KK03 — Types of vulnerabilities and risks within insecure development environments

Cyber Security · Comprehensive exam study guide

STUDY DESIGN — YOU MUST KNOW

- use of application programming interfaces (APIs)
- malware
- unpatched software
- poor identity and access management practices
- man-in-the-middle attacks
- insider threats
- cyber security incidents
- risks from software acquired by third parties
- ineffective code review practices
- combined development, testing and production environments

This is a large, high-value KK. You must recognise each listed vulnerability, what it is, and why it is dangerous. Group them mentally to remember them.

Vulnerabilities to know

Vulnerability	What it is / why it's a risk
Insecure APIs	Poorly secured interfaces can expose data or allow unauthorised actions.
Malware	Malicious software (viruses, ransomware, spyware) that damages systems or steals data.
Unpatched software	Known security flaws left unfixed can be exploited by attackers.
Poor identity & access management (IAM)	Weak passwords/excess permissions let the wrong people access systems/data.
Man-in-the-middle (MITM) attack	An attacker intercepts communication between two parties to read/alter data.
Insider threats	Staff (malicious or careless) misuse their legitimate access.
Cyber security incidents	Events such as breaches/attacks that compromise data or systems.
Third-party software risks	Components/libraries from others may contain vulnerabilities you inherit.
Ineffective code review	Bugs and security flaws slip through when code isn't properly reviewed.
Combined dev/test/prod environments	Mixing development, testing and live environments risks exposing real data and unstable code to users.

How to remember them

EXAM TIP

Group by source: **code/process** (insecure APIs, ineffective code review, combined environments, unpatched software), **people** (poor IAM, insider threats), **external attack** (malware, MITM, third-party risks, incidents).

Key definitions to memorise

Vulnerability	A weakness in a system or process that could be exploited to cause harm.
Malware	Malicious software designed to damage, disrupt or gain unauthorised access to systems/data.
Man-in-the-middle attack	An attack where a third party secretly intercepts communication between two parties.
Insider threat	A risk posed by someone with legitimate access who misuses it, whether maliciously or carelessly.
Identity and access management (IAM)	Controlling who can access systems/data and what they are permitted to do.

Exam technique

EXAM TIP

- Learn a one-line description of each — questions often ask you to define one or match a scenario to a vulnerability.
- Explain WHY each is a risk, not just what it is.

COMMON MISTAKES

- Confusing malware (malicious software) with a vulnerability (a weakness).
- Forgetting process risks like combined environments and ineffective code review.

Quick revision checklist

- ■ I can name and briefly describe all ten vulnerabilities.
- ■ I can match a scenario to the relevant vulnerability and explain the risk.

Exam practice — questions & model answers

Q1. Define a man-in-the-middle attack.

Define · 2 marks

Model answer

- An attack where a third party secretly intercepts communication between two parties (1),
- allowing them to read or alter the data being exchanged (1).

Q2. Explain why using combined development, testing and production environments is a security risk.

Explain · 2 marks

Model answer

• Real production data may be exposed during development/testing (1),
• and unstable or untested code can reach live users, increasing the chance of breaches or failures (1).

Q3. Describe the risk posed by an insider threat.

Describe · 2 marks

Model answer

• A person with legitimate access misuses it (1),
• either deliberately or carelessly, to leak, alter or destroy data — bypassing external defences (1).