

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
//

The diagram illustrates a SQL injection attack. The original query is `SELECT hash FROM passwords WHERE user = ' ;`. The injected payload is `DROP TABLE passwords -- '`. The annotations explain the components: 1. The first single quote is the closing quote for the user filter. 2. `DROP TABLE passwords` is the malicious command to delete the table. The double hyphen `--` is a SQL comment symbol, and the single quote `'` is the closing quote for the comment, effectively terminating the original query and executing the injected command.

Defense: use ?

BAD: don't do this

query =

"SELECT hash "

"FROM passwords "

"WHERE user = '" + username + "'"

trusted

untrusted

GOOD: do this

db.execute(

"SELECT hash "

"FROM passwords "

"WHERE user = ?",

(username,))

trusted

untrusted