New issue

Jump to bottom

A Directory Traversal vulnerability #40

Closed Zh3-H4ck opened this issue on Nov 11, 2019 · 3 comments

Zh3-H4ck commented on Nov 11, 2019

test version:2.4.7

0x00 description

Frontaccounting is using the function clean_file_name() to eliminate '../' in the file name submitted by the user to avoid directory traversal vulnerability.

```
398  */
399 function clean_file_name($filename) {
400     $filename = str_replace(chr(0), '', $filename);
401     return preg_replace('/[^a-zA-Z0-9.\-_]/', '_', $filename);
402 }
403
```

However, some variables do not use the function clean_file_name() in admin/inst_lang.php, which can cause attackers submit the language package containing the language code of '../'. Affter adding successfully, by deleting it, the attacker can emptied specified folder like the examples.

admin/inst_lang.php:156

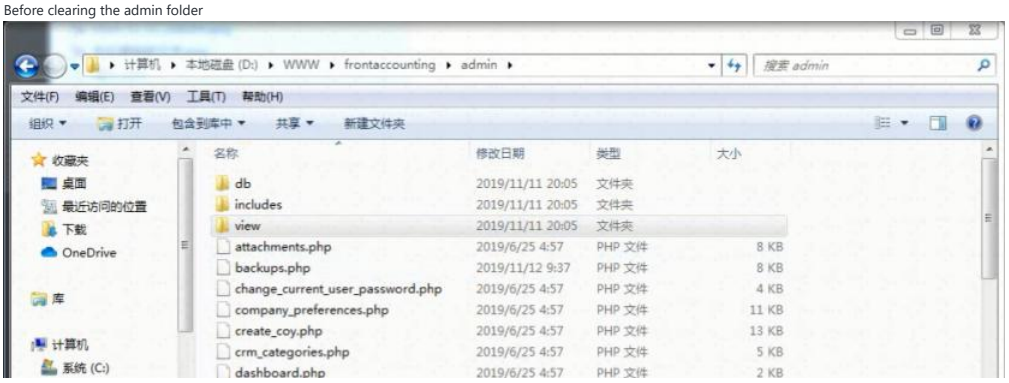
```
146 function handle_submit($id)
147 {
148     global $path_to_root, $installed_languages, $dflt_lang, $Mode;
149
150     if ($_POST['dflt']) {
151         $dflt_lang = $_POST['code'];
152     }
153
154     $installed_languages[$id]['code'] = $_POST['code'];
155     $installed_languages[$id]['name'] = $_POST['name'];
156     $installed_languages[$id]['path'] = 'lang/' . $_POST['code'];
157     $installed_languages[$id]['encoding'] = $_POST['encoding'];
158     $installed_languages[$id]['rtl'] = (bool)$_POST['rtl'];
159     $installed_languages[$id]['package'] = '';
160     $installed_languages[$id]['version'] = '';
161     if (!write_lang())
162         return false;
163     $directory = $path_to_root . "/lang/" . $_POST['code'];
164     if (!file_exists($directory))
165     {
166         mkdir($directory);
167         mkdir($directory . "/LC_MESSAGES");
168     }
169     if (is_uploaded_file($_FILES['uploadfile']['tmp_name']))
170     {
171         $file1 = $_FILES['uploadfile']['tmp_name'];
172         $code = preg_replace('/[^a-zA-Z_]/', '', $_POST['code']);
173         $file2 = $directory . "/LC_MESSAGES/$code.po";
174         if (file_exists($file2))
175             unlink($file2);
176         move_uploaded_file($file1, $file2);
177     }
178     if (is_uploaded_file($_FILES['uploadfile2']['tmp_name']))
```

