УДК 004

СОВРЕМЕННЫЙ ПОДХОД К СОЗДАНИЮ АУТЕНТИФИКАЦИИ В WEB-ПРИЛОЖЕНИЯХ

И. Ю. ДЕРЕВЯНКО, А. С. ФУРМАНОВ
Научный руководитель Н. В. ВЫГОВСКАЯ
Белорусско-Российский университет

На процессах аутентификации и авторизации основано разделение прав доступа, без которого не обходится ни одно более или менее серьезное приложение. Поэтому понимать, как они происходили раньше и происходят теперь, очень важно. Проблема правильного подхода к созданию аутентификации и авторизации является актуальной.

Существует четыре основных способа аутентификации: HTTP Basic Authentication, HTTP Digest Authentication, Forms Authentication, Token Authentication.

Первые три способа являются достаточно устаревшими и используются лишь в давно написанных системах.

Token Authentication – способ аутентификации, который обычно применяется при построении систем Single sign-on. При его использовании запрашиваемый сервис делегирует функцию проверки достоверности сведений о пользователе другому сервису. Таким образом провайдер услуг доверяет выдачу необходимых для доступа токенов собственно токен-провайдеру.

Одной из разновидностей Token Authentication является JSON web token.

Веб-токен JSON, или JWT, представляет собой стандартизированный, в некоторых случаях подписанный и/или зашифрованный формат упаковки данных, который используется для безопасной передачи информации между двумя сторонами.

JWT определяет особую структуру информации, которая отправляется по сети. Она представлена в двух формах – сериализованной и десериализованной.

В несериализованном виде JWT состоит из заголовка и полезной нагрузки, которые являются обычными JSON-объектами. В сериализованной – строка формата [Заголовок].[Тело].[Сигнатура].

Заголовок в основном используется для описания криптографических функций, которые применяются для подписи и/или шифрования токена. В теле находится информация для подтверждения пользователя. Сигнатура – результат шифрования заголовка и тела, а также «секрет». Секрет представляет собой строку, которая также шифруется и добавляется в сигнатуру, о нем знают стороны верификации пользователя.

Благодаря тому, что любое изменение данных внутри токена приведет к изменению итоговой зашифрованной строки, а также тому, что не требуется хранить сессии и «секрет» хранится на стороне верификации, JWT является отличным способом реализации аутентификации в современных web-приложениях.

JWT аутентификация была использована в разработке проекта web-приложения для клининговых компаний и показала свою эффективность.