MySQL Security: More Than Just ACL's

http://bit.ly/KX8sVM

Sheeri Cabral

Senior DB Admin/Architect, Mozilla

@sheeri www.sheeri.com

General Security

- Patching
- Prevent access
- Prevent meaningful info gathering

Access

- Network access
- Direct db access
- Access to backups
- OS access – data, logs

Encryption

SSL is per-client

Unencrypted MySQL data streams can be seen with tcpdump

Access Points

- Who can login?
  - Network, seeing traffic
    - http://forge.mysql.com/snippets/view.php?id=15

```
shell> tcpdump -l -i eth0 -w -src or dst
  port 3306 | strings
```

Operating System

- Authentication
- Firewall
- Other installed programs

OS Files and Permissions

- mysql server user
- mysql server files & logs
- Passwords on commandline

Securing your Application

- Authentication
- Config files – gazzang.com
- User-entered data
  - SQL injection

Who has access?

- pt-show-grants
- SELECT user, host, password, ssl_type FROM mysql.user

WHERE Super_priv='Y'

or

WHERE user=''

Where is the access from?

- %
- %.company.com
- 10.0.% or 192.168.%

GRANTing Access

```
GRANT priv_type [(column_list)] [, priv_type [(column_list)]] ...
    ON [object_type]
        {tbl_name | * | *.* | db_name.* | db_name.routine_name}
    TO user [IDENTIFIED BY [PASSWORD] 'password']
    [REQUIRE        NONE |      [{SSL| X509}]
   [CIPHER 'cipher' [AND]]       [ISSUER 'issuer' [AND]]
        [SUBJECT 'subject']]   [WITH with_option [with_option] …]
```

http://dev.mysql.com/doc/refman/5.5/en/grant.html

Other ACL's

- Object access
- Password policies
- Roles

Access from...?

- localhost only, --skip-networking
- firewall
- Who can [attempt to] DOS you?

Test Database

- Anyone can access it
- Stuff with data
- Starts with “test”

ACLs – to do what?

- --local-infile=0
- GRANT
  - MAX_QUERIES_PER_HOUR
  - MAX_UPDATES_PER_HOUR
  - MAX_CONNECTIONS_PER_HOUR

Changing ACLs

- Who changes ACLs?
- How are ACL changes audited?
- When do ACL changes happen?

Securich

- Darren Cassar, http://www.securich.com/
- Create/drop roles

```
call create_update_role('add','role1','select');
```

Create users with roles, adding objects

Drop users, revoke privileges

```
call grant_privileges('username','hostname', 'databasename',
'tablename','tabletype','rolename', 'email');
```

```
call grant_privileges('john','machine.domain.com',
 'employees', '','alltables','role1', 'john@domain.com');
```

Securich

- Block users
- Rename users
- Clone users
- Reconciliation

Server Options

- --bind-address
- --skip-name-resolve

How Does Your Data Flow?

- Where is data encrypted?
- Where do errors go?
  - Are those logs checked?
- Where does the traffic flow?

Separating Admin Apps

- Same data, different interface
- Performance, e.g. reporting
- Only allowed from VPN?
  - Public vs. easily accessible

Plaintext information

- Passwords
- Credit card info
- Identification numbers (e.g. SSN in USA)

Hashes

- Passwords

*2470C0C06DEE42FD1618BB99005ADCA2EC9D1E19 = 'password'

*13824B0ECE00B527531D2C716AD36C23AC11A30B

SQL Injection

- http://bit.ly/kscope_sqlinject

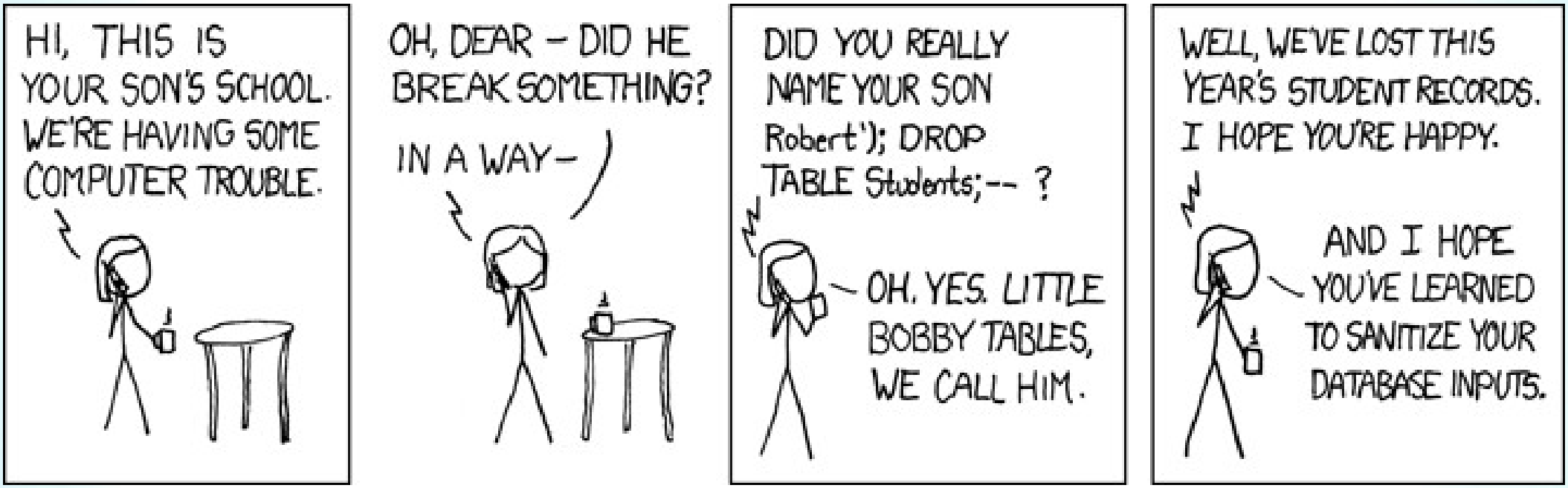
```
SELECT count(*) FROM users WHERE
   username='$user' and pass='$pass';

-- if count(*)>0, log in!
```

- Pass: hi' or 1=1

```
SELECT count(*) FROM users WHERE
  username='foo' and pass='hi' or 1=1';
```

What + How


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR - DID HE BREAK SOMETHING?
IN A WAY-
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

A Real Example

scabral$ curl --head www.reddit.com

HTTP/1.1 200 OK

Content-Type: text/html; charset=UTF-8

Set-Cookie: reddit_first=%7B%22organic_pos%22%3A%201%2C
%20%22firsttime%22%3A%20%22first%22%7D;
Domain=reddit.com; expires=Thu, 31 Dec 2037 23:59:59 GMT;
Path=/

Server: '; DROP TABLE servertypes; --

Date: Sat, 12 May 2012 13:54:20 GMT

Connection: keep-alive

What Should be Sanitized

- ; \g \G ' “ UNION
- HTML encoding
- NULL or char(0)

Sanitizing Data

- Save yourself time
- Prevent buffer overflows
- Plenty of libraries to help you

Prepared Statements

```
PREPARE stmt1 FROM 'SELECT uname FROM
   UserAuth WHERE uname=? and pass=?';

SET @a = "sheeri";  SET @b = md5("mypassword");

EXECUTE stmt1 USING @a, @b;
```

Stored Code

- Stored procedures / functions
- Views
- Events
  - Instead of cron

Auditing and Monitoring

- Prevention is one part of security

- Auditing - review and assess security

MacAfee (3/2012)

  - https://github.com/mcafee/mysql-audit

- Monitoring – alerting of security issues

Auditing and Monitoring

- General log to see all login attempts
- Locking out accounts with max_connect_errrors
  - global
  - FLUSH HOSTS

Authentication Plugin

- MySQL 5.5 (since Dec 2010)
- MySQL Enterprise Plugins
  - Windows Authentication
  - PAM Authentication

Creating Policies

- There will be exceptions
  - But it's still a good idea to have the policies!

Questions? Comments?

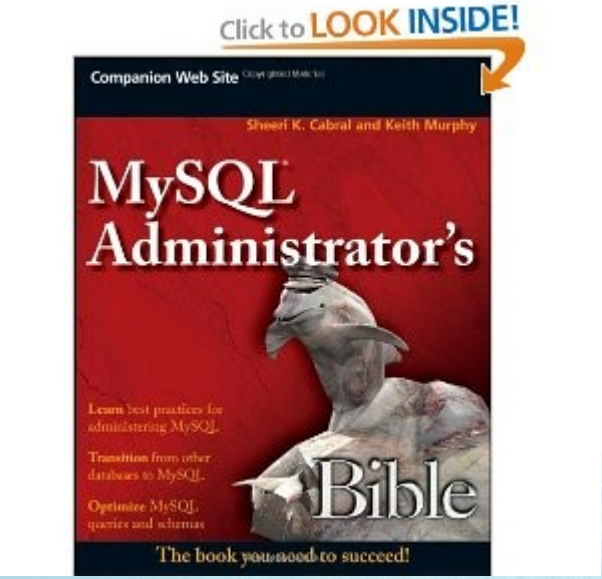
scabral@mozilla.com

@sheeri

www.oursql.com

MySQL Administrator's Bible

- tinyurl.com/mysqlbible



kimtag.com/mysql

planet.mysql.com

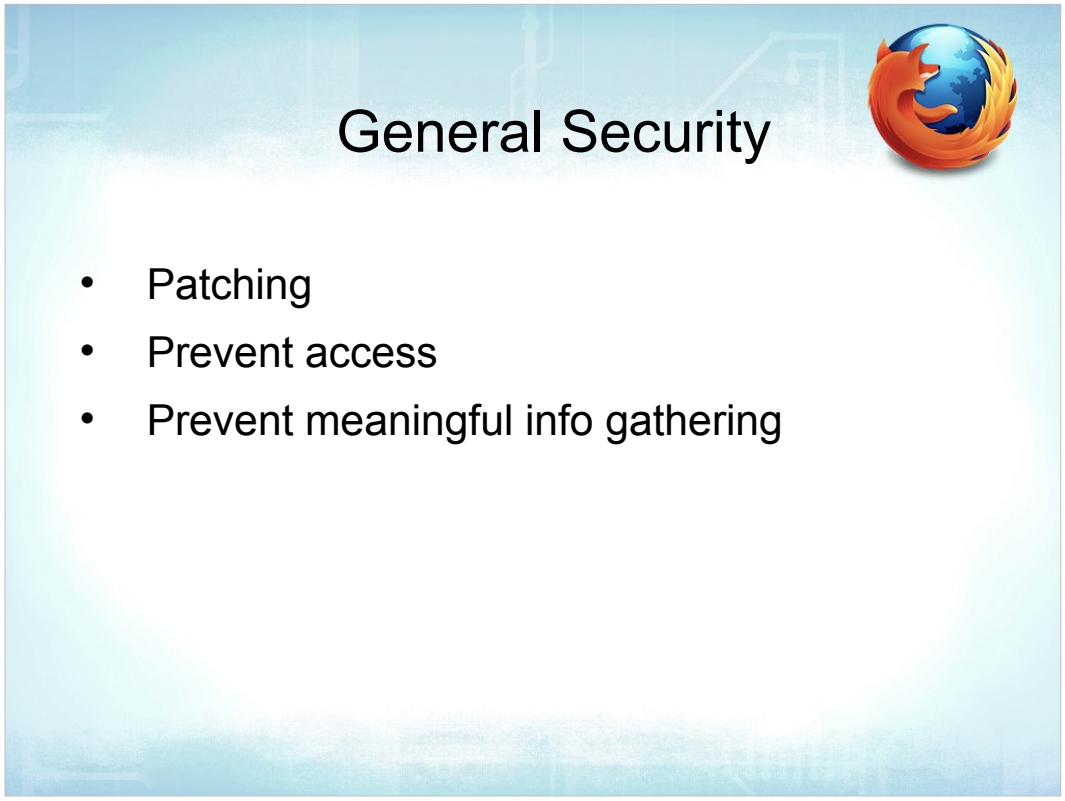
MySQL Security: More Than Just ACL's

http://bit.ly/KX8sVM

Sheeri Cabral

Senior DB Admin/Architect, Mozilla

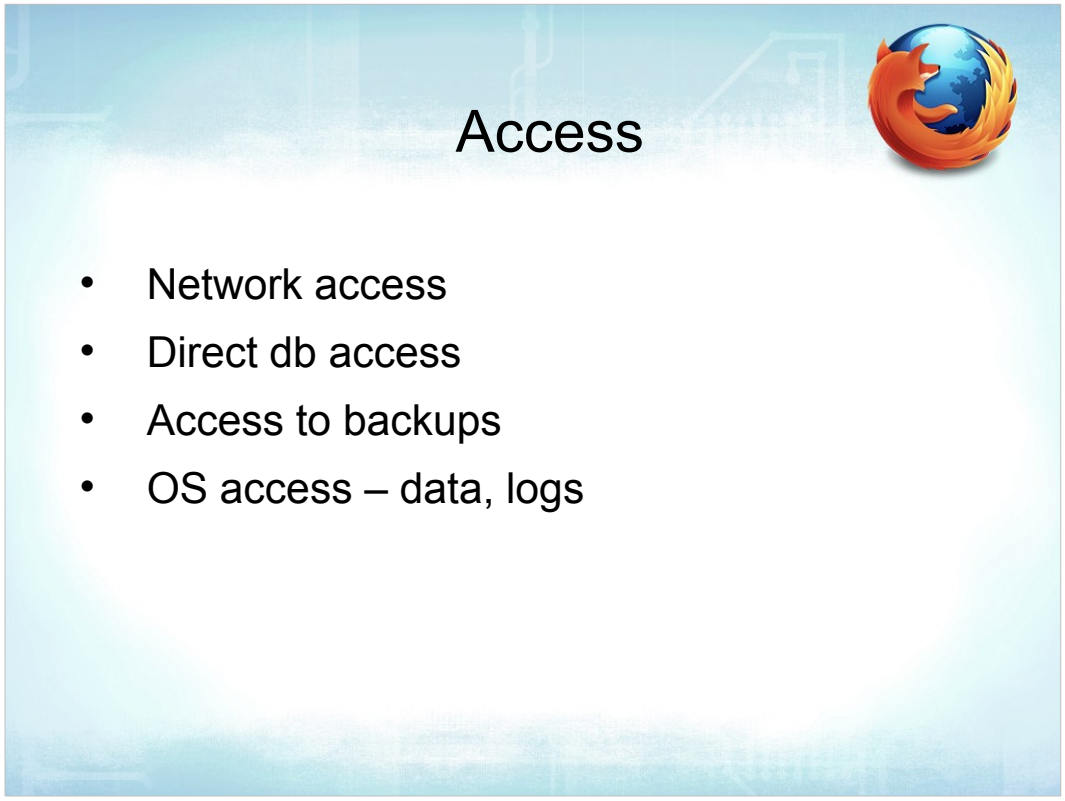
@sheeri www.sheeri.com



MySQL has a new version each month! Can't patch every month, but you should upgrade every 6-12 months.
MySQL 5.1 GA Nov 2008
MySQL 5.5 GA Dec 2010

As for meaningful info gathering, e.g. encryption!

