Partner question

- Here's a username that causes issues

```
'; DROP TABLE passwords --
```

- Question: what's the problem?

```
# BAD: don't do this
query =
  "SELECT hash "
  "FROM passwords "
  "WHERE user = '" + username + "'"
```

Explanation

```
SELECT hash
FROM passwords
WHERE user = ''; DROP TABLE passwords --'
```

①

②

comment

//

Defense: use ?

trusted

untrusted

```
# BAD: don't do this
query =
  "SELECT hash "
  "FROM passwords "
  "WHERE user = '" + username + "'"
```

```
# GOOD: do this
db.execute(
 "SELECT hash "
 "FROM passwords "
 "WHERE user = ?",
 (username,))
```

trusted

untrusted