cs50.ly/favorites
Favorite TV Shows

Sign in to Google to save your progress. Learn more

* Required

**title**
Title of your favorite TV show

Your answer

**genres**
Genre(s) of that TV show

- Action
- Adventure
- Animation
flat-file database
regular expressions
. any character
.* 0 or more characters
.+ 1 or more characters
? optional
^ start of input
$ end of input
relational database
SQL
CREATE
READ
UPDATE
DELETE
CREATE, INSERT
SELECT
UPDATE
DELETE, DROP
...
CREATE TABLE table (column type, ...);
SELECT columns FROM table;
...

AVG
COUNT
DISTINCT
LOWER
MAX
MIN
UPPER
...
WHERE
LIKE
ORDER BY
LIMIT
GROUP BY
...

INSERT INTO table (column, ...) VALUES(value, ...);
UPDATE table SET column = value WHERE condition;
DELETE FROM table WHERE condition;
BLOB
INTEGER
NUMERIC
REAL
TEXT
NOT NULL
UNIQUE
PRIMARY KEY
FOREIGN KEY
CREATE INDEX name ON table (column, ...);
B-trees
JOIN
...

JOIN
...

JOIN

...
CREATE INDEX name ON table (column, ...);
SQL injection attacks
Make sure your session is secure

Before entering your NetID and password, verify that the URL for this page begins with:

https://secure.its.yale.edu

To protect your privacy, quit your web browser when you are finished with your session

Sign In

NetID

Password

Forgot My Password

SIGN IN
Sign In

Email Address

Password

SIGN IN

FORGOT YOUR PASSWORD?
Sign In

Email Address
malan@harvard.edu

Password

SIGN IN

FORGOT YOUR PASSWORD?
rows = db.execute("SELECT * FROM users WHERE username = ? AND password = ?", username, password)

if len(rows) == 1:
    # Log user in
rows = db.execute("SELECT * FROM users WHERE username = ? AND password = ?", username, password)

if len(rows) == 1:
    # Log user in
rows = db.execute("SELECT * FROM users WHERE username = ? AND password = ?", username, password)
if len(rows) == 1:
    # Log user in
rows = db.execute(f"SELECT * FROM users WHERE username = '{username}' AND password = '{password}'")

if len(rows) == 1:
    # Log user in
rows = db.execute(f"SELECT * FROM users WHERE username = '{username}' AND password = '{password}'")

if len(rows) == 1:
    # Log user in
rows = db.execute(f"SELECT * FROM users WHERE username = '{malan@harvard.edu}'-- AND password = '{password}'")

if len(rows) == 1:
    # Log user in
rows = db.execute(f"SELECT * FROM users WHERE username = 'malan@harvard.edu'--' AND password = '{password}'")

if len(rows) == 1:
    # Log user in
rows = db.execute("SELECT * FROM users WHERE username = ? AND password = ?", username, password)

if len(rows) == 1:
    # Log user in
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.
race conditions
rows = db.execute("SELECT likes FROM posts WHERE id = ?", id);
likes = rows[0]["likes"]
db.execute("UPDATE posts SET likes = ? WHERE id = ?", likes + 1, id);
rows = db.execute("SELECT likes FROM posts WHERE id = ?", id);
likes = rows[0]["likes"]
db.execute("UPDATE posts SET likes = ? WHERE id = ?", likes + 1, id);
BEGIN TRANSACTION
COMMIT
ROLLBACK
db.execute("BEGIN TRANSACTION")
rows = db.execute("SELECT likes FROM posts WHERE id = ?", id);
likes = rows[0]["likes"]
db.execute("UPDATE posts SET likes = ? WHERE id = ?", likes + 1, id);
db.execute("COMMIT")
This is CS50