Preventing access includes permissions and ACL's but it's not limited to that



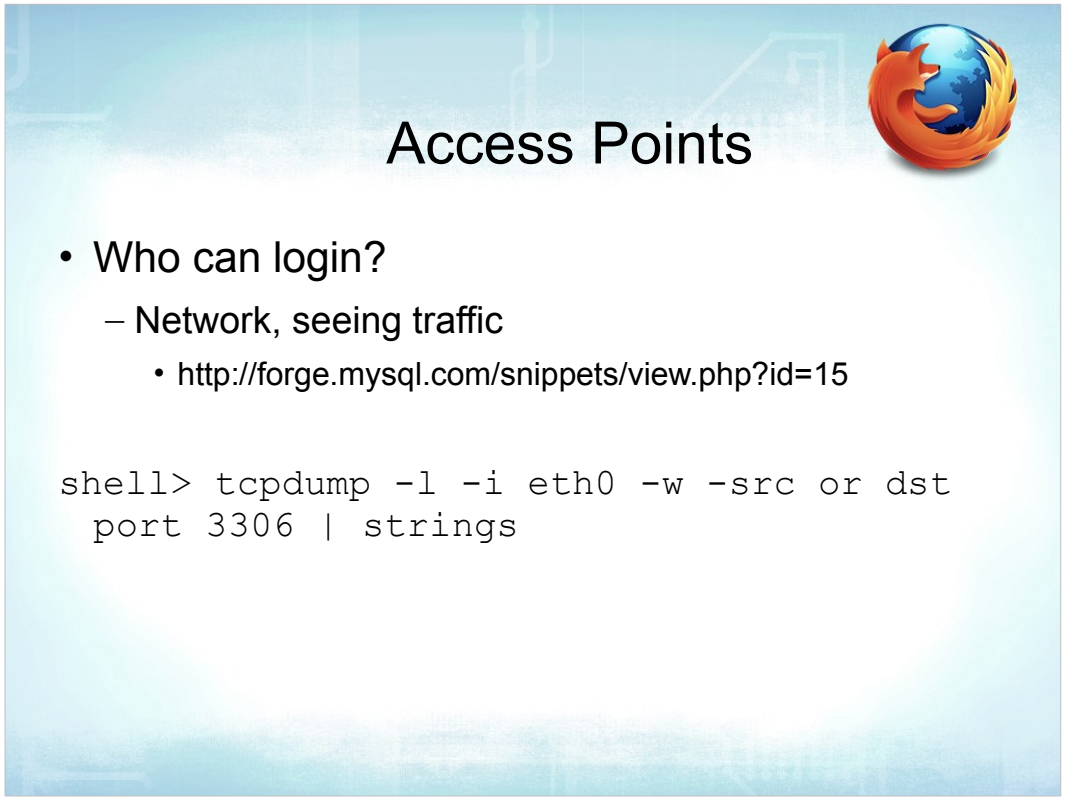
Can someone sniff traffic going across the network? What about replication or backups?

Can anyone try to login to port 3306 with telnet?

Encryption

SSL is per-client

Unencrypted MySQL data streams can be seen with tcpdump

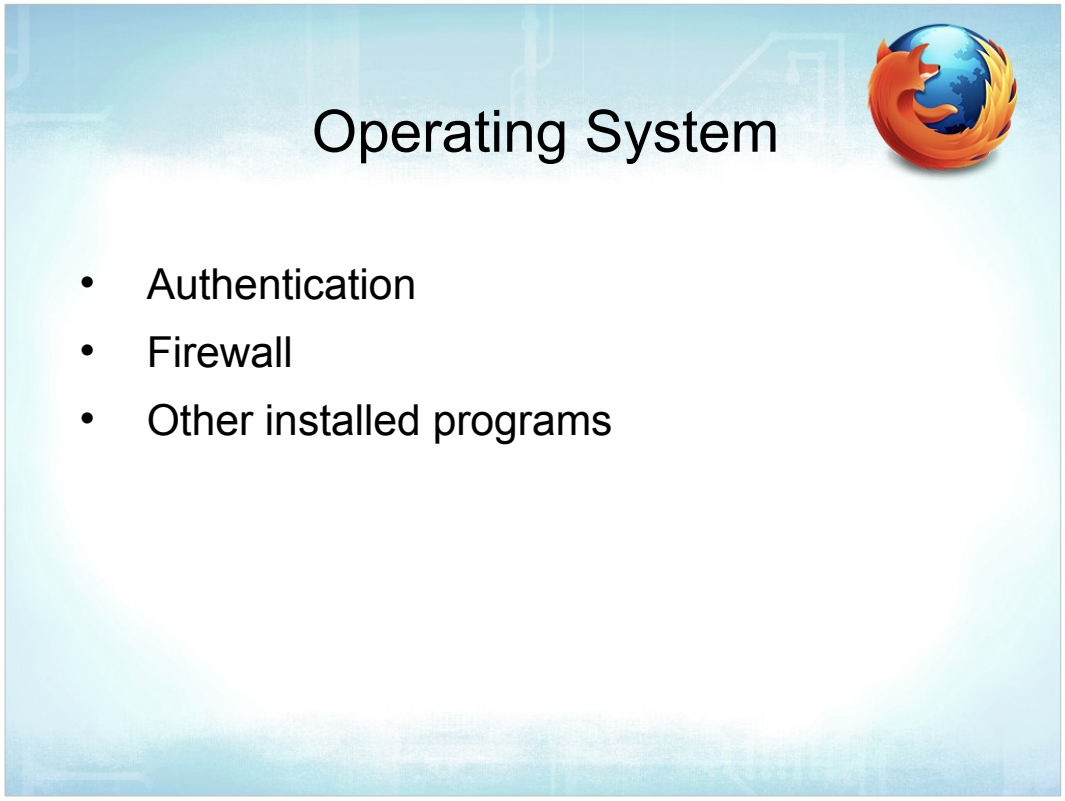


Poor man's query profiler

Who can login to the OS and see the data? Strings on a MyISAM table can get data!

Who can login and read the logs? Slow, binary logs?

Read the backups?

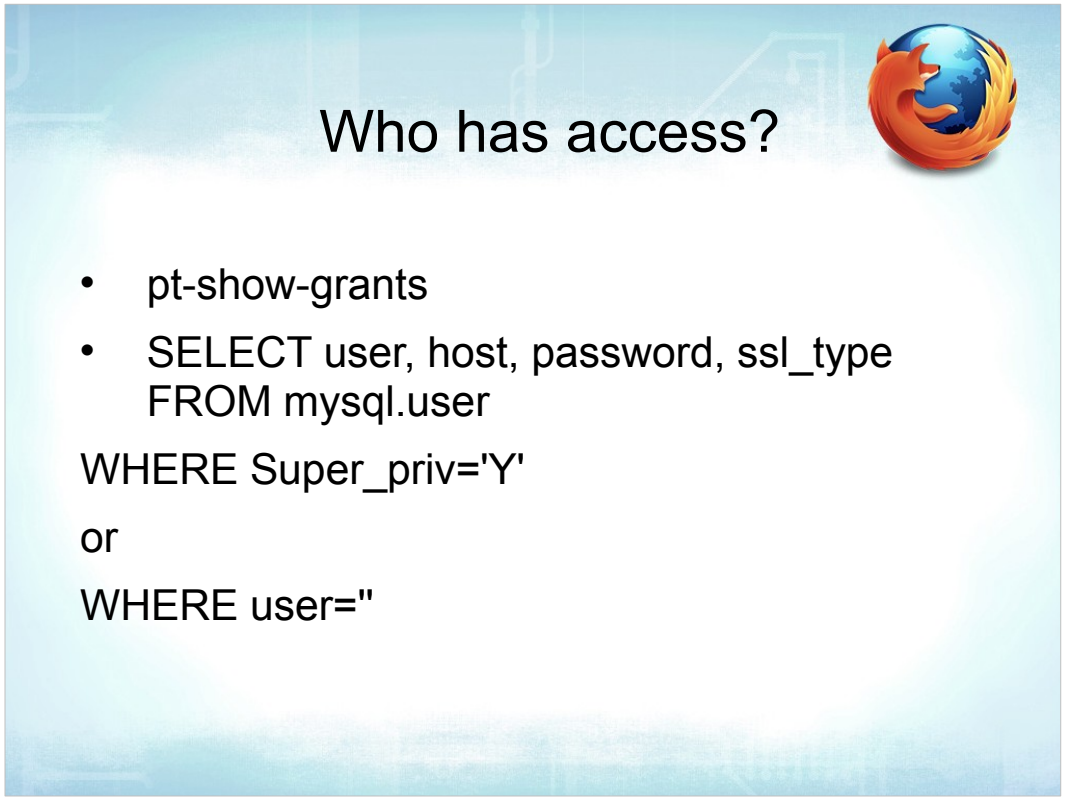


Are there other installed programs that are running on the same user, such as “nobody”? What other people have access due to the other installed programs?

OS Files and Permissions

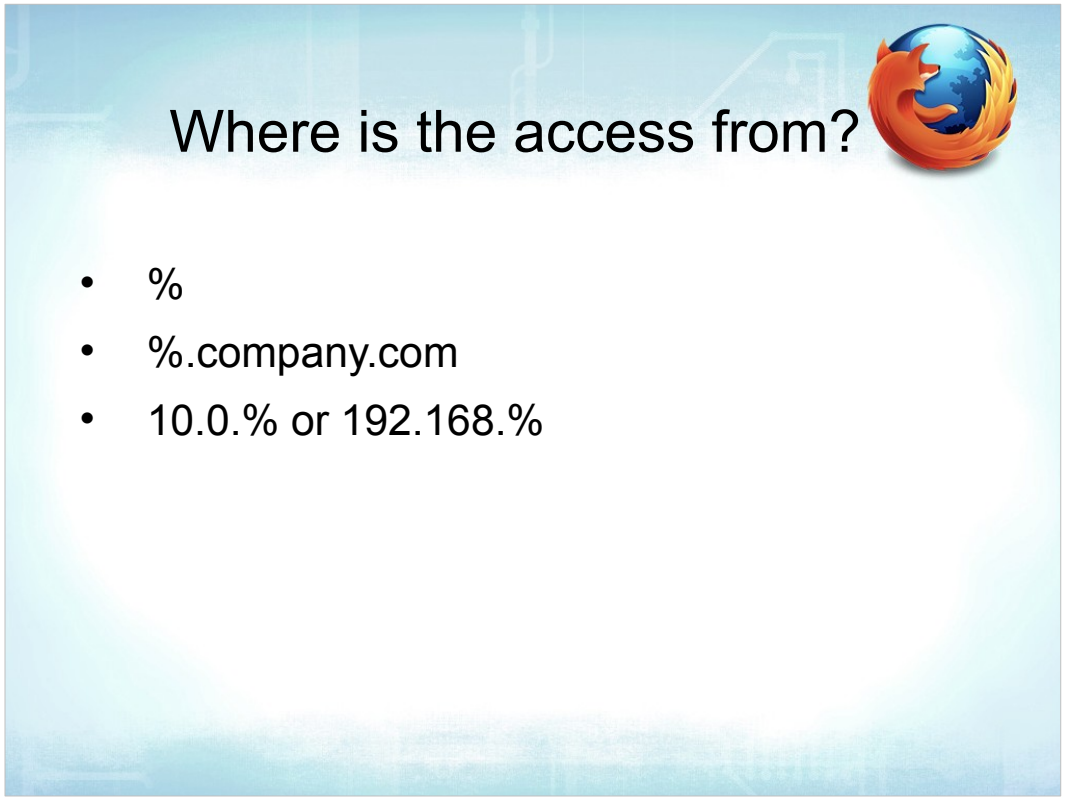
- mysql server user
- mysql server files & logs
- Passwords on commandline

I talk about SQL injection and authentication more in-depth



Ways to see who has access

Super_priv can shutdown with mysqladmin shutdown. Also can write even if db is read_only. Also if max_connections is reached, 1 more user can login but only if they have the super priv.



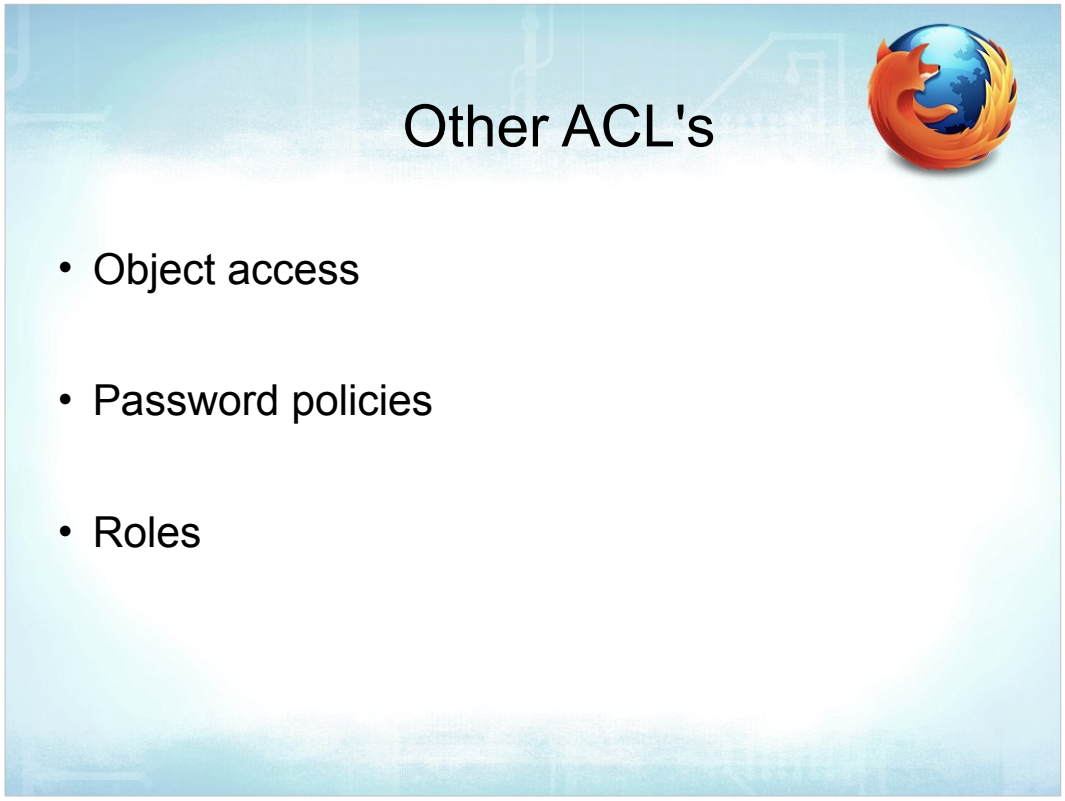
This gets tricky because IP's can be spoofed, and if you're using Amazon EC2 or other cloud solutions (including traditional shared hosting) your IP might change without notice.

