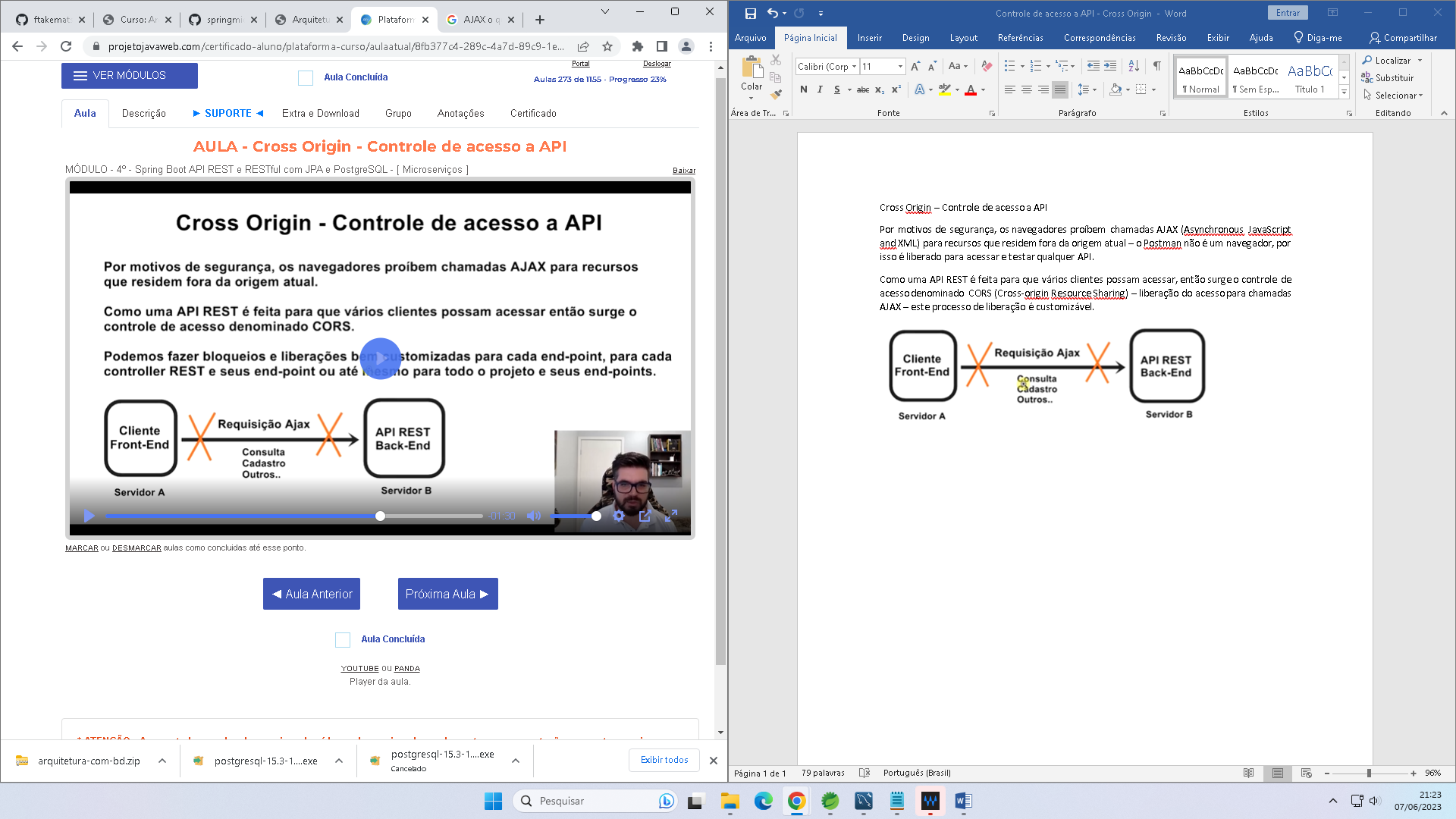
**Cross Origin – Controle de acesso a API**

Por motivos de segurança, os navegadores proíbem chamadas AJAX (Asynchronous JavaScript and XML) para recursos que residem fora da origem atual – o Postman não é um navegador, por isso é liberado para acessar e testar qualquer API.

Como uma API REST é feita para que vários clientes possam acessar, então surge o controle de acesso denominado CORS (Cross-origin Resource Sharing) – liberação do acesso para chamadas AJAX – este processo de liberação é customizável.



<script type="text/javascript">

$(document).ready(

**function** () {

$.ajax({

url: "http://localhost:8081/api/usuario/",

method: "GET"

}).then(**function** (data, status, info) {

console.log(data);

