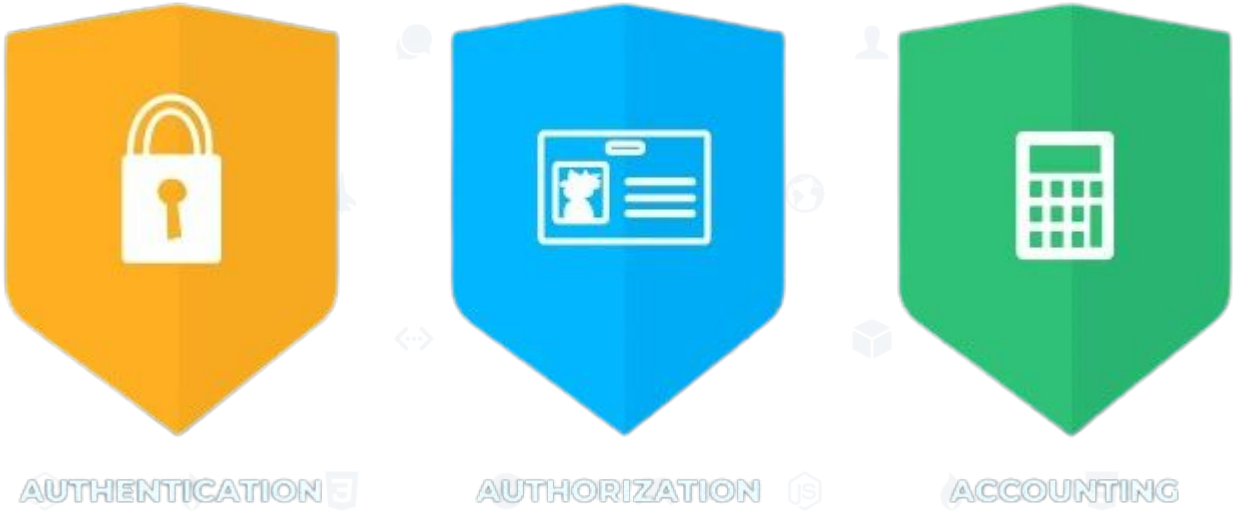
Lesson 41

20.03.2023



AAA (Authentication, Authorization and Accounting) или аутентификация, авторизация и аккаунтинг – это термин, используемый для описания трех функций в ИТ.

В основном AAA используется для управления доступом к различным ИТ-ресурсам, таким как сеть, службы, сервера и т. д.

AAA состоит из 3 которых, каждый из которых выполняет свою функцию для обеспечения идеальной безопасности.

Что такое аутентификация?

Аутентификация – это процесс идентификации пользователя или инстанса.

Простым способом проверки пользователя обычно является предоставленные пользователем данные, которые как правило представляют собой имя пользователя и пароль.

Например, во время входа в Gmail нам потребуется ввести правильное существующее имя пользователя и пароль для аутентификации.

Аутентификация также важна для безопасности, поскольку без идентификации пользователей не будет никаких ограничений безопасности и связанных с ними ограничений.

Существуют также различные методы аутентификации, такие как сертификаты, открытые/закрытые ключи, токены, изображения и т. д., а также биометрия.

Аутентификация обычно требует прохождения одного метода проверки, но в последнее время для одной аутентификации могут использоваться несколько методов, которые обычно называются двухфакторной аутентификацией или многофакторной аутентификацией.

Что такое авторизация?

Второй шаг в AAA – **авторизация**.

После аутентификации пользователя он должен быть авторизован в соответствии со своими привилегиями.

У пользователя низкого уровня не должно быть прав высокого уровня или уровня администратора.

Авторизация будет строго указывать и устанавливать права аутентифицированного пользователя.

Авторизация обычно использует уровни привилегий, которые помещают авторизованного пользователя в определенный уровень привилегий или группу пользователей, таких как пользователь, редактор, модератор, суперпользователь, администратор, чтобы управлять правами пользователей простым и легким способом.

Что такое аккаунтинг?

Когда пользователь аутентифицирован и успешно авторизован, он заходит в систему и ему предоставляется какой-то ресурс.

Пользователь будет использовать ресурсы сети, системы или службы в соответствии с предоставленными привилегиями.

При использовании этих ресурсов доступ пользователей регистрируется и сохраняется, что называется «Accounting», чтобы отслеживать действия пользователей.

- authentication
  (who I am)
- authorization
  (what I can do)
- encryption

Основные возможности

Шифрование паролей

Spring Security не ограничивается аутентификацией. Фреймворк также помогает решить проблему с безопасным хранением паролей.

Spring Security предлагает назначить объекту UserDetails собственный шифровальщик паролей. По умолчанию используется BCrypt. Также можно настроить количество раундов хеширования и реализацию случайного алгоритма.

Аутентификация In-Memory

Для сохранения информации о пользователях и выполнения аутентификации можно использовать временную базуанных, которая остается в оперативной памяти приложения.

Это полезно при разработке и тестировании. Реальная база данных при таком подходе остается нетронутой.

LDAP-аутентификация

Lightweight Directory Access Protocol (LDAP) — протокол аутентификации учетных записей пользователей в организациях. Позволяет определять структуру пользователей и групп пользователей, назначать им права доступа.

Дополнительную информацию вы можете получить в официальном руководстве по использованию аутентификации LDAP.

Управление сессией

Spring Security предоставляет механизмы для управления сеансом пользователя. Он создает эти механизмы контроля при входе в систему и уничтожает при выходе.

Для обеспечения безопасности доступны дополнительные средства, которые помогают, например, избежать отслеживания сеансов.

Remember Me Authentication

Это встроенный механизм распознавания, благодаря которому пользователям не нужно вводить учетные данные при каждом посещении сайта.

Spring Security предлагает несколько способов реализации этого типа аутентификации — например, хеширование данных с помощью секретного ключа или хранение постоянного токена в базе данных.

OAuth 2.0

Open Authorization 2.0 — открытый стандарт проверки прав пользователя с помощью сервиса авторизации. Он также используется для реализации таких функций, как вход через учетные записи Facebook, Google и других крупных площадок.

Настройка сервера авторизации и внедрение OAuth сопряжены с высоким риском и могут отнять много времени. В этом процессе легко ошибиться и создать уязвимость. Spring Security предлагает защитить сайт с помощью готовых инструментов — например, Auth0.

Основными блоками Spring Security являются:

SecurityContextHolder, чтобы обеспечить доступ к SecurityContext.

SecurityContext, содержит объект Authentication и в случае необходимости информацию системы безопасности, связанную с запросом.

Authentication представляет принципала (пользователя авторизованной сессии) с точки зрения Spring Security.

GrantedAuthority отражает разрешения выданные доверителю в масштабе всего приложения.

UserDetails предоставляет необходимую информацию для построения объекта Authentication из DAO объектов приложения или других источника данных системы безопасности.

UserDetailsService, чтобы создать UserDetails, когда передано имя пользователя в виде String (или идентификатор сертификата или что-то подобное).