暑期练习web13：web test（i春秋）百度杯 九月场

原创

何家公子 于 2018-08-19 17:13:00 发布 158 收藏

分类专栏： ctf web 文章标签： web ctf

本文链接：https://blog.csdn.net/qq_41618162/article/details/81839590

ctf 同时被 2 个专栏收录

32 篇文章 0 订阅

订阅专栏

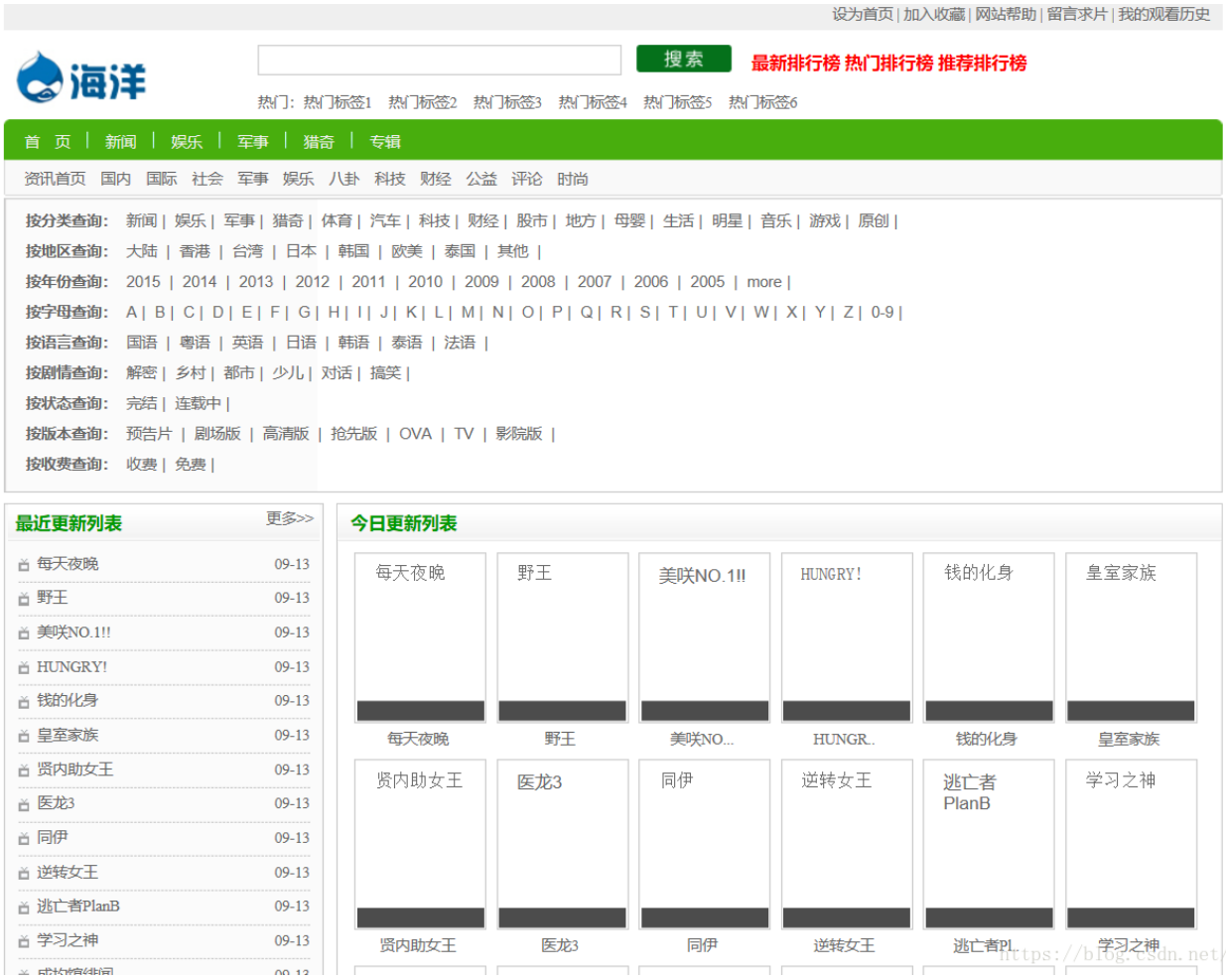
web

32 篇文章 0 订阅

订阅专栏

头一回做这样的题啊，感觉特新鲜！

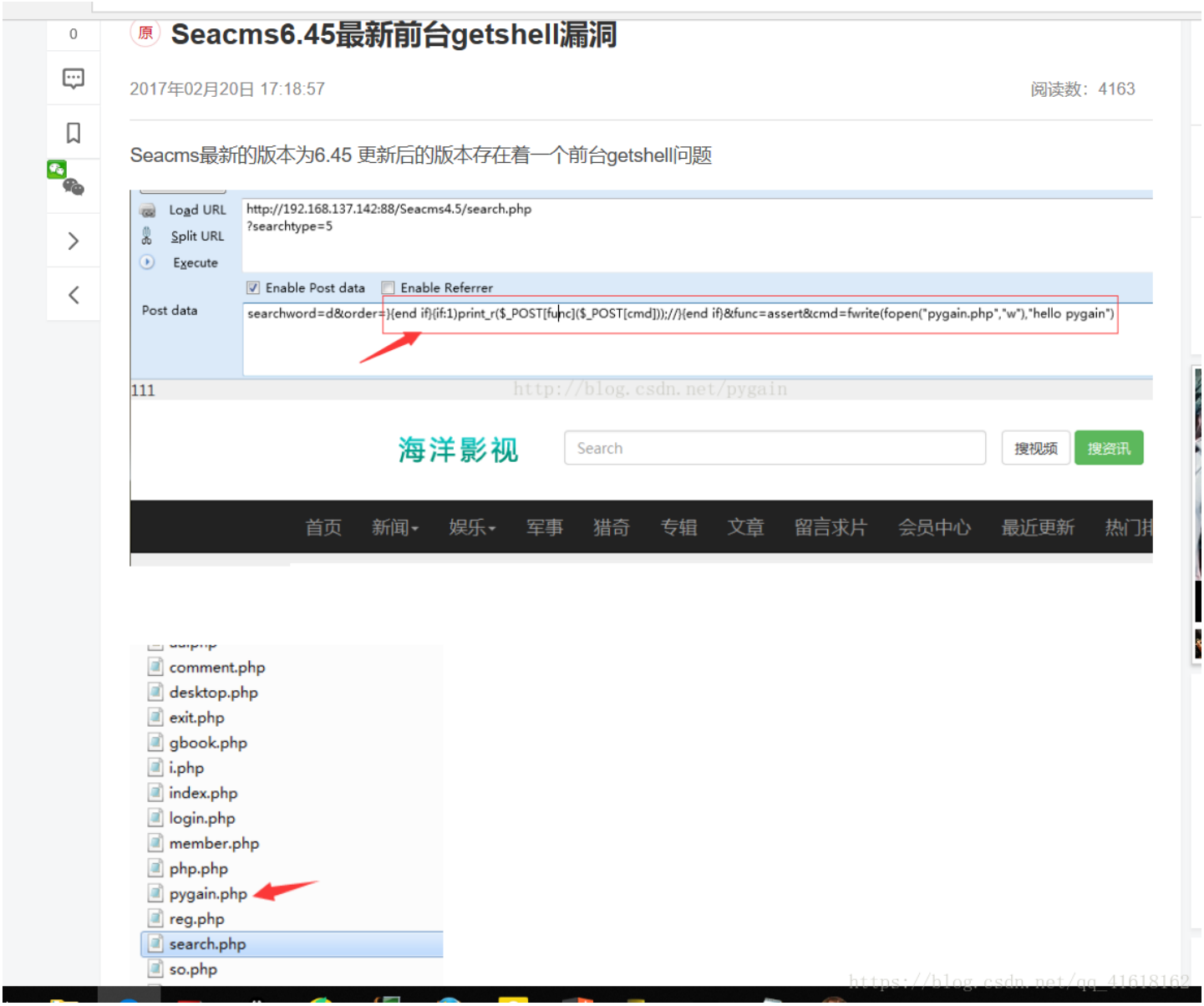
这次题目一打开居然是一个比较成型的网页了，源码也复杂到你根本不会去看



题目的hint是让我们善于搜索。。所以我就最后就搜出几篇wp来看看了。。。。

翻翻这个页面可以知道一个关键词：海洋cms

于是感觉去百度这个东西，发现它是一个具有许多漏洞的cms，这也是他会被选为靶机的原因吧。。现在我们一头雾水根本不知道这是什么玩意，知道我看到了一个可以前台getshell的博客



