Redmine - Defect #40647

Attachment Download fails due to Content Security Policy in Safari

2024-04-30 10:42 - Christian Thieme

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Attachments	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Invalid	**Affected version:**	5.1.1

Description

Hello, recently an issue arised that attachment downloads (for instance PDF) don't work using Safari.

There is an error message in the Javascript console:

Blocked script execution in 'https://redmine.test.domain/attachments/download/1234/letter.pdf' because the document's frame is sandboxed and the 'allow-scripts' permission is not set.

It is triggered by the CSP in app/controllers/attachments_controller.rb

headers['content-security-policy'] = "default-src 'none'; style-src 'unsafe-inline'; sandbox"

but is not affecting Firefox or Chrome so it might be a Safari Bug.

Redmine: 5.1.1
Mac OS Version: Sonoma
Safari Version: 17.4.1

History

#1 - 2024-05-22 11:51 - Go MAEDA

- File clipboard-202405221849-ombs9.png added

- Status changed from New to Confirmed

Confirmed the issue.

clipboard-202405221849-ombs9.png

#3 - 2024-05-22 13:25 - Go MAEDA

I found the following change fixes the issue.

```
diff --git a/app/controllers/attachments_controller.rb b/app/controllers/attachments_controller.rb
index 90c3c7070..1819f058e 100644
--- a/app/controllers/attachments_controller.rb
+++ b/app/controllers/attachments_controller.rb
@@ -323,7 +323,11 @@ class AttachmentsController < ApplicationController
   end

   def send_file(path, options={})
-    headers['content-security-policy'] = "default-src 'none'; style-src 'unsafe-inline'; sandbox"
+    if options[:type] == 'application/pdf'
+      headers['content-security-policy'] = "default-src 'none'; style-src 'unsafe-inline'"
+    else
+      headers['content-security-policy'] = "default-src 'none'; style-src 'unsafe-inline'; sandbox"
+    end
     super
   end
 end
```

#4 - 2024-06-03 11:08 - Go MAEDA

- Target version set to 5.1.3

Setting the target version to 5.1.3.

#5 - 2024-06-03 18:48 - Holger Just

- File sample.pdf added

The root cause of this (along with Safari being weird) is that we are always serving PDF files with content-disposition: inline (#22483), precisely to please the browser's builtin PDF viewers. For PDF files, the download behavior is thus different from all other filetypes.

Initially, Gregor proposed in #22483 to also provide an inline preview of PDF files (similar to images). Unfortunately, Jean-Philippe rejected this inline preview in #22483#note-14 at the time. Personally, I still believe that this would be the more elegant solution as then we could (from the user-perspective) have the consistent interface of an online preview and an actual download button (which would then also send the PDF with content-disposition: attachment). This would allow to avoid weakening the CSP just to please Safari's weird inline PDF viewer. At Planio, we use something quite similar for a long time now.

In any case, please note that removing the sandbox attribute may possible cause an XSS vulnerability if a raw malicious PDF file containing Javascript can be opened in the origin of a Redmine site (which may be possible due to the inline display. The various inline PDF viewers of browsers handle Javascript in PDFs differently internally, but they generally do not execute JS within the download origin (thus avoiding an XSS).

In any case, I do believe that this is an actual browser bug in Safari as it should not apply the PDF file's CSP for its inline reader component. Instead, the reader itself should respect the CSP of the file.

Both Firefox and Chromium / Chrome had similar bugs once which fixed by exempting their respective builtin PDF viewers from CSP restrictions. I believe that Safari should resolve this issue in the same way.

#6 - 2024-06-03 19:00 - Holger Just

- File deleted (sample.pdf)

#7 - 2024-06-11 09:58 - Go MAEDA

- Target version changed from 5.1.3 to 5.1.4

#8 - 2024-07-18 13:55 - Go MAEDA

- Target version deleted (5.1.4)

#9 - 2025-03-18 01:43 - Katsuya HIDAKA

Safari 18.4 may resolve this issue. Here is an excerpt from the Safari 18.4 Beta release notes :

> Fixed main frame PDFs served with a CSP sandbox header not loading. (141166987)

I have confirmed that PDFs display correctly in Safari Technology Preview 215, which includes this fix.

(For reference) Here is the WebKit pull request that addresses this issue:
https://github.com/WebKit/WebKit/pull/37882

#10 - 2025-03-18 08:19 - Marius BĂLTEANU

- Status changed from Confirmed to Closed

- Resolution set to Invalid

The issue is fixed in the upcoming Safari 18.4, nothing to do on Redmine side.

#11 - 2025-04-07 04:55 - Katsuya HIDAKA

Safari 18.4 has been released, and I've confirmed that this issue is resolved in that version.

> Safari 18.4 Release Notes
> Released March 31, 2025 — 18.4 (20621.1.15)
> https://developer.apple.com/documentation/safari-release-notes/safari-18_4-release-notes

Files

clipboard-202405221849-ombs9.png	125 KB	2024-05-22	Go MAEDA