Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

Лабораторна робота 5
з дисципліни
«Безпера програмного забезпечення»

Виконав:
студент групи ІП-03
Янишин Віталій

Перевірив:
Іваніщев Б.В

Київ 2023

Лабораторна робота 5

Засвоювання базових навичок роботи з валідацією токенів

Завдання:

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, або за формулою https://[API_DOMAIN]/pem Надати код рішення.

Виконання:

Для валідації використаємо метод verify з jsonwebtoken

```
const validateJwt = async (jwt) => {
  const cert = fs.readFileSync("cert.pem");
  verify(jwt, cert, { algorithms: ["RS256"] }, (error, payload) => {
    if (error) throw new Error(error);
    console.log("jwt validated");
    console.log(payload);
  });
};

app.get("/", async (req, res) => {
  if (req.session.access_token) {
    validateJwt(req.session.access_token);
    if (true) {
      const response = await refreshToken(req.session.refresh_token);
      const responseObj = JSON.parse(response);
      req.session.access_token = responseObj.access_token;
      req.session.expires_at =
        Math.floor(Date.now() / 1000) + responseObj.expires_in;
      console.log(`token refreshed:
        ${response}
      `);
    }

    return res.json({
      username: req.session.username,
      logout: "http://localhost:3000/logout",
    });
  }
  res.sendFile(path.join(__dirname + "/index.html"));
});
```

```
jwt validated
{
  iss: 'https://dev-7whj26jw4qopw248.us.auth0.com/',
  sub: 'auth0|6592d3e2e46a733206842954',
  aud: 'https://dev-7whj26jw4qopw248.us.auth0.com/api/v2/',
  iat: 1704121769,
  exp: 1704208169,
  azp: '7EsexnfRLQ8LvVB1ywrhMB758y9ShFtR',
  scope: 'read:current_user update:current_user_metadata delete:current_user_metadata create:current_user_me
eate:current_user_device_credentials delete:current_user_device_credentials update:current_user_identities d
cess',
  gty: [ 'refresh_token', 'password' ]
}
```