xinhu-oa

xinhu oa Information leakage xinhu V2.1.9 After the user logged in, open the following page poc： /index.php?a=gettotal&m=index&d=home&atype=&loadci=&optdt=&nums=gong,kqdk,apply,officic,syslog,about&ajaxbool=true

Display the information in the picture

{"optdt":"2020-12-09 16:23:07","todo":0,"reimstotal":"1","showkey":"UslXT8rXkA8OygtfV8kJn4plyo9PjohIns:","menuarr":[{"id":"43","num":"daiban","name":"\u5f85\u529e\/\u5904
\u7406","url":"main,fwork,bill,atype=daib","color":"#3BBDDB","icons":"time"},{"id":"100","num":"todo","name":"\u63d0\u9192\u4fe1
\u606f","url":"system,geren,todo","color":"#EFBB62","icons":"bell"},{"id":"3","num":"user","name":"\u7528\u6237\u7ba1
\u7406","url":"flow,page,user,atype=all,pnum=all","color":"#5AAAE2","icons":"user"},{"id":"67","num":"workwwc","name":"\u6211\u672a\u5b8c\u6210\u4efb
\u52a1","url":"flow,page,work,atype=wwc","color":"#BFC462","icons":"book"},{"id":"207","num":"flowtodo","name":"\u5355\u636e\u63d0
\u9192","url":"main,fwork,todo","color":"#ADCC61","icons":"star-empty"},{"id":"29","num":"danerror","name":"\u5355\u636e\u5f02\u5e38\u76d1
\u63a7","url":"main,flow,error","color":"#800000","icons":"briefcase"}],"token":"rdg8lp0l","authkey":"","usedt":"MjAyMC0xMi0xNg::","sqlmodel":"NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION
","","],"gongarr":[{"id":"6","typename":"\u901a\u77e5\u516c\u544a","optdt":"2020-11-19 09:54:19","title":"\u4fe1\u547c\u66f4\u65b0\u53d1\u5e03V2.1.9\u7248\u672c","optname":"\u7ba1\u7406
\u5458","zuozhe":"\u4fe1\u547c\u5f00\u53d1\u56e2\u961f","indate":"2020-11-19","recename":"\u4fe1\u547c\u5f00\u53d1\u56e2\u961f","fengmian":"images
\/logo.png","mintou":"0","status":"1","istop":"1","appxs":"1"},{"id":"9","typename":"\u901a\u77e5\u516c\u544a","optdt":"2019-06-03 13:17:05","title":"\u4f60\u4eec\u89c9\u5f97\u8fd9\u4e2a\u7cfb
\u7edf\u5982\u4f55\uff1f(\u6295\u7968)","optname":"\u7ba1\u7406\u5458","zuozhe":"\u5f00\u53d1\u90e8","indate":"2017-08-26","recename":"\u4fe1\u547c\u5f00\u53d1\u56e2
\u961f","fengmian":null,"mintou":"1","status":"1","istop":"0","appxs":"0"},{"id":"2","typename":"\u89c4\u5219\u5236\u5ea6","optdt":"2019-04-13 19:54:43","title":"\u5173\u4e8e\u5199\u65e5\u62a5
\u5236\u5ea6\u8bf4\u660e","optname":"\u7ba1\u7406\u5458","zuozhe":"\u4eba\u529b\u884c\u653f\u90e8","indate":"2016-08-01","recename":null,"fengmian":"images
\/kqbanner1.jpg","mintou":"0","status":"1","istop":"0","appxs":"0"},{"id":"1","typename":"\u901a\u77e5\u516c\u544a","optdt":"2018-04-26 17:27:10","title":"\u6b22\u8fce\u4f7f\u7528\u4fe1\u547c
\u5de5\u4f5c\u53f0","optname":"\u7ba1\u7406\u5458","zuozhe":"\u4fe1\u547c\u5f00\u53d1\u56e2
\u961f","indate":"2016-08-01","recename":null,"fengmian":null,"mintou":"0","status":"1","istop":"0","appxs":"0"}],"kqdkarr":{"sbarr":[{"id":"12","name":"\u4e0a
\u73ed","stime":"09:00:00","etime":"12:00:00","qtype":"0","sort":"0","iskt":"0","iskq":"1","isxx":"0","state":"\u672a\u6253\u5361<\/font>"},{"id":"2","name":"\u4e0b
\u73ed","stime":"13:00:00","etime":"18:00:00","qtype":"1","sort":"3","iskt":"0","iskq":"1","isxx":"0","state":"\u672a\u6253\u5361<\/font>"}],"dkarr":[]},"applyarr":[{"cont":"\u3010\u6863\u6848\u501f
\u9605\u3011\u5355\u53f7:DA-20200928-001,\u65e5\u671f:2020-09-28\uff0c\u5f85\u5927\u4e54<\/font>\u5904\u7406","modename":"\u6863\u6848\u501f
\u9605","modenum":"danganjy","id":"3","count":8},{"cont":"\u3010\u4efb\u52a1\u3011\u5355\u53f7:XW-20200703-001,\u65e5\u671f:2020-07-03\uff0c\u5f85\u8d75\u5b50\u9f99<\/font>\u6267
\u884c","modename":"\u4efb\u52a1","modenum":"work","id":"2","count":8},{"cont":"\u3010\u5f00\u7968\u7533\u8bf7\u3011\u5355\u53f7:FF-20181022-001,\u65e5\u671f:2018-10-22\uff0c\u5f85
\u8c82\u8749<\/font>\u5904\u7406","modename":"\u5f00\u7968\u7533\u8bf7","modenum":"finkai","id":"12","count":8},{"cont":"\u3010\u79bb\u804c\u7533\u8bf7\u3011\u5355\u53f7:HB-
20161007-0001,\u65e5\u671f:2016-10-07\uff0c\u5f85\u78d0\u77f3<\/font>\u5904\u7406","modename":"\u79bb\u804c\u7533\u8bf7","modenum":"hrredund","id":"11","count":8},{"cont":"\u3010
\u8f66\u8f86\u9884\u5b9a\u3011\u5355\u53f7:CJ-20180903-001,\u65e5\u671f:2018-09-03\uff0c\u5f85\u5f20\u98de<\/font>\u5904\u7406","modename":"\u8f66\u8f86\u9884
\u5b9a","modenum":"carmrese","id":"11","count":8}],"officiarr":[{"id":"9","uid":"1","title":"\u5173\u4e8e\u56fd\u5e86\u653e\u5047\u901a\u77e5","titles":"\u56fd\u5e86 \u653e\u5047","class":"
\u51b3\u8bae","type":"0","grade":"\u5e73\u6025","optname":"\u7ba1\u7406\u5458","optdt":"2020-06-19 22:29:41","status":"1","content":null,"receid":"d1","recename":"\u4fe1\u547c\u5f00\u53d1
\u56e2\u961f","applydt":"2020-06-19","num":"\u4fe1\u547c\u30142020\u30151\u53f7","optid":"1","explain":null,"isturn":"1","filecontid":"13","zinum":"\u4fe1\u547c","unitname":"\u4fe1\u547c
\u5f00\u53d1\u56e2\u961f","unitsame":"\u5f00\u53d1\u90e8","miji":"\u516c\u5f00","laidt":null,"chaoname":null,"zuncheng":"\u5404\u4f4d\u540c\u4e8b","thid":"-1","yzid":"-
1","ffid":"4","enddt":null,"startdt":null,"comid":"1","ffdt":"2020-06-20","pdfid":"0"},{"id":"4","uid":"1","title":"\u5173\u4e8e\u8c03\u6574\u793e\u4fdd\u57fa\u6570\u7684\u901a\u77e5","titles":"
\u793e\u4fdd\u57fa\u6570","class":null,"type":"1","grade":"\u5e73\u6025","optname":"\u7ba1\u7406\u5458","optdt":"2019-05-12 23:10:41","status":"1","content":"