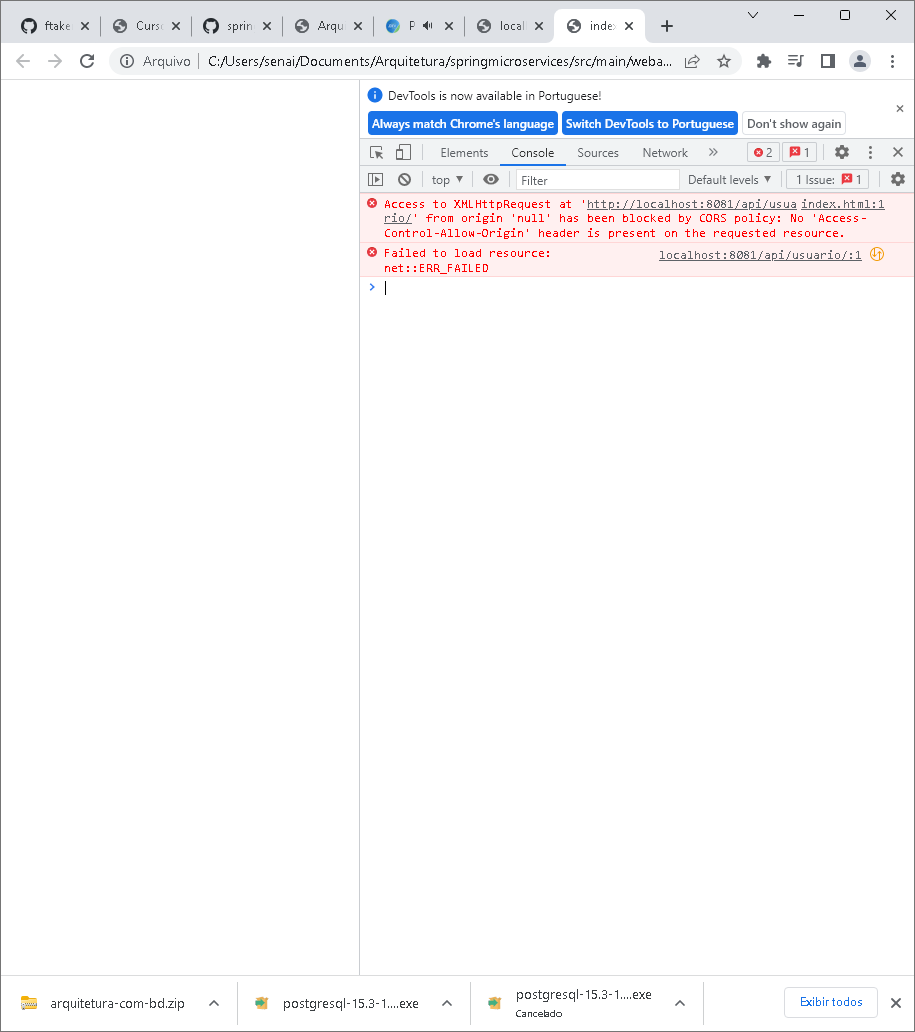
});

}

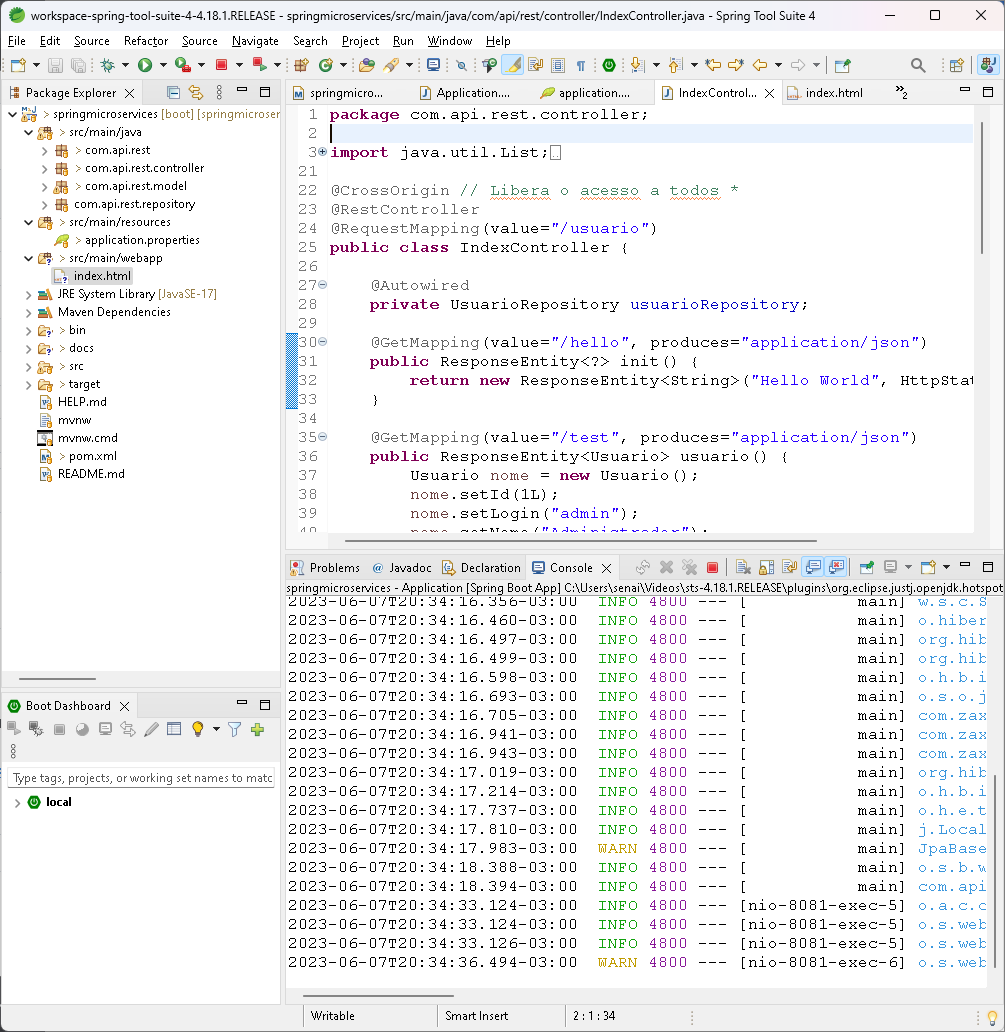
)

</script>

Erro de CORS no navegador:



Solução: colocar anotações para os controllers liberarem acesso a um grupo de endpoints.



**Configurando Roles**

Para realização de login como usuário.

**JWT - autenticação por tokens**

É uma hash criptografada que identifica um usuário, que serve para validar o acesos a uma API. É uma forma de interligar a aplicação front-end com a API. Diferentemente de um sistema monolítico, em que existe uma sessão compartilhada com o front-end e o back-end (sistemas amarrados).