要弄明白Rails 4 中Strong Parameters机制，首先我们要看看Rails3中的Parameters

在 Rails3 中创建或更新 Active Record 对象时，会有 Mass Assignment 安全问题。所以 Model 中需要列一个白名单，声明哪些属性可以被 parameter 的数据更新。

Rails 3

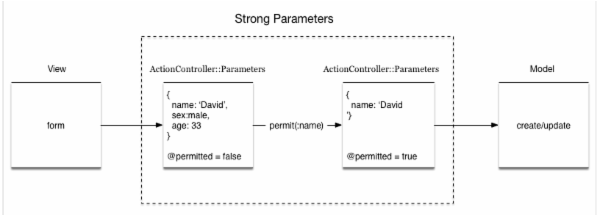
# kings\_controller.rb def create #{ name: ‘David', sex:male, age: 31} @king = King.new(params[:king]) if @king.save redirect\_to @king else render 'new' end end # king.rb class King attr\_accessible :name end

Rails 4

Rails 4 引入了 Strong Parameters 的机制，Model 不再负责白名单的维护，把过滤非法属性的职责推给了 Controller。

# kings\_controller.rb def create # new parameter { name: ‘David' } @king = King.new(king\_params) if @king.save redirect\_to @king else render 'new' end end private def king\_params # old parameter { name: ‘David', sex:male, age: 31} # new parameter { name: ‘David' } params[:king].permit(:name) end # king.rb class King end

什么是 Strong Parameters?



说白了 Strong Parameter 其是就是一层白名单过滤。

View 层穿过来的数据会转化为一个 ActionController::Parameters 对象

过滤老的 ActionController::Parameters 对象，生成一个新的 ActionController::Parameters 对象。

\* 只保留白名单属性  
\* 实例变量 @permitted  赋为 true  
把过滤后的 ActionController::Parameters 对象传给 model，创建或更新对应的的 ActiveRecord 对象。  
可以硬传给 model，霸王硬上弓吗？

未经 Strong Parameter 过滤的 ActionController::Parameters 对象的 @permitted 为 false（过滤后为 true）。如果硬传给 Model，会报错 ActiveModel::ForbiddenAttributesError

对于rails的一些使用技巧的代码

git仓库输出   
git archive --format=tar --prefix=actasfavor/ HEAD | (cd /home/holin/work/ && tar xf -)   
输出到/home/holin/work/actasfavor/目录下   
  
Posted by holin At May 16, 2008 16:42   
加载plugins中的controller和model   
  
# Include hook code here   
require 'act\_as\_favor'   
# make plugin controller, model, helper available to app   
config.load\_paths += %W(#{ActAsFavor::PLUGIN\_CONTROLLER\_PATH} #{ActAsFavor::PLUGIN\_HELPER\_PATH} #{ActAsFavor::PLUGIN\_MODELS\_PATH})   
Rails::Initializer.run(:set\_load\_path, config)   
# require the controller   
require 'favors\_controller'   
# require models   
require 'favor'   
  
Posted by holin At May 15, 2008 15:36   
使用最频繁的前5个命令   
history | awk {'print $2'} | sort | uniq -c | sort -k1 -rn| head -n5   
  
Posted by holin At May 15, 2008 10:40   
按数组元素的某属性排序   
@users.sort!{|a, b| a.last <=> b.last }   
  
Posted by holin At May 11, 2008 14:35   
按日期备份数据库   
mysqldump db\_name -uroot > "/root/db\_backup/kaoshi\_web\_`date +"%Y-%m-%d"`.sql"   
  
Posted by holin At May 08, 2008 12:05   
用memcached手动cache数据   
  
sql = "SELECT \* FROM blogs LIMIT 100"   
Blog.class   
k = MD5.new(sql)   
@blogs = Cache.get k   
if @blogs.blank?   
@blogs = Blog.find\_by\_sql(sql)   
Cache.put k, @blogs, 60\*30 #expire after 30min   
end   
memcache-client 1.5.0:   
get(key, expiry = 0)   
put(key, value, expiry = 0)   
  
Posted by devon At May 04, 2008 20:39   
shuffle an array   
  
class Array   
def shuffle   
sort\_by { rand }   
end   
def shuffle!   
self.replace shuffle   
end   
end   
  
