Отзывы на первое издание

«Одно из лучших руководств по Spring Security 6 – практичное и простое в освоении, охватывающее все аспекты, которые вам, вероятно, пригодятся в работе».

Амарджит Бхандал, старший Java-разработчик

«Одна из лучших технических книг, которые я прочитала за последний год. Удивительно, насколько хорошо она рассказывает про фреймворк Spring Security!»

Симона Сгуацца, младший научный сотрудник,
Университет прикладных наук и искусств Южной Швейцарии

«Это прекрасный и емкий обзор фреймворка Spring Security!»

Сачин Хандиекар, ведущий инженер-программист в JPMC

«Незаменимое руководство по освоению тонкостей Spring Security. Абсолютно авторитетное, непревзойденное по глубине и ясности».

Наджиб Ариф, старший консультант в Thoughtworks

«Вы должны иметь эту книгу под рукой, если собираетесь использовать Spring Security. И почти каждому приложению Spring требуется Spring Security».

Луиджи Рубино, архитектор программного обеспечения в Unimatica S.p.A.

Оглавление

Содержание

Предисловие

Я впервые познакомился с Лауренциу Спилкэ в 2022 г., когда мы дистанционно работали над презентацией Spring-One, и я был счастлив наконец встретиться с ним лично на Devoxx 2023 в Бельгии. Меня взволновала и обрадовала его просьба написать это предисловие. Я начну с отрывка из книги:

> *«Если вы неправильно применяете фреймворк, то получаете приложение, которое трудно поддерживать. Что еще хуже, иногда те, кто не использует фреймворк, считают, что это вина фреймворка».*

Золотые слова! За последние годы я несколько раз слышал мнение о том, что Spring Security сложен для понимания и имеет слишком крутую кривую обучения. Так это или нет, если вы погрузитесь во внутреннее устройство фреймворка и по-настоящему хорошо разберетесь в архитектуре аутентификации, вы невольно изучите возможности этого мощного инструмента, и в конечном итоге вам станет проще его использовать. Эта книга попадает точно в цель и дает нам детальное описание архитектуры аутентификации Spring Security с помощью простых и понятных диаграмм, сопровождаемых подробными объяснениями каждого из основных компонентов, которые взаимодействуют в процессе аутентификации.

На протяжении всей книги Лауренциу умело использует аналогии, чтобы упростить рассматриваемую тему. Мне очень нравится аналогия, приведенная в главе про архитектуру аутентификации, поскольку она хорошо передает идею:

> *«Если вы знаете эту архитектуру, то вы похожи на шеф-повара, который знает все ингредиенты на кухне и может приготовить любой рецепт».*

Диаграмма взаимодействий, использованная для демонстрации процесса аутентификации, превосходна. Она дает общее понимание потока аутентификации и подробно описывает назначение и зону ответственности каждого из основных компонентов по мере чтения книги.

Повествование логично и последовательно начинается с очень простых примеров и плавно переходит к более сложным, не перегружая читателя.

После подробного изучения архитектуры аутентификации автор переходит к авторизации. Я сразу вспоминаю вопрос, который часто встречаю в сообществе разработчиков: «В чем разница между полномочиями, ролью и разрешением?» Вы получите хороший ответ на этот вопрос, потому что в книге даны очень простые реальные примеры полномочий, ролей и разрешений, а также варианты их привязки к пользователю. Далее автор дает общие рекомендации по моделированию полномочий в вашем приложении на основе доступных функций и типов пользователей системы. Затем он демонстрирует применение общих принципов на примере определения правил авторизации в конфигурации Spring Security для ограниченного контролируемого доступа.

