7 Cybersecurity (fms27)

A web application uses an SQL database that contains a `student` table with fields `id`, `studentName`, `pwdHash` (all `varchar`) and `studentGrade` (`integer`). The `pwdHash` field contains the unsalted SHA-256 hash of the user's password, encoded in Base 32 (A–Z and 2–7) with `b32enc()`. [*Note:* In this question, SQL statements are written over several lines for greater legibility, but assume there are no newlines.]

(*a*) A web form of that application has input fields for `id` and `password`. On submission, it displays the corresponding `studentGrade`, obtained by running the following SQL query, where the items inside the single quotes are replaced by the content of the corresponding form fields. Describe an attack that displays the grade of student `abc78`, whose password you do not know. First write out the SQL resulting from your attack, then what to type in the fields. [3 marks]

```
SELECT studentGrade
FROM student
WHERE id = 'id' AND pwdHash = b32enc(sha256('password'));
```

(*b*) Another web form of the same application lets you change your own display name and password: you must supply fields `studentID`, `newStudentName`, `oldPassword`, `newPassword`. On submission, the form sends the following SQL statement to the database, with the items inside the single quotes replaced by the content of the corresponding form fields. Describe an attack to change the grade of existing student `zzz666` to `100` but without changing this student's name or password, neither of which you know. First explain your strategy, then write out the resulting SQL, then what to type in the fields. Assume the database is configured to parse only one SQL statement per supplied string. [10 marks]

```
UPDATE student
SET studentName = 'newStudentName',
    pwdHash = b32enc(sha256('newPassword'))
WHERE id = 'id' AND pwdHash = b32enc(sha256('oldPassword'));
```

(*c*) The developer augments all forms with code that removes every non-alphanumeric character from the fields before inserting them in the SQL statement. Describe the main advantages and drawbacks of this approach. [4 marks]

(*d*) Describe a better approach than the one in Part (*c*) and justify why it is better. [3 marks]