



### **OBJECTIVE**

- Identify MySQL security issues
- Improve MySQL installation process
- Identify data issues
- Improve data integrity and security
- Auditing options

**EffectiveMySQL.com** - Its all about **Performance** and **Scalability** 

### ABOUT AUTHOR RONALD BRADFORD

- I2 years with MySQL / 22 years with RDBMS
  - Senior Consultant at MySQL Inc (06-08)
  - Consultant for Oracle Corporation (96-99)
- 7 years presenting MySQL content
- All time top MySQL blogger
- Published author
- Oracle ACE Director

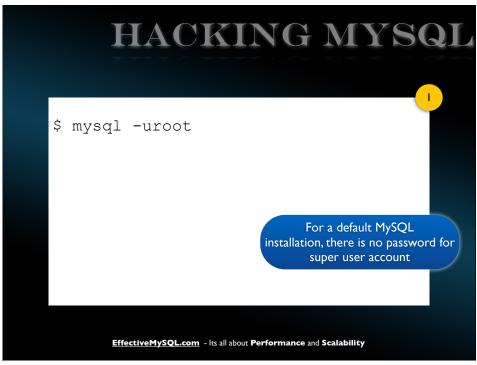
Available NOW for consulting

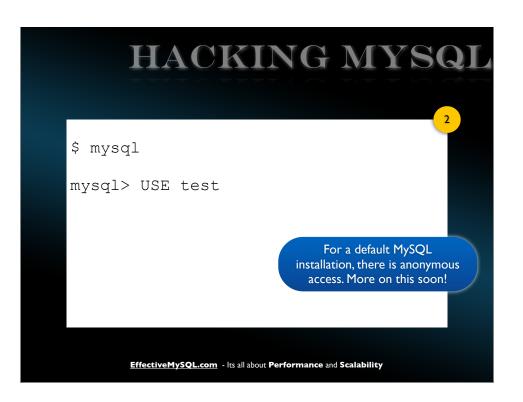
http://RonaldBradford.com

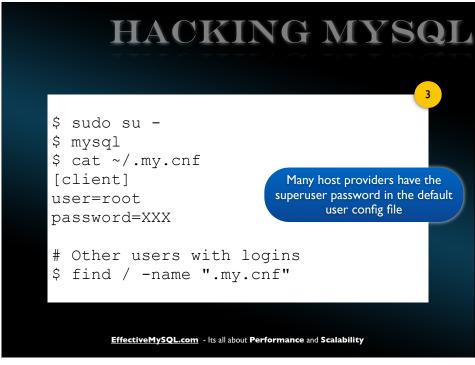




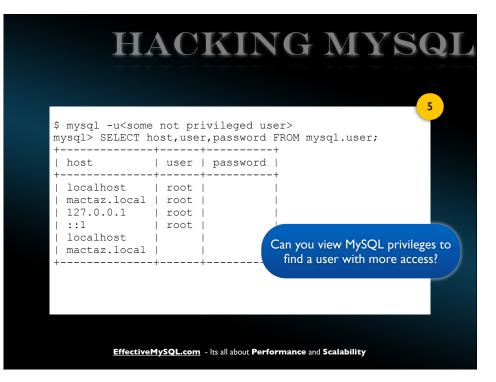








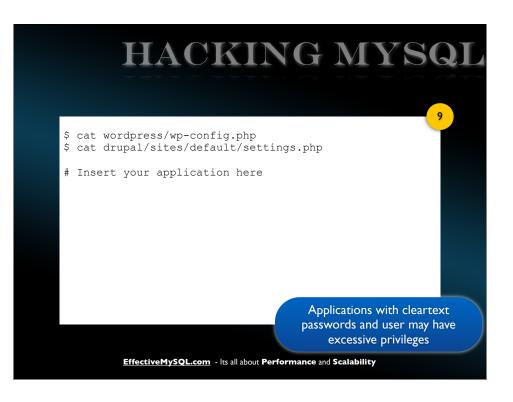


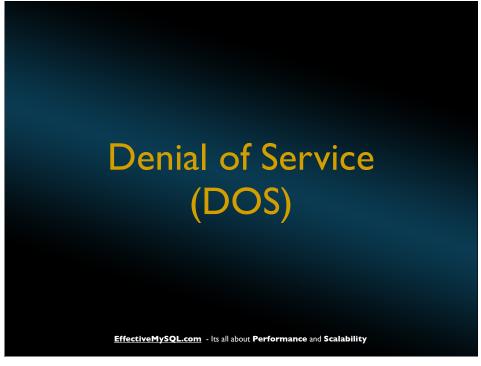


```
HACKING MYSQL
$ cd [mysql-data-dir] # e.g. /var/lib/mysql
$ cat master.info
mysql-bin.001536
20160154
10.0.0.1
repl
XXX
3306
60
$ mysql -urepl -pXXX -h10.0.0.1
mysql> SHOW GRANTS;
                                  Are datadir permissions secure?
                               Does replication connection have global
                                          permissions?
         EffectiveMySQL.com - Its all about Performance and Scalability
```