\n\t\u7531\u4e8e\u7cfb\u7edf\u5df2\u5347\u7ea7\uff0c\u57fa\u6570\u539f\u6765\u7684\u6700\u4f4e\u5de5\u8d441700\u8c03\u6574\u4e3a1800\u3002\n<\/p>\n

\n\t\u8bf7\u5404\u4e2a\u4f01\u4e1a\u5355\u4f4d\u52a1\u5fc5\u9075\u5b88\u3002\n<\/p>","receid":"d1","recename":"\u4fe1\u547c\u5f00\u53d1\u56e2\u961f","applydt":"2019-05-12","num":"

Check the source code and find that nums is not restricted，/webmain/home/index/indexAction.php

```
<script>
$(document).ready(function(){
    var optdt = '',loadci=0, taskarr={}, miao=200,reimtitle='REIM';
    var c= {
        itot:function(rlx){
            clearTimeout(this.tims);
            var nums = '',i;
            for(i=0;i<homenums.length;i++){
                nums+=','+homenums[i]+'';
            }
            if(!rlx)rlx='';
            var url  = js.getajaxurl('gettotal','index','home', {atype:rlx,loadci:loadci,optdt:optdt,nums:nums.substr(1)});
            $('#refresh_text').html(this.bd2('5Yi35paw57uf6K6h5LitLi4u'));
            js.ajaxbool =false;
            js.ajax(url,{},function(da){
                c.itots(da);
            },'get,json');
            homeobject.refresh=function(){c.refresh();};
        },
        init:function(){
            this.itot();
            var i,nust;
            for(i=0;i<homenums.length;i++){
                nust = homenums[i];
                if(homeobject[''+nust+'_init'])homeobject[''+nust+'_init']();
            }
        },
        refresh:function(){
            this.itot();
        },
        bd2:function(s){
```

Change ajaxbool = false to ajaxbool = true