

Міністерство освіти і науки України Національний технічний університет України "КПІ імені Ігоря Сікорського"

Факультет інформатики та обчислювальної техніки Кафедра інформаційних систем та технологій

3BIT

лабораторна робота №2 з

курсу «Безпека програмного забезпечення»

Тема: «Засвоювання базових навичок OAuth2 авторизаційного протокола»

Перевірив: Виконав:

Група ІП-11 Головня Олександр

Завдання:

1) Використовуючи наведені налаштування, створити запит на отримання токену

через client credential grant

https://auth0.com/docs/api/authentication#client-credentials-flow

curl --request POST \

--url 'https://YOUR DOMAIN/oauth/token' \

--header 'content-type: application/x-www-form-urlencoded' \

--data

'audience=API_IDENTIFIER&grant_type=client_credentials&client_id=YOUR_
CLIENT ID&client secret=YOUR CLIENT SECRET'

Domain: kpi.eu.auth0.com

ClientID: JIvCO5c2IBHlAe2patn6l6q5H35qxti0

Client Secret: ZRF8Op0tWM36p1_hxXTU-B0K_Gq_-

eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB

Audience: https://kpi.eu.auth0.com/api/v2

2) Створити юзера з власним email в системі використовуючи метод

https://auth0.com/docs/api/management/v2#!/Users/post_users

та отриманий токен

Для отримання додаткового балу — зробити власний акаунт в auth0 https://auth0.com/

Створити application та запити описані вище вже використовуючи власні налаштування. Детальну інформацію розбирали на практичному завданні.

Результати виконання:

Повний лістинг файлів можна знайти тут:

https://github.com/YeaLowww/KPI-

ALL/tree/main/Fourth%20year/Software%20security

Підставивши усі параметри, отримаємо відповідний запит:

curl --request POST --url "https://kpi.eu.auth0.com/oauth/token" --header "contenttype:application/x-www-form-urlencoded" --data

"audience=https://kpi.eu.auth0.com/api/v2/&grant_type=client_credentials&client
_id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0&client_secret=ZRF8Op0tWM36p1_h

xXTU-B0K_Gq_-eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB"

curl --request POST --url 'https://kpi.eu.auth0.com/oauth/token' --header 'contenttype:application/x-www-form-urlencoded' --data
'audience=https://kpi.eu.auth0.com/api/v2/&grant_type=client_credentials&client_
'audience=https://kpi.eu.auth0.com/api/v2/&grant_type=client_credentials&client_

id=JIvCO5c2IBHlAe2patn6l6q5H35qxti0&client secret=ZRF8Op0tWM36p1 hx

Результат запиту можна побачити на рисунку:

XTU-B0K_Gq_-eAVtlrQpY24CasYiDmcXBhNS6IJMNcz1EgB'

C:\Users\Cawa Головня\Desktop\security\lab2>curl --request POST --url "https://kpi.eu.aut h0.com/oauth/token" --header "content-type:application/x-www-form-urlencoded" --data "aud ience=https://kpi.eu.auth0.com/api/v2/&grant_type=client_credentials&client_id=JIvC05c2IB HlAe2patn6l6q5H35qxti0&client_secret=ZRF80p0tWM36p1_hxXTU-B0K_Gq_-eAVtlrQpY24CasYiDmcXBhN S6IJMNcz1EgB"
{"access_token":"eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR1dZYjdk ViJ9.eyJpc3Mi0iJodHRwczovL2twaS5ldS5hdXRoMC5jb20vIiwic3ViIjoiSkl2Q081YzJJQkhsQWUycGF0bjZs NnE1SDM1cXh0aTBAY2xpZW50cyIsImF1ZCI6Imh0dHBz0i8va3BpLmV1LmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0IjoxNzEzMDExNjk1LCJleHAi0jE3MTMw0Tgw0TUsInNjb3BlIjoicmVhZDp1c2VycyBjcmVhdGU6dXNlcnMiLCJndHki0iJjbGllbnQtY3JlZGVudGlhbHMiLCJhenAi0iJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxeHRpMCJ9.QJoyWnQEsQDqlWDUcqeKLaonvHaciAyyp87LIQNQ5P9wHp3HWvrQvZTqGwm0MbereR09VT9_Qie9F2zUzlmYsCafNHAW2rAPQ3qVBt6GIU_-nVB49R3gzYZhJTl0reZ65cljgKY17A4dkOhmHrDlrXMTMp9f60PWFvVZhB0LY5_e0N-IWhyXDf2ugYZusi37ea9tL0mqctL4mHKxFnKxDuetEDA6GX39ju6hyl0P0JcV9ZnFsJkhtNSqeMrKnjIF2x32U55HEJsG_puZ7Yq3GWaPd8BcM-Ypt0Ifrb_LQAM-J0KV0xYI2hqwdQPtmafjeeL2PhMsw8yKOKLAY-img", "scope":"read:users create:users", "expires_in":86400, "token_type":"Bearer"}
C:\Users\Cawa Головня\Desktop\security\lab2>

