютерных наук и бизнес-информатики, и он двукратный обладатель премии Кнута.

Об иллюстрации на обложке

Изображение на обложке книги – «Венецианка», взято из сборника Жака Грассе де Сен-Совера, опубликованного в 1797 г. Каждая иллюстрация тщательно прорисована и раскрашена вручную. В те дни было легко определить, где жили люди, какова их профессия или положение в обществе, просто по одежде. Мы в Manning отмечаем изобретательность и инициативу компьютерного бизнеса с помощью книжных обложек, основанных на разнообразии жизни в разных регионах несколько веков назад, которое оживает благодаря изображениям из этой коллекции.