04

Evitando SQL Injection

Agora que fomos capazes de efetuar a SQL Injection, vamos nos proteger dele. No método index do JobsController, alteramos nossa query para utilizar o formato de parâmetros definidos com "?", como em:

```
def index
  @id_minimo = params[:id_minimo]
  if @id_minimo
    @jobs = Job.where("id > ?", @id_minimo).most_recent.includes(:company).all
  else
    @jobs = Job.most_recent.includes(:company).all
  end
  # ... codigo continua aqui
end
```

Como a chamada a most_recent, includes e all está nos dois casos, extraímos a variável list_partial:

```
  @id_minimo = params[:id_minimo]
  if @id_minimo
    list_parcial = Job.where("id > ", @id_minimo)
  else
    list_parcial = Job
  end

    @jobs = list_parcial.most_recent.includes(:company).all
```

Teste sua aplicação com id_minimo, sem id_minimo e tentando SQL Injection. Compartilhe aqui o código do seu método index.

Responda

INSERIR CÓDIGO		FORMATAÇÃO