

Spring Security

Четвертое издание

Эффективная защита веб-приложений,
RESTful-сервисов, облачных приложений
и микросервисных архитектур

Бадр Насслахсен

Краткое содержание

От издательства.....	21
Введение.....	23

Часть I **Основы безопасности приложений**

Глава 1. Анатомия небезопасного приложения.....	30
Глава 2. Начало работы со Spring Security.....	49
Глава 3. Пользовательская аутентификация.....	76

Часть II **Методы аутентификации**

Глава 4. Аутентификация на основе JDBC.....	108
Глава 5. Аутентификация с использованием Spring Data.....	135
Глава 6. Службы каталогов LDAP.....	155
Глава 7. Функция «Запомнить меня» (Remember-me Services).....	192
Глава 8. Аутентификация с использованием клиентских сертификатов в TLS.....	216

Часть III **OAuth 2 и SAML 2**

Глава 9. Возможности OAuth 2.....	238
Глава 10. Поддержка SAML 2.....	264

Краткое содержание

От издательства	21
Введение	23

Часть I
Основы безопасности приложений

Глава 1. Анатомия небезопасного приложения	30
Глава 2. Начало работы со Spring Security	49
Глава 3. Пользовательская аутентификация	76

Часть II
Методы аутентификации

Глава 4. Аутентификация на основе JDBC	108
Глава 5. Аутентификация с использованием Spring Data	135
Глава 6. Службы каталогов LDAP	155
Глава 7. Функция «Запомнить меня» (Remember-me Services)	192
Глава 8. Аутентификация с использованием клиентских сертификатов в TLS	216

Часть III
OAuth 2 и SAML 2

Глава 9. Возможности OAuth 2	238
Глава 10. Поддержка SAML 2	264

Часть IV

Усовершенствование механизмов авторизации

Глава 11. Детализированный контроль доступа	284
Глава 12. Списки управления доступом (ACL)	306
Глава 13. Пользовательская авторизация.....	337

Часть V

Продвинутые возможности безопасности и оптимизация развертывания

Глава 14. Управление сессиями	367
Глава 15. Дополнительные возможности Spring Security.....	385
Глава 16. Миграция на Spring Security 6.....	413
Глава 17. Безопасность микросервисов с использованием OAuth 2 и JSON Web Tokens (JWT).....	449
Глава 18. Единый вход с использованием Central Authentication Service (CAS).....	470
Глава 19. Создание нативных образов с помощью GraalVM.....	499
Дополнительные справочные материалы.....	510

Оглавление

От издательства.....	21
О научном редакторе русского издания.....	21
Об авторе.....	22
О рецензенте	22
Введение.....	23
Для кого эта книга	23
О чем эта книга	23
Как извлечь максимальную пользу из книги.....	26
Условные обозначения.....	27
Загрузка файлов с примерами кода.....	28
Код в действии	28

Часть I

Основы безопасности приложений

Глава 1. Анатомия небезопасного приложения	30
Стили архитектуры программного обеспечения	31
Монолитная архитектура.....	32
N-уровневая архитектура (многослойная архитектура).....	32
Сервис-ориентированная архитектура (SOA).....	32
Микросервисная архитектура	32
Выбор между традиционными веб-приложениями и одностраничными приложениями	33
Аудит безопасности.....	34
Изучение примера приложения.....	34
Архитектура приложения JBCP Calendar.....	36
Рассмотрение результатов аудита.....	38
Устранение недочетов после аудита безопасности	39
Аутентификация.....	40
Авторизация.....	42

Безопасность учетных данных базы данных	44
Конфиденциальная информация	45
Защита на транспортном уровне	45
Использование Spring Security 6 для решения проблем безопасности	46
Технические требования	46
Краткое содержание	48
Глава 2. Начало работы со Spring Security	49
Привет, Spring Security	50
Импорт тестового приложения	50
Обновление зависимостей	50
Применение конфигурации Spring Security	52
Обновление веб-конфигурации	53
Запуск защищенного приложения	58
Распространенные проблемы	59
Небольшие улучшения	60
Настройка входа в систему	61
Конфигурирование выхода из системы	64
Неправильное перенаправление страницы	65
Базовая авторизация на основе ролей	66
Авторизация на основе выражений	69
Условное отображение информации об аутентификации	70
Настройка поведения после входа в систему	72
Краткое содержание	75
Глава 3. Пользовательская аутентификация	76
Архитектура аутентификации в Spring Security	76
Класс SecurityContextHolder	77
Интерфейс SecurityContext	77
Интерфейс Authentication	77
Интерфейс AuthenticationManager	78
Класс ProviderManager	78
Интерфейс AuthenticationProvider	79
Архитектура календаря JBCP Calendar	80
Объект CalendarUser	80
Объект Event	80
Интерфейс CalendarService	81
Интерфейс UserContext	81
Интерфейс SpringSecurityUserContext	82