Posted by holin At May 04, 2008 15:39   
让所有的ajax请求都不render :layout   
  
def render(\*args)   
args.first[:layout] = false if request.xhr? and args.first[:layout].nil?   
super   
end   
  
Posted by devon At May 03, 2008 10:53   
Find with Hash   
  
Event.find(   
:all,   
:conditions => [ "title like :search or description like :search",   
{:search => "%Tiki%"}]   
)   
  
Posted by devon At May 03, 2008 10:49   
执行sql语句脚本   
  
mysql -uroot -p123<<END   
use dbame;   
delete from results;   
delete from examings;   
quit   
END   
  
Posted by holin At May 01, 2008 12:14   
SQL Transaction in Rails   
  
def fetch\_value   
sql = ActiveRecord::Base.connection();   
sql.execute "SET autocommit=0";   
sql.begin\_db\_transaction   
id, value =   
sql.execute("SELECT id, value FROM sometable WHERE used=0 LIMIT 1 FOR UPDATE").fetch\_row;   
sql.update "UPDATE sometable SET used=1 WHERE id=#{id}";   
sql.commit\_db\_transaction   
value;   
end   
  
Posted by holin At April 30, 2008 09:37   
显示 Flash 消息的动态效果   
  
<% if flash[:warning] or flash[:notice] %>   
<div id="notice" <% if flash[:warning] %>class="warning"<% end %>>   
<%= flash[:warning] || flash[:notice] %>   
</div>   
<script type="text/javascript">   
setTimeout("new Effect.Fade('notice');", 15000)   
</script>   
<% end %>   
15000 毫秒后自动 notice Div 自动消失。   
  
Posted by devon At April 29, 2008 13:02   
删除环境中的常量   
  
Object.send(:remove\_const, :A)   
>> Math   
=> Math   
>> Object.send(:remove\_const, :Math)   
=> Math   
>> Math   
NameError: uninitialized constant Math   
  
Posted by devon At April 28, 2008 18:24   
手动加上 authenticity\_token   
<div style="margin:0;padding:0"><input name="authenticity\_token" type="hidden" value="<%= form\_authenticity\_token %>" /></div>   
  
Posted by devon At April 28, 2008 14:24   
Rails group\_by   
  
<% @articles.group\_by(&:day).each do |day, articles| %>   
<div id='day' style="padding: 10px 0;">   
<h2><%= day.to\_date.strftime('%y年%m月%d日') %></h2>   
<%= render :partial => 'article', :collection => articles %>   
</div>   
<% end %>   
articles 按天数分组   
  
Posted by devon At April 25, 2008 22:32   
读写文件   
  
# Open and read from a text file   
# Note that since a block is given, file will   
# automatically be closed when the block terminates   
File.open('p014constructs.rb', 'r') do |f1|   
while line = f1.gets   
puts line   
end   
end   
# Create a new file and write to it   
File.open('test.rb', 'w') do |f2|   
# use "\n" for two lines of text   
f2.puts "Created by Satish\nThank God!"   
end   
  
Posted by holin At April 17, 2008 02:10   
遍历目录   
Dir.glob(File.join('app/controllers', "\*\*", "\*\_controller.rb")) { |filename| puts filename }   
  
Posted by holin At April 16, 2008 15:28   
字符串到 model   
1   
2   
>> 'tag\_course'.camelize.constantize.find(:first)   
=> #<TagCourse id: 7, tag\_id: 83, course\_id: 2>   
\*camelize(lower\_case\_and\_underscored\_word, first\_letter\_in\_uppercase = true)\*   
By default, camelize converts strings to UpperCamelCase. If the argument to camelize is set to ":lower" then camelize produces lowerCamelCase.   
\*constantize(camel\_cased\_word)\*   
Constantize tries to find a declared constant with the name specified in the string. It raises a NameError when the name is not in CamelCase or is not initialized.   
  
Posted by devon At April 07, 2008 17:32   
调用Proc   
1   
2   
3   
a = Proc.new { |i| puts i }   
a['haha']   
a.call('hehe')   
  
Posted by holin At March 28, 2008 23:10   
Rails中Host静态文件   
1   
2   
config.action\_controller.asset\_host = "http://assets.example.com"   
config.action\_controller.asset\_host = "http://assets-%d.example.com"   
The Rails image\_path and similar helper methods will then use that host to reference files in the public directory.   
The second line will distribute asset requests across assets-0.example.com,assets-1.example.com, assets-2.example.com, and assets-3.example.com.   
  
