Redmine - Feature #2244

protection, apache + mod_rails a.k.a. phusion passenger

2008-11-28 19:58 - Keith Cascio

Status:	Closed	**Start date:**	2008-11-28
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix		

Description

Now that many admins deploy Redmine using Apache + Phusion Passenger a.k.a. mod_rails or modrails, it makes sense to add .htaccess files to protect the non-public parts of Redmine from inadvertent/malicious download. Here's why:

If we use the Passenger sub-URI **method** to deploy Redmine, i.e. we simply copy a fresh distribution of Redmine anywhere under Apache's web document root, unless precautions are taken, we expose private files to download, e.g. config/database.yml

By my count, there are 13 first-level directories that would benefit from .htaccess protection: { app/ config/ db/ doc/ extra/ files/ lang/ lib/ log/ script/ test/ tmp/ vendor/ }

For each of those, you could add an .htaccess file (e.g. config/.htaccess) looking like this:

```
order deny,allow
deny from all
```

History

#1 - 2008-11-30 23:26 - Markus Knittig

+1

#2 - 2008-12-02 07:59 - Eric Davis

- Category deleted (Permissions and roles)

According to the Passenger documents, you should link only the public directory to be in the web root. This would make all the directories you listed above outside the document root, thus not exposed.

> To do this, make a symlink from your Ruby on Rails application's public folder to a directory in the document root. For example:
>
> ln -s /webapps/mycook/public /websites/phusion/rails

#3 - 2008-12-02 23:37 - Keith Cascio

Eric Davis wrote:

> ... outside the document root, thus not exposed ...

You're right Eric. I didn't realize Passenger could work like that. Please close this issue if you want.

#4 - 2008-12-07 15:11 - Jean-Philippe Lang

- Status changed from New to Closed

- Resolution set to Wont fix