Часть IV охватывает темы OAuth 2 и OpenID Connect 1.0. Набор спецификаций OAuth 2 и OpenID Connect 1.0 очень обширен, поэтому новичкам сложно в полной мере понять их назначение и возможности. Тем не менее эта книга дает превосходный обзор основных понятий (роли, типы предоставления авторизации, форматы токенов доступа и т. д.), определенных в спецификациях, и их реализации в Spring Security и Spring Authorization Server. Я согласен с тем, что спецификация OAuth 2 очень похожа на систему доступа в офисное здание, где вам нужна карта ограниченного доступа, чтобы войти в конференц-зал внутри здания. На примере этого реального сценария безопасности в книге показаны различные части системы OAuth 2 и их предназначение. Затем автор переходит к простому примеру использования Spring Authorization Server вместе с поддержкой клиента и сервера ресурсов Spring Security. Автор начинает с простейших примеров, а затем демонстрирует применение клиентов при реализации прав доступа разного типа, например кода авторизации (с PKCE), учетных данных клиента и обновления токена. Далее демонстрируются общие сценарии конфигурации, например настройка непрозрачных токенов и использование интроспекции и отзыва токенов. На следующем шаге показаны более сложные сценарии настройки многопользовательской аренды для серверов ресурсов.

Подводя итог, можно сказать, что эту книгу должны прочитать все, кто хочет тщательно изучить архитектуру аутентификации Spring Security и внутренние компоненты фреймворка, потому что только так вы сможете в полной мере воспользоваться его возможностями.

Джо Гранджа,
инженер по безопасности Spring, VMware by Broadcom

Введение

Путь разработчика программного обеспечения – это захватывающее переплетение творчества, обучения, преподавания, но часто – переучивания. Моя карьера началась в 2007 г., и я сам не заметил, как из простого разработчика превратился в разработчика-наставника. Хотя обе роли имеют свое уникальное очарование, именно искусство передачи знаний, воспитания любопытства и наблюдения за моментами озарения у других учеников по-настоящему зажигает во мне огонь. Но давайте посмотрим правде в глаза: сферы разработки и обучения глубоко переплетены. Чтобы нести факел, освещая путь другим, нужно самому хорошо разбираться в постоянно меняющемся мире прикладного программного обеспечения. С годами приходит ясное понимание: в то время как функциональные аспекты программного обеспечения служат его сердцем, нефункциональные атрибуты, такие как безопасность, производительность и удобство обслуживания, становятся его спасательным кругом. Разработчику проще обнаружить и исправить ошибку в коде функции, чем барахтаться в мутных водах уязвимостей безопасности или падения производительности. Неудивительно, что многие разработчики, независимо от опыта, часто испытывают растерянность, сталкиваясь с этими побочными сложностями.

Безопасность не просто важна для приложения – это неоспоримый императив. Spring Security является лидером в обширной области фреймворков безопасности, что неудивительно, если учитывать широкое распространение и надежность экосистемы Spring в области корпоративных приложений. Тем не менее остается очевидная проблема – крутая кривая обучения при освоении Spring Security. Обильные, но разрозненные ресурсы в сети часто выглядят как кусочки пазла, которые отказываются складываться в единое целое, что сбивает с толку даже самых упорных учеников.

Именно эти проблемы в сочетании с примерами неправильного или, что еще хуже, уязвимого применения Spring Security и побудили меня написать первое издание данной книги. Моя цель была ясна: показать путеводную звезду любому желающему освоить Spring Security, будь то новичок или опытный поклонник Spring.

Во втором издании мы глубоко погрузимся в Spring Security, размышляя об инновациях, изменениях и опыте, накопленном сообществом с момента первого издания. Я улучшил то, что было, доба-

вил то, чего не было, и сделал акцент на том, что наиболее актуально сегодня. Я искренне надеюсь, что второе издание будет не просто полезной книгой, но и надежным спутником на вашем пути к созданию безопасных, надежных приложений. Я представлял себе эту книгу как маяк, который гарантирует, что вы не только сэкономите время, но и будете работать с уверенностью, зная, что ваши приложения устойчивы к постоянно меняющимся угрозам цифровой сферы.

Благодарности

Создание этой книги было увлекательным путешествием, в которое я не смог бы отправиться без коллективной мудрости, поддержки и опыта множества исключительных людей из моего окружения.

Прежде всего сердечное спасибо Даниэле, моей жене и путеводной звезде. Ее проницательность, постоянная поддержка и непоколебимая вера в мои силы сыграли неоценимую роль на протяжении всего проекта.

Сотрудники издательства Manning, работавшие над этой книгой, заслуживают особого упоминания. Благодаря их приверженности своему делу она обрела свои лучшие качества. Среди них я хотел бы выразить особую признательность Марине Михелс и Жану-Франсуа Морену. Их профессионализм, поддержка и бесценные советы значительно обогатили эту книгу.

Сердечная благодарность моей подруге Иоане Гёз – талантливому художнику, создавшему иллюстрации. Ее умение переводить мои абстрактные мысли в восхитительные визуальные образы добавило страницам уникальное очарование и позволило читателям найти повод для улыбки среди технических диаграмм.

Эта книга стала значительно лучше благодаря дотошному вниманию и отзывам многочисленных рецензентов. Их проницательные и конструктивные отзывы сыграли важную роль в уточнении содержания. Особая благодарность преданным рецензентам из Manning: Амарджиту Бхандалу, Асифу Икбалу, Козимо Дамиано Прете, Джеффу Уильямсу, Давиду Аскерову, Джастину Райзеру, Луиджи Рубино, Маноджу Кумару, Маркусу Гезелю, Мишелю Аддучи, Микаэлю Бистрему, Майклу Малеву, Наджибу Арифу, Патрику Ванджау, Ричарду Мейнсену, Сачину Хандиекару, Симеону Лейзерзону и Симону Сквацца, а также моим друзьям, которые поделились своим опытом.

Наконец, спасибо моим коллегам в Endava: ваша постоянная поддержка, идеи и непоколебимая вера в мои начинания заставляли меня двигаться вперед. Я дорожу вашей поддержкой и глубоко ценю ее.

Все, кто прикоснулся к этому проекту, в большом и малом, пожалуйста, знайте, что ваш вклад стал одной из нитей, из которых соткан гобелен этой книги. Спасибо!

Об этой книге

Безопасность имеет первостепенное значение в разработке программного обеспечения, и очень важно позаботиться о ней с первых шагов. Во втором издании этой книги мы глубоко погружаемся в тематику использования Spring Security для обеспечения безопасности ваших проектов на уровне приложений. Знание Spring Security и его правильное применение необходимы каждому разработчику. Углубляться в разработку приложений без этих знаний – слишком большой риск.

Кому следует прочитать эту книгу?

Эта книга адресована разработчикам, использующим фреймворк Spring для корпоративных приложений. Хотя я адаптировал эту книгу для начинающих осваивать Spring Security, читателю потребуется базовое знание фреймворка Spring, включая

- использование контекста Spring;
- создание конечных точек REST;
- работу с источниками данных.

Глава 15 посвящена конфигурации безопасности реактивных приложений. Следовательно, перед прочтением этой главы важно иметь представление о реактивных приложениях и их разработке с использованием Spring. По мере необходимости я буду предлагать вам ссылки на дополнительные ресурсы для закрепления или дополнения необходимых тем.

Все примеры в этой книге написаны на Java. Учитывая популярность Java в экосистеме Spring, предполагается, что читатели уже имеют практические навыки программирования на этом языке. Но при желании все примеры можно без труда адаптировать к программированию на Kotlin.

Если вы чувствуете, что вам нужно освежить в памяти базовые знания перед началом работы с этой книгой, я настоятельно рекомендую прочитать еще одну мою книгу – «Spring быстро» (Питер, 2023).

Как организована эта книга

Я создал эту книгу, чтобы познакомить вас с обширной экосистемой Spring Security, от фундаментальных понятий до продвинутых при-

емов работы. Каждая часть книги естественным образом перетекает в следующую, делая ваш путь последовательным и комфортным. Книга состоит из следующих частей:

Часть I. Знакомство с Spring Security

В этой части я познакомлю вас с современным ландшафтом безопасности и Spring Security. Мы заложим основу для дальнейшего изучения, обсудив ключевую роль безопасности в сегодняшнюю цифровую эпоху и то, как Spring Security решает эту задачу.