Posted by devon At March 26, 2008 18:18   
打包gems到项目目录中   
  
$ mkdir vendor/gems   
$ cd vendor/gems   
$ gem unpack hpricot   
Unpacked gem: 'hpricot-0.4'   
config.load\_paths += Dir["#{RAILS\_ROOT}/vendor/gems/\*\*"].map do |dir|   
File.directory?(lib = "#{dir}/lib") ? lib : dir   
end   
  
Posted by devon At March 26, 2008 18:12   
在当前上下文中执行文件中的代码   
  
instance\_eval(File.read('param.txt'))   
# such as   
@father = 'Father'   
instance\_eval("puts @father")   
#Produces:   
#Father   
  
Posted by holin At March 20, 2008 01:13   
将当前文件所在目录加入require路径   
  
$LOAD\_PATH << File.expand\_path(File.dirname(\_\_FILE\_\_))   
# or   
$: << File.expand\_path(File.dirname(\_\_FILE\_\_))   
# this one puts current path before the other path.   
$:.unshift( File.expand\_path(File.dirname(\_\_FILE\_\_)) )   
\*\_\_ FILE \_\_\* 当前文件路径   
  
Posted by holin At March 19, 2008 01:40   
多字段模糊搜索   
  
conditions = []   
[:name, :school, :province, :city].each { |attr| conditions << Profile.send(:sanitize\_sql, ["#{attr} LIKE ?", "%#{params[:q]}%"]) if params[:q] }   
conditions = conditions.any? ? conditions.collect { |c| "(#{c})" }.join(' OR ') : nil   
在profile表里，按name, school, province, city模糊搜索   
  
Posted by devon At March 17, 2008 17:25   
nginx 启动脚本   
  
  
#! /bin/sh   
# chkconfig: - 58 74   
# description: nginx is the Nginx daemon.   
# Description: Startup script for nginx webserver on Debian. Place in /etc/init.d and   
# run 'sudo update-rc.d nginx defaults', or use the appropriate command on your   
# distro.   
#   
# Author: Ryan Norbauer   
# Modified: Geoffrey Grosenbach http://topfunky.com   
# Modified: David Krmpotic http://davidhq.com   
set -e   
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin   
DESC="nginx daemon"   
NAME=nginx   
DAEMON=/usr/local/nginx/sbin/$NAME   
CONFIGFILE=/usr/local/nginx/conf/nginx.conf   
DAEMON=/usr/local/nginx/sbin/$NAME   
CONFIGFILE=/usr/local/nginx/conf/nginx.conf   
PIDFILE=/usr/local/nginx/logs/$NAME.pid   
SCRIPTNAME=/etc/init.d/$NAME   
# Gracefully exit if the package has been removed.   
test -x $DAEMON || exit 0   
d\_start() {   
$DAEMON -c $CONFIGFILE || echo -en "\n already running"   
}   
d\_stop() {   
kill -QUIT `cat $PIDFILE` || echo -en "\n not running"   
}   
d\_reload() {   
kill -HUP `cat $PIDFILE` || echo -en "\n can't reload"   
}   
case "$1" in   
start)   
echo -n "Starting $DESC: $NAME"   
d\_start   
echo "."   
  
stop)   
echo -n "Stopping $DESC: $NAME"   
d\_stop   
echo "."   
  
reload)   
echo -n "Reloading $DESC configuration..."   
d\_reload   
echo "."   
  
restart)   
echo -n "Restarting $DESC: $NAME"   
d\_stop   
# One second might not be time enough for a daemon to stop,   
# if this happens, d\_start will fail (and dpkg will break if   
# the package is being upgraded). Change the timeout if needed   
# be, or change d\_stop to have start-stop-daemon use --retry.   
# Notice that using --retry slows down the shutdown process   
# somewhat.   
sleep 1   
d\_start   
echo "."   
  
