



Open Source > Web System > Content Management System

轻舞飞沙 / 易思ESPCMS-P8企业建站管理系统

Watch 8 Star

Code Issues 4 Wiki Insights

Issues / 详情

There is a Remote Code Execution

Backlog #15WSA0 azraeluemo Open

Here I choose the latest version downloaded from the official website. It is the latest version.

The official url is <https://www.ecisp.cn/html/cn/>

Gitee Pages

PHPDoc

sonarqube Quality Analysis

Jenkins for Gitee

Baidu Efficiency Cloud

Tencent CloudBase

Tencent Cloud Serverless

OPENSCA 悬镜安全

Don't show this again

on is not the

Status

Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull request issue.

Branches

No related branch

Planned to start - Planned to end

Unscheduled - Unschedule

Top level

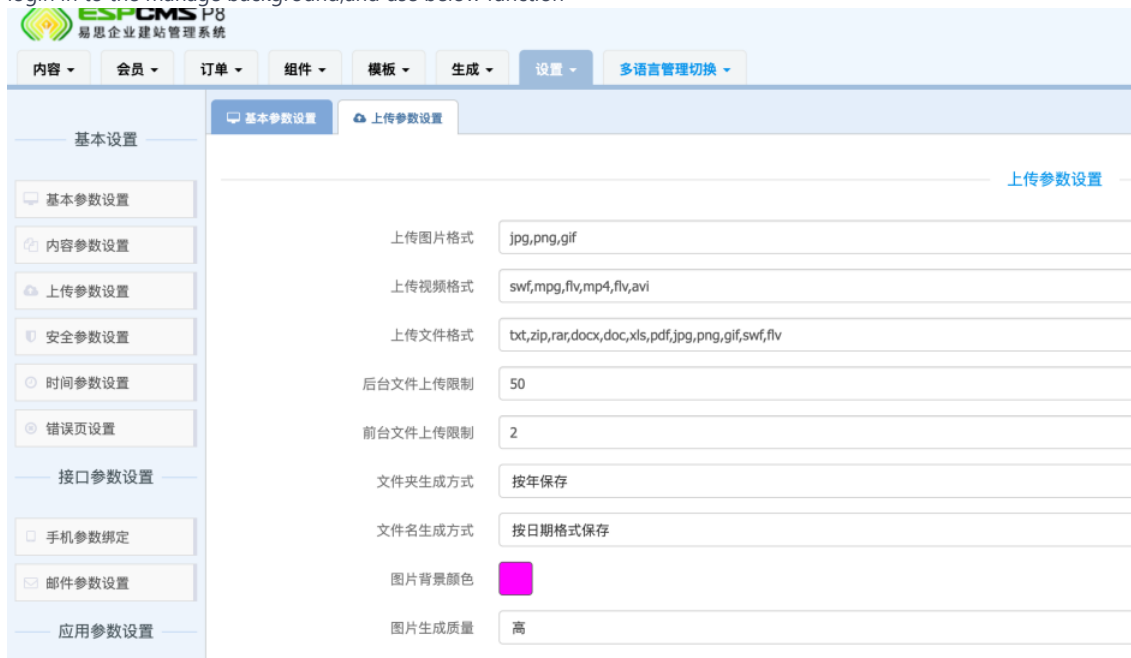
Not Top

Priority

Not specified




login in to the manage background,and use below function



参与者 (1)





Gitee 已支持 CLA 协议签署

- 第一方功能集成，签署流程更高效
- 内置可自定义的协议模板
- 让开源贡献也能有据可依

[I know](#)[View Details](#)

```

espcms > espcms_datacache > espcms_command.php
29      'CON_ENCRYPT_CODE'=>'6bdfc19d5cccb86045801093ad6bc0c',
30      'CON_ISDB0'=>'0',
31      'CON_DBOSN'=>'0',
32      'CON_VOL'=>'8621120101',
33      'CON_VOLSTR'=>'P8.21120101专业版',
34      'WEB_ICON_16'=>'upfile/espcms_16.png',
35      'WEB_ICON_32'=>'upfile/espcms_32.png',
36      'WEB_ICON_64'=>'upfile/espcms_64.png',
37      'ERRPAGE_500'=>'500',
38      'ERRPAGE_404'=>'403',
39      'INPUT_ISDES'=>1,
40      'INPUT_ISDESCRIPTION'=>200,
41      'INPUT_ISDELLINK'=>1,
42      'INPUT_CLICK'=>0,
43      'IS_KEYLINK'=>1,
44      'INPUT_COLOR'=>'#000040',
45      'IS_URLSTERN'=>0,
46      'UPFILE_FILE_PIC_TYPE'=>'jpg,png,gif',
47      'UPFILE_FILE_MOVER_TYPE'=>'swf,mpg,flv,mp4,flv,avi',
48      'UPFILE_FILE_OTHER_TYPE'=>'txt,zip,rar,docx,doc,xls,pdf,jpg,png',
49      'UPFILE_SIZE'=>50,
50      'UPFILE_SAVEDIR'=>'m2',
51      'UPFILE_FORMATFILE_TYPE'=>'1',
52      'UPFILE_PIC_BACKGROUND_COLOR'=>'#ff00ff',
53      'UPFILE_PIC_CREATE_QUALITY'=>'80',
54      'UPFILE_PIC_ISZOOM'=>0,
55      'UPFILE_PIC_ZOOMTYPE'=>'1',
56      'UPFILE_ISWATERMARK'=>0,
57      'UPFILE_WATERMARK_TYPE'=>1,
58      'UPFILE_WATERMARK_POSITION'=>'6',
59      'UPFILE_WATERMARK_PIC_FILENAME'=>'1'

