New issue

Jump to bottom

Bug:V1.1.10 Cross Site Scripting Vulnerability #3

Open **Richard1266** opened this issue on Mar 11, 2019 · 0 comments

Richard1266 commented on Mar 11, 2019 • edited

There is an Stored Cross Site Scripting vulnerability in your latest version of the CMS v1.1.10
Download link: "http://down.ukcms.com/down.php?v=1.1.10"

In the UKCMSv1.1.10\application\home\controller\Single.php, No filtering to data in the index( ) function:

```php
public function index($id = '') {
    $result = $this->validate(['modelId' => $id], ['modelId|模型ID' => 'require|number']);
    if (true !== $result) {
        $this->error($result);
    }
    //模型用途检查
    $info = Db::name('Model')->where('id', $id)->find();
    if ('column' == $info['purpose']) {
        $this->error('不可以是栏目模型');
    }

    if ($this->request->isPost()) {
        if (!$info['ifsub']) {
            $this->error($info['title'] . '模型禁止投稿~');
        }
        $data = $this->request->post();
        // 验证码
        if (config('captcha_signin_model')) {
            $captcha = $data['captcha'];
            $captcha == '' && $this->error('请输入验证码');
            if (!captcha_check($captcha, '', config('captcha'))) {
                //验证失败
                $this->error('验证码错误或失效');
            }
        }
        //令牌验证
        $vresult = $this->validate($data, ['__token__|令牌' => 'require|token']);
        if (true !== $vresult) {
            $this->error($vresult);
        }
        $ModelField = model('ModelField');
        //后置审核
        $data['modelField']['status'] = 0;
        $data['modelFieldExt'] = isset($data['modelFieldExt']) ? $data['modelFieldExt'] : [];
```

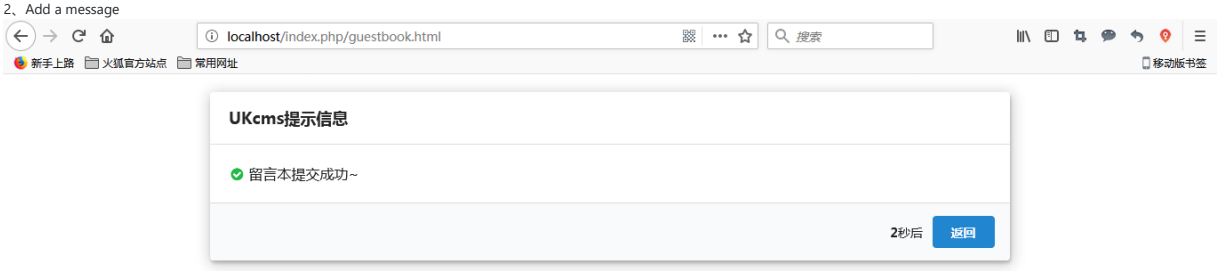
没有对data参数进行过滤

Vulnerability trigger point

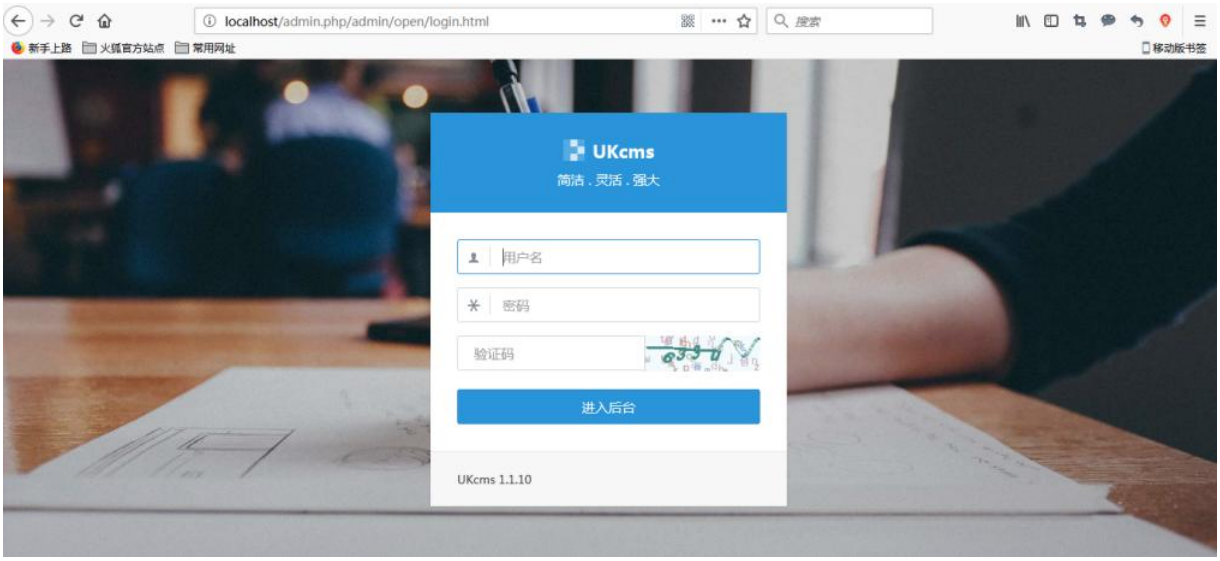
http://localhost/admin.php/admin/content/guestbook.html

1、Go to the front page to find the message board

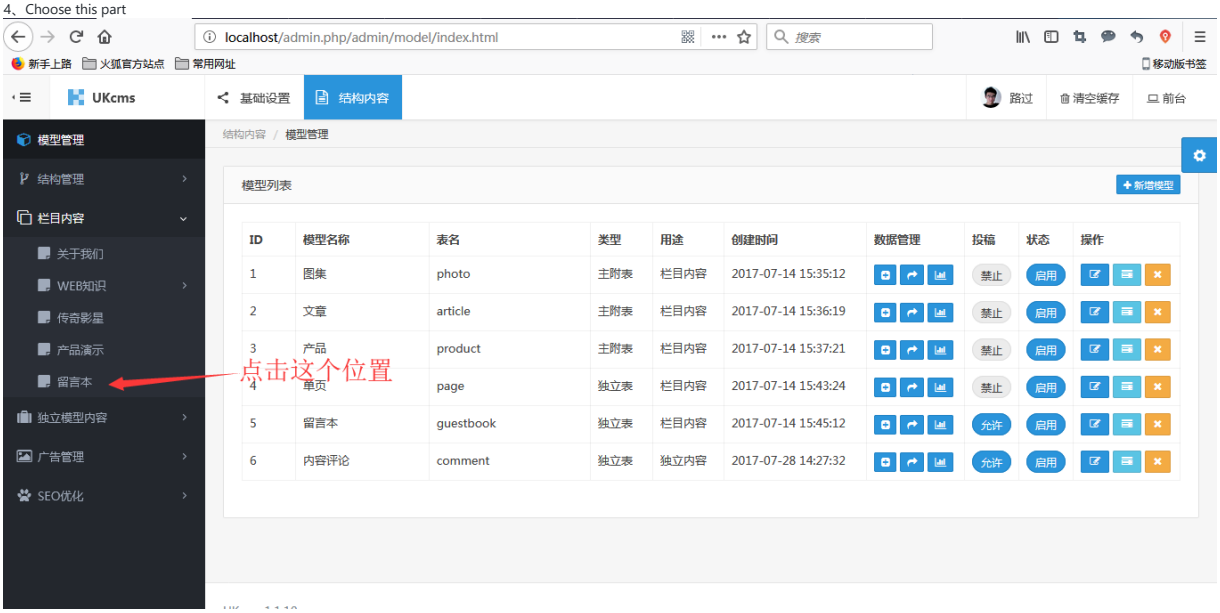
2、Add a message



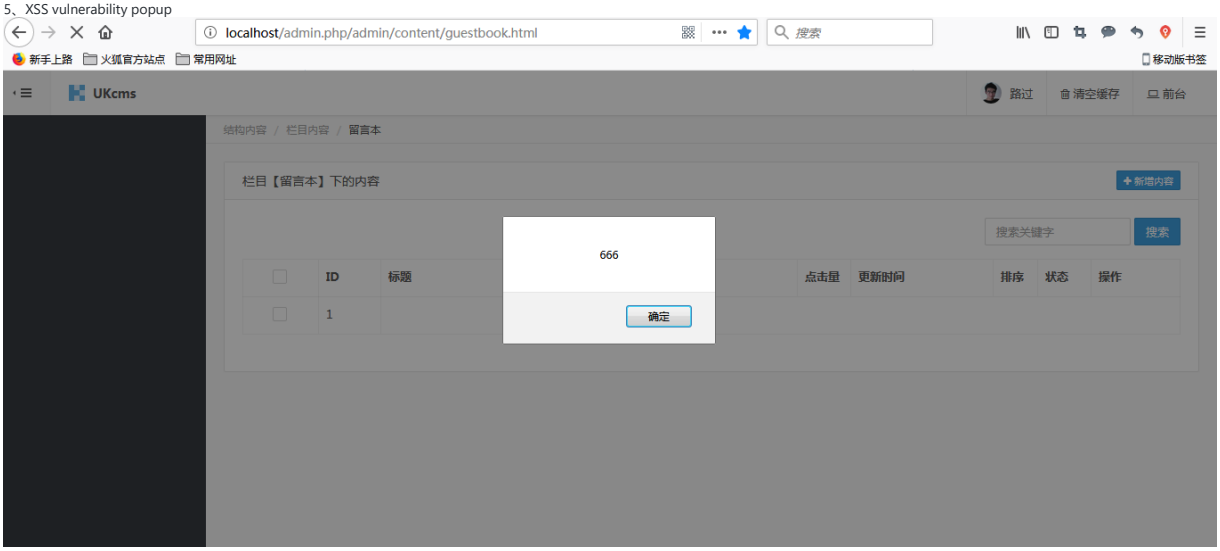
3、Log in as admin



4、Choose this part



5、XSS vulnerability popup



Fix:
This is an XSS vulnerability, this vulnerability is because no filtering to data in the index( ) function.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant