



VICTORIA UNIVERSITY OF
WELLINGTON
TE HERENGA WAKA

EXAMINATIONS – 2026

TEST 1

FRONT PAGE

CYBR 271

CODE SECURITY

Time Allowed: 50 minutes

Instructions:

- Answer all questions. This is a closed-book test; no materials are permitted.
- Suggested section times total 43 minutes; use the remaining 7 minutes for checking your answers.
- Write your name and Student ID in the spaces provided on the first page, do not worry about subsequent pages.
- Concise answers, bullet points, short phrases, tables and labelled diagrams are acceptable; polished prose is not required.
- When asked for evidence, refer to a specific fact from the scenario. Exact quotation is not required.
- Use the STRIDE, DREAD and secure-design terminology used in the course.

SECTION A – MULTIPLE CHOICE

(5 marks; suggested 4 minutes)

Select the single best answer.

A1. A shopping app sends an order to its server. An attacker changes the total price while the request is in transit. Which STRIDE category best fits? **(1 mark)**

- A. Spoofing
- B. Tampering
- C. Information disclosure
- D. Elevation of privilege

A2. Every newly created user account receives administrator rights that are rarely removed. Which secure-design principle is most directly violated? **(1 mark)**

- A. Economy of mechanism
- B. Open design
- C. Least privilege
- D. Defence in depth

A3. A seller denies having posted a listing. Which control would most directly support investigation and make the action difficult to deny? **(1 mark)**

- A. An integrity-protected audit log recording user, action and time
- B. Requiring MFA before a seller can post a listing
- C. Encryption of listing photographs
- D. Nightly backups of the listings database

A4. A developer deliberately inserts a hidden backdoor into the product's own source code. Which supply-chain weakness best describes this? **(1 mark)**

- A. Compromised third-party library
- B. Third-party misconfiguration
- C. Insider threat in development
- D. Compromised update channel

A5. A threat model identifies a risk that a signed-in customer could read another customer's records. Testing time is limited. Which action best uses the threat model to guide testing? **(1 mark)**

- A. Prioritise adversarial authorisation tests derived from that threat
- B. Add input-validation tests for the listing and messaging forms
- C. Scan third-party dependencies before the next release
- D. Increase load testing of the customer-record pages

SECTION B – VERY SHORT ANSWER**(3 marks; suggested 2 minutes)****B1–B3: Write exactly one word in each answer box. Do not include working or justification.**

B1. A phishing campaign targets a clinic that has no MFA. In the risk equation $\text{Risk} = \text{Threat} \times \text{_____}$, one term has been replaced by a blank. **Write the missing term only (one word). (1 mark)**

B2. A team gives the Affected users category a score of 10 because it assumes every account could be affected. Later evidence shows that the exploit could reach only a small subset of users. Should the score be increased, reduced or left unchanged? **Write one word only. (1 mark)**

B3. A threat is scored 5 for Damage, 5 for Reproducibility, 5 for Exploitability, 5 for Affected users and 10 for Discoverability. Later evidence shows that it is very hard to discover and requires source code or administrator access. Using the reference table, what is the corrected overall risk band? **Write the band name only (one word). (1 mark)**

DREAD scoring reference

Score each category from 0 to 10. The table gives the taught anchor descriptions.

Category	0	5	10
Damage potential	Nothing	Individual user data compromised	Complete system or data destruction
Reproducibility	Very hard or impossible, even for administrators/DBAs	One or two steps; may need an authorised user	A web browser alone is enough
Exploitability	Advanced programming and networking knowledge	Malware or suitable tools are available online	A web browser alone is enough
Affected users	None	Some users, but not all	All users
Discoverability	Very hard or impossible; needs source code or administrator access	Can be found by guessing or monitoring network traces	Visible in the browser, address bar, form or a hidden variable

Overall score bands: Critical 40–50; High 25–39; Medium 11–24; Low 0–10.

SECTION C – STRUCTURED SHORT ANSWER

(27 marks; suggested 22 minutes)

C1 – Community clinic booking system

(9 marks)

A community clinic uses an online appointment system:

- Patients sign in with an email address and hashed password; the booking page uses plain HTTP.
- There is no limit on failed login attempts.
- A receptionist dashboard shows each patient's name, date of birth and reason for visit.
- Appointment data is held in one database; reminders are sent by SMS.

(a) **(4 marks)** Identify two threats from different STRIDE categories. For each threat, name the category and identify one scenario fact that enables it.

- (b) The clinic adds this control: *after five failed logins, the account locks and can be unlocked only by phoning reception.*

(i) **(1 mark)** What immediate threat does this reduce?

(ii) **(1 mark)** Identify one new security risk or attacker adaptation introduced by the lockout and phone-unlock process.

(iii) **(2 marks)** For your answer in (ii), describe one concrete action of the attacker and one consequence or way the attack could be scaled up.

(iv) **(1 mark)** Name one additional control or monitoring measure that would reduce the risk described in (ii)–(iii).

C2 – Staff file-sharing service**(9 marks)****A file-sharing service stores customer documents for staff:**

- Any signed-in user can create a public share link; links never expire and link creation is not logged.
- Every staff account can open every customer folder, regardless of role.
- The administrator console can delete accounts and change permissions. It is public-internet facing and password-only.

- (a) **(4 marks)** Name two different secure-design principles from the course framework that this design violates. For each, identify the design detail that demonstrates the violation.

--

- (b) **(3 marks)** Give one plausible persona non grata. Present your answer under these four headings: **Actor and access**; **Motivation**; **Concrete misuse**; and **Design weakness enabling the misuse**.

Actor and access	
Motivation	
Concrete misuse	
Design weakness enabling the misuse	

- (c) **(2 marks)** Recommend one control for misuse of the over-broad folder access. State whether its primary function is preventative, detective or responsive.

--

C3 – Mobile banking dependencies

(9 marks)

A mobile banking app imports 40 open-source libraries:

- An image-processing library is pinned to a version released two years ago; that version has a public remote-code-execution CVE.
- The other dependencies are unpinned; each build downloads their latest published versions.
- The team has no software bill of materials (SBOM).
- A released version of the app exposes a web address intended for developers to inspect internal server logs. Anyone can open it without signing in.

- (a) **(4 marks)** Identify two supply-chain weaknesses. For each, name the weakness and identify the dependency-management decision or related supply-chain practice that creates it. Not every security weakness in the scenario is supply-chain related.

--

- (b) **(2 marks)** For each weakness from part (a), recommend one appropriate mitigation and state briefly how it reduces that weakness.

--

- (c) **(3 marks)** Choose which issue to address first: the vulnerable image library or the publicly accessible debug-log page. Compare the two issues in terms of (i) their probable security impact and (ii) how easily each could be exploited. Use scenario information and justify your choice of priority. Either issue may be placed first if the comparison supports the decision.

SECTION D – INTEGRATED CASE STUDY**(15 marks; suggested 15 minutes)****D1 – Student marketplace****(15 marks)**

A university student marketplace is available on the web and through a mobile app.

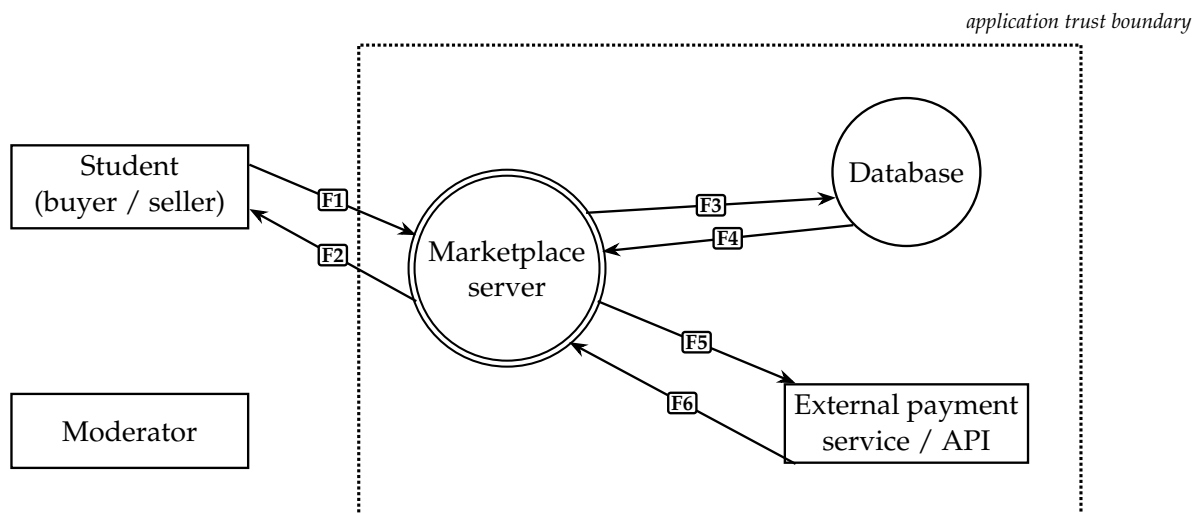
A typical student journey is:

- A student signs in. Password reset uses security questions such as “What is your pet’s name?”
- A buyer can browse listings and message a seller.
- After messaging a seller, the buyer can rate that seller even if no purchase occurred.
- A purchase is processed through an external payment service / API using an SDK that has not been updated for more than a year.

Other design details are:

- Policy permits moderators to read only messages reported for abuse, but the system allows any moderator to read any message and does not log that access.
- After login, the server trusts an `is_admin` value supplied by the client when deciding whether to allow administrator actions.
- A central database stores user details, messages, ratings and transaction records.

Figure D1. Use the DFD notation in the legend and consider only the five components shown. The diagram contains three modelling errors.



Flow key: F1 login/listing/message data; F2 pages/results; F3 users/messages/ratings; F4 stored records; F5 payment request; F6 payment result.

Legend: rectangle = interactor; circle = process; double circle = multi-process; two parallel lines = data store; one-way arrow = data flow; dotted line = trust boundary.

Figure D1 – Proposed data-flow diagram for the student marketplace

- (a) **(3 marks)** Complete the table by identifying each of the three errors in Figure D1 and explaining how it could cause a threat to be missed.

Modelling error	How it could cause a threat to be missed
1.	
2.	
3.	

- (b) **(6 marks)** Identify three threats, each from a different STRIDE category. For each, name the category and explain how a specific scenario detail enables the threat.

- (c) **(4 marks)** Choose two threats from part (b) and rank them first and second. Compare them using the DREAD categories **Damage potential** and **Exploitability**, then explain how those comparisons support your ranking. You do not need to calculate complete numerical DREAD scores.

- (d) **(2 marks)** The team is considering two separate changes: **A** – an SMS one-time code at login; **B** – a one-time password-reset link sent to the user’s university email. For each change, identify one new security risk or dependency it introduces.
