УДК 004.056

JWT АУТЕНТИФИКАЦИЯ ЧЕРЕЗ HTTP-ONLY COOKIE

Листванович А.А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Воробей А.В. – магистр технических наук, ассистент кафедры ИПиЭ

Аннотация. В данной статье рассматривается эффективное сочетание *JWT (JSON Web Token)* аутентификации и использования *HTTP-Only Cookie* в веб-приложениях. Автор подробно рассказывает о преимуществах *JWT*, особенностях *HTTP-Only Cookie* и их совместном использовании для обеспечения безопасности аутентификации. Описан процесс аутентификации, включая создание, передачу и хранение токенов, а также проверку и обновление токена на стороне сервера. Данная методика предоставляет удобство использования и повышенный уровень безопасности веб-приложений.

Ключевые слова: *JWT, Cookie*, аутентификация, веб-приложения, безопасность.

Введение. Безопасность в наши дни играет ключевую роль в жизни любого информационного продукта. *JWT (JSON Web Token)* – это стандарт обмена данными в формате *JSON* между сторонами, и он нашел широкое применение, в том числе в области аутентификации. В данной научной работе рассмотрим использование *JWT* для аутентификации через *HTTP-Only Cookie* и проанализируем преимущества использования *HTTP-Only Cookie*.

Основная часть. *JWT* представляет собой компактный и самодостаточный способ передачи информации между сторонами в виде *JSON*-объекта. Он состоит из трех частей: заголовка, полезной нагрузки (*payload*) и подписи. Эти три части могут быть закодированы и переданы в виде строки, что делает *JWT* удобным для использования в *URL*, параметрах запросов и заголовках *HTTP* [1].

Преимущества *JWT* включают в себя легкость передачи данных, подпись для обеспечения целостности и возможность использования алгоритмов шифрования. Однако, для предотвращения злоупотреблений и обеспечения безопасности, важно правильно реализовать и использовать *JWT*.

HTTP-Only Cookie – это особый тип *cookie*, который ограничивает доступ к нему из *JavaScript*, делая его недоступным для потенциальных атак, таких как *XSS* (*Cross-Site Scripting*). При установке флага *HTTP-Only* для *cookie*, оно становится доступным только для серверных запросов, что повышает уровень безопасности [2].

Преимущества *HTTP-Only Cookie* в контексте аутентификации включают:

1) Защита от *XSS*-атак: поскольку *HTTP-Only Cookie* недоступны из *JavaScript*, они предотвращают возможность кражи токена аутентификации через внедрение вредоносного кода на клиентской стороне.

2) Повышенная безопасность: запрет доступа к *cookie* из *JavaScript* снижает риски атак, связанных с утечкой аутентификационных данных.

3) Соблюдение принципов *Same-Origin Policy: HTTP-Only Cookie* соответствуют принципам *Same-Origin Policy*, что делает их более безопасными в сравнении с другими методами хранения данных на клиентской стороне.

JWT аутентификация через *HTTP-Only Cookie*. Для обеспечения безопасности и соблюдения принципов *Same-Origin Policy*, предлагается использовать *HTTP-Only Cookie*

для хранения *JWT*. После успешной аутентификации, сервер создает *JWT* и передает его клиенту в виде *HTTP-Only Cookie*. Клиент хранит токен и автоматически включает его в каждый запрос к серверу.

Процесс аутентификации:

6) Пользователь вводит учетные данные: пользователь вводит учетные данные для аутентификации.

7) Создание *JWT* и установка *HTTP-Only Cookie*: сервер создает *JWT* и отправляет его клиенту в виде *HTTP-Only Cookie*.

8) Хранение токена и автоматическая отправка: клиент хранит токен в *HTTP-Only Cookie* и автоматически включает его в каждый запрос к серверу.

9) Проверка и обновление токена: сервер проверяет подлинность токена при каждом запросе. При необходимости, сервер может обновлять токен, предоставляя новый *HTTP-Only Cookie* с обновленным *JWT*.

Заключение. *JWT* аутентификация через *HTTP-Only Cookie* предоставляет эффективный и безопасный механизм для аутентификации пользователей в веб-приложениях. Объединяя удобство использования *JWT* и безопасность *HTTP-Only Cookie*, данная методика обеспечивает надежную защиту веб-приложений от различных видов атак, сохраняя при этом высокий уровень удобства для конечного пользователя.

Список литературы

1. Свободная энциклопедия «Википедия» [Электронный ресурс] / Свободная энциклопедия «Википедия» – Таллин, 2023. – Режим доступа: https://ru.wikipedia.org/wiki/JSON_Web_Token – Дата доступа: 19.01.2024

2. Mozilla Foundation Web Docs [Электронный ресурс] / Mozilla Foundation Web Docs – Калифорния, 2023. – Режим доступа: https://developer.mozilla.org/ru/docs/Web/HTTP/Cookies – Дата доступа: 19.01.2024

UDC 004.056

JWT AUTHENTICATION WITH HTTP-ONLY COOKIE

Listvanovich A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Vorobey A.V. – master of technical sciences, assistant of the department of EPE

Annotation. This article explores the effective combination of JWT (JSON Web Token) authentication and the use of HTTP-Only Cookies in web applications. The author provides a detailed overview of the advantages of JWT, the characteristics of HTTP-Only Cookies, and their collaborative use to ensure authentication security. The authentication process is described, covering token creation, transmission, and storage, as well as token verification and updates on the server side. This methodology offers convenience and an enhanced level of security for web applications.

Keywords: JWT, Cookie, authentication, web applications, security.