03

Mass Assignment

Transcrição

[00:00] Quando nós vamos registrar um usuário como nós vimos, nós vamos ter esses parâmetros do nome, do e-mail, da senha e a imagem do nosso usuário. Esses valores vão ser associados ao quê? Vão ser associados nesses atributos da nossa classe modelo usuário. Então nós temos o atributo e-mail, senha, nome do usuário, o nome da imagem que ele cadastrou no perfil, e nós temos esse outro atributo, roles.

[00:21] Esse atributo roles nós não temos no nosso formulário de registro nenhum checkbox para dizer se o usuário é o quê, é um administrador ou ele é um usuário comum. O que faz todo o sentido, porque senão qualquer usuário que for se cadastrar na Alura shows poderia dizer que ele é um usuário administrador e poderia simplesmente na parte administrativa cadastrar os eventos que ele quisesse, com os valores dos ingressos que ele quisesse.

[00:46] Então por isso que nós estamos na nossa classe usuário controller, falando que quando esse novo usuário for registrado, nós estamos sempre vinculando para esse novo usuário o perfil aqui de role user, para ele ser um usuário comum do sistema, para ele só acessar a partir de perfil, para ele poder ver o preço dos ingressos, para ele poder comprar os ingressos. Mas que ele não vai ter direito a acessar a parte administrativa da Alura shows.

[01:15] Só que o que nós vamos fazer? Vamos tentar verificar se a aplicação da Alura shows de fato está segura como deveria. Então vamos voltar na nossa aplicação e nós vamos tentar cadastrar um novo usuário, que vai ser a Joviane.

[01:30] Então nós viemos aqui, nós vamos tentar cadastrar, nós colocamos o e-mail dela, joviane@gmail.com, e a senha da Joviane nós vamos colocar 012345 e aqui nós colocamos a imagem do perfil da Joviane.

[01:43] Só que vamos entender. Nós temos aquele atributo roles na nossa classe usuário. E esses valores estão sendo associados com aqueles atributos da nossa classe usuário. Então o que é que nós vamos tentar fazer? Vamos entender como é que está estruturado esse atributo roles da nossa classe usuária. Vamos voltar para cá.

[02:04] Então, esse atributo roles, é uma lista do tipo role. Vamos clicar aqui na classe role para ver como ela é? Na classe role, nós temos esse atributo name, nos indicando qual que é o perfil do usuário, se ele é do tipo role usar ou se ele é role admin de mim que teria, no caso do role admin, os privilégios de acessar a parte administrativa da Alura shows.

[02:30] O que é que a Josiane vai tentar fazer? Ela que já tem bastante experiência com programação, que já conhece bastante sobre algumas vulnerabilidades, o que ela vai tentar fazer? Ela sabe que muito provavelmente tem diferentes perfis de usuários na Alura shows. Então o que é que ela vai tentar fazer? Ela vai tentar manipular esse formulário HTML com o objetivo de manipular aquele atributo roles da classe usuário para dizer que o perfil dela é administrador. Vamos tentar fazer isso?

[03:01] Como é que ela conseguiria fazer a manipulação desse formulário que está indo para o nosso controle e está fazendo associação com a classe usuário? Ela poderia vir aqui e simplesmente clicar com o botão direito do mouse, inspecionar, e nós vamos nesse nosso formulário de registro e clicamos com o botão direito do mouse, e nós fazemos a edição desse HTML, porque o que está sendo passado nesse formulário é o que está chegando no nosso controller, não é?

[03:25] Então o que a Joviane vai tentar fazer? Ela vai colocar uma tag html, e ela vai escrever para input, para inserir. O tipo desse input vai ser escondido, vai ser aquele tipo hidden, então nós colocamos “<input type=”hidden””.

[03:42] Agora, o que ela quer fazer? Nós temos na nossa classe modelo, como nós vimos, do usuário, aquele atributo roles. Então nós vamos tentar colocar a tag, a chave name, e nós queremos o quê? Nós queremos manipular esse atributo roles que está na nossa classe usuário.