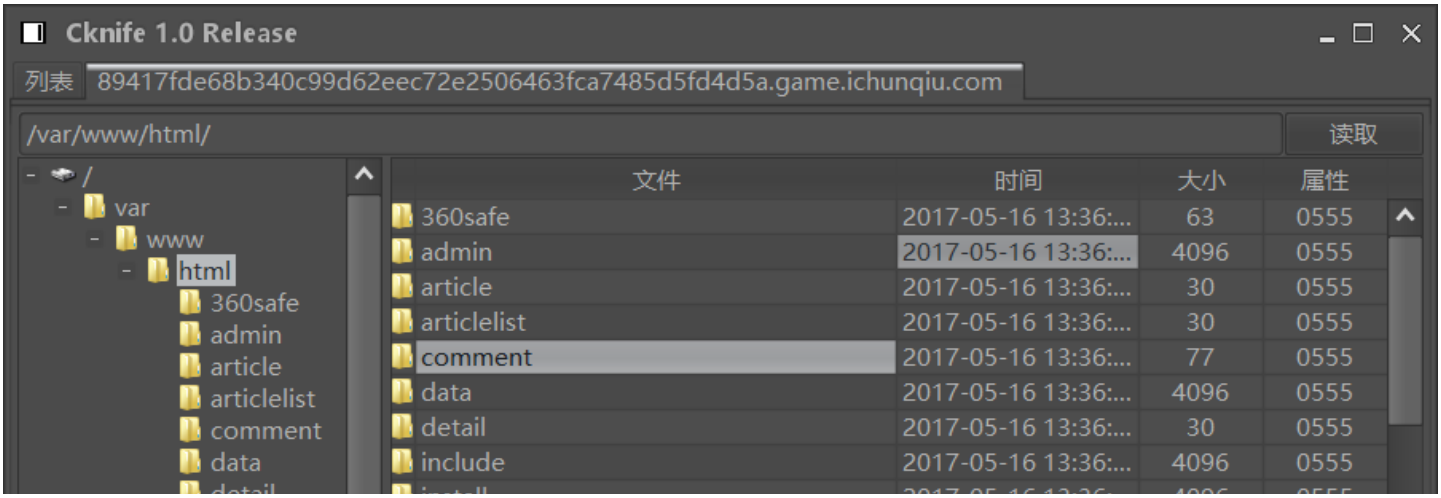
于是就开始了这方面的搜索

http://0day5.com/archives/4180/

https://blog.csdn.net/fsdzsec/article/details/53132362

这两篇都是在说海洋csm 6.28版本的一个漏洞

然后利用菜刀来抓一波：



然后我就想着找flag。。。结果文件太多了，根本找不着，这时候就想着找一波数据库配置文件
百度一下一般叫啥文件名

常用CMS数据库配置文件地址

DEDECMS:

data/common.inc.php

PHPCMS:

PHPCMS 2008的 include/config.inc.php

PHPCMS v9的 caches/configs/database.php

帝国CMS:

e/class/config.php

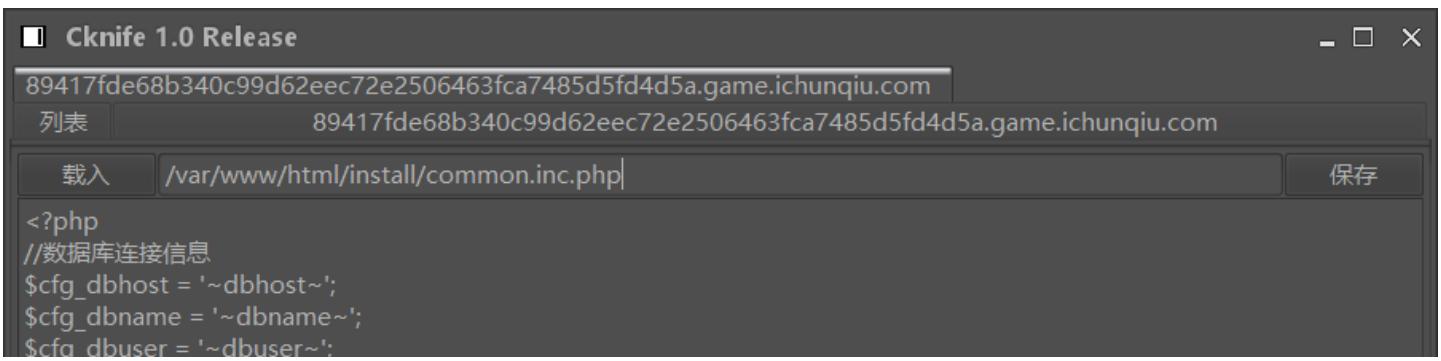
DZ论坛:

config\config_global.php

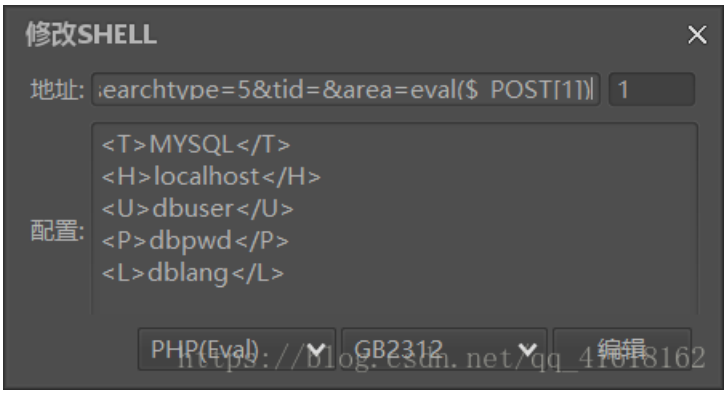
config\config_ucenter.php

uc_server\data\config.inc.php

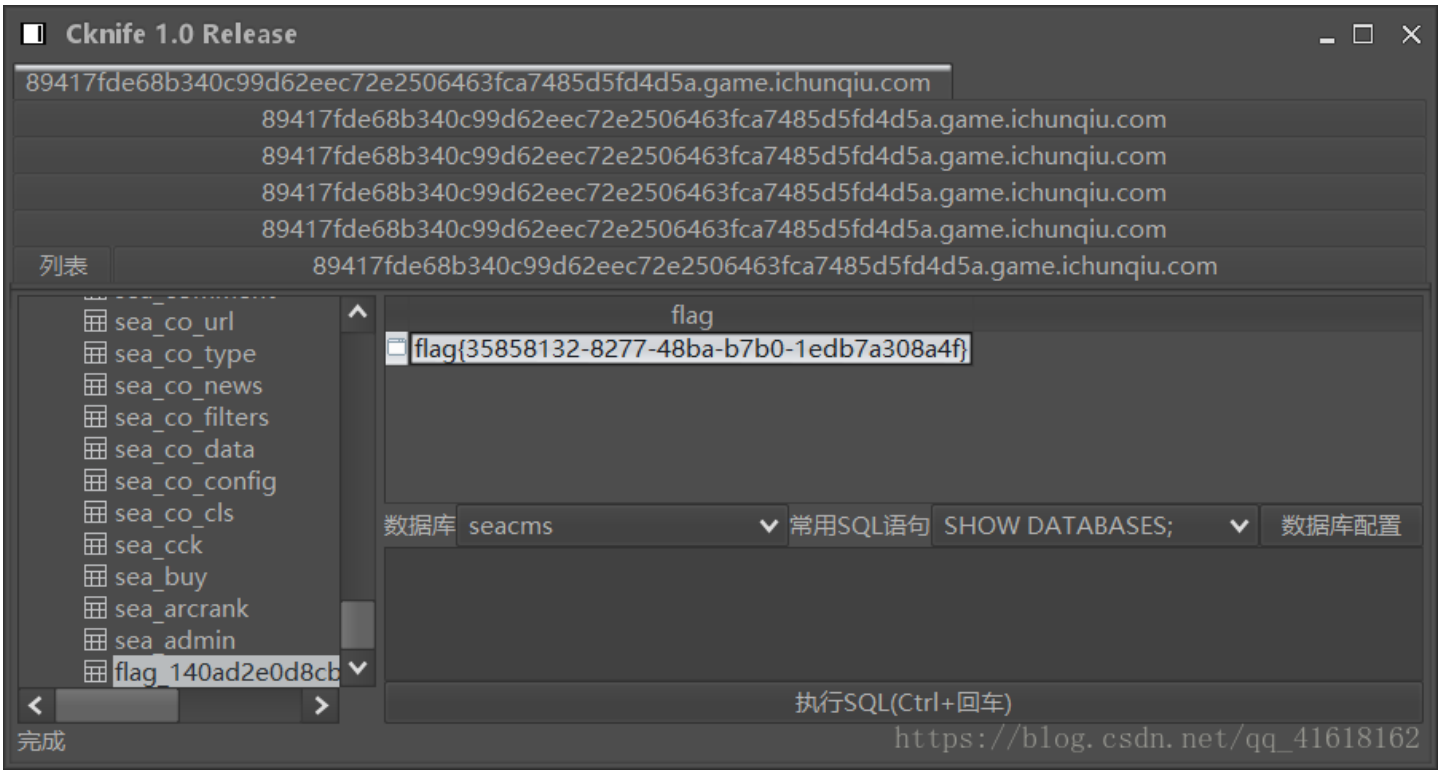
在install文件夹中找到了这个



这里发一个菜刀的教程，里面有说配置数据库的格式
https://blog.csdn.net/lixue20141529/article/details/78024525



（字符编码utf-8也行）
这样设置好了后，右键点击配置数据库
在seacms数据库中找到了flag



总结：这题就现在来说还是很新颖的，今后再遇见这样的题目也会有点路数，同时也是初步了解了菜刀的一些基础用法，也算不错啦


EX-AID
KAMEN RIDER
LV2
@KR-光之影字幕组