

Logo da Orange Talents

# Retornando dados em JSON

## Cenário:

Imagine uma tarefa para criar uma API REST para exibir os dados básicos do usuário em uma página pública, dessa forma outros usuários do sistema podem pesquisar e visualizar quem é determinado usuário no sistema através de sua foto de perfil, seu username, nome, email e quando ele foi registrado no sistema. É o tipo de funcionalidade comum em redes sociais ou serviços gratuitos na internet que almejam aumentar a interação de seus usuários.

Agora, imagine que o novo desenvolvedor(a) do time implementa essa tarefa e submete uma PR (Pull Request) para que alguém do time possa fazer a revisão de código (Code Review). Por coincidência você estava livre para revisar o código no momento da submissão. Portanto, o trecho de código importante para essa atividade de revisão é este abaixo:

@Controller  
class ExibirPerfilDoUsuarioController(@Inject val repository: UsuarioRepository) {  
  
 @Get("/api/users/{username}/profile")  
 fun exibir(@PathVariable username: String): HttpResponse<Any> {  
  
 val usuario = repository.findByUsername(username)  
 if (usuario == null) {  
 return HttpResponse.notFound()  
 }  
  
 return HttpResponse.ok(usuario)  
 }  
}  
  
@Entity  
class Usuario(  
 @Id  
 @GeneratedValue  
 val id: Long,   
 val username: String,   
 val nome: String,  
 val email: String,  
 val senha: String,  
 val fotoUrl, String,  
 val endereco: String,  
 val telefone: String,  
 val token: String,  
 val registradoEm: LocalDateTime,  
 val criadoEm: LocalDateTime,  
 val atualizadoEm: LocalDateTime,  
 // outros atributos  
)

Olhando para o código cima, responda:

1. Você passaria esse código pela revisão? Explique sua resposta.
2. Com relação ao código, que sugestão de melhoria você daria para o desenvolvedor(a) que abriu a PR (pull request)?

## O que seria bom ver nessa resposta?

* **Peso 5**: Perceber que existe uma brecha de segurança ao retornar a entidade como resposta da API, pois existem diversos dados sensíveis na entidade;
* **Peso 4**: Sugerir criar um DTO contendo somente as informações solicitadas na tarefa;
* **Peso 1**: Qualquer outra sugestão sobre design de código não relacionado a segurança e/ou retorno da API REST;

## Resposta do Especialista:

1. Não passaria este código. O motivo é que o payload da resposta da API está retornando a entidade Usuario com todos seus dados, incluindo informações sensíveis como senha, endereço, telefone entre outras. E isso é uma **brecha grave de segurança**, pois um hacker poderia se aproveitar dessas informações de N maneiras. Se o requisito da API REST informa que precisa somente de alguns poucos dados então é importante que o desenvolvedor(a) leve isso em consideração;
2. Reler o requisito da tarefa para confirmar quais dados precisam de fato ser retornados na resposta da API. Após confirmar os dados na tarefa, deve-se evitar expor os dados sensíveis **criando um DTO para representar esta resposta contendo somente as informações solicitadas**, que no caso são: foto de perfil, username, nome, email e data de registro no sistema;