

master

...

cve / readme.MD

Houziaux mike / Jenaye

History

0 contributors

39 lines (15 sloc) | 943 Bytes

...

## CVE

### OpenUpload 0.4.3

- Description : allow attacker to inject arbitrary malicious HTML or JavaScript code in user web browser.
- Affected version : All <= 0.4.3

### Information :

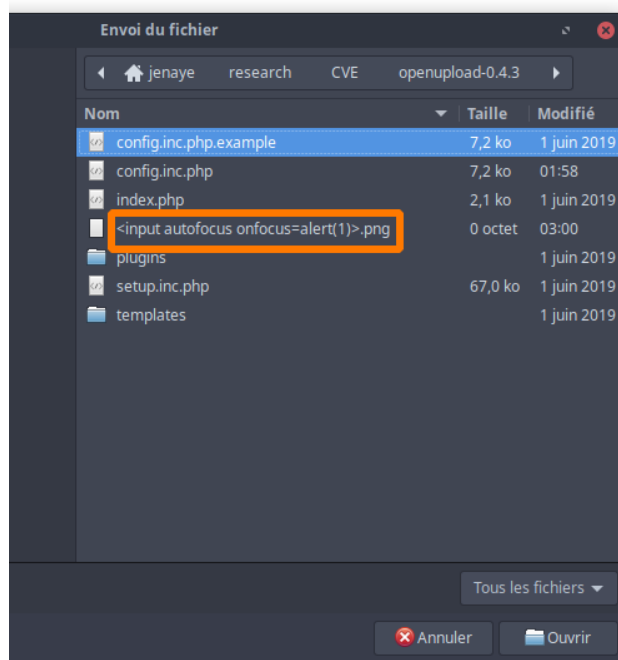
To make this POC, i just install Openupload 0.4.3 from <http://openupload.sourceforge.net> and configure it using nginx/php-fpm.

- Vulnerability Type: Cross Site Scripting (XSS Stored)

## POC

You have to upload file into <http://localhost/index.php?action=u> and set ure payload into filename field.

```
1444/index.php?lang=en&action=u&step=1
```

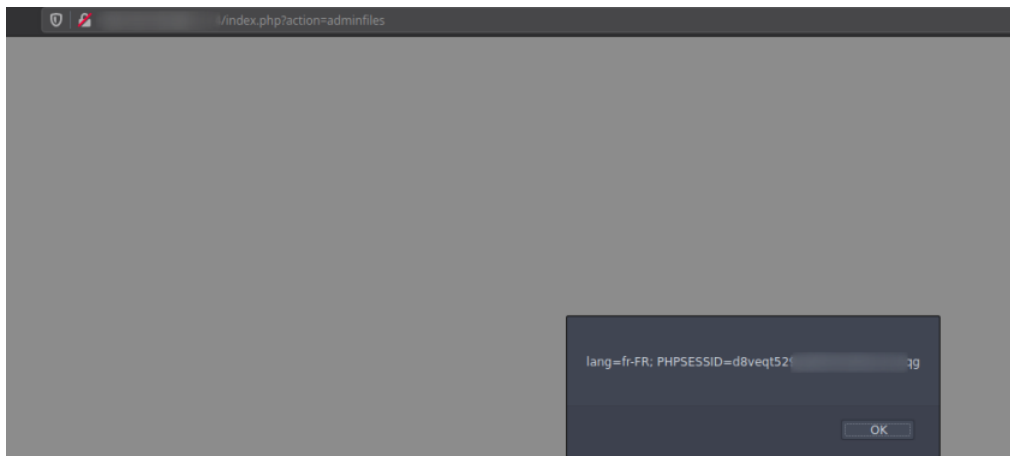


Select the file to be uploaded

Parcourir...

Aucun fichier sélectionné.

Maximum allowed upload size: 100 MB



There is two way to exploit it:

1. Send Link to your uploaded file to admin by email for exemple
2. let admin navigate himself into `http://localhost/index.php?action=adminfiles`

In both cases, your payload will be executed.