redmineorg-copy202205 - Vote #79470

Support header Content Security Policy

2022/05/09 18:35 - Admin Redmine

ステータス:	New	**開始日:**	2022/05/09
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Security_51	**予定工数:**	0.00時間
対象バージョン:		**作業時間:**	0.00時間
Redmineorg_URL:	https://www.redmine.org/issues/29405	**status_id:**	1
category_id:	51	**tracker_id:**	2
version_id:	0	**plus1:**	0
issue_org_id:	29405	**affected_version:**	
author_id:	360211	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	
comments:	1		

説明

Hi,

According Google, this a basic Content Security Policy.

Content-Security-Policy: default-src https:; script-src https: 'unsafe-inline'; style-src https: 'unsafe-inline'

Redmine crash with it because there is some call to eval in javascript in some pages.

Regards,
Ludovic

journals

Hello

A workaround is to enable all via a *config/initializers/csp.rb*

```
Rails.application.config.content_security_policy do |policy|
    policy.default_src "*", :data, :blob, "'unsafe-inline'", "'unsafe-eval'"
    policy.font_src "*", :data, :blob, "'unsafe-inline'", "'unsafe-eval'"
    policy.img_src "*", :data, :blob, "'unsafe-inline'", "'unsafe-eval'"
    policy.object_src "*", :data, :blob, "'unsafe-inline'", "'unsafe-eval'"
    policy.script_src "*", :data, :blob, "'unsafe-inline'", "'unsafe-eval'"
    policy.style_src "*", :data, :blob, "'unsafe-inline'", "'unsafe-eval'"

    # Specify URI for violation reports
    # policy.report_uri "/csp-violation-report-endpoint"
end

#Rails.application.config.content_security_policy_report_only = true
```

履歴

#1 - 2022/05/10 17:04 - Admin Redmine

- カテゴリ を Security_51 にセット