### HACKING MYSQL mysql> CREATE SCHEMA IF NOT EXISTS hack; mysql> use hack; mysql> CREATE TABLE words (word VARCHAR(100)); mysql> LOAD DATA LOCAL INFILE '/tmp/passwords' -> INTO TABLE words (word); mysql -uroot -e "SELECT word, PASSWORD (word) FROM hack.words" --skip-column-names > /tmp/mysql-passwords \$ cat /tmp/mysql-passwords password \*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 passwd \*59C70DA2F3E3A5BDF46B68F5C8B8F25762BCCEF0 \*2447D497B9A6A15F2776055CB2D1E9F86758182F changeme \*7ACE763ED393514FE0C162B93996ECD195FFC4F5 \*3D56A309CD04FA2EEF181462E59011F075C89548 Brute force checking











```
# Force disk I/O
mysql> SET SESSION tmp_table_size=1024*4; # 4K
mysql> SELECT ...
```







```
DATA SECURITY
  $ ls -ld /var/lib/mysql
drwxr-xr-x 6 mysql mysql 4096 Oct 13 16:45 /var/lib/mysql
$ ls -l /var/lib/mysql
total 3749488
drwx----- 2 mysql mysql
                             4096 Oct 6 18:50 db1
drwx----- 2 mysgl mysgl
                           4096 Jun 6 14:11 db2
-rw-rw---- 1 mysql mysql 3298820096 Oct 16 20:42 ibdata1
-rw-rw---- 1 mysql mysql 268435456 Oct 16 20:42 ib logfile0
-rw-rw--- 1 mysql mysql 268435456 Oct 16 20:42 ib logfile1
drwx----- 2 mysql mysql
                            4096 Jun 6 09:37 mysql
srwxrwxrwx 1 mysql mysql
                               0 Oct 12 20:09 mysql.sock
                                       Change default configuration for
                                      socket=/var/run/mysql/mysql.sock
          EffectiveMySQL.com - Its all about Performance and Scalability
```



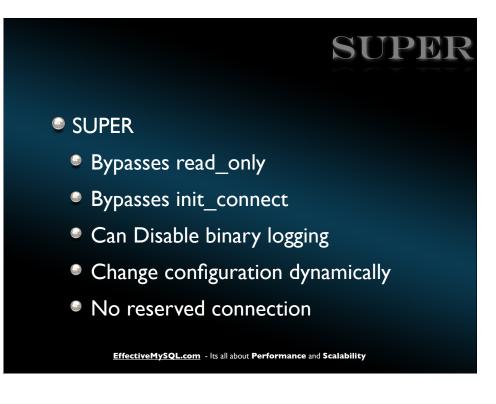


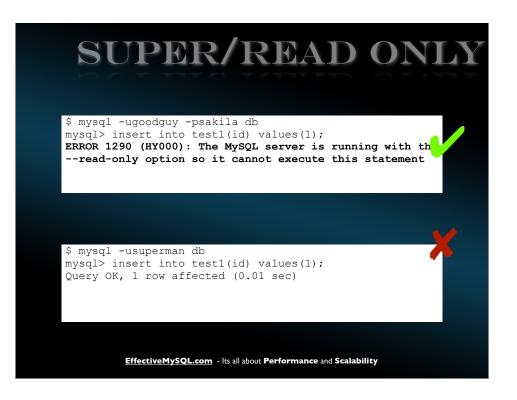
# MySQL listens on one TCP/IP port Default port is 3306 --skip-networking disables TCP/IP Database does not require physical web access generally Firewall management

