

Data and Knowledge Management – COIY061H7 - 2021/22

Coursework Assignment

Description, Guidelines and Marking Scheme

1. Aim of the Coursework Assignment

This coursework contributes 20% to the overall DKM assessment.

The aim of the Coursework Assignment is to help you learn more about and get experience of security in relational databases.

The assignment is further explained in Section 2. Section 3 explains the marking scheme. Section 4 gives submission instructions. Section 5 explains the penalties for late submissions. Section 6 explains how the College deals with plagiarism. Section 7 provides additional information on learning resources on plagiarism and study skills. Section 8 provides guidance on how to give appropriate references your answers.

2. Description of the assignment

An Oracle relational database is used to record marks for projects undertaken by students on an MSc course.

A student first submits a project proposal which is marked out of 100 by 2 or more examiners whose marks are combined by taking the average, rounded to the nearest whole mark, to give the mark for the proposal. Similarly, a student subsequently submits a project report which is also marked by 2 or more examiners whose marks are combined by taking the average, rounded to the nearest whole mark, to give the mark for the report. The overall project mark is calculated by combining the proposal mark (20%) and report mark (80%) and rounding to the nearest whole mark.

The database includes tables created as follows:

```
PROJ_EXAMINERS (EXAMINER)
PROJ_DETAILS (STUDENT, TITLE, SUPERVISOR)
PROJ_PROPOSAL_EXAMINER_MARKS (STUDENT, EXAMINER, MARK, YEAR)
PROJ_REPORT_EXAMINER_MARKS (STUDENT, EXAMINER, MARK, YEAR)
```

A row is stored in PROJ_EXAMINERS for each staff member who is permitted to examine projects, for example ('ADA').

A row is stored in PROJ_DETAILS for each project recording the student, project title and supervisor, for example ('MARY01', 'concurrency visualisation tool', 'ADA').

For each project, examiners are appointed consisting of the supervisor and one or more other examiners. Rows in PROJ_PROPOSAL_EXAMINER_MARKS and PROJ_REPORT_EXAMINER_MARKS record the marks awarded by examiners for the proposal and report respectively, together with the year the project is examined. Marks are initially NULL. So, for example, assuming that in 2019 for student MARY01 examiners JAMES and GRACE are appointed together with the supervisor ADA, the following rows would be inserted into both

PROJ_PROPOSAL_EXAMINER_MARKS and PROJ_REPORT_EXAMINER_MARKS:

```
('MARY01', 'ADA', NULL, 2019)
('MARY01', 'JAMES', NULL, 2019)
('MARY01', 'GRACE', NULL, 2019)
```

The NULL values are updated with the examiners' marks once they are known.

Values stored for STUDENT and EXAMINER are the Oracle usernames of students and examiners respectively.

Tables with example rows may be accessed as:

```
PROJ_EXAMINERS
PROJ_DETAILS
PROJ_PROPOSAL_EXAMINER_MARKS
PROJ_REPORT_EXAMINER_MARKS
```

Task 1: Security

An application developer has written an SQL statement to be used within a host language as described in the handout [Host Language Support for SQL](#). The developer wishes to give students access to rows in PROJ_DETAILS so that they can check that their project details are correctly recorded, but not the project details of other students.

The application asks the student to enter their Oracle username which is stored in a variable username. The application then builds a string in a variable querystring for the SQL query to be executed by concatenating:

- SELECT TITLE, SUPERVISOR FROM PROJ_DETAILS WHERE STUDENT = '
- The name entered and stored in username
- '

If, for example, the student enters MARY01 as their username, the application builds a querystring

```
SELECT TITLE, SUPERVISOR FROM PROJ_DETAILS WHERE STUDENT = 'MARY01'
```

which it then prepares with

```
EXEC SQL PREPARE QUERY_STMT FROM :querystring;
```

before processing with a cursor in the normal way to enable the application to handle the result rows.

A common form of attack against databases is by exploiting **SQL injection** techniques in applications. See: https://www.owasp.org/index.php/SQL_Injection

Explain in your own words (1500-2000 words in total):

- (a) Explain what an SQL injection attack is and discuss the problems which this can cause.
(12 marks)
- (b) Explain, giving two examples specific to the schema described, how the application outlined could lead to an SQL injection attack.
(8 marks)
- (c) The application is clearly vulnerable in any case to a user guessing or knowing another student's username. If user passwords were also stored in the database, and the user entered a password as well as a username with the `querystring` built to test for both in the `WHERE` clause, would SQL injection attacks be prevented? Explain your answer and give an example specific to the schema described. **(8 marks)**
- (d) How can such attacks be guarded against by more careful use of prepared statements when building applications which use SQL from a host language? Illustrate your answer with the changes you would make to the SQL statements of the application outlined above.
(16 marks)

Task 2: Views

Views are an additional mechanism which can help support secure access to table data when used with appropriate privileges. The following views are proposed to control the data visible to different Oracle users when logged on to Oracle.

Give the SQL statements for the creation of views in Oracle to support these requirements.

Note that in Oracle you may reference the function `USER` in an SQL statement, for example in a `SELECT` or `WHERE` clause. It returns the username of the person executing the SQL statement. Also, a function `ROUND(n, 1)` returns `n` rounded to one decimal place.

- (a) One view is required with the same columns as `PROJ_DETAILS` which gives access to all rows to staff permitted to examine projects, but gives students access to only the row for their own project. **(16 marks)**
- (b) Two views are required summarising the project proposal marks and project report marks obtained by combining the individual examiners' marks:

```
PROJ_PROPOSAL_MARKS (YEAR, STUDENT, MARK)
PROJ_REPORT_MARKS (YEAR, STUDENT, MARK)
```

For example, a row in `PROJ_PROPOSAL_MARKS` (2019, 'NEIL01' 62) and a row in `PROJ_REPORT_MARKS` (2019, 'NEIL01' 57) record that NEIL01 had his project examined in 2019 with proposal mark 62 and report mark 57.

Only projects which have all proposal marks recorded should be included in `PROJ_PROPOSAL_MARKS` while only projects which have all report marks recorded should be included in `PROJ_REPORT_MARKS`.

Rows in each view should be accessible by staff permitted to examine projects but a student should only have access to rows for their own project. **(24 marks)**

(c) One view is required summarising the overall project marks in each year

```
PROJ_OVERALL_MARKS (YEAR, STUDENT, PROPOSAL_MARK,  
                    REPORT_MARK, PROJECT_MARK)
```

which summarises the marks for the proposal, report and overall project mark each year. So, for NEIL01, a row for his project result in 2019 should be recorded:

```
(2019, 'NEIL01' 62, 57, 58)
```

Rows in the view should be accessible by staff permitted to examine projects but a student should only have access to the row for their own project. **(16 marks)**

3. Marking Scheme

Marks will be allocated as shown in the description of the task. The total possible mark is 100.

For Task 1, marks will be awarded for correctness, clarity, originality and depth of understanding demonstrated in the answer.

For Task 2, full marks will be given for fully correct solutions. Otherwise marks will be awarded for partially correct aspects of the solution.

4. Submission Instructions

You should complete the tasks 1 and 2 detailed in section 2 of this document.

Submission is only through Moodle using the Gradescope platform. Two submission links are provided on Moodle for each part of the assignment.

For Task 1, your answers must be in PDF format.

For Task 2, your answer can consist of either:

- a single plain text file for all questions.
- a zip file containing a plain text file for each part of the question, with the individual files named a.sql, b.sql and c.sql.

Note that for Task 2, submissions in any other format than plain text will **not** be accepted.

You should upload your submission to Moodle by **23:59 on Sunday 9th January 2022** (this is Moodle's time not your PC's time). In case you are planning to upload your file whilst at a remote location make sure you check the Moodle system's time and take into account any time zone differences.

It is your responsibility to ensure that files transferred from your own machine are in the correct format and that any programs execute as intended (where applicable) on the Department's systems prior to the submission date.

The submitted work must include an *Academic Declaration* that certifies that the author has read and understood the sections on plagiarism in the document

<https://www.bbk.ac.uk/downloads/registry/policies-2020-21/assessment-offences-policy.pdf>

that describes the College's Policy on assessment offences. Confirm that the work is your own, with the work of others fully acknowledged. Submissions must also be accompanied by a declaration giving us permission to submit your work to the plagiarism testing database that the College is using.

The Academic Declaration should read as follows: *"I have read and understood the sections on plagiarism in the College Policy on assessment offences and confirm that the work is my own, with the work of others clearly acknowledged. I give my permission to submit my work to the plagiarism testing database that the College is using and test it using plagiarism detection software, search engines or meta-searching software."*

You should note that all original material is retained by the Department for reference by internal and external examiners when moderating and standardising the overall marks after the end of the module.

5. Late submission

It is college policy to accept and mark late submissions, up to 23:59 on the 14th day after the stated deadline. You do not need to negotiate new deadlines and there is no need to obtain prior consent of the module leader.

N.B. The cut-off time is the Moodle system's time not your PC's time. In case you are planning to upload your files whilst at a remote location make sure you check the Moodle system's time and take into account any time zone differences. This is the absolute cut-off deadline for coursework submission.

Note that a penalty of up to 50% applies to late submissions. Full details can be found here:

<https://www.bbk.ac.uk/downloads/registry/policies-2021-22/late-submission-of-coursework.pdf>

If you believe you have good cause to be excused the penalty for late submission, you must make a written request using the mitigating circumstances form and attach any evidence. Your form should be handed in or emailed to the MSc Programme Administrator (with a carbon copy to the module lecturer and the Programme Director) as soon as possible, ideally by the cut-off deadline. This letter/email does not need to be submitted at the same time as you submit the coursework itself but must be submitted within 10 days of the cut-off deadline at the latest.

Even if the personal circumstances that prevented you from submitting the coursework by the last day are extreme, the Department will not accept coursework after this date. We will, naturally, be very sympathetic, and the MSc Programme Director will be happy to discuss ways in which you can proceed with your studies, but please do not ask us to accept coursework after this date; we will not be able to do so as there is a College-wide procedure for managing late submissions and extenuating circumstances in student assessment. As soon as you know that you will not be able to meet the deadline, it will be useful for you to inform the module lecturer. They will be able to advise you on how best to proceed. Another person to speak to, particularly if the problem is serious, is the MSc Programme Director. You will then have the opportunity to discuss various options as to how best to continue your studies.

Further details concerning the rules and regulations with regard to all matters concerning assessment (which naturally includes coursework), you should consult the College Regulations at

<http://www.bbk.ac.uk/mybirkbeck/services/rules>

Please see your programme handbook for the rules governing Late Submissions and consideration of Mitigating Circumstances, and the Policy for Mitigating Circumstances on the College's website at the above URL.

6. Plagiarism

The College defines plagiarism as “copying a whole or substantial parts of a paper from a source text (e.g. a web site, journal article, book or encyclopaedia), without proper acknowledgement; paraphrasing of another's piece of work closely, with minor changes but with the essential meaning, form and/or progression of ideas maintained; piecing together sections of the work of others into a new whole; procuring a paper from a company or essay bank (including Internet sites); submitting another student's work, with or without that student's knowledge; submitting a paper written by someone else (e.g. a peer or relative), and passing it off as one's own; representing a piece of joint or group work as one's own”.

The College considers plagiarism a serious offence, and as such it warrants disciplinary action. This is particularly important in assessed pieces of work where the plagiarism goes so far as to dishonestly claim credit for ideas that have been taken from someone else.

Each piece of submitted work must have an *Academic Declaration* by the student which certifies that the student has read and understood the sections on plagiarism in the College Regulations and confirms that the work is their own, with the work of others fully acknowledged. Submissions must be also accompanied by a declaration giving us permission to submit coursework to a plagiarism testing database to which the College is subscribed.

If you submit work without acknowledgement or reference of other students' (or other peoples') work, then this is one of the most serious forms of plagiarism. When you wish to include material that is not the result of your own efforts alone, you should make a reference to their contribution, just as if that were a published piece of work. You should put a clear acknowledgement (either in the text itself, or as a footnote) identifying the students that you have worked with, and the contribution that they have made to your submission.

7. Useful Resources

Here are some general resources on plagiarism and study skills that can help you to manage your coursework and avoid plagiarism.

On Plagiarism:

<https://owl.english.purdue.edu/owl/resource/589/1/>

On Study Skills:

<http://www.bbk.ac.uk/student-services/learning-development>

8. Referencing

For 2.1, you will of course consult the online resource indicated and possibly others. You should rephrase what you find out in your own words or use quotation marks for direct quotes, giving appropriate references. Even where you rephrase material, you should give a reference to the source for the information. The references should not be included in the word count.

References include the full bibliographic information about the source, such as the author(s)'s name(s), date of publication, title of work, place of publication, and publisher. This information is usually given in the section called Reference List or Bibliography at the end of the text. The key principle is that you should give enough information to allow another person to find the source for themselves.

Here are some examples using the Harvard referencing system:

[when you are referring to a book]

Lewin, K., 1951. *Field Theory in Social Science*. New York: Harper and Row.

[when you are referring to a chapter in a book, where 'ed.' means editor, and 'edn.' means 'edition']

Piaget, J., 1970. Piaget's theory. In: P. Smith, ed., *Handbook of child psychology*. 3rd edn. New York: Wiley, 1970, pp. 34-76.

[when you are referring to a journal article]

Holmqvist, M., 2003. A Dynamic Model of Intra- and Interorganizational Learning. *Organization Studies*, 24(1), 95-123.