Часть II. Настройка аутентификации

Здесь мы погрузимся в детали процесса аутентификации. Я расскажу о таких важных темах, как управление пользователями, протоколы паролей, решающая роль фильтров в безопасности веб-приложений и реализация аутентификации.

Часть III. Настройка авторизации

Далее мы перейдем от аутентификации к авторизации. Вместе мы рассмотрим авторизацию на уровне конечных точек, меры защиты от таких угроз, как CSRF, и управление CORS, а также изучим более сложную авторизацию и фильтрацию на уровне методов.

Часть IV. Реализация OAuth 2 и OpenID Connect

В этой части я проведу вас по миру OAuth 2 и OpenID Connect. Вы узнаете об их значении и настроите серверы OAuth 2, серверы ресурсов и клиентов, тем самым укрепив безопасность вашего приложения.

Часть V. Переход к реактивному программированию

Здесь я познакомлю вас с парадигмой реактивного программирования, подробно описав, как защитить реактивные приложения, чтобы вы могли гарантировать, что ваши асинхронные операции останутся защищенными от несанкционированного доступа.

Часть VI. Тестирование конфигураций безопасности

Я отмечаю и объясняю необходимость тестирования перед развертыванием. Мы рассмотрим различные методы тестирования, позволяющие убедиться, что ваши конфигурации безопасности функционируют точно так, как задумано.

Приложения

Приложения содержат ссылки на ресурсы официальной документации и списки литературы для дополнительного чтения.

Хотя я задумал эту книгу как последовательность взаимосвязанных тем, читатели, имеющие некоторый опыт работы с Spring Security, могут сразу перейти к интересующим их главам. Однако имейте

в виду, что эти главы могут опираться на содержание предыдущих глав. Если вы уже знакомы с основами Spring Security, попробуйте начать с части III или IV для изучения основ OAuth 2 и OpenID. Если вы интересуетесь реактивным программированием, можете сразу перейти к части V.

Независимо от того, с чего вы начнете, убедитесь, что полностью усвоили текущую тему, прежде чем переходить к следующей главе.

О примерах кода

В этой книге представлено более 70 проектов, над которыми мы будем работать, начиная с главы 2 и до главы 18. При работе над конкретным примером я упоминаю название проекта, который реализует пример. Я рекомендую вам попробовать написать свой собственный пример с нуля в соответствии с объяснениями в книге, а затем воспользоваться примером только для сравнения вашего решения с моим. Такой подход поможет вам лучше понять конфигурации безопасности, которые вы изучаете.

Каждый из проектов создан с помощью Maven, что упрощает их импорт в любую IDE. Для разработки проектов я использовал IntelliJ IDEA, но вы можете открывать и запускать их в Eclipse, STS, NetBeans или любой другой среде разработки по вашему выбору. Приложение поможет вам освежить знания о том, как создать проект Spring Boot.

Эта книга содержит множество примеров исходного кода как в виде отдельных листингов, так и в тексте. В обоих случаях исходный код выделен шрифтом фиксированной ширины. Во многих случаях исходный код был переформатирован; в него добавлены переносы строк и изменены отступы для оптимального размещения на странице книги. В редких случаях ширины страницы было недостаточно, и в листинги пришлось добавить маркеры продолжения строки (➥). Кроме того, из листинга удалены комментарии, если исходный код описан в тексте. Многие листинги сопровождаются пояснениями к коду.

Вы можете скопировать исполняемые фрагменты кода из liveBook (онлайн-версии этой книги) по адресу https://livebook.manning.com/book/spring-security-in-action-second-edition. Полный код примеров размещен в файловом архиве перевода книги на сайте издательства «ДМК Пресс».

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.