Question Group A

1. An attacker makes the following SQLi attempt, but it didn't work. Spot their mistake(s).

server side code

```
query = "select ip_addr from Camera where cam_id='" + id + "' AND pass='" + pass + "';"
```

attacker input

```
cam9" OR 3=3;
```

2. What is perturbation? Explain any two methods of performing perturbation.
3. Use a diagram to explain how stack protection works to prevent buffer overflow attacks.

[3 + 4 + 3 marks]

Question Group B

1. Briefly explain how can you use SQLi to launch a DoS attack against a service.
2. Write SQL statements to add user accounts `salman` and `hira` to `sales` group. Then permit this group to only add new records in `Order` table (without providing any other privileges).
3. Discuss any two run-time defenses against buffer overflow attacks.

[3 + 3 + 4 marks]

Group A

Q1

To terminate string, attacker should use a single quote after cam9 instead of double quote.

They also need a comment mark – at the end so that the remaining part of query becomes ineffective.

Q2

Lec 14 slides 46-47

Q3

Lec 12 slide 21

Group B

Q1

By injecting a SQL code that keeps the db server busy in long and useless calculations.

An example needed, such as L14 slide 23

Q2

GRANT sales to salman, hira *(or grant separately for each user)*

GRANT INSERT on Order to sales

Q3

Lec 12 slides 23-25