[03:58] Mas como nós vimos, esse atributo roles da classe usuário é o quê? Ele é uma lista. Então a Joviane vai falar "bom, eu vou colocar nesse atributo roles que tem na nossa classe usuária que nós sabemos que é uma lista, e eu vou pegar a posição 0, a primeira posição dessa lista e eu quero desse atributo roles, que ele é do tipo role, eu quero manipular o atributo name dele, aquele atributo que nós vimos que tem na classe role".

[04:24] Eu quero moldar esse atributo name desse roles do usuário para que o valor dele seja admin. Então eu vou colocar o valor desse atributo name do roles como sendo um role admin. Então nós colocamos value role admin. Então, com isso, vamos só fechar a tag, olha só o que é que a Josiane fez? Ela pegou aquele atributo roles que está na classe usuário, esse atributo roles, ela pegou. É uma lista, não é? Então ela pegou, por exemplo, a primeira posição, posição zero.

[05:00] Esse atributo roles, ele é o quê? Ele é do tipo role e dentro dessa classe role, tem esse atributo name, que especifica o role user ou o role admin, para especificar se é usuário comun do meu sistema ou se é um usuário administrador.

[05:11] Então o que a Josiane fez? Ela quer se cadastrar como administradora do sistema. E ela vem aqui, deixa eu só voltar para cá, editar HTML, aqui. Ela pegou esse atributo roles da classe usuário, é uma lista, ela pegou a posição zero e quer manipular esse atributo name da role para que esse name da role seja um perfil de usuário administrador e ela poder se logar na aplicação como sendo um administrador da Alura shows.

[05:40] Vamos ver se essa manipulação da Josiane vai dar certo? Eu vou fechar aqui o inspecionar elemento e nós vamos o quê? Vamos registrar a Joviane. A Joviane foi registrada aqui na nossa aplicação. Agora, será que de fato a Joviane conseguiu se cadastrar na aplicação como um usuário administrador? Vamos ver no banco o que é que nós temos.

[06:02] Vamos voltar no MySQL Workbench e nós vamos nas nossas tabelas e eu vou clicar aqui nessa tabela usuário role e vamos selecionar as roles, as linhas, nessa tabela usuário role. Agora, a Joviane tem esses dois perfis, porque é uma lista, nós estamos forçando uma dessas entradas para ser o quê? Para ser o role user, que é o que está aqui, mas a Joviane conseguiu o quê? Conseguiu manipular esse atributo no formulário HTML para forçar que o atributo roles mudasse o status para ser um role admin.

[06:40] E agora ela conseguiu se cadastrar como administradora do sistema da Alura shows. Será que ela vai conseguir acessar agora aquela parte administrativa da Alura shows? Vamos ver. Vamos voltar.

[06:53] Então a Joviane deveria ser uma usuária comum do sistema. Então agora, o que é que ela vai tentar fazer? Ela vai tentar, já que ela fez essa tentativa desse ataque, de manipular esse atributo que tem na nossa classe usuário, e ela vai verificar se ela consegue de fato logar no sistema como se ela fosse administrador.

[07:09] Então ela vai colocar o e-mail dela, o e-mail dela joviane@gmail.com, e a senha que ela tinha se cadastrado era 012345. E ela clica em login e conseguiu se logar no painel administrativo que nós temos todas as informações da Alura shows.

[07:29] Então essa parte é a parte administrativa da Alura shows e só deveria ser acessado pelos usuários internos da Alura shows, mas a Joviane, através dessa manipulação do formulário HTML, conseguiu alterar o status, o atributo da classe modelo e ela configurou para ela ser um administrador do sistema.

[07:50] Esse tipo de ataque é conhecido, como Mass Assignment e ele já foi realizado contra grandes empresas, inclusive teve um caso famoso contra o Github.

[08:12] Então nós temos que esse ataque é realmente muito perigoso. Imagina só se um usuário consegue fazer a manipulação do atributo da sua classe para que ele seja cadastrado como administrador e você tem essa grande vulnerabilidade no seu sistema.

[08:27] Vamos ver como é que nós conseguimos corrigir isso e evitar que esse ataque de mass assignment aconteça. Vamos ver na sequência.