Ми отримали наш токен:

{"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTIB ZFhrMERaUjhmR1dZYjdkViJ9.eyJpc3MiOiJodHRwczovL2twaS5ldS5hdXRoM C5jb20vIiwic3ViIjoiSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTBA Y2xpZW50cyIsImF1ZCI6Imh0dHBzOi8va3BpLmV1LmF1dGgwLmNvbS9hcGk vdjIvIiwiaWF0IjoxNzEzMDExNjk1LCJIeHAiOjE3MTMwOTgwOTUsInNjb3BII joicmVhZDp1c2VycyBjcmVhdGU6dXNlcnMiLCJndHkiOiJjbGllbnQtY3JlZGVu dGlhbHMiLCJhenAiOiJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxe HRpMCJ9.QJoyWnQEsQDqlWDUcqeKLaonvHaciAyyp87LIQNQ5P9wHp3HW vrQvZTqGwm0MbereR09VT9_Qie9F2zUzlmYsCafNHAWm2rAPQ3qVBt6GIU

nVB49R3gzYZhJTl0reZ65cljgKY17A4dkOhmHrDlrXMTMp9f6OPWFvVZhBO

LY5 e0N-

IWhyXDf2ugYZusi37ea9tL0mqctL4mHKxFnKxDuetEDA6GX39ju6hylOP0JcV9 ZnFsJkhtNSqeMrKnjIF2x32U55HEJsG_puZ7Yq3GWaPd8BcM-YptOIfrb_LQAM-J0KVOxYI2hqwdQPtmafjeeL2PhMsw8yKOKLAYimg","scope":"read:users create:users","expires_in":86400,"token_type":"Bearer"} **2.**

Sasha Holovnia, Створимо користувача 3 іменем скринькою fakeyealow@gmail.com та ніком YeaLow. Запит матиме такий вигляд: curl --request POST --url "https://kpi.eu.auth0.com/api/v2/users" --header "Contentapplication/json" --header "Accept: application/json" Type: "\"email\":\"fakeyealow@gmail.com\",\"user metadata\":\\,\"blocked\":false,\"e mail verified\":false,\"app metadata\":{},\"given name\":\"Sasha\",\"family name \":\"Holovnia\",\"name\":\"Sasha\",\"nickname\":\"YeaLow\",\"picture\":\"https://kt pu.kpi.ua/wp-

 $content/uploads/2016/12/89dd0d645592478b0b8933e8eb525806.jpg \verb|\|, \| connection \verb|\| '': \| Username-Password-$

Authentication\",\"password\":\"IP11Holovnia\",\"verify_email\":false}" --header "Authorization: Bearer

eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjVCZTlBZFhrMERaUjhmR 1dZYjdkViJ9.eyJpc3MiOiJodHRwczovL2twaS5ldS5hdXRoMC5jb20vliwic3ViIjo iSkl2Q081YzJJQkhsQWUycGF0bjZsNnE1SDM1cXh0aTBAY2xpZW50cyIsImF 1ZCI6Imh0dHBzOi8va3BpLmV1LmF1dGgwLmNvbS9hcGkvdjIvIiwiaWF0Ijox NzEzMDExNjk1LCJleHAiOjE3MTMwOTgwOTUsInNjb3BIIjoicmVhZDp1c2Vy cyBjcmVhdGU6dXNlcnMiLCJndHkiOiJjbGllbnQtY3JlZGVudGlhbHMiLCJhenA iOiJKSXZDTzVjMklCSGxBZTJwYXRuNmw2cTVIMzVxeHRpMCJ9.QJoyWn QEsQDqlWDUcqeKLaonvHaciAyyp87LIQNQ5P9wHp3HWvrQvZTqGwm0Mbe reR09VT9_Qie9F2zUzlmYsCafNHAWm2rAPQ3qVBt6GIU_-

nVB49R3gzYZhJTl0reZ65cljgKY17A4dkOhmHrDlrXMTMp9f6OPWFvVZhBOLY5_e0N-

IWhyXDf2ugYZusi37ea9tL0mqctL4mHKxFnKxDuetEDA6GX39ju6hylOP0JcV9

ZnFsJkhtNSqeMrKnjIF2x32U55HEJsG_puZ7Yq3GWaPd8BcM-YptOIfrb LQAM-J0KVOxYI2hqwdQPtmafjeeL2PhMsw8yKOKLAY-img

