УДК 004
Неласа Г.В.[1], Слива О.М.[2]
[1] проф. НУ «Запорізька політехніка»
[2] студ. гр. РТ-719м НУ «Запорізька політехніка»

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧА НА ВЕБ-САЙТІ З ВИКОРИСТАННЯМ JWT

JSON Web Token (JWT) – це відкритий стандарт (RFC 7519) який визначає компактний і автономний спосіб безпечної передачі інформації між сторонами в якості об'єкта JSON. Ця інформація може бути перевірена і довірена, тому що вона має цифровий підпис. JWTs може бути підписаний з допомогою секрету (з допомогою алгоритму HMAC) або пари відкритого та закритого ключів з використанням RSA або ECDSA.

Хоча JWTs може бути зашифрований, щоб забезпечити секретність між сторонами, ми зосередимося на підписаний жетони. Підписані токени можуть підтвердити цілісність з тверджень, що містяться в ньому, в той час як зашифровані маркери приховати це претензії з боку інших сторін. Коли токени підписуються з допомогою пар відкритого та закритого ключів, підпис також засвідчує, що тільки сторона, що володіє закритим ключем, підписала його.

Ось деякі сценарії, де веб-маркери JSON корисні:

1. Авторизація: Це найбільш поширений сценарій для використання JWT. Після того, як користувач увійшов в систему, кожний наступний запит буде включати JWT, дозволяючи користувачеві отримати доступ до маршрутів, службам і ресурсів, які можна з цим маркером. Єдиний вхід-це функція, яка широко використовує JWT в даний час, із-за його невеликих накладних витрат і його здатності легко використовуватися в різних доменах.

2. Обмін інформацією: Веб-маркери JSON є хорошим способом безпечної передачі інформації між учасниками. Оскільки JWTs може бути укладено, наприклад, з допомогою пар відкритого та закритого ключів—ви можете бути впевнені, що відправники є тими, за кого він себе видає. Крім того, оскільки підпис обчислюється з використанням заголовка і корисних даних, можна також перевірити, що вміст не було змінено.

У своїй компактній формі веб-маркери JSON складаються з трьох частин, розділених крапками (.), які є:

Заголовок

Корисне навантаження

Підпис

Тому JWT зазвичай виглядає наступним чином.

xxxxx.yyyyy.zzzzz

Заголовок зазвичай складається з двох частин: тип сертифіката, який є JWT, і використовуваний алгоритм підпису, такий як HMAC SHA256 або RSA.

Друга частина маркера-це корисні дані, які містять твердження. Затвердження-це інструкції про сутність (як правило, користувач) і додаткових даних. Існує три типи претензій: зареєстровані , публічні та приватні претензії.

Зареєстровані претензії: це набір попередньо визначених претензій, які не є обов'язковими, але рекомендуються для забезпечення набору корисних, взаємозамінних претензій. Деякі з них: iss (емітент), exp (строк дії), sub (суб'єкт), aud (аудиторія) та інші .

Публічні претензії: вони можуть бути визначені за бажанням тими, хто використовує JWTs. Але щоб уникнути конфліктів, вони повинні бути визначені в реєстрі веб-маркерів IANA JSON або визначені як URI, що містить стійкий до конфліктів простір імен.

Приватні твердження: це користувальницькі твердження, створені для обміну інформацією між сторонами, які згодні їх використовувати і не є зареєстрованими або публічними твердженнями.

Щоб створити частина підпису, ви повинні взяти закодований заголовок, закодоване корисне навантаження, секрет, алгоритм, зазначений у заголовку, і підписати його.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. JSON Web Token введення – jwt.io [Електронний ресурс]. – Режим доступу до ресурсу: https://jwt.io/introduction/.

2. П'ять простих кроків для розуміння JSON Web Tokens (JWT) [Електронний ресурс]. – Режим доступу до ресурсу: https://habr.com/ru/post/340146/.