攻防世界misc——mysql

原创

Captain杰派罗 于 2021-12-24 15:34:35 发布 1854 收藏

分类专栏： 攻防世界WP 文章标签： mysql 网络安全

本文链接：https://blog.csdn.net/weixin_45770420/article/details/122129370

下载得到附件压缩包

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# zipinfo c4b7dcaae4544a859c6013790e8e340d.zip
Archive:  c4b7dcaae4544a859c6013790e8e340d.zip
Zip file size: 614768 bytes, number of entries: 99
drwx---     6.3 fat        0 bx stor 17-Apr-12 13:37 mysql/
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/debian-5.5.flag
-rw----     6.3 fat 18874368 bx defN 17-Apr-12 11:42 mysql/ibdata1
-rw----     6.3 fat  5242880 bx defN 17-Apr-12 11:42 mysql/ib_logfile0
-rw----     6.3 fat  5242880 bx defN 17-Apr-12 11:42 mysql/ib_logfile1
drwx---     6.3 fat        0 bx stor 17-Apr-12 13:37 mysql/mysql/
-rw----     6.3 fat     8820 bx defN 17-Apr-12 11:42 mysql/mysql/columns_priv.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/columns_priv.MYD
-rw----     6.3 fat     4096 bx defN 17-Apr-12 11:42 mysql/mysql/columns_priv.MYI
-rw----     6.3 fat     9582 bx defN 17-Apr-12 11:42 mysql/mysql/db.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/db.MYD
-rw----     6.3 fat     2048 bx defN 17-Apr-12 11:42 mysql/mysql/db.MYI
-rw----     6.3 fat    10223 bx defN 17-Apr-12 11:42 mysql/mysql/event.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/event.MYD
-rw----     6.3 fat     2048 bx defN 17-Apr-12 11:42 mysql/mysql/event.MYI
-rw----     6.3 fat     8665 bx defN 17-Apr-12 11:42 mysql/mysql/func.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/func.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/func.MYI
-rw----     6.3 fat       35 bx defN 17-Apr-12 11:42 mysql/mysql/general_log.CSM
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/general_log.CSV
-rw----     6.3 fat     8776 bx defN 17-Apr-12 11:42 mysql/mysql/general_log.frm
-rw----     6.3 fat     8700 bx defN 17-Apr-12 11:42 mysql/mysql/help_category.frm
-rw----     6.3 fat     1120 bx defN 17-Apr-12 11:42 mysql/mysql/help_category.MYD
-rw----     6.3 fat     3072 bx defN 17-Apr-12 11:42 mysql/mysql/help_category.MYI
-rw----     6.3 fat     8612 bx defN 17-Apr-12 11:42 mysql/mysql/help_keyword.frm
-rw----     6.3 fat   105001 bx defN 17-Apr-12 11:42 mysql/mysql/help_keyword.MYD
-rw----     6.3 fat    18432 bx defN 17-Apr-12 11:42 mysql/mysql/help_keyword.MYI
-rw----     6.3 fat     8630 bx defN 17-Apr-12 11:42 mysql/mysql/help_relation.frm
-rw----     6.3 fat    10044 bx defN 17-Apr-12 11:42 mysql/mysql/help_relation.MYD
-rw----     6.3 fat    20480 bx defN 17-Apr-12 11:42 mysql/mysql/help_relation.MYI
-rw----     6.3 fat     8770 bx defN 17-Apr-12 11:42 mysql/mysql/help_topic.frm
-rw----     6.3 fat   487524 bx defN 17-Apr-12 11:42 mysql/mysql/help_topic.MYD
-rw----     6.3 fat    19456 bx defN 17-Apr-12 11:42 mysql/mysql/help_topic.MYI
-rw----     6.3 fat     9510 bx defN 17-Apr-12 11:42 mysql/mysql/host.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/host.MYD
-rw----     6.3 fat     2048 bx defN 17-Apr-12 11:42 mysql/mysql/host.MYI
-rw----     6.3 fat     8778 bx defN 17-Apr-12 11:42 mysql/mysql/ndb_binlog_index.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/ndb_binlog_index.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/ndb_binlog_index.MYI
-rw----     6.3 fat     8586 bx defN 17-Apr-12 11:42 mysql/mysql/plugin.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/plugin.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/plugin.MYI
-rw----     6.3 fat     9996 bx defN 17-Apr-12 11:42 mysql/mysql/proc.frm
-rw----     6.3 fat      844 bx defN 17-Apr-12 11:42 mysql/mysql/proc.MYD
-rw----     6.3 fat     4096 bx defN 17-Apr-12 11:42 mysql/mysql/proc.MYI
-rw----     6.3 fat     8875 bx defN 17-Apr-12 11:42 mysql/mysql/procs_priv.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/procs_priv.MYD
-rw----     6.3 fat     4096 bx defN 17-Apr-12 11:42 mysql/mysql/procs_priv.MYI
-rw----     6.3 fat     8800 bx defN 17-Apr-12 11:42 mysql/mysql/proxies_priv.frm
-rw----     6.3 fat     1386 bx defN 17-Apr-12 11:42 mysql/mysql/proxies_priv.MYD
-rw----     6.3 fat     5120 bx defN 17-Apr-12 11:42 mysql/mysql/proxies_priv.MYI
-rw----     6.3 fat     8838 bx defN 17-Apr-12 11:42 mysql/mysql/servers.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/servers.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/servers.MYI
-rw----     6.3 fat       35 bx defN 17-Apr-12 11:42 mysql/mysql/slow_log.CSM
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/slow_log.CSV
-rw----     6.3 fat     8976 bx defN 17-Apr-12 11:42 mysql/mysql/slow_log.frm
-rw----     6.3 fat     8955 bx defN 17-Apr-12 11:42 mysql/mysql/tables_priv.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/tables_priv.MYD
-rw----     6.3 fat     4096 bx defN 17-Apr-12 11:42 mysql/mysql/tables_priv.MYI
-rw----     6.3 fat     8636 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone.MYI
```

