Unit 7 · Cybersecurity in Practice

ANSWER KEY · FOR TEACHERS

Full marks 32

Give the marks for the points in the marking scheme; an answer in other words that says the same is right.

1 Key words

1. assets
2. trust boundary
3. attack surface
4. parameterized query
5. allow-list
6. escaping
7. salt
8. responsible disclosure

K · 4

Each carries 0.5 mark.

2 Which kind of threat?

1. A student signs in as a member of staff with a password he guessed. → **b.** spoofing
2. Someone changes the date on a report that somebody else made. → **a.** tampering
3. A program sends thousands of fake reports, and the board stops answering. → **e.** denial of service
4. A student deletes items, which only staff are allowed to do. → **c.** elevation of privilege

U · 2

Each carries 0.5 mark.

3 Multiple choice

i. **c.** keeping the backup drive in a locked drawer — K · 1

A locked drawer protects a device in the real world. The other three protect programs and data.

ii. **c.** `db.execute("SELECT * FROM items WHERE id = ?", (item_id,))` — A · 1

A placeholder keeps the command and the data apart. Note that this query has no quote marks at all, so checking for them would miss the problem entirely: a number can be joined into SQL as dangerously as text.

iii. **b.** Each guess is hashed once and looked up among all the stored hashes at once. — U · 1

Users with the same password have the same hash, so one hash of each guess is compared with every user's together, in about one step with a dictionary. A different salt for each user forces a separate hash of each guess for each user.

iv. **c.** social engineering, using staff tools that gave one person too much power — U · 1

No code was broken: employees were tricked over the phone into signing in on a fake page. The harm was so great because the staff tools behind those accounts could take over any account, with no second person to approve it.

v. **c.** Stop, write down what you saw, and tell the school's office or a teacher privately. — A · 1

Checking more numbers means looking at other students' marks without permission, which is exactly what Section 45 forbids. Posting it tells everyone how to do it before it is fixed. Asking for a reward first is a form of blackmail. Report it quietly, with what you saw, and let the owner fix it.

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking

4 What does it print?

a. MARKING SCHEME U · 3

- ✓ The first line exactly as the notice was typed, inside `<li>` and `</li>`.
- ✓ The second line with `<`, `>`, `&` and `"` in place of <, >, & and ".
- ✓ The second line is safe: escaped text is shown, never read as part of the page.

b. MARKING SCHEME A · 2

- ✓ The two queries for `place` and `found_on`, in order.
- ✓ `Refused: Can't sort by 'Place'` between them: the allow-list holds only the exact strings, and Place with a capital isn't one of them.

5 Trace the program

ANSWER A · 3

address	counts[address]	Output
10.0.0.5	1	
10.0.0.7	1	
10.0.0.5	2	
10.0.0.5	3	refused: 10.0.0.5
10.0.0.7	2	
		{'10.0.0.5': 3, '10.0.0.7': 2}

MARKING SCHEME

- ✓ The counts 1, 1, 2, 3, 2: each address counted on its own.
- ✓ `refused: 10.0.0.5` only in the fourth round, when its count passes 2.
- ✓ The dictionary printed after the loop: `{'10.0.0.5': 3, '10.0.0.7': 2}`.

6 Review the code

ANSWER A · 4

1. Line 5: a fast hash with no salt. If the table is copied, a thief checks billions of guesses a second, against every user at once. Fix: a slow, salted hash, such as `hashlib.scrypt()` with a salt from `secrets`, stored with the salt.
2. Line 8: a session ID with only 9,000 values, from `random`, which can be predicted; someone could try values until one is a signed-in staff member's. Fix: `return secrets.token_urlsafe(32)`.
3. Line 11: the place is joined into the SQL, so text from outside can change what the query does (injection); an honest `Sita's classroom` already breaks it. Fix: `db.execute("SELECT what FROM items WHERE place = ?", (place,))`.
4. Line 14: the report is put into the page unescaped, so HTML in it would be read as part of the page, and a script in it would run in every visitor's browser (cross-site scripting). Fix: `"<li>" + html.escape(item["what"]) + "</li>"`.

MARKING SCHEME

- ✓ Line 5, a fast unsalted hash: a copied table falls to fast guessing; use a slow, salted hash (scrypt, with a salt from secrets).
- ✓ Line 8, a guessable session ID (few values, from random): someone could take over a session; use `secrets.token_urlsafe()`.
- ✓ Line 11, SQL joined from the input (injection): use a `?` placeholder with the value passed separately.
- ✓ Line 14, text not escaped (cross-site scripting): use `html.escape()`.

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking

7 The thief's work

ANSWER **A · 3**

Slow and salted: guesses = 10^6 passwords × 2,000 users = 2×10^9; each costs 10^5 fast hashes, so $2 \times 10^9 \times 10^5 = 2 \times 10^{14}$ fast hashes; $2 \times 10^{14} \div 10^{10} = 20{,}000$ seconds ≈ **5.6 hours.**
Fast and unsalted: each of the 10^6 passwords is hashed once and looked up among all 2,000 users at once: $10^6 \div 10^{10} = 10^{-4}$ seconds, **a tenth of a millisecond.**
Good storage multiplies the thief's work by 2,000 × 100,000 = 200 million.

MARKING SCHEME

- ✓ 2×10^9 guesses, because with a salt each password is tried for each user separately.
- ✓ 2×10^{14} fast hashes ÷ 10^{10} a second = 20,000 seconds, about 5.6 hours.
- ✓ Fast and unsalted: $10^6 \div 10^{10} = 10^{-4}$ seconds, since one hash of each guess covers every user.

8 Long answer

ANSWER **A · 4**

Using a computer or its data without the owner's permission, or beyond the permission given, is a crime under Section 45 of Nepal's Electronic Transactions Act, 2063, even if nothing is changed and the intention is good: up to three years in prison, a fine of up to Rs 2 lakh, or both. Downloading the list would be using data without permission, and would put the customers' numbers in one more place they could leak from; posting about it before the shop fixes it would show others how to take the list, harming the customers. He should stop, keep nothing, write down what he saw (the address, the time, what appeared), and tell the shop privately (its owner, or its security contact if the website has one), giving them time to fix it. That is responsible disclosure. If the shop doesn't respond, a teacher can help him find who else to tell.

MARKING SCHEME

- ✓ Using a computer or its data without the owner's permission, or beyond it, is a crime under Section 45 of the Electronic Transactions Act, 2063, even with good intentions (up to 3 years in prison, a fine of up to Rs 2 lakh, or both).
- ✓ Downloading the list harms the customers (their numbers in one more place) and posting first shows others how to take it before it is fixed.
- ✓ He should stop, keep nothing, and write down what he saw (the address, the time, what appeared).
- ✓ He should tell the shop privately and give it time to fix the flaw (responsible disclosure), with a teacher's help if the shop doesn't answer.

9 Think

ANSWER **HA · 2**

Hiding is not checking. The page's JavaScript, and every request the page sends, can be read in the developer tools by anyone (Unit 6); addresses are guessed, shared, found in old versions of the page, or tried automatically by programs that scan websites. A system must stay safe when everything about it is known except the secrets (passwords, keys, session IDs): the same principle Grade 9 met for ciphers, where the method is public and only the key is secret. Security that depends on nobody noticing lasts until somebody does.

MARKING SCHEME

- ✓ Hiding isn't checking: the page's code and requests can be read in the developer tools, and addresses are guessed, shared or found by programs that scan websites.
- ✓ A system must stay safe when everything about it is known except its secrets (passwords, keys, session IDs), so the server must check the staff session on every Delete.

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking

10 Activity: A threat model of your own

(not marked)

WHAT STUDENTS SHOULD FIND

For a library register, for example: spoofing, someone borrows a book in another student's name (defense: the librarian checks the ID card; price: users, a moment and a card to carry); tampering, a late return date changed by hand (defense: entries in pen, signed, or a log of every change; price: devices or the librarian's time); information disclosure, anyone can read who borrowed what (defense: show each student only their own record; price: data, the list is less useful to friends); denial of service, the register lost or the only computer broken (defense: a backup copy kept somewhere else; price: devices and a little time). Good groups say which defense costs least for the most risk removed, and notice that a defense people get round (a password on a sticky note) makes things worse.

Marks by level	Knowledge	Understanding	Application	Higher ability	**Total**
Marks	5	7	18	2	**32**

Science Playground, Katunje, Bhaktapur
Book a class visit: https://science-playground.com/booking