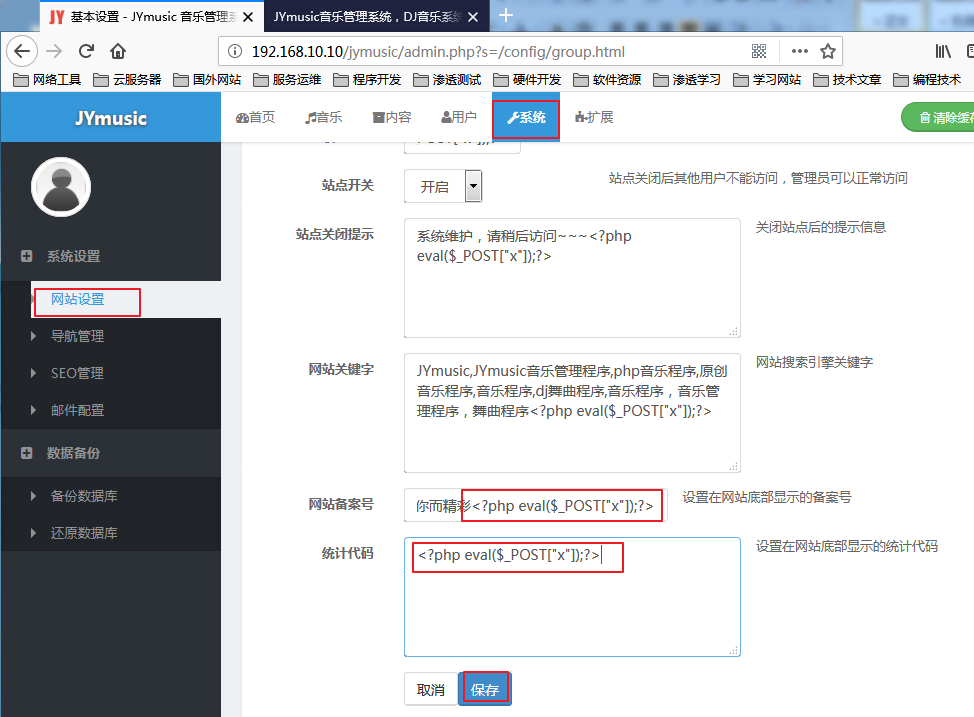
# 镜像搭建拿webshell

所谓镜像搭建，就是信息收集目标网站所使用的cms，去网上找到相同版本号的对应cms源码，然后本地搭建一个网站进行渗透测试，比如网站信息插马，但是不知道写入到哪个文件，因为是本地搭建，所以可以直接去翻目录，来确定具体的位置，再去对目标进行同样的访问，下面两个源码 jymusic和xyhcms就是利用这个思路，来拿webshell，这两个实验的前提是已经能够进入web后台管理界面了。



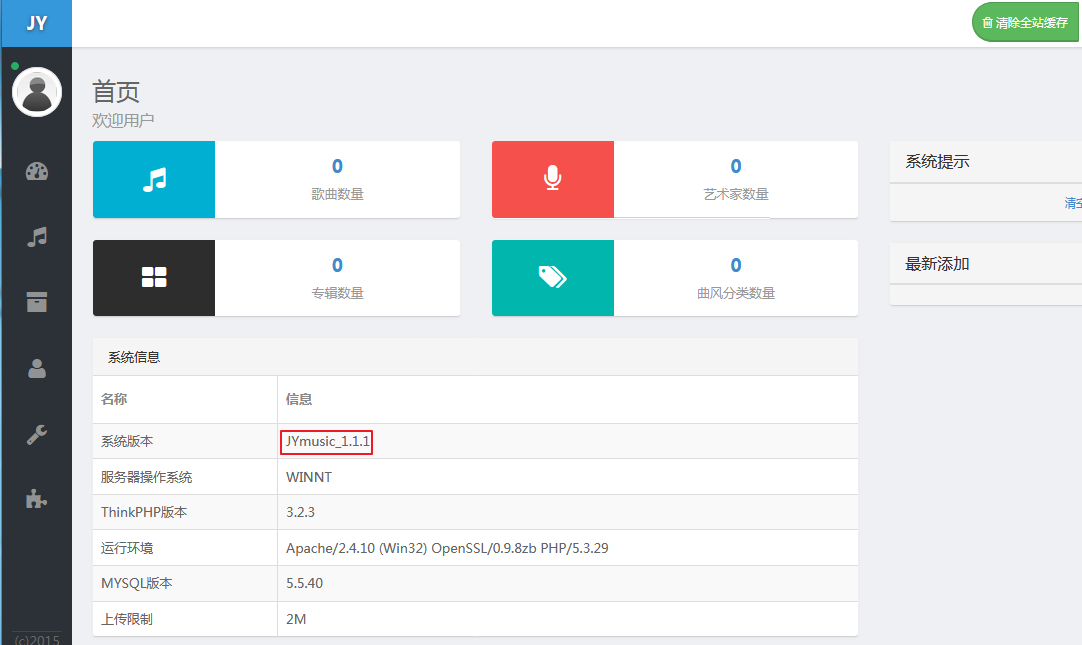
进入后台管理界面，默认账号admin,密码无默认自己设定的

在系统，网站设置里，有一些配置信息，往里头写入一句话木马

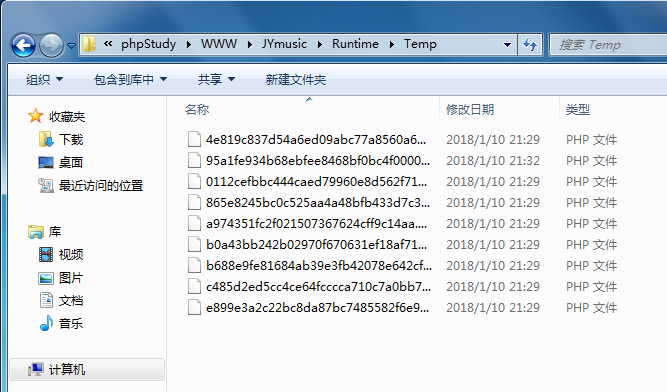




此时写入成功了，但是不知道写入的文件位置是哪里，所以可以去网上下载对应的cms来搭建，版本号可以在管理界面首页上看到。



本地搭建目录，经过搜索和测试发现，刚刚写入的一句话木马的配置信息放在一个临时目录

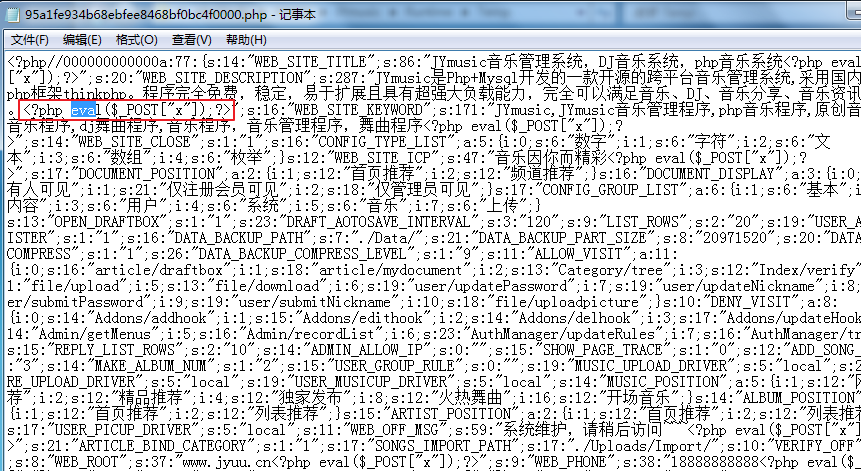


虽然这一串都是乱文，但是他其实是固定不会改变的，去首页清掉缓存重新生成也不会改变

对于jymusic的配置临时文件为：95a1fe934b68ebfee8468bf0bc4f0000.php

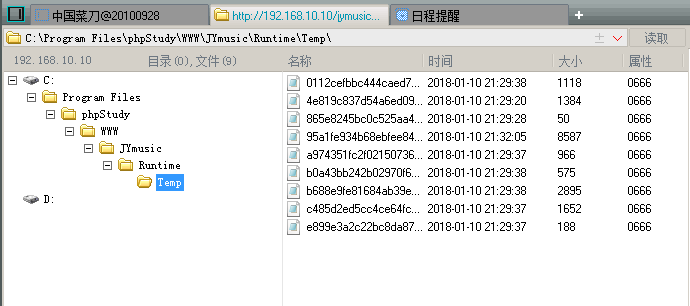
所在的相对网站路径为： Runtime/Temp/

可以打开文件搜索关键字eval查看一句话木马是否在里头



然后访问对应的URL，拿webshell即可

http://192.168.10.10/jymusic/Runtime/Temp/95a1fe934b68ebfee8468bf0bc4f0000.php

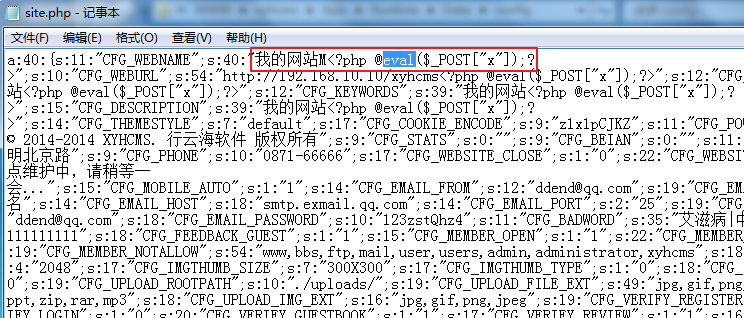


虽然很麻烦，但是很有效，知己知彼，方能百战百胜，下面是xyhcms的配置文件路径

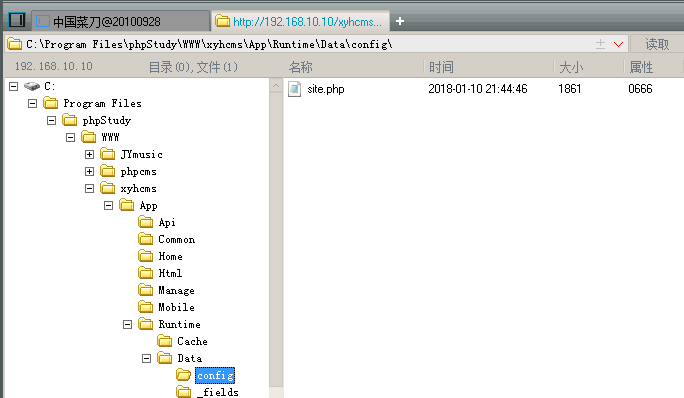




相对路径在：App\Runtime\Data\config\site.php



URL: http://192.168.10.10/xyhcms/App/Runtime/Data/config/site.php



总结可以发现，php配置信息一般都和 cache runtime data config App Application 目录有关，去里面耐心搜索就可以搜到了