redmineorg-copy202205 - Vote #80279

MIME Content Type is not properly handled while attaching the files

2022/05/09 18:52 - Admin Redmine

ステータス:	Resolved	**開始日:**	2022/05/09
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:	Attachments_19	**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/31968	**status_id:**	3
category_id:	19	**tracker_id:**	1
version_id:	0	**plus1:**	0
issue_org_id:	31968	**affected_version:**	
author_id:	411935	**closed_on:**	
assigned_to_id:	0	**affected_version_id:**	151
comments:	4		

説明

Recently upgraded to 4.0.4. While doing the Information security testing, Team raised a vulnerability
"The application does not validate the content type of file being uploaded. This would enable an adversary to upload a malicious file onto the server."

If I change the extension of a file from *.com* to *.pdf*, Redmine allows file upload in issues as attachment and stores contenttype as "*application/pdf*" in table.

Due to this issue we are unable to roll out new version.

Urgent help required.
Thanks

journals

What do you think about this workaround? It prevents web browsers from opening crafted PDF files inline.

```
diff --git a/app/models/attachment.rb b/app/models/attachment.rb
index a334024b4..3ec3e0e69 100644
--- a/app/models/attachment.rb
+++ b/app/models/attachment.rb
@@ -249,7 +249,7 @@ class Attachment < ActiveRecord::Base
       end


def is_pdf?
-  [redacted]n/pdf"
+  [redacted]pplication
   end

def is_video?
```

Thanks for prompt help.

Made necessary Changes. Still file is getting uploaded in the system.

We need to block the upload itself if both types are not matching.

---

added a new code in attachment.rb, en.yml(for custom error message).

Attaching new file for further reference.

Thanks for the help

履歴

#1 - 2022/05/10 17:03 - Admin Redmine

- カテゴリ を Attachments_19 にセット