Результат виконання – створений користувач, що бачимо на рисунку:

```
C:\Users\Cawa Fonosha\Desktop\security\lab2>curl --request POST --url "https://kpi.eu.auth0.com/api/v2/users" --header "Content-Type: application/json" --deader "Accept: application/json" --deader "\"email\":\"fakeyealow@gmail.com\",\"user_metadata\":\{},\"blocked\":false,\"email_verified\":false,\"app_metadata\":\{},\"blocked\":false,\"email_name\":\"https://ktpu.kpi.ua/wp-content/uploads/2016/12/89dd0d645592478b0b8933e8eb525806.jpg\",\"connection\":\"Username-Password-Authentication\","password\":\"PIPIHIDlovnia\",\"verify_email\":false\",-false\",-false\",-false\",-yenify_ewail\":\"false\",-yenify_ewail\":\"false\",-yenify_ewail\":false\",-yenify_ewail\":\"false\",-yenify_ewail\":\"false\",-yenify_ewail\":\"false\",-yenify_ewail\":\"false\",-yenify_ewail\":false\",-yenify_ewail\":\"false\",-yenify_ewail\":\"false\",-yenify_ewail\":false\",-yenify_ewail\":\"false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\":false\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\",-yenify_ewail\
```

Додаткове завдання:

Створимо файл ENV для збереження ключів, токенів:

AUTH0 URL = https://dev-eh2lg4o74zpq0730.us.auth0.com

AUTHO TOKEN=

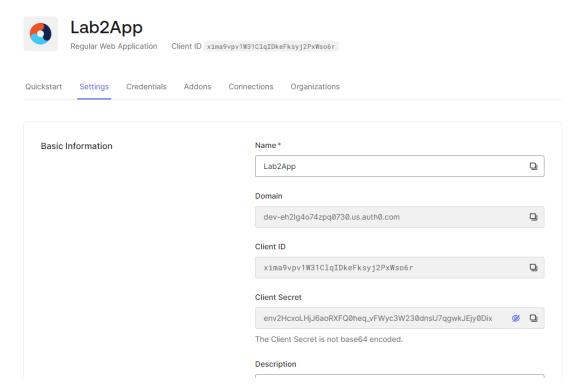
AUTH0_CLIENT_ID= xima9vpv1W31ClqIDkeFksyj2PxWso6r

AUTHO_CLIENT_SECRET=

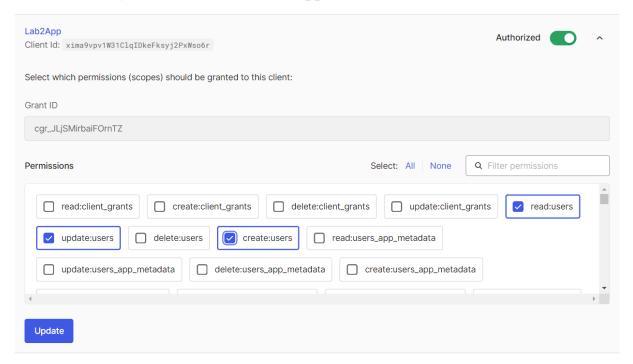
env2HcxoLHjJ6aoRXFQ0heq_vFWyc3W230dnsU7qgwkJEjy0DixRqmgVhseoz_

vO

Створимо application lab2app:



Надаємо доступи в API для нашого application:



За допомогою js файлу main.js, отримуємо токен:

PS C:\Users\Cama FonoBHq\Desktop\security\lab2> node main.js

(node:10812) [DEP0040] DeprecationWarning: The `punycode` module is deprecated. Please use a userland alternative instead.

