8 Simple Rules to Design Secure Apps with MySQL

Augusto Bott
Team Lead
bott@pythian.com

Nick Westerlund
Senior DBA
westerlund@pythian.com

The Pythian Group

- 80+ DBAs
- Highly distributed
- 24x7 Coverage
- Scopeless Model

- Services:
  - Oracle
  - SQL Server
  - MySQL
  - SA services

The Pythian Group

- Offices in:
  - Ottawa, Canada (HQ North America)
  - Prague, Czech Republic (HQ EMEA)
  - Boston, USA
  - Sydney, Australia (HQ Asia, Pacific)
  - Hyderabad, India

The Pythian Group

- Satellite locations:
  - Toronto, Montreal, Kitchener-Waterloo, and Sherbrooke, Canada
  - Seattle, Manitowoc and Madison, USA
  - Paris, France
  - Mellieha, Malta
  - Kiev, Ukraine
  - Cairo, Egypt
  - Capetown, South Africa
  - Porto Alegre, Brazil

Who we are

- DBAs
- Paranoid Architects

- Design so it does not need patching
- Don't patch around something

- This is based on our observations
  - people break even the most basic rules, daily

Why we're doing this

- Apps get visibility
- DBs grow

- Your App becomes a target
- Data gets interesting to be owned
- You're in trouble

The basic Rules

- Don't trust anything that comes from outside the Firewall
- Use and abuse of stored procedures and views
- Isolate raw data from the App user
- Make sure you have proper credentials management
- Do not send data in plain text (ever!)
- Do not store passwords anywhere
- Make sure your application is Auditable
- Make sure it's recoverable

Outside the Firewall

- Your enemy is outside of the firewall
- But might be inside already
- Double-check and validate everything
- Sanitize your data
- Prevent execution privileges

Filesystem privileges

```
user@server:~$ cd www
user@server:~/www$ ls -lad .
drwxr-x--- 2 www web 4096 2009-06-25 11:35 .
user@server:~/www$ ls -la
total 8
drwxr-xr-x  2 www web 4096 2009-06-25 11:36 .
drwxr-xr-x 44 www web 4096 2009-06-25 11:35 ..
-rw-r--r--  1 www web    0 2009-06-25 11:36 index.html
-rw-r--r--  1 www web    0 2009-06-25 11:36 index.php
user@server:~/www$
```

Filesystem privileges (2)

- Where you write, you don't read or execute
- Where you read, you don't write
- Where execute, you don't write (and avoid read)

(Ab)use Stored Procedures

- Mask your data
- add_to_cart(session_id, product_id, qty)
- see_cart_content(session_id)
- ! SELECT * FROM cart;

Isolate Raw Data

```
mysql> CREATE DEFINER='root'@'localhost' SQL SECURITY
DEFINER VIEW t3 AS SELECT a FROM t1 WHERE b = 5 AND
active=1;
Query OK, 0 rows affected (0.42 sec)
mysql> GRANT SELECT (a) ON example.t3 to 'app'@'172.16.1.%'
identified by 'secret';
Query OK, 0 rows affected (0.04 sec)
```

Credentials Management

- users != app users
- Passwords
  - Change regularly
  - Make them complex
    - PCI compliance
- Minimal Privileges
- Restrict Access

Credentials Management (2)

What is wrong with this?

```
user@server:~$ mysql -uroot
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 35
Server version: 5.1.31-1ubuntu2 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Credentials Management (3)

```
mysql> DELETE FROM mysql.user WHERE user='' OR host='';
Query OK, 0 rows affected (0.00 sec)

mysql> DELETE FROM mysql.db WHERE user='' OR host='';
Query OK, 0 rows affected (0.01 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql>
```

Don't send plain-text data

- Encrypt everything
  - Use asymmetrical encryption
    - App has public key
    - Accounting has the private key
- Privacy should be considered
- Use certificates
- Do not store plain-text sensitive data

Don't store passwords

- Use an application server

- Do not store plain text passwords on the filesystem
  - Decrypt them on-the-fly
  - Decrypt them on startup and keep in RAM

Audit?

- Logging
- Split historical data
  - Off-load production
  - OLAP, BI, DW
- Keep track of who did what
- Record every single access to the system

Make sure you can recover

- Backups
- Replication
- Use a DR site
- Be able to retrace all the steps, if needed

Questions?

bott@pythian.com

westerlund@pythian.com

http://www.sans.org/top25errors/?cat=top25

http://www.pythian.com/news/

http://www.pythian.com/about/careers.php