Вход новых пользователей с использованием SecurityContextHolder	85
Управление пользователями в Spring Security	85
Вход нового пользователя в приложение	86
Обновление SignupController	87
Создание пользовательского объекта UserDetailsService	88
Класс CalendarUserDetailsService	89
Конфигурация UserDetailsService	90
Удаление ссылок на UserDetailsManager	90
Объект CalendarUserDetails	91
Упрощения в SpringSecurityUserContext	92
Создание пользовательского объекта AuthenticationProvider	94
Создание CalendarUserAuthenticationProvider	94
Настройка объекта CalendarUserAuthenticationProvider	96
Аутентификация с разными параметрами	97
Какой метод аутентификации лучше использовать?	104
Краткое содержание	105

Часть II

Методы аутентификации

Глава 4. Аутентификация на основе JDBC	108
Установка необходимых зависимостей	108
Использование базы данных H2	109
Предоставленные JDBC-скрипты	110
Настройка встроенной базы данных H2	110
Настройка реализации JDBC UserDetailsManager	111
Стандартная схема пользователей Spring Security	111
Определение пользователей	112
Определение прав пользователей	112
Интерфейс UserDetailsManager	113
Доступ на основе групп	114
Настройка доступа на основе групп	115
Поддержка пользовательской схемы	118
Определение правильных SQL-запросов для JDBC	118
Обновление загружаемых SQL-скриптов	119
SQL для прав CalendarUser	119
Добавление пользовательских прав	120
Настройка JdbcUserDetailsManager для пользовательских SQL-запросов	121

Настройка безопасного хранения паролей	122
Интерфейс PasswordEncoder	123
Реализация DelegatingPasswordEncoder.....	125
Настройка кодирования паролей	126
Настройка метода PasswordEncoder.....	126
Подключение метода PasswordEncoder к Spring Security	126
Использование соли в Spring Security	130
Обновление конфигурации Spring Security.....	131
Миграция существующих паролей.....	131
Обновление DefaultCalendarUserService.....	131
Пробуем пароли с солью.....	132
Краткое содержание	134
Глава 5. Аутентификация с использованием Spring Data	135
Spring Data JPA.....	137
Обновление зависимостей.....	137
Перенастройка конфигурации базы данных	137
Инициализация базы данных	138
Рефакторинг с SQL на ORM.....	139
Маппинг объектов домена с использованием JPA.....	139
Репозитории Spring Data.....	141
Объекты доступа к данным (DAO)	142
Сервисы приложения	145
Объект UserDetailsService	146
Рефакторинг с RDBMS на документоориентированную базу данных.....	147
Реализация документоориентированной базы данных с MongoDB.....	147
Обновление зависимостей.....	147
Перенастройка конфигурации базы данных в MongoDB.....	148
Инициализация базы данных MongoDB.....	148
Маппинг доменных объектов для MongoDB.....	151
Объекты доступа к данным (DAO) в MongoDB.....	153
Краткое содержание	154
Глава 6. Службы каталогов LDAP	155
Понимание LDAP	155
Что такое LDAP?.....	156
Устранение проблем со встроенным LDAP.....	161

Как работает аутентификация в Spring LDAP	162
Аутентификация учетных данных пользователя.....	162
Демонстрация аутентификации с использованием JXplorer.....	163
Определение ролей с использованием JXplorer.....	168
МAPPING дополнительных атрибутов в UserDetails.....	169
Расширенная конфигурация LDAP	170
Кодирование и хранение паролей в LDAP	173
Настройка объекта UserDetailsContextMapper.....	175
Неявная настройка UserDetailsContextMapper	175
Просмотр дополнительных данных о пользователях.....	176
Настройка LdapUserDetailsService	179
Обновление AccountController для использования LdapUserDetailsService	180
Интеграция Spring Security с внешним сервером LDAP	181
Явная конфигурация бинов LDAP	183
Настройка ссылки на внешний сервер LDAP.....	183
Выполнение поиска для локализации пользователя в каталоге LDAP.....	184
Делегирование определения ролей UserDetailsService	185
Интеграция с Microsoft Active Directory через LDAP	188
Встроенная поддержка AD в Spring Security 6.1.....	190
Краткое содержание	191
Глава 7. Функция «Запомнить меня» (Remember-me Services)	192
Что такое «Запомнить меня»?.....	192
Зависимости.....	193
Функция «Запомнить меня» на основе токенов.....	193
Алгоритм SHA-256	196
Подпись remember-me	196
Насколько безопасна функция «Запомнить меня»?	199
Правила авторизации для функции «Запомнить меня»	200
Постоянная функция «Запомнить меня».....	201
Настройка функции «Запомнить меня» с хранилищем данных.....	202
Как работает механизм «Запомнить меня» на основе постоянного хранилища	203
PersistentTokenRepository на основе JPA.....	204
Пользовательская реализация RememberMeServices	207
Хранимые в базе данных токены более безопасны?	208
Очистка устаревших сессий «Запомнить меня»	208