\*)   
echo "Usage: $SCRIPTNAME {start|stop|restart|reload}" >&2   
exit 3   
  
esac   
exit 0   
将文件写入到 /etc/init.d/nginx   
sudo chmod +x /etc/init.d/nginx   
测试是否可正确运行   
sudo /etc/init.d/nginx start   
设置自动启动   
sudo /sbin/chkconfig --level 345 nginx on   
  
Posted by devon At March 16, 2008 12:26   
link\_to\_remote 取静态页面   
1   
2   
<%= link\_to\_remote "update post", :update => 'post', :method => 'get', :url => '/post\_1.html' %>   
<div id='post'></div>   
将 url 改为静态面页的地址即可。   
  
Posted by devon At March 16, 2008 11:07   
in\_place\_editor for rails2.0   
  
module InPlaceMacrosHelper   
# Makes an HTML element specified by the DOM ID +field\_id+ become an in-place   
# editor of a property.   
#   
# A form is automatically created and displayed when the user clicks the element,   
# something like this:   
# <form id="myElement-in-place-edit-form" target="specified url">   
# <input name="value" text="The content of myElement"/>   
# <input type="submit" value="ok"/>   
# <a onclick="javascript to cancel the editing">cancel</a>   
# </form>   
#   
# The form is serialized and sent to the server using an AJAX call, the action on   
# the server should process the value and return the updated value in the body of   
# the reponse. The element will automatically be updated with the changed value   
# (as returned from the server).   
#   
# Required +options+ are:   
# <tt>:url</tt>:: Specifies the url where the updated value should   
# be sent after the user presses "ok".   
#   
# Addtional +options+ are:   
# <tt>:rows</tt>:: Number of rows (more than 1 will use a TEXTAREA)   
# <tt>:cols</tt>:: Number of characters the text input should span (works for both INPUT and TEXTAREA)  
# <tt>:size</tt>:: Synonym for :cols when using a single line text input.   
# <tt>:cancel\_text</tt>:: The text on the cancel link. (default: "cancel")   
# <tt>:save\_text</tt>:: The text on the save link. (default: "ok")   
# <tt>:loading\_text</tt>:: The text to display while the data is being loaded from the server (default: "Loading...")   
# <tt>:saving\_text</tt>:: The text to display when submitting to the server (default: "Saving...")   
# <tt>:external\_control</tt>:: The id of an external control used to enter edit mode.   
# <tt>:load\_text\_url</tt>:: URL where initial value of editor (content) is retrieved.   
# <tt>:options</tt>:: Pass through options to the AJAX call (see prototype's Ajax.Updater)   
# <tt>:with</tt>:: JavaScript snippet that should return what is to be sent   
# in the AJAX call, +form+ is an implicit parameter   
# <tt>:script</tt>:: Instructs the in-place editor to evaluate the remote JavaScript response (default: false)   
# <tt>:click\_to\_edit\_text</tt>::The text shown during mouseover the editable text (default: "Click to edit")  
def in\_place\_editor(field\_id, options = {})   
function = "new Ajax.InPlaceEditor("   
function << "'#{field\_id}', "   
function << "'#{url\_for(options[:url])}'"   
js\_options = {}   
if protect\_against\_forgery?   
options[:with] ||= "Form.serialize(form)"   
options[:with] += " + '&authenticity\_token=' + encodeURIComponent('#{form\_authenticity\_token}')"   
end   
js\_options['cancelText'] = %('#{options[:cancel\_text]}') if options[:cancel\_text]   
js\_options['okText'] = %('#{options[:save\_text]}') if options[:save\_text]   
js\_options['loadingText'] = %('#{options[:loading\_text]}') if options[:loading\_text]   
js\_options['savingText'] = %('#{options[:saving\_text]}') if options[:saving\_text]   
js\_options['rows'] = options[:rows] if options[:rows]   
js\_options['cols'] = options[:cols] if options[:cols]   
js\_options['size'] = options[:size] if options[:size]   
js\_options['externalControl'] = "'#{options[:external\_control]}'" if options[:external\_control]   
js\_options['loadTextURL'] = "'#{url\_for(options[:load\_text\_url])}'" if options[:load\_text\_url]   
js\_options['ajaxOptions'] = options[:options] if options[:options]   
# js\_options['evalScripts'] = options[:script] if options[:script]   
js\_options['htmlResponse'] = !options[:script] if options[:script]   
js\_options['callback'] = "function(form) { return #{options[:with]} }" if options[:with]   
js\_options['clickToEditText'] = %('#{options[:click\_to\_edit\_text]}') if options[:click\_to\_edit\_text]   
js\_options['textBetweenControls'] = %('#{options[:text\_between\_controls]}') if options[:text\_between\_controls]   
function << (', ' + options\_for\_javascript(js\_options)) unless js\_options.empty?   
function << ')'   
javascript\_tag(function)   
end   
# Renders the value of the specified object and method with in-place editing capabilities.   
def in\_place\_editor\_field(object, method, tag\_options = {}, in\_place\_editor\_options = {})   
tag = ::ActionView::Helpers::InstanceTag.new(object, method, self)   
tag\_options = {:tag => "span", :id => "#{object}\_#{method}\_#{tag.object.id}\_in\_place\_editor", :class => "in\_place\_editor\_field"}.merge!(tag\_options)   
in\_place\_editor\_options[:url] = in\_place\_editor\_options[:url] || url\_for({ :action => "set\_#{object}\_#{method}", :id => tag.object.id })   
tag.to\_content\_tag(tag\_options.delete(:tag), tag\_options) +   
in\_place\_editor(tag\_options[:id], in\_place\_editor\_options)   
end   
end   
解决在rails2.0以上版本使用in\_place\_editor时出现的 ActionController::InvalidAuthenticityToken 错误。   
  