```
-rw----     6.3 fat     8624 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_leap_second.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_leap_second.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_leap_second.MYI
-rw----     6.3 fat     8606 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_name.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_name.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_name.MYI
-rw----     6.3 fat     8686 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_transition.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_transition.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_transition.MYI
-rw----     6.3 fat     8748 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_transition_type.frm
-rw----     6.3 fat        0 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_transition_type.MYD
-rw----     6.3 fat     1024 bx defN 17-Apr-12 11:42 mysql/mysql/time_zone_transition_type.MYI
-rw----     6.3 fat    10630 bx defN 17-Apr-12 11:42 mysql/mysql/user.frm
-rw----     6.3 fat      320 bx defN 17-Apr-12 11:42 mysql/mysql/user.MYD
-rw----     6.3 fat     2048 bx defN 17-Apr-12 11:42 mysql/mysql/user.MYI
-rw----     6.3 fat        6 bx defN 17-Apr-12 11:42 mysql/mysql_upgrade_info
drwx---     6.3 fat        0 bx stor 17-Apr-12 13:37 mysql/performance_schema/
-rw----     6.3 fat     8624 bx defN 17-Apr-12 11:42 mysql/performance_schema/cond_instances.frm
-rw----     6.3 fat       61 bx defN 17-Apr-12 11:42 mysql/performance_schema/db.opt
-rw----     6.3 fat     9220 bx defN 17-Apr-12 11:42 mysql/performance_schema/events_waits_current.frm
-rw----     6.3 fat     9220 bx defN 17-Apr-12 11:42 mysql/performance_schema/events_waits_history.frm
-rw----     6.3 fat     9220 bx defN 17-Apr-12 11:42 mysql/performance_schema/events_waits_history_long.frm
-rw----     6.3 fat     8878 bx defN 17-Apr-12 11:42 mysql/performance_schema/events_waits_summary_by_instance.frm
-rw----     6.3 fat     8854 bx defN 17-Apr-12 11:42 mysql/performance_schema/events_waits_summary_by_thread_by_event_name.frm
-rw----     6.3 fat     8814 bx defN 17-Apr-12 11:42 mysql/performance_schema/events_waits_summary_global_by_event_name.frm
-rw----     6.3 fat     8654 bx defN 17-Apr-12 11:42 mysql/performance_schema/file_instances.frm
-rw----     6.3 fat     8800 bx defN 17-Apr-12 11:42 mysql/performance_schema/file_summary_by_event_name.frm
-rw----     6.3 fat     8840 bx defN 17-Apr-12 11:42 mysql/performance_schema/file_summary_by_instance.frm
-rw----     6.3 fat     8684 bx defN 17-Apr-12 11:42 mysql/performance_schema/mutex_instances.frm
-rw----     6.3 fat     8776 bx defN 17-Apr-12 11:42 mysql/performance_schema/performance_timers.frm
-rw----     6.3 fat     8758 bx defN 17-Apr-12 11:42 mysql/performance_schema/rwlock_instances.frm
-rw----     6.3 fat     8605 bx defN 17-Apr-12 11:42 mysql/performance_schema/setup_consumers.frm
-rw----     6.3 fat     8637 bx defN 17-Apr-12 11:42 mysql/performance_schema/setup_instruments.frm
-rw----     6.3 fat     8650 bx defN 17-Apr-12 11:42 mysql/performance_schema/setup_timers.frm
-rw----     6.3 fat     8650 bx defN 17-Apr-12 11:42 mysql/performance_schema/threads.frm
-rw----     6.3 fat     1688 bx defN 17-Apr-12 11:40 structure.sql
99 files, 30434450 bytes uncompressed, 597772 bytes compressed:  98.0%
```


由题意推测，需要还原数据库，推测应该有.bak文件，但是附件中没有

用strings命令查看.sql文件，没什么有效信息

```
┌──(root💀kali)-[ ]
└─# strings structure.sql
-- MySQL dump 10.13  Distrib 5.5.54, for debian-linux-gnu (i686)
--  Host: localhost    Database: ctf
-- ------------------------------------------------------
-- Server version       5.5.54-0+deb8u1
/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;
-- Table structure for table `user`
/*!40101 SET @saved_cs_client     = @@character_set_client */;
/*!40101 SET character_set_client = utf8 */;
CREATE TABLE `user` (
  `id` smallint(5) unsigned NOT NULL AUTO_INCREMENT,
  `name` varchar(10) NOT NULL,
  `password` varchar(32) NOT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB AUTO_INCREMENT=5 DEFAULT CHARSET=utf8;
/*!40101 SET character_set_client = @saved_cs_client */;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;
/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;
-- Dump completed on 2017-04-12 11:39:32
```


挨个strings先看看

在ib_logfile0和ibdata1均发现flag子串

“.flag”后面字符串即为正确flag