Архитектура механизма «Запомнить меня»	210
Жизненный цикл пользователя в remember-me	211
Ограничение функции «Запомнить меня» по IP-адресу	212
Пользовательские имена cookie и HTTP-параметров	214
Краткое содержание	215
Глава 8. Аутентификация с использованием клиентских сертификатов в TLS	216
Как работает аутентификация с использованием клиентского сертификата?	216
Настройка инфраструктуры аутентификации с использованием клиентских сертификатов	218
Импорт пары ключей сертификата в браузер	222
Поиск и устранение проблем с аутентификацией по клиентскому сертификату	225
Настройка аутентификации по клиентскому сертификату в Spring Security	226
Настройка аутентификации по клиентскому сертификату с использованием пространства имен security	226
Настройка аутентификации по клиентскому сертификату с использованием Spring-бинов	232
Дополнительные возможности конфигурации на основе Spring-бинов	233
Что следует учитывать при реализации аутентификации по клиентскому сертификату	235
Краткое содержание	236
 Часть III OAuth 2 и SAML 2	
Глава 9. Возможности OAuth 2	238
Многообещающий мир OAuth 2	238
Зачем нужен OpenID Connect?	241
Как работает OpenID Connect?	242
Регистрация OAuth 2-приложения	242
Включение входа через OAuth 2.0 в Spring Security	243
Настройка страницы входа	248
Дополнительные провайдеры OAuth 2	250
Настройка свойств пользовательского провайдера	253
Включение поддержки Proof Key for Code Exchange (PKCE)	254
Выход из системы в OpenID Connect 1.0	256
Автоматическая регистрация пользователей	258
Маппинг прав пользователей	261

Насколько безопасен OAuth 2?	262
Краткое содержание	263
Глава 10. Поддержка SAML 2	264
Что такое SAML?	264
Вход в систему через SAML 2 с помощью Spring Security	266
Добавление SAML-приложения в Okta	269
Создание учетной записи в Okta	270
Дополнительные необходимые зависимости	271
Указание метаданных IdP	272
Получение аутентифицированного субъекта SAML 2	272
Парсинг метаданных SAML 2	273
Генерация метаданных SAML 2	273
Адаптация поиска RelyingPartyRegistration	274
Переопределение автоматической конфигурации SAML в Spring Boot	274
Создание пользовательского RelyingPartyRegistrationRepository	275
Создание пользовательских прав доступа с использованием Spring Security SAML	277
Выполнение единого выхода	279
Краткое содержание	282

Часть IV

Усовершенствование механизмов авторизации

Глава 11. Детализированный контроль доступа	284
Интеграция Spring Expression Language (SpEL)	284
Класс WebSecurityExpressionRoot	286
Класс MethodSecurityExpressionRoot	286
Авторизация на уровне страницы	287
Условное отображение с использованием библиотеки тегов Thymeleaf Spring Security	288
Условное отображение на основе правил доступа по URL	288
Условное отображение с использованием SpEL	289
Использование логики контроллера для условного отображения контента	290
Класс WebInvocationPrivilegeEvaluator	291
Как лучше всего настроить авторизацию на странице?	292
Безопасность на уровне методов	293
Прокси на основе интерфейсов	296

