Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра Обчислювальної Техніки

Лабораторна робота №5

з дисципліни "Безпека програмного забезпечення"

Тема: "Засвоювання базових навичок роботи з валідацією токенів"

Виконав:

студент групи ІП-93

Домінський В.О.

Київ 2023

**Зміст**

[Завдання: 3](#_Toc124004272)

[Виконання: 3](#_Toc124004273)

[Висновок: 8](#_Toc124004274)

[Посилання: 8](#_Toc124004275)

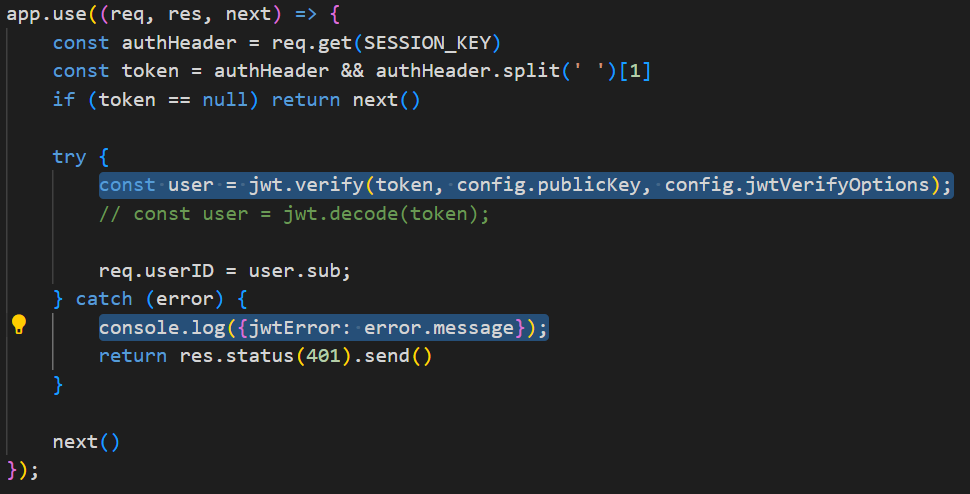
### Завдання:

1. Розширити Лабораторну работу 4 перевіркой сігнатури JWT токена. Приклади SDK <https://auth0.com/docs/quickstart/backend>. У випадку асиметричного ключа, public є можливість отримати за посиланням <https://kpi.eu.auth0.com/pem>, aбо за формулою <https://[API_DOMAIN]/pem>

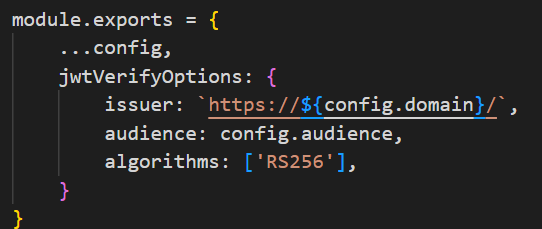
### Виконання:

У даній лабораторній роботі треба дописати функціонал верифікації JWT токена та, якщо використовується асиметричне шифрування, отримати public ключ:

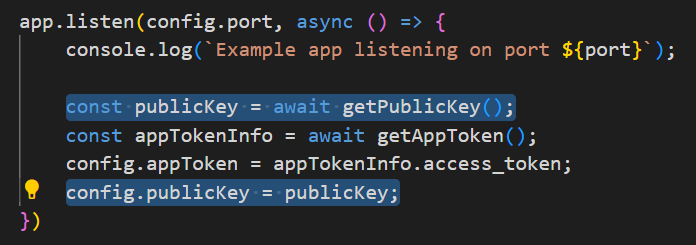
Почнемо з перевірки сигнатури JWT токена



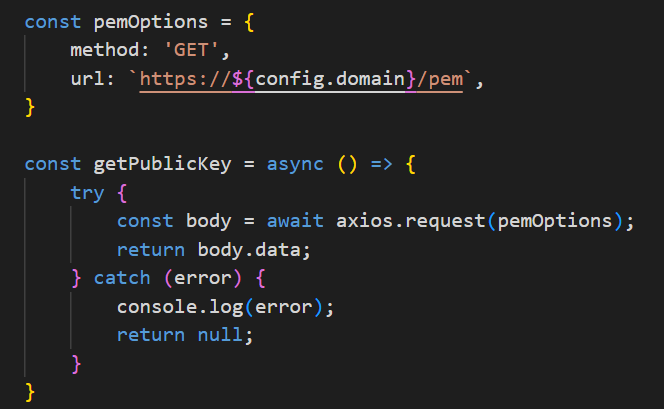
Тепер замість простого декодування Ми використовуємо верифікацію, де першим аргументом йде сам token, другим – public key (про це дещо пізніше), а останнім – параметри для верифікації:



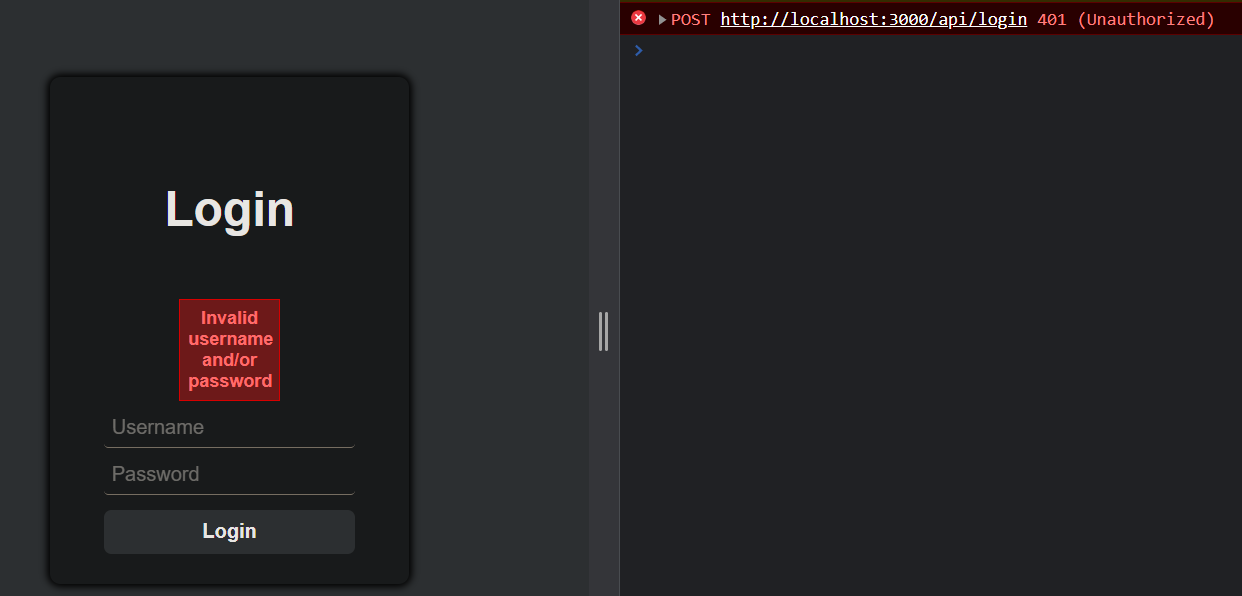
Перейдемо до public key:



