

プラグイン名

SafeERBプラグイン

このプラグインができること

1. ERBテンプレートで、`<%= ar.hoge %>`など、DBや入力パラメータ由来の文字に対して、サニタイズを忘れていたときに例外を出してくれる

ちょー簡単な使い方

```
./script/plugin install http://safe-erb.rubyforge.org/svn/plugins/safe\_erb
```

これだけ。簡単。

公式ページ

- ▶ [Safe ERB in Ruby on Rails](#)

日本語解説ページ

- ▶ ないねえ。を、[Ruby札幌の資料](#)があったか。

外国語解説ページ

- ▶ [SafeErb for Rails 2](#)

のうほう

- ▶ 例外を出すかどうかはtaintという機能(? フラグ?)を使っている
- ▶ DBや入力パラメータ由来の文字はtaint状態になっていて、手動でコレを解除するにはstring.untaintとすればよい
- ▶ SafeERBプラグインではERB::Util#h(`<%=h ar.hoge %>`みたいなやつ)とActionView::Helpers::TextHelper#strip_tags(`<%= ar.hoge.strip_tags %>`みたいなやつ)を拡張しているので、これを使ったときには自動的にuntaintが呼ばれるので例外が発生しない

コメント

名前: