Solutions

Marking: **M1** a correct method, **A1** the correct answer, **B1** an independent mark.

Each answer shows the steps, then the **result**.

2.1

parameterised queries, and a length limit on the input

HTTPS only, `Secure` and `HttpOnly` cookies, short session expiry

signed email (SPF/DKIM); emails never ask for passwords and give no loan details

2.2

```
cursor.execute("SELECT * FROM members WHERE name = ?", (q,))
```

the database treats `q` as data, never as SQL

2.3

$18 - 4 = \mathbf{14}$

a forgotten or new action is closed until someone allows it on purpose

2.4

keep name and class (needed to lend books)

drop home address and photo; the school already holds contact details

delete or anonymise loan history after a set time, e.g. when the student leaves

3.1

(a) $26^8 \approx \mathbf{2.1 \times 10^{11}}$

(b) SHA-256: $2.1 \times 10^{11} / 10^{10} \approx \mathbf{21}$ s; bcrypt: $2.1 \times 10^{11} / 10^{4} \approx 2.1 \times 10^{7}$ s $\approx \mathbf{240}$ days

(c) each user gets a random salt, so equal passwords give different hashes and one guess cannot test every account at once

(d) log in with the school's existing accounts (single sign-on), so BookShare never sees or stores passwords

3.2

(a) reading choices are personal, and older students may not want parents to see them; the data was collected for lending, not for reports

(b) raise the concern honestly with the library, before building it; put the public good and the students' privacy first: ask what the report is for

(c) send totals ("12 books this term"), and let students choose to share titles

3.3

(a) students and parents (whose data it is); the school, the library, and the company

(b) the data may be used for adverts or profiling of children; if the company changes or is hacked, the school cannot get the data back or stop its use

exercises.lol exercises.com.cn

(c) exactly what data, for what use, and for how long? can the data be anonymised, and who can audit that?

(d) refuse the deal as offered; accept only a contract that limits use to running BookShare, with deletion on request, or pay for hosting