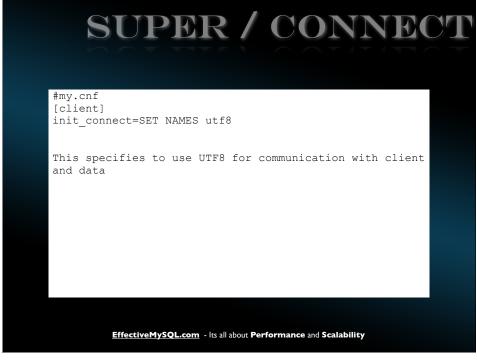


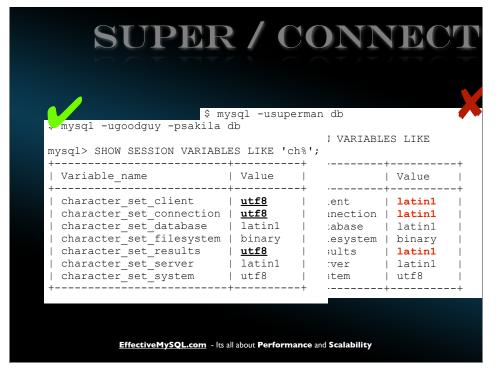


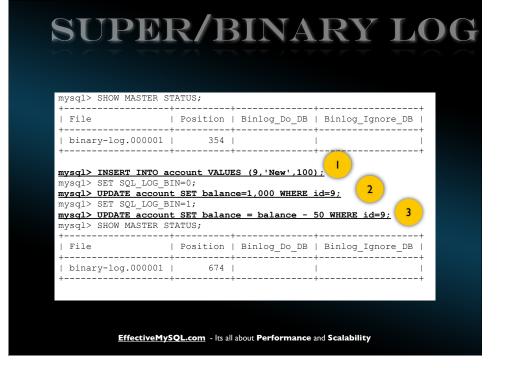




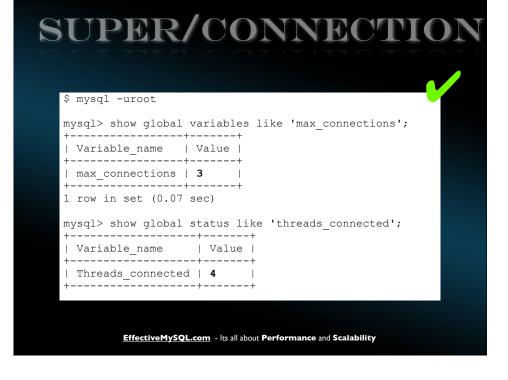


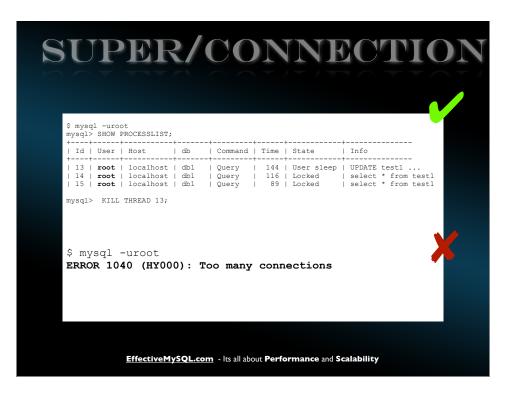


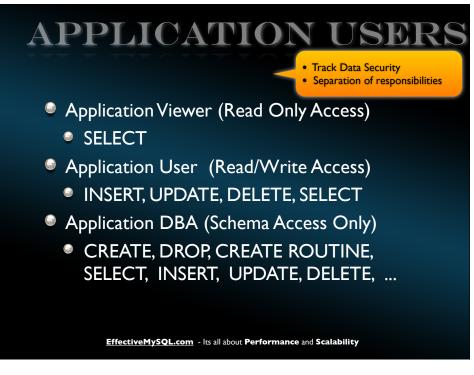




```
SUPER / BINARY LOG
     $ mysqlbinlog binary-log.000001 --start-position=354 --stop-position=674
     #100604 18:00:08 server id 1 end log pos 450 Query thread_id=1 exec_time=0
     error code=0
     use \overline{\text{mysql}}/*!*/;
     SET TIMESTAMP=1275688808/*!*/;
     INSERT INTO account VALUES (9,'New',100);
     #100604 18:04:31 server id 1 end log pos 674 Query thread id=2 exec time=
     error code=0
     use mysql/*!*/;
     SET TIMESTAMP=1275689071/*!*/;
     mysql> UPDATE balance SET balance = balance - 50 WHERE id=9;
     DELIMITER ;
     # End of log file
     ROLLBACK /* added by mysqlbinlog */;
                EffectiveMySQL.com - Its all about Performance and Scalability
```



