



NSW SOFTWARE ENGINEERING 11–12 STAGE 6 • YEAR 12 TRIAL HSC EXAMINATION

Software Engineering

Trial HSC Examination

Total marks: 79

Programming for the Web • Secure Software Architecture • Software Automation

Name: _____ Class: _____

This paper covers all content taught across the full Year 12 course.

Note: the real HSC Software Engineering exam is delivered online (80 marks, 2 hours 30 minutes incl. 10 minutes reading time). This is a paper-based practice adaptation calibrated to the same marks and time allowance.

Contents

General Instructions	3
Section I — Multiple Choice	4
Section II — Short Answer.....	10
Section III — Extended Response	16

General Instructions

- Reading time — 10 minutes
- Working time — 140 minutes
- Total marks — 79
- The real HSC Software Engineering exam is delivered ONLINE (80 marks, 2 hours 30 minutes incl. 10 minutes reading time, via computer with wired headphones) — this is a paper-based practice version calibrated to match those marks and time
- Write using black or blue pen
- Calculators may be used
- A NESA-approved reference sheet is not required for this course
- Answer all questions in the spaces provided in this booklet
- Show relevant working/reasoning for short-answer and extended-response questions where applicable
- Extended responses are marked holistically using the criteria provided in the marking guidelines

Structure of this Paper

Section	Marks	Description
Section I — Multiple Choice	19	19 questions, 1 mark each, spanning all three strands. Circle the correct answer.
Section II — Short Answer	33	12 questions of increasing mark value, spanning all three strands.
Section III — Extended Response	27	6 questions, including a final synthesis question spanning all three strands.

Section I — Multiple Choice

19 marks. Attempt Questions 1–19. Circle the correct answer for each question.

Question 1

What is a key feature of progressive web apps (PWAs)?

- (A) Require a constant Internet connection
- (B) Can be installed like native apps
- (C) Only work in Internet Explorer
- (D) Do not use JavaScript

Question 2

Which language is typically used for client-side programming?

- (A) SQL
- (B) PHP
- (C) Python
- (D) JavaScript

Question 3

Which record types map a hostname to an IPv4 or IPv6 address?

- (A) MX and SRV
- (B) NS and SOA
- (C) A and AAAA
- (D) CNAME and TXT

Question 4

Which protocol and default port does HTTPS use?

- (A) HTTP over UDP, port 80
- (B) HTTP over TLS on TCP, port 443
- (C) TLS over UDP, port 443
- (D) HTTP over TCP, port 80

Question 5

Which is true about TCP vs UDP?

- (A) TCP establishes a connection and guarantees ordered delivery; UDP does not
- (B) Both TCP and UDP use handshakes
- (C) Both TCP and UDP retransmit lost packets by default
- (D) UDP guarantees delivery and ordering; TCP does not

Question 6

What does TLS primarily provide?

- (A) Confidentiality, integrity, authentication
- (B) Compression, routing, congestion control
- (C) Name resolution, caching, negative responses
- (D) Load balancing, multiplexing, prioritisation

Question 7

Place these in the correct order for a first HTTPS request with a cold DNS cache: DNS resolution, TCP handshake, TLS handshake, HTTP request.

- (A) TCP handshake, DNS resolution, HTTP request, TLS handshake
- (B) HTTP request, TCP handshake, TLS handshake, DNS resolution
- (C) DNS resolution, TCP handshake, TLS handshake, HTTP request
- (D) TLS handshake, DNS resolution, HTTP request, TCP handshake

Question 8

Which of the following is an INDIRECT cost of a security breach?

- (A) Customer churn and reputation damage
- (B) Customer notification expenses
- (C) Incident response and forensics
- (D) Legal fees and regulatory fines

Question 9

Which of the following is a business benefit of strong security, beyond simply "avoiding attacks"?

- (A) It always slows down every feature with no other benefit
- (B) It removes the need for regulatory compliance
- (C) It has no effect on customer behaviour
- (D) It can build customer trust and act as a market differentiator

Question 10

A weak password policy that allows "password123" as a valid password is an example of which type of security failure?

- (A) Process failure
- (B) Human failure
- (C) Not a security failure
- (D) Technical failure

Question 11

Which STRIDE category describes an attacker gaining higher access than they were intended to have?

- (A) Spoofing
- (B) Repudiation
- (C) Elevation of privilege
- (D) Denial of service

Question 12

Roughly how much more expensive is it, on average, to fix a security flaw in production compared to preventing it at the design phase?

- (A) There is no meaningful difference
- (B) About 5 times
- (C) About 15 times
- (D) About 48 times

Question 13

Which STRIDE category describes an attacker pretending to be someone else?

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

Question 14

What does the "security-usability paradox" describe?

- (A) Usability has no relationship to security
- (B) Users always prefer the most secure option available
- (C) Security and usability always improve together
- (D) Overly difficult security controls often get bypassed, creating new vulnerabilities

Question 15

Which statement correctly describes the relationship between AI and ML?

- (A) ML is a subset of AI
- (B) AI is a subset of ML
- (C) AI and ML are exactly the same thing
- (D) AI and ML are unrelated, separate fields

Question 16

Which of the following is an example of AI that is NOT machine learning?

- (A) A spam filter that learns from labelled examples
- (B) A recommendation system trained on user data
- (C) A rule-based expert system with hand-coded decision rules
- (D) An image classifier trained on thousands of photos

Question 17

Which type of automation focuses on redesigning and optimising an entire end-to-end business process, often integrating multiple systems?

- (A) RPA
- (B) BPA
- (C) Manual processing
- (D) None of the above

Question 18

Which ML training paradigm uses ONLY labelled data, where every example has a known correct answer?

- (A) None of the above
- (B) Unsupervised learning
- (C) Supervised learning
- (D) Reinforcement learning

Question 19

Which ML training paradigm is most suitable for grouping customers into segments based on purchasing behaviour, with no predefined "correct" groups?

- (A) Reinforcement learning
- (B) None of the above
- (C) Supervised learning
- (D) Unsupervised learning

Section II — Short Answer

33 marks. Attempt all questions. Answer in the spaces provided.

Question 1 (3 marks)

Trace through the SQL query below and explain exactly what it returns, describing the effect of each clause in order.

SQL

```
SELECT category_id, COUNT(*)  
FROM posts  
WHERE published = 1  
GROUP BY category_id;
```

Question 2 (3 marks)

The query below is intended to join every post to its author's username, but it contains a syntax error. Identify the error and rewrite the query correctly.

SQL — CONTAINS AN ERROR

```
SELECT users.username, posts.title  
FROM users  
INNER JOIN posts WHERE users.id = posts.author_id;
```

Question 3 (2 marks)

Explain why DNS primarily uses UDP, but sometimes switches to using TCP instead. Give ONE specific reason TCP is used.

Question 4 (3 marks)

List the THREE security guarantees TLS provides, and briefly explain what each one means in the context of a user logging into an online banking site.

Question 5 (3 marks)

The Python code below builds a login query. Identify the vulnerability, and state exactly what a malicious user could type into "username" to bypass the password check entirely.

PYTHON

```
query = "SELECT * FROM users WHERE username = '" + username + "' AND password = '" +  
password + "'" +  
cursor.execute(query)
```

Question 6 (3 marks)

The Flask endpoint below has a security flaw. Identify it, naming the specific security principle it violates, and describe the fix.

PYTHON (FLASK)

```
@app.route("/api/orders/<order_id>")  
def get_order(order_id):  
    order = db.get_order(order_id)  
    return jsonify(order)
```

Question 7 (3 marks)

The Flask route below transfers money but is vulnerable to CSRF. Identify what is missing, and rewrite the route to fix it.

PYTHON (FLASK) — VULNERABLE

```
@app.route("/transfer", methods=["POST"])
def transfer_money():
    amount = request.form["amount"]
    to_account = request.form["to_account"]
    process_transfer(current_user, to_account, amount)
    return "Transfer complete"
```

Question 8 (2 marks)

A vulnerability is rated likelihood 2/5 and impact 5/5. Calculate the risk score and identify which risk-response category it falls into.