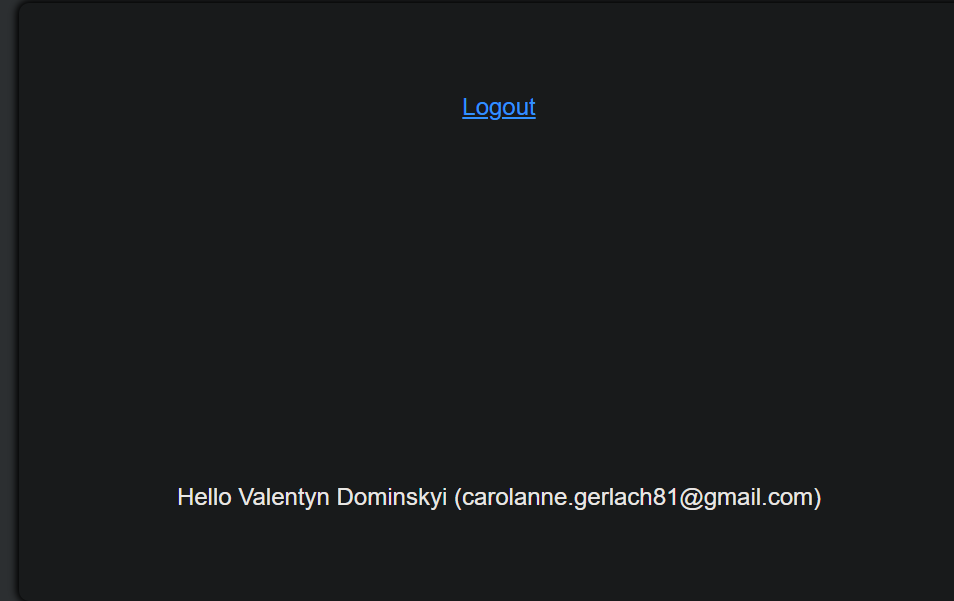
На самому старті Нашого застосунку Ми записуємо ключ до конфігу, а перед цим – отримуємо його за допомогою функції getPublicKey:



Давайте запустимо Наш застосунок та спробуємо ввести неправильні дані:

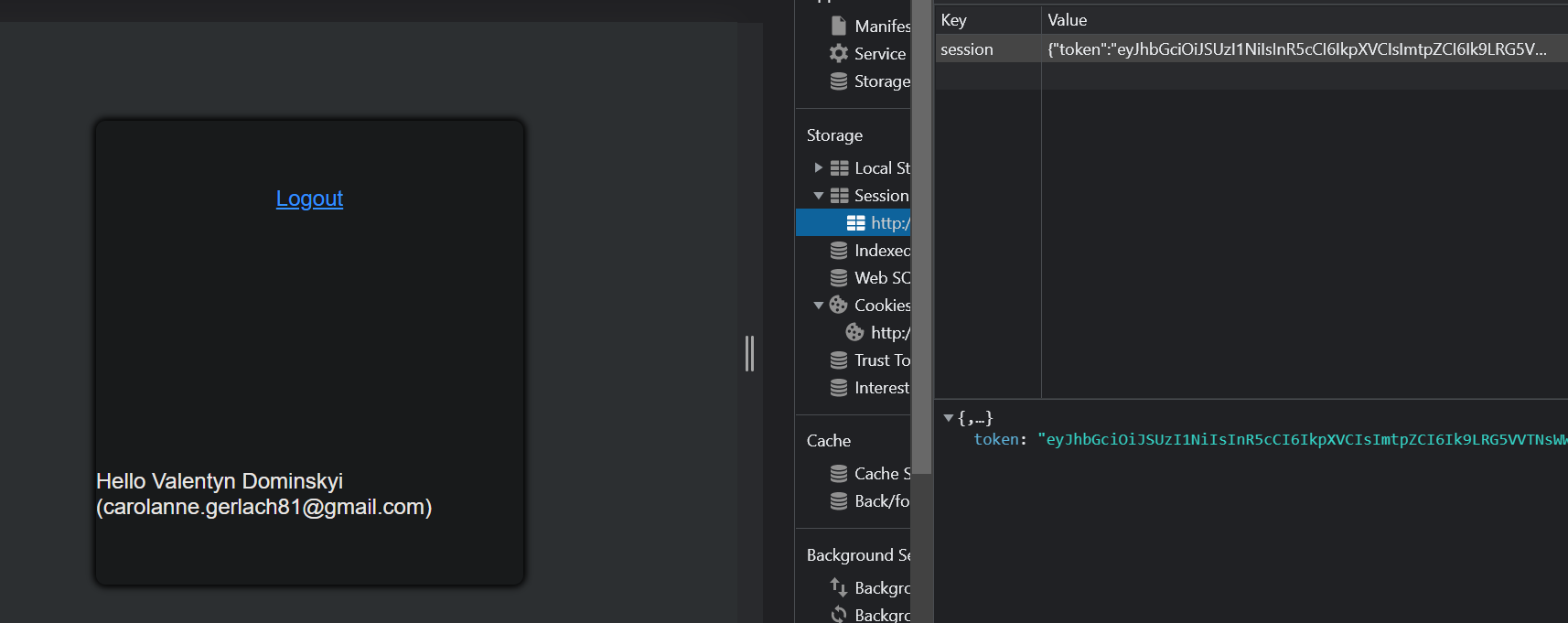


Як видно з консолі – Нам видало помилку 401. Тепер увійдемо в Нашого користувача:

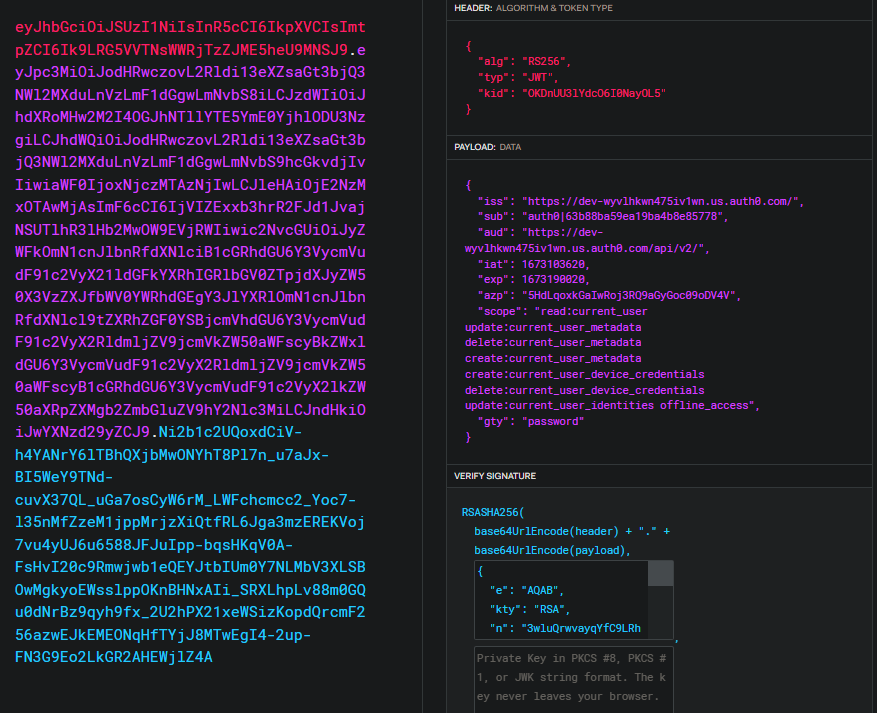


Усе пройшло успішно!

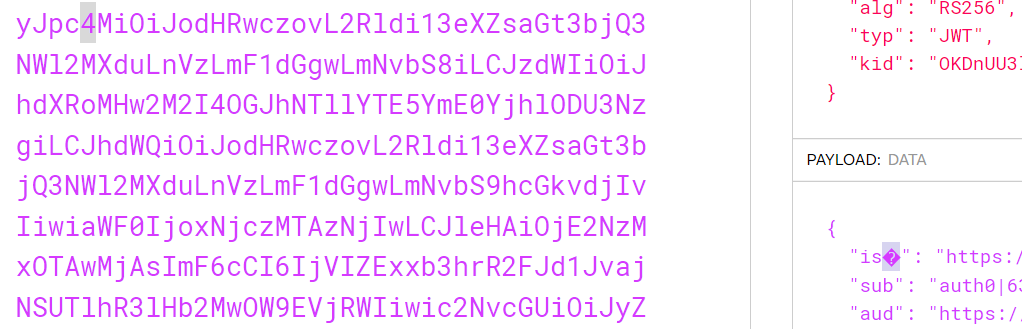
Проте давайте розглянемо, чи дійсно працює Наша перевірка JWT токену. При вдалому вході Ми можемо побачити значення Нашого токену:



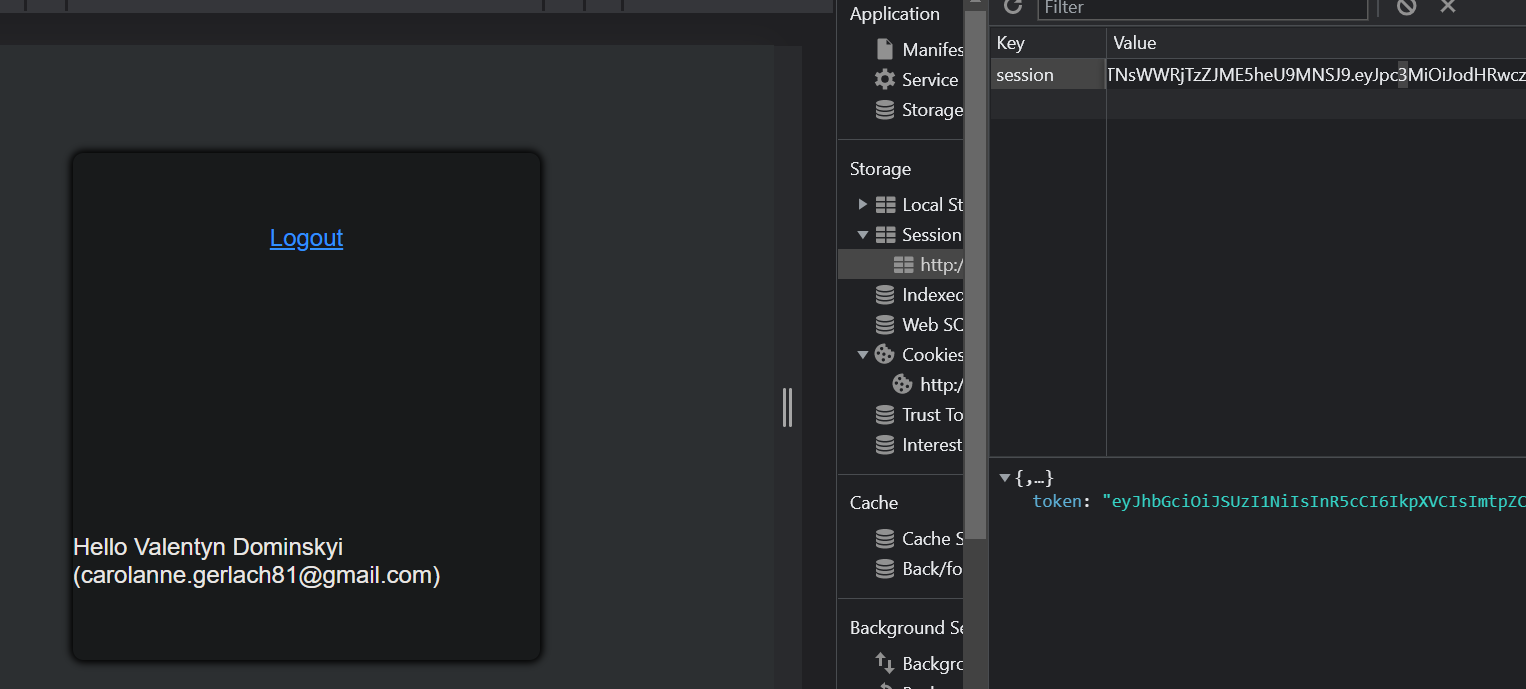
Якщо перейдемо на сайт jwt.io та спробуємо його розшифрувати, то отримаємо ось такі значення:



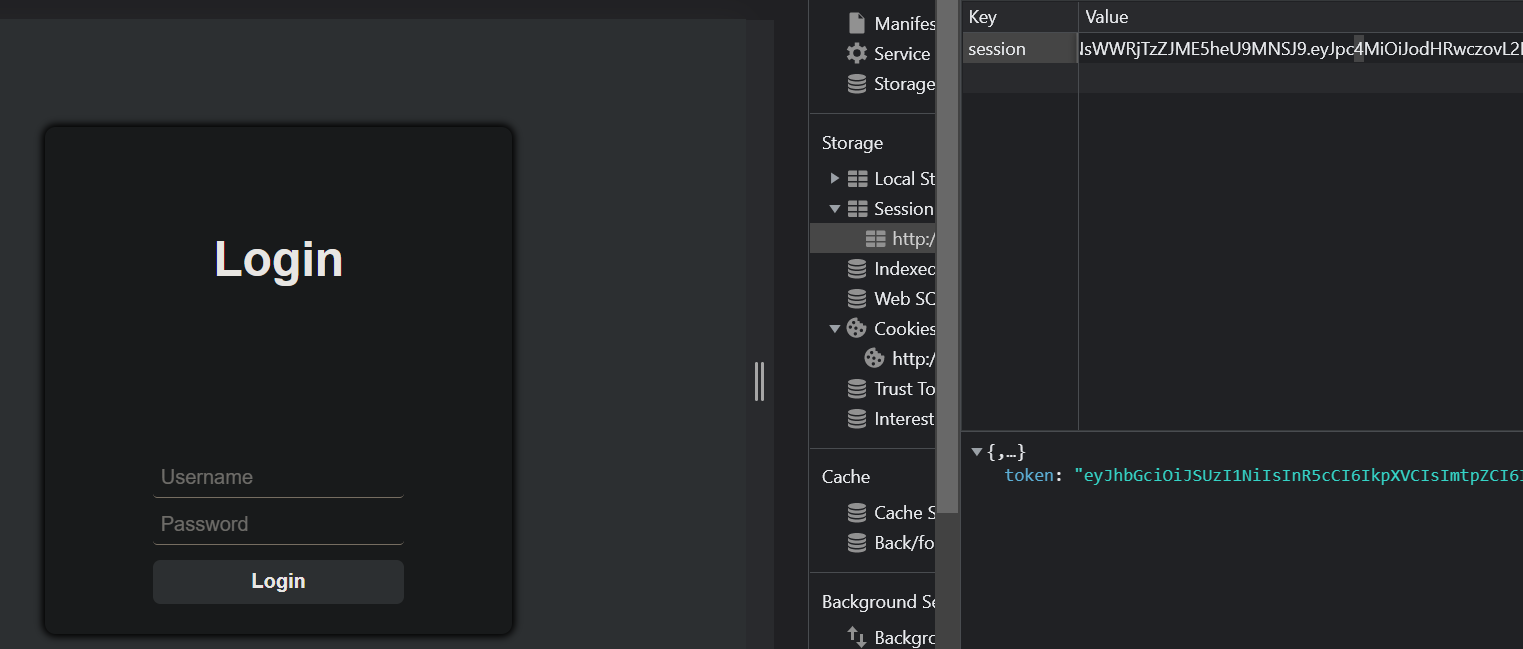
Пропоную зараз замінити один символ у частині з Data і отримуємо результат:



Але треба подивитися, що станеться у Нашому застосунку:



Змінимо цю цифру та перезавантажимо сторінку:



Ми не змогли верифікувати токен, тому Нас викинуло на початкову сторінку!

# Висновок:

Під час виконання роботи Я отримав кращі практичні знання у верифікації JWT токенів та що відбувається, коли вони не проходять перевірку (наприклад при зміні токену власноруч). Попрацював з асинхронним шифруванням, яке має публічний ключ

# Посилання:

* [Проект на GitHub](https://github.com/VsIG-official/Software-Security/tree/master/Labs/Lab5)