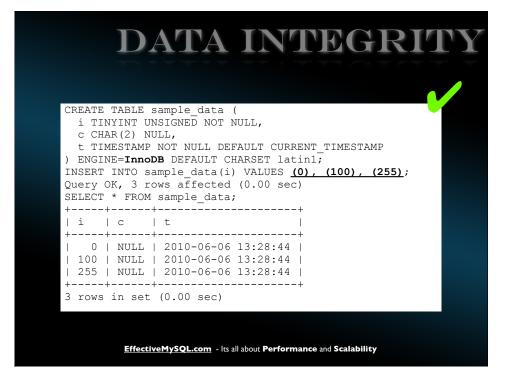


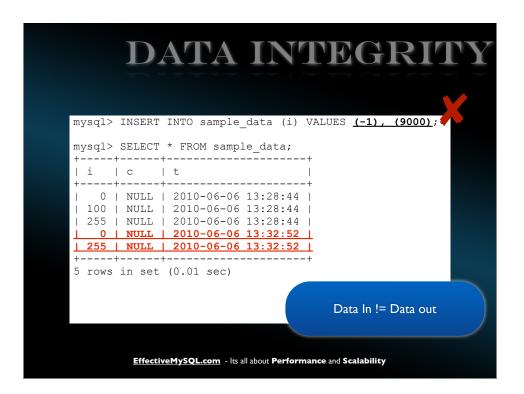
















# Current version is 5.5 http://dev.mysql.com/downloads/ RedHat current version is 5.0.77 - 28 JAN 2009 Ubuntu version is 5.1.44 - 04 FEB 2010

### **UPDATES**

- MySQL is open source
  - More frequent updates
  - MySQL enterprise monthly updates
  - MySQL community ~ 6 months updates
- Release notes

http://dev.mysql.com/doc/refman/5.5/en/news-5-5-x.html

EffectiveMySQL.com - Its all about Performance and Scalability

### INSTALLATION

- MySQL 5.5 via distro
  - Oracle has no yum repository
    - No immediate plans for community
  - Canonical (Ubuntu) has no ETA

EffectiveMySQL.com - Its all about Performance and Scalability

### INSTALLATION

- Recommendations
  - Use MySQL created rpms
  - Use MySQL Tar Binary
- Issues
  - Dependencies
    - PHP/Perl etc

**EffectiveMySQL.com** - Its all about **Performance** and **Scalability** 

### Auditing

### AUDITING OPTIONS Status variables Binary log Schema compare Audit plugin (5.5) Oracle Audit Vault

### STATUS VARIABLES mysql> SELECT variable name, variable value -> FROM INFORMATION SCHEMA.GLOBAL STATUS -> WHERE variable name LIKE 'COM ALTER%' -> OR variable name LIKE 'COM DROP%' -> OR variable name LIKE 'COM CREATE%'; | variable value | variable name COM ALTER DB COM ALTER DB UPGRADE | 0 COM ALTER EVENT | 0 COM ALTER FUNCTION | 0 COM ALTER PROCEDURE | 0 COM ALTER SERVER COM ALTER TABLE | 4 COM ALTER TABLESPACE | 0 EffectiveMySQL.com - Its all about Performance and Scalability

### BINARY LOG

```
$ mysqlbinlog /path/to/file > binlog.txt
$ grep -ie ALTER -e CREATE -e DROP binlog.txt

ALTER TABLE example ADD COLUMN i INT;
ALTER TABLE example ADD INDEX (i);
ALTER TABLE example DROP INDEX y;
ALTER TABLE example DROP COLUMN y;
```

**EffectiveMySQL.com** - Its all about **Performance** and **Scalability** 

EffectiveMySQL.com - Its all about Performance and Scalability

### SCHEMA

```
$ mysqldump -uroot -p \
    --no-data --all-databases --skip-dump-date \
    | sed -e "s/AUTO_INCREMENT=[^\ ] //"
    > schema.`date +%Y%m%d.%H%M`sql

# Compare with a previous version
$ diff schema.20111018.sql schema.20111017.sql
```





### CONCLUSION

- MySQL is not secure by default
  - Responsibility on you (DBA/SA)
- Starts with OS security
- Use appropriate privileges

**EffectiveMySQL.com** - Its all about **Performance** and **Scalability** 

### NOT COVERED

- Replication
- SSL
- Backups
- SQL Injection
  - Sanitize your database inputs

http://xkcd.com/327/