```



```

61 'UPFILE_WATERMARK_FONT'=>'ES
62 'UPFILE_WATERMARK_FONT_SIZE'
63 'UPFILE_WATERMARK_FONT_COLOR'
64 'UPFILE_SAVAPATH'=>'upfile/'
65 'UPFILE_PIC_ZOOM_WIDTH'=>200
66 'UPFILE_PIC_ZOOM_HEIGHT'=>200
67 'WEB_UPFILE_SIZE'=>2

```

← → 不安全 | 192.168.1.132/espms/espms_datacache/espms_command.php

PHP Version 7.4.3

System	Linux ubuntu 5.15.0-48
Build Date	Aug 17 2022 13:29:58
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/10-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-filter.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-ldap.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-redis.ini, /etc/php/7.4/apache2/conf.d/20-session.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-syssem.ini, /etc/php/7.4/apache2/conf.d/20-sysshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

I know

View Details

The reason was that,ESPCMS_Core::command_creat() will save the config

```

...  espcms_load.php  espcms_command.php  SettingMain.php X
espcms > espcms_admin > control > SettingMain.php
77 $espcms_admin_templates->into('first_field', $first_field);
78 $espcms_admin_templates->into('config_category_id', $config_category_id);
79 $espcms_admin_templates->into('setting', $array);
80 $espcms_admin_templates->into('espcms_command', $espcms_command);
81 $espcms_admin_templates->into('link', SettingLink::SettingMain_link_array());
82 $espcms_admin_templates->into('fileDialog', SettingLink::FileManage_link_array('dialog', $_GET));
83 $espcms_admin_templates->output('admin/setting');
84 }
85 public static function saveSettingMain() {
86     global $espcms_link_db;
87     $db_table = ESPCMS_DB_PREFIX . "config";
88     if (!ESPCMS_AdminAuthority::authorityVerify('editSetting')) {
89         espcms_public_dialog('espcms_public_dialog', 'public_pack-espcms_authority_function_fail', 'false');
90     }
91     foreach ($_POST as $key => $value) {
92         $update_sql = "UPDATE $db_table SET config_value='$value' WHERE config_name='$key'";
93         $espcms_link_db->db_query($update_sql);
94     }
95     if (!ESPCMS_Core::command_creat()) {
96         espcms_public_dialog('espcms_info_save_ok', 'setting_pack-espcms_setting_creat_err', 'false', array
97     }
98     if ($_POST['TS_HTML'] < 55 && $espcms_ismatches($_POST['TS_HTML'])) {

```

And there are no check for the param.

```

public static function command_creat() {
    global $espcms_link_db;
    $sConfig = "<?php\n";
    $sConfig = $sConfig . "\r\nPHP version 5\r\nCopyright (c) 2012-2022 ECISP.CN,ESPCMS.CN\r\n警告：这不是一个免费的";
    $sConfig = $sConfig . "\$espcms_command = Array(\n";
    $db_table = ESPCMS_DB_PREFIX . "config";
    $db_sql = "SELECT * FROM $db_table ORDER BY config_category_id,config_id";
    $db_query = $espcms_link_db->db_query($db_sql);
    while ($fetch_row = $espcms_link_db->db_array_list($db_query)) {
        $valname = addslashes($fetch_row['config_name']);
        $value = addslashes($fetch_row['config_value']);
        $valtype = $fetch_row['config_type'];

        if ($valtype == 'int' || $valtype == 'bool') {
            $value = empty($value) ? 0 : $value;
            $sConfig = $sConfig . "\$espcms_command['$valname'] = " . ($valtype == 'int' ? $value : ($value ? 'true' : 'false')) . ";\n";
        } else {
            $sConfig = $sConfig . "\$espcms_command['$valname'] = " . addslashes($value) . ";\n";
        }
    }
    $sConfig = $sConfig . "\n";
    $update_sql = "UPDATE $db_table SET config_value='$sConfig' WHERE config_category_id=1";
    $espcms_link_db->db_query($update_sql);
}

```





```
}  
$sConfig = $sConfig . ");\n";  
$commandfile = ESPCMS_FILE_ROOT . 'espcms_datacache'  
if (!ESPCMS_FileTool::writeFile($commandfile, $sCon  
    return false;  
}  
return true;
```

Since this project will addslashed automatic. So i. chose to modify t

azraelxuemo created **任务** a month ago

[Sign in to comm](#)



Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[I know](#)

[View Details](#)



©OSCHINA. All rights reserved

[Git Resources](#)

[Learning Git](#)

[CopyCat](#)

[Downloads](#)

[Gitee Reward](#)

[Gitee Stars](#)

[Featured Projects](#)

[Blog](#)

[Nonprofit](#)

[Gitee Go](#)

[OpenAPI](#)

[Help Center](#)

[Self-services](#)

[Updates](#)

[About Us](#)

[Join us](#)

[Terms of use](#)

[Feedback](#)

[Partners](#)



777320883



git@oschina.cn



Gitee



+86 400-606-0201



Mini Program

OpenAtom Foundation Cooperative code hosting platform



违法和不良信息举报中心

粤ICP备12009483号

简体中文