admin/inst_lang.php:240

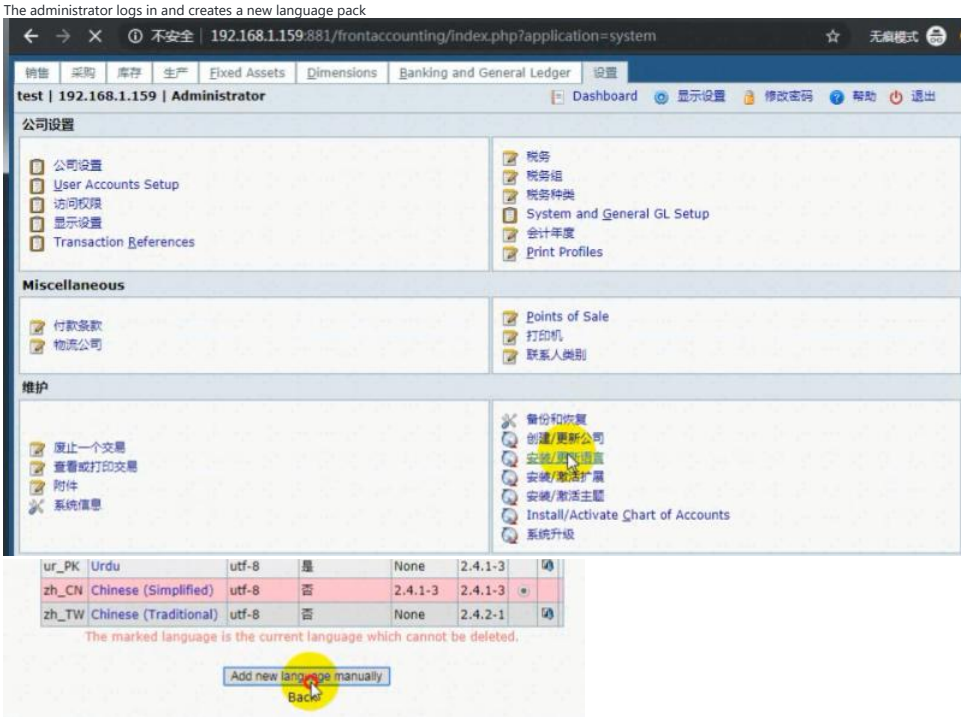
```php
function handle_delete($id)
{
    global  $path_to_root, $installed_languages, $dflt_lang;

    $lang = $installed_languages[$id]['code'];
    if ($installed_languages[$id]['package'])
        if (!uninstall_package($installed_languages[$id]['package']))
            return;

    if ($lang == $dflt_lang ) {
        // on delete set default to current.
        $dflt_lang = $_SESSION['language']->code;
    }

    unset($installed_languages[$id]);
    $installed_languages = array_values($installed_languages);

    if (!write_lang())
        return;

    $dirname = "$path_to_root/lang/$lang";
    if ($lang && is_dir($dirname)) {    // remove nonstadard language dir

        flush_dir($dirname, true);
        rmdir($dirname);
    }
}
```

0x01 Example:empty admin folder

0. Before clearing the admin folder

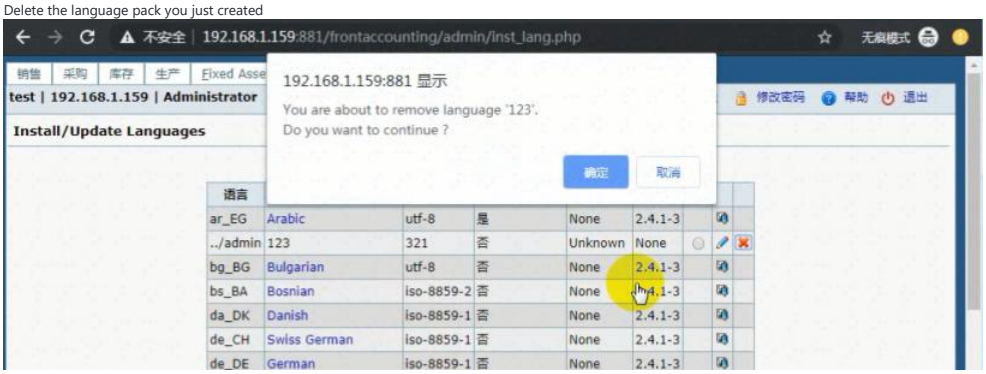


1. The administrator logs in and creates a new language pack



2. Set the language code to ../admin and save it

3. Delete the language pack you just created



4. After deleting successfully, the admin folder will be emptied

Zh3-H4ck changed the title ~~a Directory Traversal vulnerability~~ **A Directory Traversal vulnerability** on Nov 11, 2019

FrontAccountingE... commented on Jul 13, 2020 — Owner

Yes, indeed. Fix is added to the repo.

apmuthu added a commit to apmuthu/frontac24 that referenced this issue on Jul 23, 2020

`Install/Update Languages: fixed directory traversal issue` ... `606acdc`

cambell-prince commented on Nov 11, 2021 — Contributor

> Yes, indeed. Fix is added to the repo.

Should this issue be closed?

Zh3-H4ck commented 3 weeks ago — Author

ok

Zh3-H4ck closed this as completed 3 weeks ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants