Аутентификация с помощью JWT

№ урока: 6 **Курс:** Flask

Средства обучения: Python3 и любимая среда разработки, например, PyCharm.

Обзор, цель и назначение урока

Узнать, что такое аутентификация и авторизация пользователя, чем они отличаются друг от друга. Также, рассмотреть способы и протоколы аутентификации в веб-приложениях и добавить в наше приложение аутентификацию на базе JWT.

Изучив материал данного занятия, учащийся сможет:

- Различать, что такое авторизация и аутентификация.
- Использовать различные способы аутентификации пользователя в конкретных случаях.
- Использовать JWT аутентификацию.

Содержание урока

1. Разница между аутентификацией и авторизацией
2. Способы аутентификации в веб-приложениях
3. Аутентификация с помощью JWT

Резюме

- **Идентификация** — это заявление о том, кем вы являетесь. В зависимости от ситуации, это может быть имя, адрес электронной почты, номер учетной записи, и т.д.
- **Аутентификация** — предоставление доказательств, что вы на самом деле есть тот, кем идентифицировались (от слова “authentic” — истинный, подлинный).
- **Авторизация** — проверка, что вам разрешен доступ к запрашиваемому ресурсу.
- **Аутентификация по паролю.**
  Этот метод основывается на том, что пользователь должен предоставить username и password для успешной идентификации и аутентификации в системе. Пара username/password задается пользователем при его регистрации в системе, при этом в качестве username может выступать адрес электронной почты пользователя.
- При использовании HTTP-протокола простейший способ аутентификации — Basic access authentication. Первым, что при обращении к защищенному ресурсу сервер выдаст пользователю, не имеющему доступа, будет ошибка 401 Unauthorized. При этом ответ также содержит информацию о типе аутентификации (в нашем случае – Basic), который он может принимать, и контекст, в рамках которого эта аутентификация действует (Realm). Пользователь вводит логин и пароль, они упаковываются в Base64 и отправляются на сервер для проверки. Здесь существуют различные опасности. Самая распространенная — угроза man-in-the-middle attack, или атаки посредника, в ходе которой при использовании незащищенного соединения учетные данные могут перехватить злоумышленники в момент передачи от клиента к серверу или обратно.
- **Аутентификация по одноразовым паролям.**
  Аутентификация по одноразовым паролям обычно применяется дополнительно к аутентификации по паролям для реализации two-factor authentication (2FA). В этой концепции пользователю необходимо предоставить данные двух типов для входа в систему: что-то, что он знает (например, пароль), и что-то, чем он владеет (например,

CyberBionic Systematics ®
19 Eugene Sverstyuk Str., 5 floor
Kyiv, Ukraine

Tel. 0 800 750 312
E-mail: edu@cbsystematics.com
Site: www.edu.cbsystematics.com | itvdn.com

устройство для генерации одноразовых паролей). Наличие двух факторов позволяет в значительной степени увеличить уровень безопасности.

- **Аутентификация по токенам.**
  Следующее поколение способов аутентификации представляет Token Based Authentication, который обычно применяется при построении систем Single sign-on (SSO). При его использовании запрашиваемый сервис делегирует функцию проверки достоверности сведений о пользователе другому сервису. Т. е. провайдер услуг доверяет выдачу необходимых для доступа токенов собственно токен-провайдеру (Identity provider).
- Дальнейшее усовершенствование процесса понадобилось ввиду того, что токен-аутентификация требует присутствия пользователя в момент получения доступа к защищенному ресурсу. Потому что Identity provider при передаче ему управления будет с пользователем взаимодействовать, запрашивая, например, логин и пароль.
  В случае сервиса, который от имени пользователя должен через определенные промежутки времени опрашивать некий третий ресурс, — допустим, получать доступ к списку контактов в социальной сети — токен-аутентификация работать уже не будет. Дело в том, что идентификаторы сессии обычно живут очень недолго, чтобы в случае их перехвата злоумышленники получили доступ к сервису лишь на ограниченное время. Но из-за короткого срока действия токена не хватает, например, на ночной процесс.
- В 2006 году в ходе работы над реализацией протокола Open ID для Twitter обнаружилась потребность в новом открытом протоколе авторизации. В 2007 инженеры Google и AOL начали совместную работу над ним, а в 2009 Twitter предложил своим пользователям решение, делегировавшее сторонним сервисам доступ к аккаунтам и основанное на протоколе OAuth. Три года спустя была опубликована новая версия — OAuth 2, упростившая разработку клиентских приложений и получившая целый ряд новых возможностей, среди которых оказалось и обновление токена без участия пользователя.
- **JSON Web Token (JWT)** — содержит три блока, разделенных точками: заголовок, набор полей (claims) и подпись. Первые два блока представлены в JSON-формате и дополнительно закодированы в формат base64. Набор полей содержит произвольные пары имя/значения, притом стандарт JWT определяет несколько зарезервированных имен (iss, aud, exp и другие). Подпись может генерироваться при помощи и симметричных алгоритмов шифрования, и асимметричных. Кроме того, существует отдельный стандарт, отписывающий формат зашифрованного JWT-токена.

Закрепление материала

- Что такое аутентификация?
- Что такое авторизация?
- В чем разница между аутентификацией и авторизацией?
- Опишите процесс аутентификации с помощью токенов.

Дополнительное задание

Задание

Реализуйте авторизацию пользователя. Для этого, разделите ваши представления на логичные блоки, для которых нужна не только аутентификация, но и права доступа, например, изменение или удаление фильма. Добавьте проверку, чтобы фильм мог изменять только пользователь, у которого есть is_admin=True.

Самостоятельная деятельность учащегося

CyberBionic Systematics ®
19 Eugene Sverstyuk Str., 5 floor
Kyiv, Ukraine

Tel. 0 800 750 312
E-mail: edu@cbsystematics.com
Site: www.edu.cbsystematics.com | itvdn.com

Задание 1
Выучите основные понятия, рассмотренные на уроке.

Задание 2
Изучите материалы из рекомендуемых ресурсов.

Задание 3
Реализуйте один из предложенных способов аутентификации веб-приложений, кроме аутентификации с помощью токенов.

Рекомендуемые ресурсы

Зачем нужен Refresh Token, если есть Access Token?
https://habr.com/ru/company/voximplant/blog/323160/

JWT Theory:
https://www.youtube.com/playlist?list=PLvTBThJr861y60LQrUGpJNPu3Nt2EeQsP

Пять простых шагов для понимания JSON Web Tokens (JWT)
https://habr.com/ru/post/340146/

OAuth 2.0 простым и понятным языком
https://habr.com/ru/company/mailru/blog/115163/

CyberBionic Systematics ®
19 Eugene Sverstyuk Str., 5 floor
Kyiv, Ukraine

Tel. 0 800 750 312
E-mail: edu@cbsystematics.com
Site: www.edu.cbsystematics.com | itvdn.com