Modul 6

# Authentication and Authorization

Purwadhika
Startup and Coding School

# Authentication VS Authorization

- Authentication, in the form of a key. The lock on the door only grants access to someone with the correct key in much the same way that a system only grants access to users who have the correct credentials.

- Authorization, in the form of permissions. Once inside, the person has the authorization to access the kitchen and open the cupboard that holds the pet food. The person may not have permission to go into the bedroom for a quick nap.

Purwadhika
Startup and Coding School

## Let’s create Authentication System

Purwadhika
Startup and Coding School

## Authentication Flow

New User Registration Flow

- User type the form (email and password)
- Frontend send the data to our Rest API
- Rest API will hash the password
- Rest API will send the hashed password and email to database
- Database will save the data and mark the email as unverified email
- Rest API will send the email and other data to jwt token to generate the token
- Rest API will send the email to nodemailer
- Nodemailer will send token to the user with verification link
- User will received the email, and click the link
- Link will open the new pages on the website and will send the token to API
- API will verify the token and send the email to database
- Database will mark the email as verified

Purwadhika
Startup and Coding School

# Authentication Flow

## Login User Flow

- User type the form (email and password)
- Frontend send the data to our Rest API
- Rest API will hash the password
- Rest API will send the hashed password and email to database
- Database will check the email and password
- If email and password didnt match, login will failed
- If email and password match, rest api will fire the JWT to generate token
- Token will  be send to frontend
- Login Success

Purwadhika
Startup and Coding School

# Tools for Authentication

1. React (Frontend)
2. Express (RestAPI)
3. Mysql (Database)
4. Nodemailer (Email sender)
5. JWT Token (generate token)
6. Crypto (Hash the Password)

Purwadhika
Startup and Coding School

## Authentication Rules

We will create some rule on our authentication system. The rules will depend on the business needs. But for example, we will create the rule like the following below

- User can login to the system only if email has been verified
- We will create expired time on token

## Let’s create Authorization System

Purwadhika
Startup and Coding School

## Authorization Flow

On frontend sides

- User will go to the some pages
- Frontend will check either the page accessable to the user or not
- If user not have permission to the page, will redirect to 401 page
- If user have permission they will see the pages

On backend sides

- If user have permission on frontend side, than frontend will request data to backend
- API will check either the user have permission to the data or not
- If user have not permission frontend will get 401 response, otherwise frontend will get success response and user will see the data displayed on the web

So we will have double checked on the both frontend side and backend sides

## Tools for Authorization

- JWT Token
- Middleware
- React HOC

## Authorization Rules

- We will create 3 different roles on our system, superadmin ,customer, admin and finance
- Every roles will have access to different page
- Only superadmin that will have access to entire pages

## Study Case

Purwadhika
Startup and Coding School

## Study Case : 2 Factor Authentication Flow

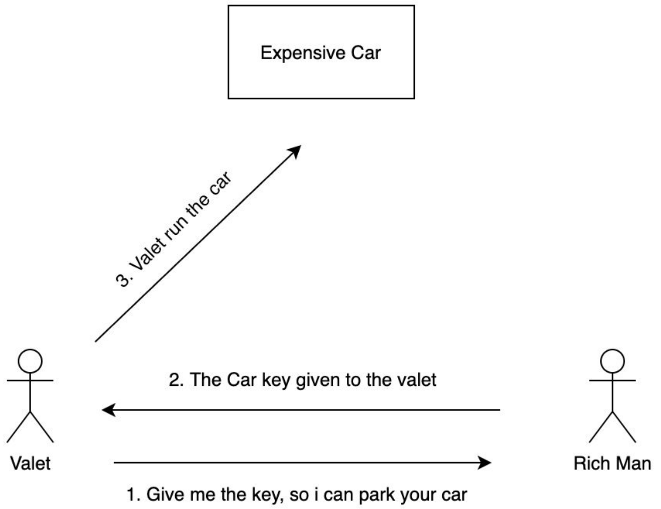
It's easier than you think for someone to steal your password, 2-Step Verification can help keep bad guys out, even if they have your password.

How it works??

- User enter their password
- Then, a code will be sent to users phone via text, voice call, or our mobile app.
- Then, user need to verify the code (OTP)

## Study Case : Oauth 2.0

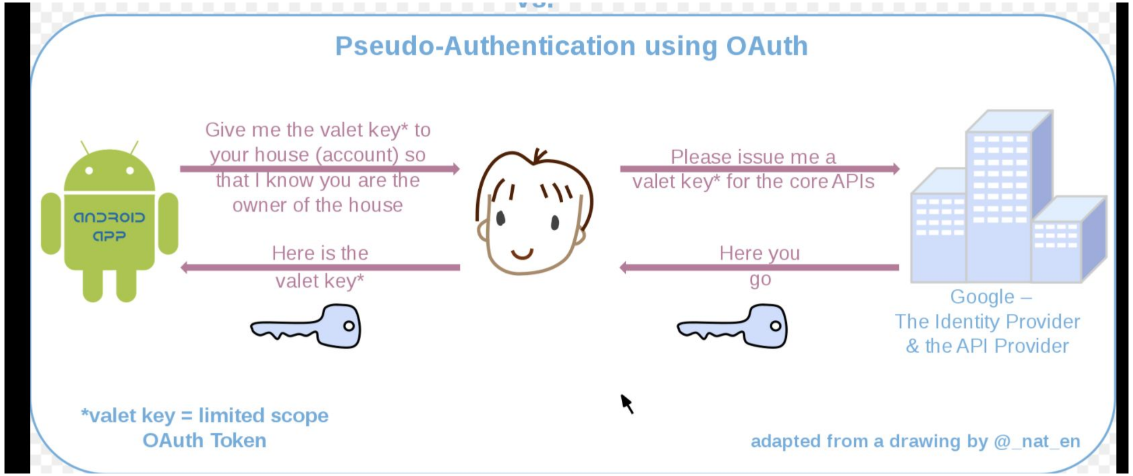
OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords (Wikipedia)


Expensive Car
3. Valet run the car
2. The Car key given to the valet
Valet
Rich Man
1. Give me the key, so i can park your car

Common Analogy

## Study Case : Oauth 2.0

Google Oauth System


Pseudo-Authentication using OAuth
ANDROID APP
Give me the valet key* to your house (account) so that I know you are the owner of the house
Here is the valet key*
Please issue me a valet key* for the core APIs
Here you go
Google – The Identity Provider & the API Provider
*valet key = limited scope OAuth Token
adapted from a drawing by @_nat_en