Стандартизированные правила, совместимые с JSR-250	297
Зависимости Gradle.....	297
Безопасность методов с использованием аннотации @Secured в Spring.....	299
Правила безопасности методов с проверкой параметров	299
Правила безопасности методов с проверкой возвращаемых значений	301
Защита данных метода с использованием фильтрации на основе ролей.....	301
Предварительная фильтрация наборов данных с @PreFilter.....	303
Сравнение типов авторизации методов	303
Практические аспекты безопасности на основе аннотаций	304
Краткое содержание	304
Глава 12. Списки управления доступом (ACL).....	306
Концептуальная модель ACL	306
Списки управления доступом в Spring Security	308
Базовая конфигурация поддержки Spring Security ACL.....	310
Зависимости Gradle.....	310
Определение простого целевого сценария.....	310
Добавление таблиц ACL в базу данных H2	311
Настройка SecurityExpressionHandler	313
Объект AclPermissionCacheOptimizer.....	314
Оптимизация кеша AclPermission.....	314
Объект JdbcMutableAclService.....	314
Класс BasicLookupStrategy	315
Создание простой записи ACL.....	317
Сложные аспекты ACL	320
Как работают разрешения.....	321
Пользовательское объявление разрешений ACL	323
Включение проверки разрешений ACL в пользовательском интерфейсе.....	326
Изменяемые ACL и авторизация.....	328
Важные особенности стандартного внедрения ACL	331
Масштабируемость и производительность ACL	331
Не стоит недооценивать затраты на пользовательскую разработку	334
Стоит ли использовать Spring Security ACL?	335
Краткое содержание.....	336
Глава 13. Пользовательская авторизация	337
Авторизация запросов	337
Обработка вызовов	339

Класс AuthorizationManager.....	339
Реализации AuthorizationManager на основе делегирования	340
Модификация AccessDecisionManager и AccessDecisionVoter.....	341
Устаревшие компоненты авторизации.....	343
AccessDecisionManager.....	343
Реализации AccessDecisionManager на основе голосования (voting)	343
Динамическое определение контроля доступа к URL-адресам	347
Конфигурация RequestConfigMappingService.....	347
Регистрация собственной реализации SecurityMetadataSource	350
Создание пользовательского выражения.....	351
Конфигурация пользовательского SecurityExpressionRoot.....	351
Конфигурация пользовательского SecurityExpressionHandler	352
Конфигурация и использование CustomWebSecurityExpressionHandler	353
Альтернативный подход без CustomWebSecurityExpressionHandler	354
Объявление собственного AuthorizationManager.....	361
Краткое содержание.....	363

Часть V

Продвинутые возможности безопасности и оптимизация развертывания

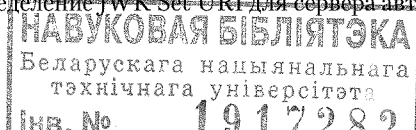
Глава 14. Управление сессиями	367
Настройка защиты от фиксации сессии.....	367
Что такое атака фиксации сессии?.....	367
Предотвращение атак фиксации сессии в Spring Security	369
Имитация атаки на фиксацию сессии.....	370
Сравнение вариантов защиты от фиксации сессии	372
Ограничение количества одновременных сессий для одного пользователя	372
Настройка контроля параллельных сеансов	372
Как работает контроль параллельных сессий	373
Тестирование контроля параллельных сессий.....	374
Настройка перенаправления после истечения сессии.....	375
Типичные проблемы контроля параллельных сессий.....	376
Предотвращение повторной аутентификации вместо завершения предыдущей сессии.....	377
Другие преимущества контроля параллельных сессий.....	378
Отображение активных сессий пользователя.....	379
Как Spring Security использует HttpSession?.....	381

Интерфейс HttpSessionSecurityContextRepository	382
Конфигурация использования HttpSession в Spring Security	382
Отладка с помощью DebugFilter в Spring Security	383
Краткое содержание	384
Глава 15. Дополнительные возможности Spring Security	385
Уязвимости безопасности	385
Межсайтовый скриптинг (Cross-Site Scripting, XSS)	386
Межсайтовая подделка запроса (Cross-Site Request Forgery, CSRF)	387
Synchronizer token pattern	388
Когда использовать защиту от CSRF?	389
Защита от CSRF по умолчанию	392
Особенности защиты от CSRF-атак	395
HTTP-заголовки безопасности ответа	397
Cache-Control	399
Content-Type-Options	400
HTTP Strict Transport Security (HSTS)	400
HTTP Public Key Pinning (HPKP)	401
X-Frame-Options	402
Content Security Policy, CSP	403
Referrer Policy	404
Feature Policy	405
Политика разрешений (Permissions Policy)	405
Clear Site Data	406
Статические заголовки	406
Экземпляр HeadersWriter	407
Класс DelegatingRequestMatcherHeaderWriter	407
Тестирование приложений Spring Security	408
Поддержка реактивных приложений	409
Краткое содержание	412
Глава 16. Миграция на Spring Security 6	413
Защита от эксплойтов	414
Защита от CSRF-атак	414
CSRF-атаки с поддержкой WebSocket	415
Миграция конфигурации	415
Добавление аннотации @Configuration к аннотациям @Enable*	415
Использование новых методов requestMatchers	415

