订单网址应该要秘密

原来的网址是“流水号”


localhost:3000/orders/3
ArtStore
Products
購物車 (1)
Hi, xdite@growthschool.com
網址呈現的是訂單 id 號碼
訂單明細
商品明細
單價
Macbook Pro with Retina 15'
79999
總計 79999 NTD
寄送資訊
訂購人
123 - 123
訂購人
123 - 123

流水号的危险

- 路人都知道你每天的生意量成交是多少
- 路人可以猜到 pattern

/orders/1

/orders/0f054ab5-2833-4a6d-bde5-0820b68fffae

実作

Step 1: 新增 token 栏位

```
> rails g migration add_token_to_order
```

```
xdite  artstore  ruby-2.2.0  store-v2  rails g migration add_token_to_orde
r
      invoke  active_record
      create    db/migrate/20151026092754_add_token_to_order.rb
```

修改 migration 档与新增 index

db/migrate/xxxx(一堆数字)_add_token_to_order.rb

```
class AddTokenToOrder < ActiveRecord::Migration
  def change
+   add_column :orders, :token, :string
+   add_index :orders, :token
  end
end
```

```
> rake db:migrate
```

Step 2：每一笔订单产生前先乱数产生 token

app/models/order.rb

```
class Order < ActiveRecord::Base
...(略)
  before_create :generate_token

  def generate_token
    self.token = SecureRandom.uuid
  end
...(略)
```

Step 3 ：设定重导到新网址

重導到 orders/0f054ab5-2833-….

4 app/controllers/orders_controller.rb

```
@@ -17,14 +17,14 @@ def create
        product_list.save
      end

-     redirect_to order_path(@order)
+     redirect_to order_path(@order.token)
    else
      render 'carts/checkout'
    end
  end

  def show
-   @order = Order.find(params[:id])
+   @order = Order.find_by_token(params[:id])
    @product_lists = @order.product_lists
  end
```