Consider the server-side (node-js) code for creating a query based on size input received from client side.

```
let query = "SELECT id, name, price FROM products
             WHERE size = '" + request.body.size + "';"
```

**Group A**

1. What could the attacker supply in size input in order to launch a SQLi attack with a piggybacked query. Provide a precise example.
2. What modification will you make to the above code to remove the injection vulnerability?
3. What could be the outcomes of a buffer overflow attack? List any three of them.
4. What will happen when following statement is run?

```
printf("hello %s");
```

**Group B**

1. What could the attacker supply in size input in order to launch a union based SQLi attack. Provide a precise example.
2. In which situation, will an attacker try blind SQL injection?
3. What are the initial steps attacker needs to go through before launching a buffer overflow attack?
4. What will happen when following statement is run?

```
printf("hello %n");
```

[ 3 + 2 + 3 + 2 marks]

**Group A**

Q1

Example answer

```
'; DROP TABLE Student; --
```

Need a single quote for string termination, semicolon for query termination, any extra query after that (that too terminated with semicolon), followed by comment mark.

Q2

Prepare a parametrized query: `SELECT * FROM Student WHERE rollno = '?';`

Then bind the request.body.size value to this prepared query.

Q3

- corruption of program data
- bypass security checks
- unexpected transfer of control
- memory access violation
- execution of code chosen by attacker (control hijacking)

Q4

During printf execution, cpu will expect a second parameter on stack. Since none is provided, cpu will read whatever is on stack (below the return address, where parameters usually are).

It will interpret the read value, say Z, as a string address. The program will start printing the characters at address Z onwards until a null terminator is encountered.

**Group B**

Q1

Example answer

```
5' UNION select id, password, age from Users; --
```

Need a single quote for string termination, UNION with another SELECT command (terminated with semicolon), followed by comment mark. The SELECT command should have same number of columns and data types as first one (id, name, price).

Q2

When attacker has already tried sending illegal queries to get information about database schema, but the web server only returns a generic error message without revealing any database details.

In such scenario, attacker will try bind injection.

Q3

Lec 12 slide 8

Q4

During printf execution, cpu will expect a second parameter on stack. Since none is provided, cpu will read whatever is on stack (below the return address, where parameters usually are).

It will interpret the read value, say Z, as an address of a variable. At address Z, it will put a count of characters processed so far, in this case 6.