(Use `node --trace-deprecation ...` to show where the warning was created)

{"access_token": "eyJhbGc:0iJSUzIINiISInR5cC16IkpXVCISImtpZC16Imt20C1WYzhiMk9uano5Y\RYbnFoaSJ9.eyJpc3Mi0iJodHRwczovL2RldillaDJsZzRvNzR6c

HEWNZMWLnVzLmFldGgwLmNvbS8iLCJzdWII0iJ4aWIh0XZwdjFXMzFDbHFJRGt\RmtzeWoyUHhXc282ckBjbGl\bnRzIiwiYXVkIjoiaHR0cHM6Ly9kZXYtZWgybGc0bzc0enBx

MDczMC51cy5hdXR0MC5jb20vYXBpl3YyLyIsIn\hdC16MTcyNTUINjMyNiwiZXhwIjoxNzIINjQyNzI2LCJzY29wZ5I6InJ\YW\GdXN\cnMgdXBkYXR0nvzXXJzIGMyZWF0ZTp

1c2VycyIsImd0eS16ImNsaWVudCljcmVkZW50aWFscyIsImF6cC16InhpbWE5dnB2MVzMVzMUNscUlLazVGa3N5ajJQeFdzbzZyIn0.SJ7iJzMHwB-kqZMrsI9GsSTTHI0EnygMvB

ZAaDHfb-hWzEryQXosh7KgtmB6QxG-x3qa5PPZSWR95isH3Vu2f-Yj_2\836LrhJJ-MEQmH3NMWQ09j4uXVn02hfkafEkWRhIBoGVFVPEMRevkLoX3NBqIlgRkPq_qVGzaktIj

QmELWjuVtkN-yXZaUSVHTe8MCjytaz1ezfPpGXqrwiiJXCD02Xn6zqDgLA0MVMR7_OT6A9rfyRWiFXOK_zuwdcYCgkZgEu0cQJDe7piToXBowx4GX4GIU_joAw8zwal419yu6nU

EiWbhFA3pzuvujEFx96DWRGprndMeP-yF0Zrxg", "scope": "read:users update:users create:users", "expires_in":86400, "token_type": "Bearer"}

За допомогою јя файлу create-user.js, створимо користувача:

```
PS C:\Users\Cawa Головня\Desktop\security\lab2> node create-user.js
(node:9780) [DEP0040] DeprecationWarning: The `punycode` module is deprecated. Please use a userland alternative instead.
(Use `node --trace-deprecation ...` to show where the warning was created)
{"blocked":false, "created_att":"2024-09-05117:17:27.0782","email":"holovnia@gmail.com","email_verified":false, "family_name":"Holovnia","
given_name":"Holovnia","identities":[{"user_id":"5123121","connection":"Username-Password-Authentication","provider":"auth0","isSocial"
:false}],"name":"Holovnia","nickname":"Holovnia", "picture":"https://unity.com/sites/default/files/styles/social_media_sharing/public/20
22-02/U_Logo_White_CMYK.jpg", "updated_at":"2024-09-05117:17:27.078Z","user_id":"auth0|5123121","user_metadata":{}}
PS C:\Users\Cawa Головня\Desktop\security\lab2>
```

Висновки: У ході виконання лабораторної роботи було отримано практичні навички роботи з OAuth2. Завдання полягало у отриманні токена у системі КПІ, а також створення користувача.

Лістинг коду.

```
const uuid = require('uuid');
const express = require('express');
const onFinished = require('on-finished');
const bodyParser = require('body-parser');
const path = require('path');
const port = 3000;
const fs = require('fs');
const jwt = require('jsonwebtoken');
const app = express();
app.use(bodyParser.json());
app.use(bodyParser.urlencoded({ extended: true }));
const JWT_SECRET = 'secret';
const users = [
        login: 'Login2',
        password: 'Password2',
        username: 'Username2',
```

```
},
        login: 'Login1',
        password: 'Password1',
        username: 'Username1',
    }
1
app.get('/', verifyToken, (req, res) => {
    res.json({
        username: req.user.username,
        logout: 'http://localhost:3000/logout'
    });
})
app.get('/logout', (req, res) => {
    res.redirect('/');
});
app.post('/api/login', (req, res) => {
    const { login, password } = req.body;
    const user = users.find((user) => {
        return user.login === login && user.password === password;
    });
    if (user) {
        const token = jwt.sign({ username: user.username, login: user.login },
JWT_SECRET);
        res.json({ token });
    } else {
        res.status(401).send('Unauthorized');
    }
});
app.listen(port, () => {
    console.log(`Example app listening on port ${port}`)
})
function verifyToken(req, res, next) {
    const token = req.header('Authorization');
    if (!token) {
        return res.sendFile(path.join(__dirname + '/index.html'));
    }
    jwt.verify(token, JWT_SECRET, (err, decoded) => {
        if (err) {
            return res.sendFile(path.join(__dirname + '/index.html'));
        req.user = decoded;
        next();
    });
}
```