Threat Modelling

Computing

Four questions that surface most design-level security problems.

Adapted from the standard four-question frame.

1. **What are we building?**
   Draw the data flow. Every arrow crossing a trust boundary matters.

2. **What can go wrong?**
   Walk STRIDE: spoofing, tampering, repudiation, disclosure, denial of service, elevation.

3. **What are we doing about it?**
   For each risk: mitigate, transfer, accept or eliminate. Write down which.

4. **Did we do a good job?**
   Revisit when the design changes. A threat model is a document, not an event.

TRUST BOUNDARIES

Browser → server
Service → service
Application → database
Anything crossing an organisational edge

> **Most breaches exploit a design decision, not a coding bug. Design is the cheapest place to find them.**