GRANTing Access

```
GRANT priv_type [(column_list)] [, priv_type [(column_list)]] ...
    ON [object_type]
        {tbl_name | * | *.* | db_name.* | db_name.routine_name}
    TO user [IDENTIFIED BY [PASSWORD] 'password']
    [REQUIRE        NONE |      [{SSL| X509}]
   [CIPHER 'cipher' [AND]]       [ISSUER 'issuer' [AND]]
        [SUBJECT 'subject']]   [WITH with_option [with_option] …]
```

http://dev.mysql.com/doc/refman/5.5/en/grant.html

priv_type is the most important thing here, show the doc with the charts in it.



Who can acces stored procedures/functions? Views?

You can also allow people to run commands they otherwise wouldn't by using stored procedures/functions, and you can allow them to see partial data by using views – a view definition is a SELECT query, so you can allow people to see certain columns and even certain rows only.

Access from...?

- localhost only, --skip-networking
- firewall
- Who can [attempt to] DOS you?

Test Database

- Anyone can access it
- Stuff with data
- Starts with “test”

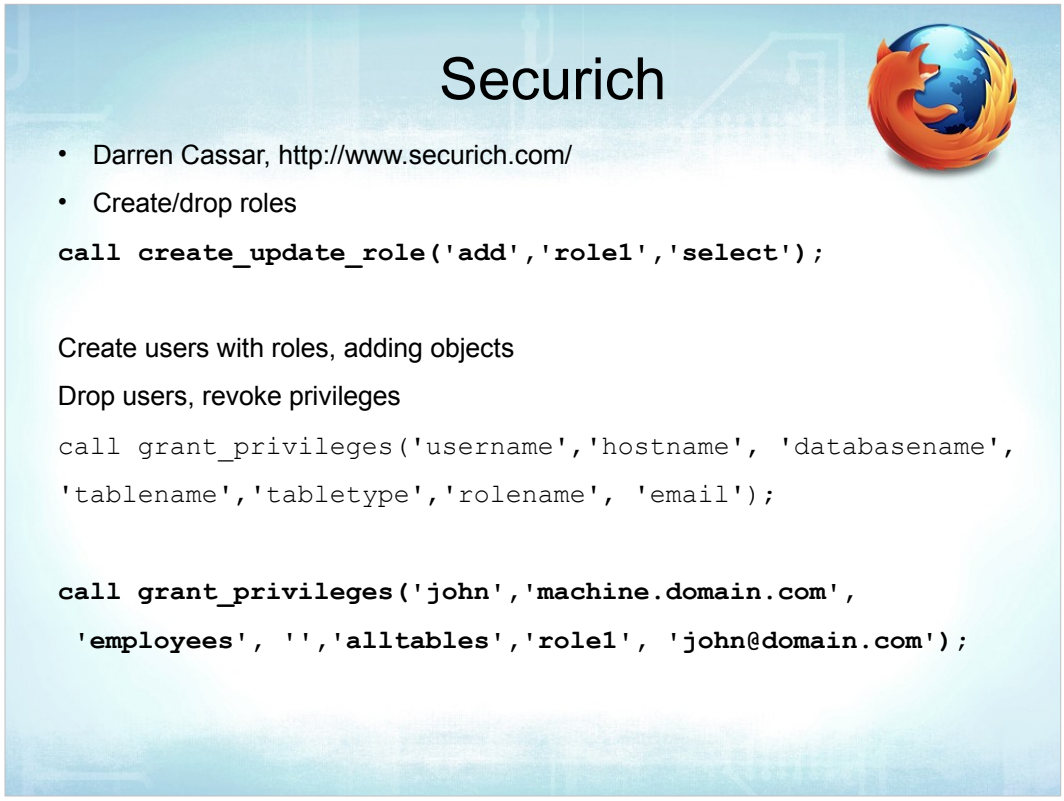
Cause DOS!

ACLs – to do what?

- --local-infile=0
- GRANT
  - MAX_QUERIES_PER_HOUR
  - MAX_UPDATES_PER_HOUR
  - MAX_CONNECTIONS_PER_HOUR

Changing ACLs

- Who changes ACLs?
- How are ACL changes audited?
- When do ACL changes happen?



There's a good tutorial too!

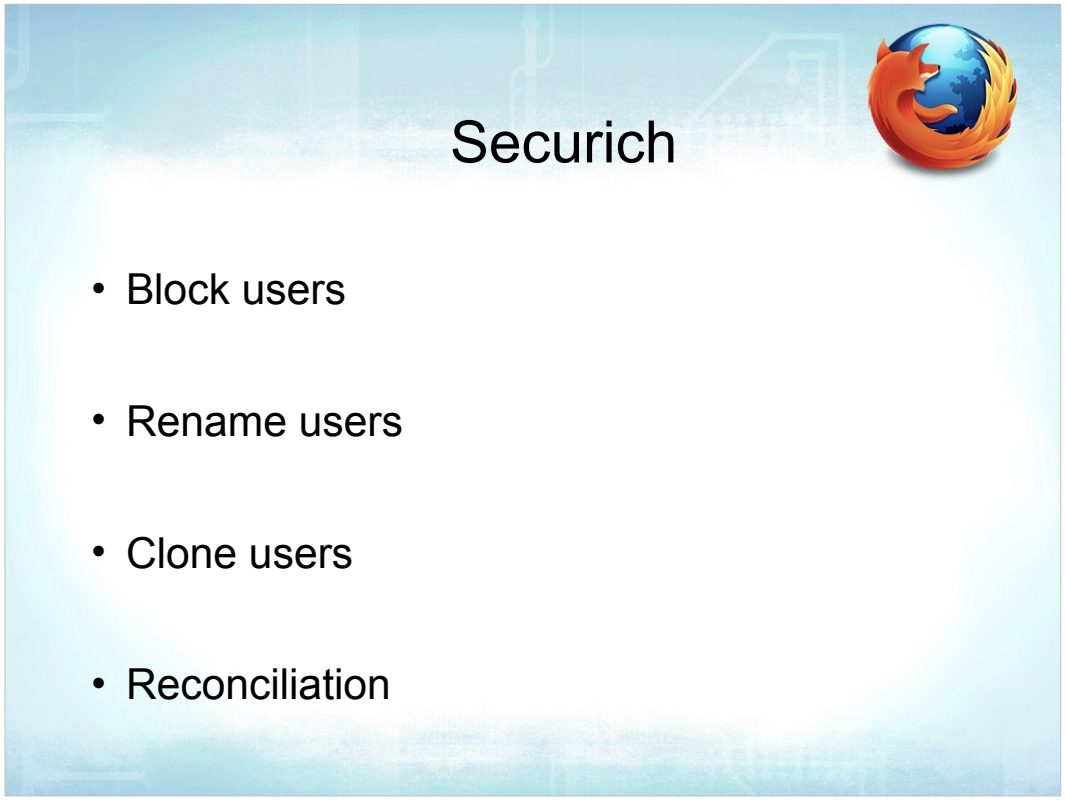
create_update_role either creates or updates the role as necessary

Can on ly drop roles if not in user

Grant privs limitation, if > then truncation happens:

FIELD	MAX LENGTH
username	16
hostname	60
databasename	64
tablename	64
tabletype	16
rolename	60
Emailaddress	50

Tablename can be tblname, regular expression, '' for all, or a stored procedure name



Block - Used to block a particular user, terminating his/her connections if necessary and leave the account around to be unblocked if necessary. This is a useful feature for when a user needs temporary rights.

Can reconcile securich's internal db with what's in securich

- password_check();

This is password_check, a procedure used to check for password discrepancies between securich and mysql.

Server Options

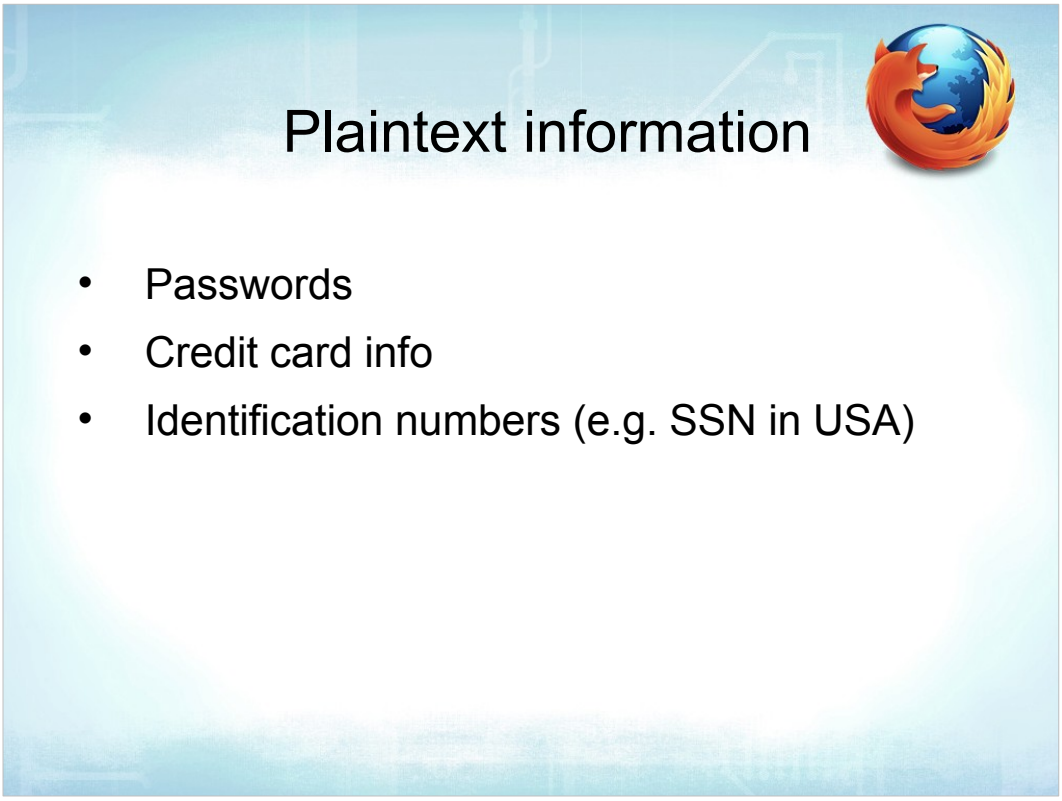
- --bind-address
- --skip-name-resolve

How Does Your Data Flow?

- Where is data encrypted?
- Where do errors go?
  - Are those logs checked?
- Where does the traffic flow?

Separating Admin Apps

- Same data, different interface
- Performance, e.g. reporting
- Only allowed from VPN?
  - Public vs. easily accessible



App users in mysql db, or app password?

mysql db is in memory, referred to every query. Don't make it too big if you don't have to!

User inputted data into mysql internal table == bad. Imagine html or injection in there...bad.

Can be stolen if db is compromised

How are they transmitted?

Normally (most important)

On reset

What about hash transmittal – if you transmit the hash unencrypted, and others can get to db, they can get to customer.

Users may use them elsewhere

Where are you encrypting?

The closer to the input source, the better

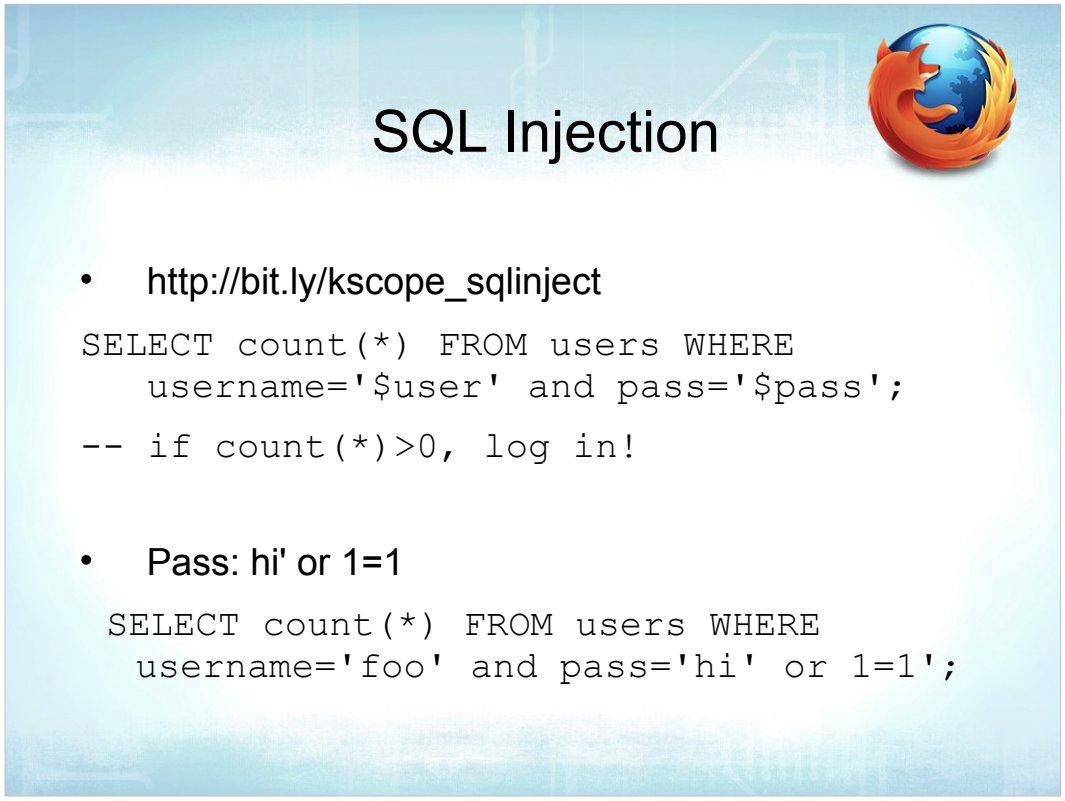
ie, Javascript for HTTP/HTTPS

How are you checking?

Password=hash('foo') ?? hash('foo') then send?

What if I make a web form on MY site that passes info to YOUR site? If checking is only on the page before, there's a problem! Only allow HTTP_REFER from inside...or specific pages.

