ROR Developer

Criterion

1. 作答時間原則上為一小時，請記錄您的作答時間，並於作答完畢後轉為pdf檔

2. You can use Google for searching information, while copy-pasting others’ answers is forbidden.(If you google any information, please let us know.)

3. 3. Express more of your thoughts instead of only answers can let us know more about you :).

4. 中英文作答皆可，請勿將試題外洩

Basic

1. What’s the difference between rails environments: *production*, *development* and *test*?

   development: 開發者於本機進行new feature 或是 bug fix的開發環境

   staging: 為運行環境與正式商轉產品盡量相同的測試環境，通常會將於開發完成之feature或bug部署到staging server進行測試，以保證該feature在正式環境下可以符合制定的spec

   test: 為執行測試時的環境，例如rspec，若不利用databasecleaner等gem做設定，則每次測試完畢，db都會rollback回起始狀態
   production: 為產品正式商轉時的運作環境

2. What's the difference between `Symbol` and `String`? (Consider operator ===)

   若兩個命名相同的symbol，則他們視為同一個object, 例： :a === :a 會回傳true, 通常在ruby裡頭會使用在Hash的key（因為具有唯一性），或是在Rails中使用在 routeing的action命名
   String則不，若我們定義兩個相同的String，則他們只是value相同，實際上為兩個不同的object，也就是實際上為兩筆不同的資料

3. What is the difference between a class and a module?

   class可以產生instance object，module則只作為class擴充行為的容器

   一般會將可重複被不同class運用的methods包裝成module給多個class引用，例如commentable

Advanced

1. What is the difference between calling `super` and calling `super()` in a ruby method?

   super會執行parent class下相同method的行為後再執行該method裏頭的行為，並且將所有arguments都傳到parent method中執行
   super()則只會傳入指定的arguments

2. Figure out and fix issues in the following javascript code. (with jquery library)

```
/*
Following is a javascript template to show a question for user to answer.
*/
var questionController = new function(){
  var thisObj, answersMapping = ['A', 'B', 'C', 'D', 'E'];
  return thisObj = {
    open: function(){
      $('#question').show();
      for(var i = 0; i < 5; ++i){
        $('#question .btn').eq(i).click(function(){
          $.post('submit_answer', {answer: answersMapping[i]}, function(){
            thisObj.close();
          });
        })
      }
    },
    close: function(){
      $('#question').hide();
    }
  }
}
$(function(){
  $('#open_question_btn').click(function(){
    questionController.open();
  });
});
```

```
var questionController = new function(){
var thisObj, answersMapping = ['A', 'B', 'C', 'D', 'E'];
return thisObj = {
open: function(){
$('#question').show();
for(var i = 0; i < 5; ++i){
$('#question .btn').eq(i).click(function(){
$.post('submit_answer', {answer: answersMapping[i-1]}, function(){
thisObj.close();
});
})
}
},
close: function(){
$('#question').hide();
}
}
}
$(function(){
$('#open_question_btn').click(function(){
questionController.open();
});
});
```

3. Write a single line (without semicolon) of Ruby code that prints the *Fibonacci sequence* of any given length n.

4. Simple explain what is XSS(Cross Site Script), how it causes and how it will endanger a website.

   XSS意指攻擊者將HTML或JS代碼注入網頁中，使一般使用者在載入網頁時執行該段代碼，有可能造成使用者資料外洩或是使攻擊者獲得該網站的存取權限
   reference: https://en.wikipedia.org/wiki/Cross-site_scripting

Bonus

1. List one and simple explain any CVE(Common Vulnerabilities and Exposures) of (any version) rails.

   CVE-2012-2660

   假設我們有以下程式碼，可以讓使用者有token的情況下去做修改password的操作。

   ```
   unless params[:token].nil?
   user = User.find_by_token(params[:token])
   user.reset_password!
   end
   ```

   攻擊者可以set params[:token] = '[nil]'的操作繞過 unless params[:token].nil? 並且使用IS_NULL來做SQL query操作

   reference: https://groups.google.com/forum/#!searchin/rubyonrails-security/2012$202660%7Csort:relevance/rubyonrails-security/8SA-M3as7A8/Mr9fi9X4kNgJ

tags: 104