SOFTWARE SECURITY

⚠ You are the last line of defense!

Attacks are real, keep us protected!

ACCESS MUST BE EXPLICIT

Setup highly restrictive defaults and grant explicit access on endpoints and resources.

NO CUSTOM DYNAMIC QUERIES

Use the ORM or access data through an API and avoid injections.

ONLY NEEDED DATA

Avoid returning more data than necessary. It can lead to disclosures.

LOG UNUSUALS

Unusual activity must be logged and noticed. Logging and monitoring disables dark spots where an attacker can work comfortably.

NO DISABLING CHECKS

Security checks must not be disabled and are there for a reason. If blocked by some, ask for help.

WRITE CAREFULLY

Undesired information disclosure can happen within an organization. Make sure logging does not leak sensitive data.

Guidelines for reference. Based on OWASP Top 10.

More information at **securitysigns.dev**