Использование новых методов securityMatchers.....	417
Замена класса WebSecurityConfigurerAdapter.....	418
Обновления кодирования паролей.....	422
Обновления управления сессиями.....	423
Обновления аутентификации.....	426
Обновления авторизации.....	427
Использование AuthorizationManager для обеспечения безопасности сообщений.....	432
Устаревание AbstractSecurityWebSocketMessageBrokerConfigurer.....	433
Использование AuthorizationManager для безопасности запросов.....	433
Обновления OAuth.....	438
Обновления SAML.....	441
Применение шагов миграции с Spring Security 5.x на Spring Security 6.x.....	444
Обзор зависимостей приложения.....	444
Миграция с пространства имен javax на jakarta.....	445
Замена WebSecurityConfigurerAdapter и внедрение бина SecurityFilterChain.....	445
Краткое содержание.....	448

Глава 17. Безопасность микросервисов с использованием OAuth 2 и JSON Web Tokens (JWT) 449

Что такое микросервисы?.....	450
Монолиты.....	450
Микросервисы.....	450
Сервис-ориентированная архитектура (SOA).....	451
Безопасность микросервисов.....	453
Спецификация OAuth 2.....	453
Токены доступа.....	454
Типы грантов.....	454
JSON Web Tokens (JWT).....	455
Структура токена.....	456
Аутентификация с использованием JWT в Spring Security.....	457
Поддержка OAuth 2 в Spring Security.....	458
Владелец ресурса.....	459
Сервер ресурсов.....	459
Сервер авторизации.....	459
Минимальные свойства конфигурации ресурса OAuth 2.....	460
Явное определение JWK-Set URI для сервера авторизации.....	461



Указание информации об аудиторрии.....	462
Настройка авторизации с использованием SecurityFilterChain	462
Запросы токена	463
Запросы к конечным точкам	464
Настройка авторизации с использованием аннотации @PreAuthorize.....	465
Краткое содержание.....	469

Глава 18. Единый вход с использованием Central Authentication Service (CAS).....	470
Что такое Central Authentication Service (CAS)?	470
Общая схема аутентификации CAS	471
Spring Security и CAS	473
Необходимые зависимости.....	473
Установка и настройка CAS.....	474
Настройка базовой интеграции с CAS.....	476
Настройка параметров CAS	476
Добавление CasAuthenticationEntryPoint.....	477
Активация проверки CAS ticket	478
Единый выход (Single Logout)	480
Конфигурация единого выхода.....	481
Кластерная среда.....	484
Аутентификация с использованием прокси-билетов для stateless-сервисов	485
Настройка аутентификации через прокси-билеты	486
Использование прокси-билетов.....	487
Аутентификация прокси-билетов	488
Настройка сервера CAS	491
WAR overlay для CAS.....	491
Как работает внутренняя аутентификация в CAS?	491
Настройка CAS для подключения к встроенному LDAP-серверу	492
Получение объекта UserDetails из утверждения CAS	494
Возвращение атрибутов LDAP в ответе CAS.....	494
Сопоставление атрибутов LDAP с атрибутами CAS.....	494
Получение объекта UserDetails из CAS	495
Объект GrantedAuthorityFromAssertionAttributesUser	496
Чем удобно извлечение атрибутов?.....	496
Дополнительные возможности CAS	497
Краткое содержание	497

Глава 19. Создание нативных образов с помощью GraalVM.....	499
Знакомство с GraalVM.....	499
Что такое нативные образы?	500
Ключевые особенности GraalVM	500
Преимущества GraalVM с точки зрения безопасности	501
Создание образов GraalVM с помощью Buildpacks.....	501
Создание образов GraalVM с использованием Buildpacks и Gradle	502
Создание образов GraalVM с использованием Buildpacks и Maven	502
Запуск образов GraalVM, созданных с помощью Buildpacks	503
Создание нативного образа с помощью Native Build Tools.....	503
Предварительные требования	503
Создание образов GraalVM с помощью Native Build Tools и Maven	504
Создание образов GraalVM с помощью Native Build Tools и Gradle	504
Запуск образов GraalVM, созданных с помощью Native Build Tools	504
Безопасность методов в нативных образах GraalVM.....	505
Краткое содержание.....	508
Дополнительные справочные материалы.....	510
Инструменты сборки	510
Инструмент сборки Gradle	510
Инструмент сборки Maven	511
Начало работы с примером кода приложения JBCP Calendar	511
Структура примеров кода	511
Работа с тестовыми проектами в IntelliJ IDEA	512
Работа с тестовыми проектами в Eclipse.....	516
Генерация серверного сертификата.....	521
Полезные ссылки	522