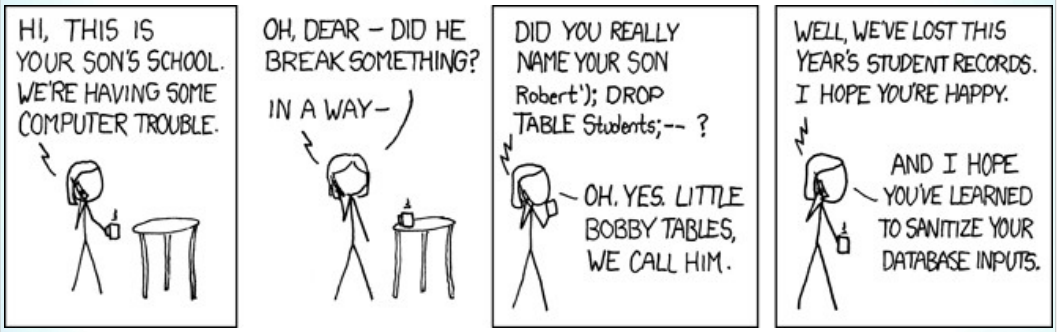
You can google search for that password hash and find it in Google

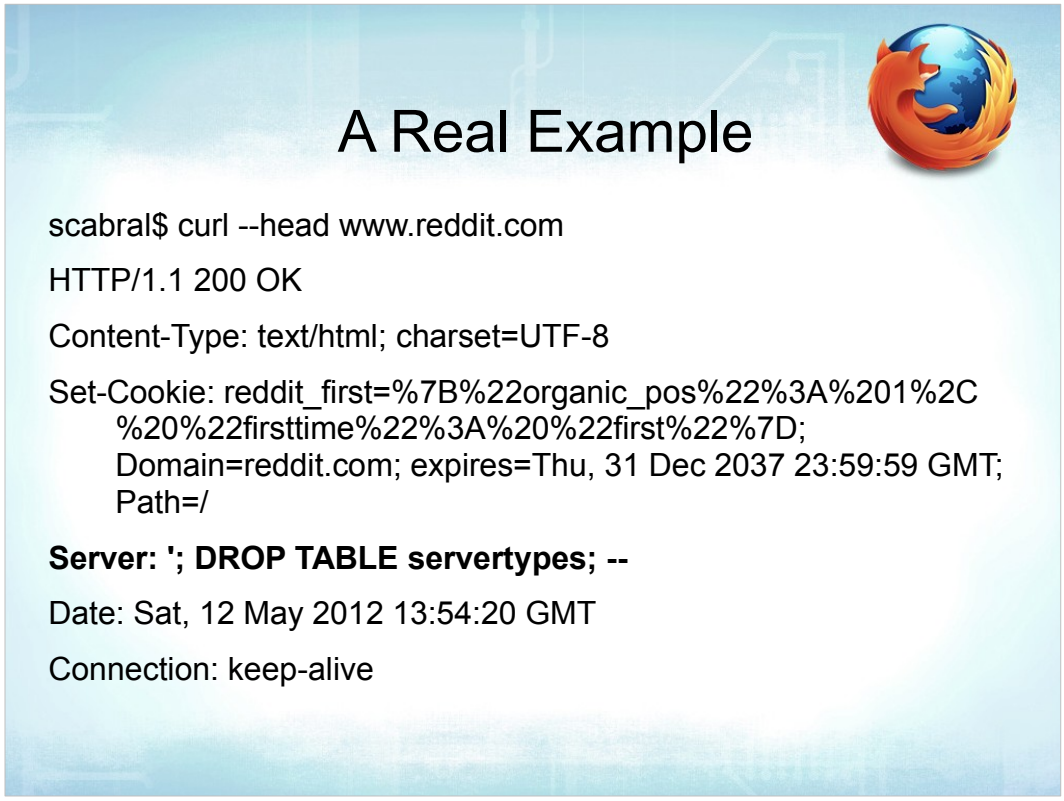


I'm not going to talk much about SQL injection, but I'll give an overview:

Let's say you put in your password

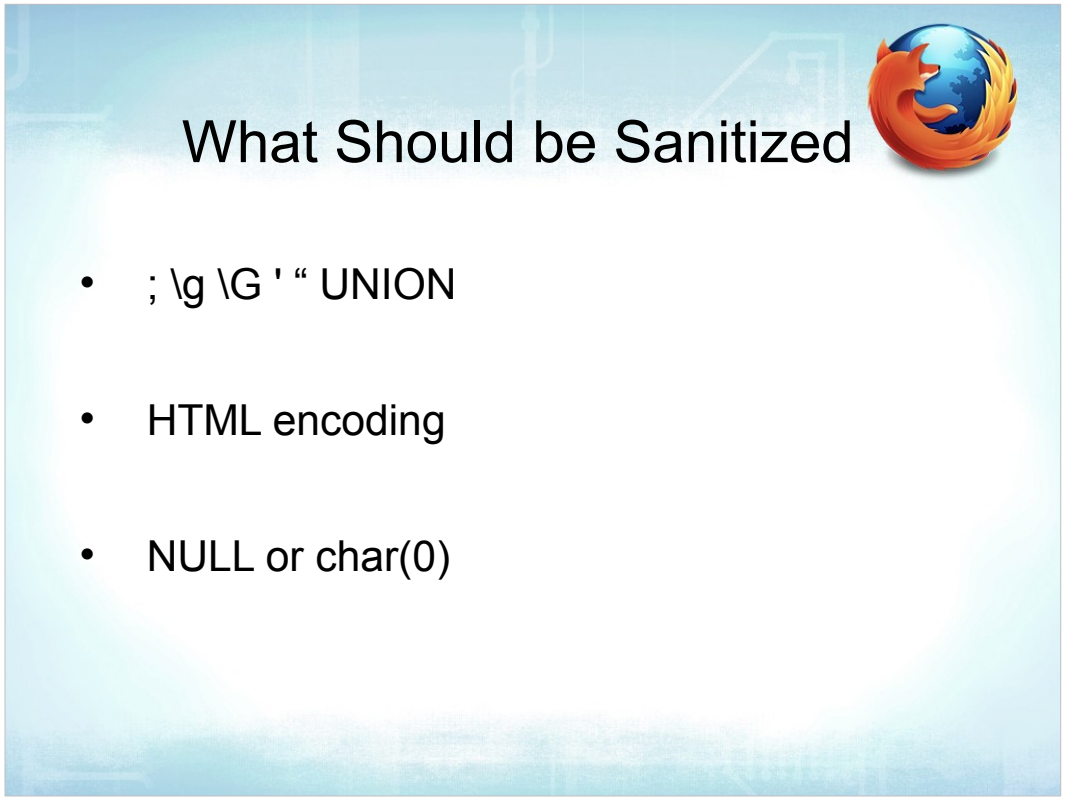
What + How


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.



I'm not going to talk much about SQL injection, but I'll give an overview:

Let's say you put in your password



Disallow or escape ; \g \G “ ' UNION (; won't always help, check if multi_query is allowed)

XSS - Do you allow HTML in stored forms? Including javascript? Personal ad and <G> in form renders weird. Not to mention <SCRIPT .... folks put links to their pay-per-click ads, whenever their page is clicked...

Type 0 XSS -- ?? page's client-side script, ie javascript, access URL request and uses info on that page for something in the current page, can be exploited – can put in another script.

