SQL Injection – Example

JDBC

```
Authenticate (String n, String p) {
…
String query =
"SELECT grade FROM students WHERE name = '" + n + "'
AND password = '" + p + "' ";
…
}
```

Input:

name = bart; password = mypword

SQL:

```
SELECT grade FROM students WHERE name = 'bart' AND
password = 'mypword'
```

SQL Injection – Example

JDBC

```
Authenticate (String n, String p) {
…
String query =
"SELECT grade FROM students
 WHERE name = '" + n + "'
 AND password = '" + p + "' ";
…
}
```

Input:

```
name = lisa; password = n' OR 'x'='x
```

SQL:

```
SELECT grade FROM students WHERE name = 'lisa' AND
password = 'n' OR 'x' = 'x'
```

SQL Injection – Example

JDBC

```
Authenticate (String n, String p) {
…
String query =
"SELECT grade FROM students
 WHERE name = '" + n + "'
 AND password = '" + p + "' ";
…
}
```

Attacker: Passes in the following strings for n and p

```
n= foo; p= n'; UPDATE students SET grade= 'A
```

Resulting value of query:

```
SELECT grade FROM students WHERE name = 'foo' AND
 password = 'n'; UPDATE students SET grade = 'A'
```