Posted by devon At March 15, 2008 16:20   
capture in view   
  
<% @greeting = capture do %>   
Welcome to my shiny new web page! The date and time is   
<%= Time.now %>   
<% end %>   
<html>   
<head><title><%= @greeting %></title></head>   
<body>   
<b><%= @greeting %></b>   
</body></html>   
The capture method allows you to extract part of a template into a variable. You can then use this variable anywhere in your templates or layout.   
  
Posted by devon At March 13, 2008 14:06   
在 before\_filter 中使用不同的layout   
before\_filter Proc.new {|controller| layout 'iframe' unless controller.request.env["HTTP\_REFERER"] =~ /localhost/ }   
如果不是从localhost这个站点来访问的，则使用 iframe 的 layout   
  
Posted by devon At March 11, 2008 17:38   
Rails中获取 HTTP\_REFERER   
request.env["HTTP\_REFERER"]   
可以取到的参数包括：   
SERVER\_NAME: localhost   
PATH\_INFO: /forum/forums   
HTTP\_USER\_AGENT: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en) AppleWebKit/522.11 (KHTML, like Gecko) Version/3.0.2 Safari/522.12   
HTTP\_ACCEPT\_ENCODING: gzip, deflate   
SCRIPT\_NAME: /   
SERVER\_PROTOCOL: HTTP/1.1   
HTTP\_HOST: localhost:3000   
HTTP\_CACHE\_CONTROL: max-age=0   
HTTP\_ACCEPT\_LANGUAGE: en   
REMOTE\_ADDR: 127.0.0.1   
SERVER\_SOFTWARE: Mongrel 1.1.3   
REQUEST\_PATH: /forum/forums   
HTTP\_REFERER: http://localhost:3000/   
HTTP\_COOKIE: \_matchsession=BAh7BzoMY3NyZl9pZCIlNWJiNzg4NDUzOWQzNWFhZTQ4MGRkNTUwYzc0MDc5%250AZGYiCmZsYXNoSUM6J0FjdGlvbkNvbnRyb2xsZXI6OkZsYXNoOjpGbGFzaEhh%250Ac2h7AAY6CkB1c2VkewA%253D268e6091590591d959128f3b17b62ff46244a0a3; \_slemail=temp%40email.com; \_slhash=9dfd86431742273e3e96e06a1c20541d69f74dc9; \_haha\_session=BAh7BiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcjo6Rmxhc2g6OkZsYXNo%250ASGFzaHsABjoKQHVzZWR7AA%253D%253D--96565e41694dc839bd244af40b5d5121a923c8e3   
HTTP\_VERSION: HTTP/1.1   
REQUEST\_URI: /forum/forums   
SERVER\_PORT: "3000"   
GATEWAY\_INTERFACE: CGI/1.2   
HTTP\_ACCEPT: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,\*/\*;q=0.5   
HTTP\_CONNECTION: keep-alive   
REQUEST\_METHOD: GET

<ul>

<% @user.errors.full\_messages.each do |msg| %>

<li><%= msg %></li>

<% end %>

</ul>

<h4>一个无序列表：</h4>

<ul>

<li>咖啡</li>

<li>茶</li>

<li>牛奶</li>

</ul>

**一个无序列表：**

* 咖啡
* 茶
* 牛奶