Type 1 XSS – server gets data from client, client can put scripts in there. Reason to strip out HTML

Type 2 XSS – when this stuff is stored.

NULL / char(0) (mysql_query("/*".chr(0)."*/ SELECT * FROM table");)

' ' and varchar

Save yourself time, include e-mail checks if you can (php checkdnsrr)

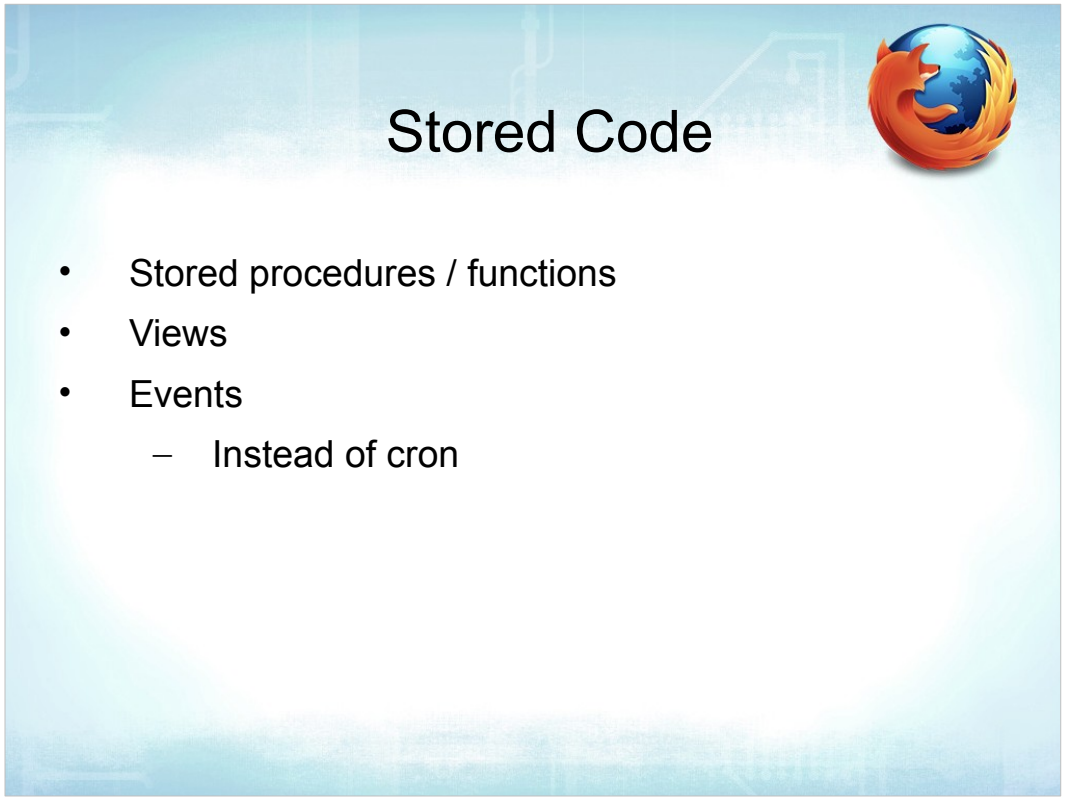
Buffer overflows

What's your CHARSET? (length of INPUT TYPE=TEXT != # of bytes!)

Prepared Statements

```
PREPARE stmt1 FROM 'SELECT uname FROM
   UserAuth WHERE uname=? and pass=?';
SET @a = "sheeri";  SET @b = md5("mypassword");
EXECUTE stmt1 USING @a, @b;
```

Slow! Caches once per SESSION.



Stored procedures? (MySQL 5)

Can use prepared statements in stored procedures, that's how I do dynamic tables in stored procedures

Auditing and Monitoring

- Prevention is one part of security
- Auditing - review and assess security

MacAfee (3/2012)

  - https://github.com/mcafee/mysql-audit

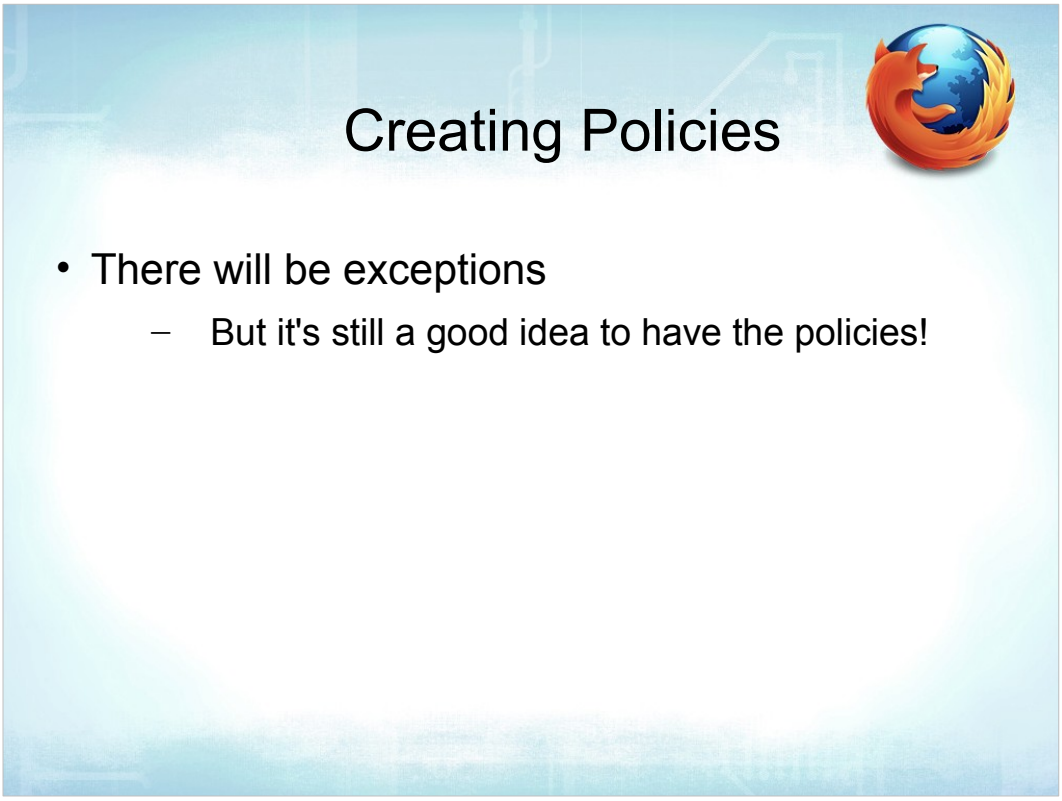
- Monitoring – alerting of security issues

Auditing and Monitoring

- General log to see all login attempts
- Locking out accounts with max_connect_errrors
  - global
  - FLUSH HOSTS

Flush hosts!

So far these are the only ones, none other yet, but we could use Kerberos auth.



Personal accounts vs. role accounts, how often are each of those passwords changed? When ppl leave? Sometimes it's hard to change app passwords.

Encrypted connections/ replication?

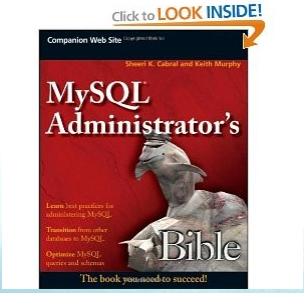
Questions? Comments?

scabral@mozilla.com

@sheeri

www.oursql.com

MySQL Administrator's Bible
- tinyurl.com/mysqlbible



kimtag.com/mysql

planet.mysql.com