MySQL Security

MySQL User Conference & Expo

Tuesday, April 24th, 2007

Sheeri Kritzer, MySQL DBA
http://www.sheeri.com
awfief@gmail.com

Overview

- ACLs
- Test dbs & anonymous accounts
- OS files and permissions

Overview

- Application data flow
- SQL Injection
- XSS

ONLINE BUDDIES

ACLs - Who Has Access?

- SELECT user,host,password FROM mysql.user;
- SUPER
- Anonymous

ONLINE BUDDIES

ACLs – From where?

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

ONLINE BUDDIES

ACLs – From where?

- localhost, --skip-networking
- firewall
- DOS

ONLINE BUDDIES

ACLs – To Do What?

- --local-infile=0
- --skip-symbolic-links
- GRANT
  - MAX_QUERIES_PER_HOUR
  - MAX_UPDATES_PER_HOUR
  - MAX_CONNECTIONS_PER_HOUR

ONLINE BUDDIES

Server Options

- --bind-address
- --skip-name-resolve
- --skip-show-database

Changing ACLs

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

Audit Example - PHP

- Create a table for information:

```
CREATE TABLE `action` (
`user` varchar(77) NOT NULL default '',
`asuser` varchar(77) NOT NULL default '',
`db` varchar(64) NOT NULL default '',
`query` mediumtext NOT NULL
) ENGINE=MyISAM DEFAULT CHARSET=utf8
    COMMENT='77=16+1+60';
```

Audit Example - PHP

- Create the function:

```
function my_mysql_query ($query, $dblink) {

$action="INSERT INTO action (user,asuser,
    db,query) VALUES (CURRENT_USER(),
    USER(), DATABASE(), $query)";

mysql_query($action, $dblink);

mysql_query($query, $dblink);
}
```

Audit Example - PHP

- Use the function:

```
$result = my_mysql_query($query,$dblink);

INSERT INTO action (user, asuser, db, query)
VALUES (CURRENT_USER(), USER(), DATABASE(),
'select foo from bar');
```

Test Databases

- Why get rid of them?
- Copying tables
- Stuff with data

ONLINE BUDDIES

OS Files and Permissions

- mysql server user
- mysql server files & logs
- Passwords on commandline
- Office policies/runbook

ONLINE BUDDIES

OS Files and Permissions

- Backups
- /etc/my.cnf, my.ini, .my.cnf
- CLI, GUI tools
- Personal history files

How Does Your Data Flow?

- Where is user data encrypted?
- Where do errors go?
- Where does the traffic flow?

ONLINE BUDDIES

Administrative Applications

- Same data, different interface
- Reporting
- VPN
- “It's public” vs. “It's easily accessible”

ONLINE BUDDIES

Plaintext Passwords Are Bad!

- Storage of customer login
- Compromised DB
- Transmission of passwords/hashes
- Users may use elsewhere

ONLINE BUDDIES

Plaintext Passwords Are Bad!

- Where are you encrypting?
- Where are you checking?

Validate User Input

- ; \g \G ' “ UNION
- HTML encoding
- NULL / char(0)
- VARCHAR and ' '

ONLINE BUDDIES

Validate User Input

- Save yourself time
- Buffer overflows
- CHARSET

Trusting GET or POST

- Only from certain pages
- Even with valid session ids, cookies
- register_globals=off in PHP

Test your site! acetunix....

ONLINE BUDDIES

Use Prepared Statements

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

ONLINE BUDDIES

Use Prepared Statements

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

  - SET @a = "alef";
  - SET @b = "alef' or 'x'='x";
  - EXECUTE stmt1 USING @a, @b;
  - DEALLOCATE PREPARE stmt1;

ONLINE BUDDIES

Use Prepared Statements

- Prepared statement speed
- Stored procedures

ONLINE BUDDIES

Prepared Statements - Code

- Perl
  - $query = $sql->prepare("SELECT uname FROM UserAuth WHERE uname = ? AND pass = ?");
  - $query->execute($uname, $pass);
- PHP
  - $stmt = $mysqli->prepare("SELECT uname FROM UserAuth WHERE uname = ? AND pass = ?");
  - $stmt->bind_param($uname, $pass);
  - $stmt->execute();

ONLINE BUDDIES

Prepared Statements - Code

- Java
  - PreparedStatement pstmt = con.prepareStatement("SELECT uname FROM UserAuth WHERE uname = ? AND pass = ?");
  - pstmt.setString(uname, pass);
  - ResultSet rset = pstmt.executeQuery();

Prepared Statements - Code

- .NET/C#
  - using(SqlCommand cmd = new SqlCommand("SELECT uname FROM UserAuth WHERE uname = @uname AND pass = @upass",con)) {
  - cmd.Parameters.AddWithValue("@userName", userName);
  - cmd.Parameters.AddWithValue("@pass", pass);
  - using(SqlDataReader rdr = cmd.ExecuteReader()){
  - ...}
  - }

Encryption

- SSL is per-client
- Unencrypted MySQL data streams

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

Feedback?

- Other ideas....

ONLINE BUDDIES