Question 9 (3 marks)

Classify the following as a technical, process or human security failure, explaining your reasoning: an employee clicks a link in a phishing email and enters their company password on a fake login page.

Question 10 (3 marks)

Trace the function below for an email where `contains_urgent = True`, `sender = "colleague"`, `has_deadline = True`. State the exact return value, and list the sequence of branches taken.

PYTHON

```
def classify_email(email):
    if email["contains_urgent"]:
        if email["sender"] == "boss":
            if email["has_deadline"]:
                return "High priority"
            else:
                return "Medium priority"
        else:
            return "Medium priority"
    else:
        return "Low priority"
```

Question 11 (3 marks)

Trace the `predict()` method below for a Perceptron object where `weights = [0.5, -0.2]`, `bias = 0.1`, using the step activation function (output 1 if $z \geq 0$, else 0). Calculate z and state the returned output for `inputs = [4, 3]`.

PYTHON

```
def activate(self, z):  
    return 1 if z >= 0 else 0  
  
def predict(self, inputs):  
    z = sum(w * x for w, x in zip(self.weights, inputs)) + self.bias  
    return self.activate(z)
```

Question 12 (2 marks)

Explain what RPA is, using the phrase "simulates user actions" in your answer.

Section III — Extended Response

27 marks. Attempt all questions. Answer in the spaces provided. Question 6 is a synthesis question spanning all three strands.

Question 1 — Extended response (4 marks)

A company is building a live video-conferencing feature into their web application. Recommend whether the underlying transport should use TCP or UDP, and justify your answer using at least TWO specific characteristics of the chosen protocol.

Question 2 — Extended response (4 marks)

Explain TWO reasons a development team should use HTTPS instead of plain HTTP for their web application, even if the application does not process payments.

Question 3 — Extended response (4 marks)

The Python function below is vulnerable to SQL injection. Rewrite it using a parameterised query so it is safe.

PYTHON — VULNERABLE

```
def find_user(username):  
    query = "SELECT * FROM users WHERE username = '" + username + "'"   
    return cursor.execute(query).fetchone()
```

Question 4 — Extended response (4 marks)

Using the risk = likelihood × impact model, explain why a company should sometimes invest more in preventing a LOW-likelihood risk than a HIGH-likelihood one, using a specific example.

Question 5 — Extended response (5 marks)

The `train_one()` method below is missing its weight and bias update logic. Complete the method so it correctly implements the perceptron learning rule: $w_i = w_i + \alpha(\text{target} - \text{prediction}) \times x_i$, and the equivalent update for the bias.

PYTHON — COMPLETE THE METHOD

```
class Perceptron:
    def __init__(self, num_inputs, learning_rate=0.1):
        self.weights = [0.0] * num_inputs
        self.bias = 0.0
        self.lr = learning_rate

    def predict(self, inputs):
        z = sum(w * x for w, x in zip(self.weights, inputs)) + self.bias
        return 1 if z >= 0 else 0

    def train_one(self, inputs, target):
        prediction = self.predict(inputs)
        # TODO: update self.weights and self.bias here
        pass
```

Question 6 — Extended response (6 marks)

Choose ONE concept from Programming for the Web, ONE from Secure Software Architecture, and ONE from Software Automation studied this year, and explain how they connect to a single, unifying idea: that good software engineering requires deliberately weighing trade-offs using specific, named factors rather than following one "default" answer. Use a specific example from each strand.

Acknowledgements

This resource references the Software Engineering 11–12 Syllabus (2022), © NSW Education Standards Authority (NESA) for and on behalf of the Crown in right of the State of New South Wales. This program is an independent teaching resource prepared for TH Software Tuition and is not affiliated with or endorsed by NESA.

Some technical explanations, worked examples and structural approaches in this program were informed by and adapted from the Software Engineering HSC Textbook (github.com/Eatham532/Software-Engineering-HSC-Textbook), an open-source educational resource used under the MIT License (Copyright 2025 Eatham532). All content here has been independently written, restructured and substantially expanded for this course. The full MIT licence text is reproduced in the Scope & Sequence document.