TOP 5 Secure Coding Practices You Actually Need: Principles for Secure Code Every Time

Get Your Cryptography Right

- DON'T store cryptographic keys in the same place as the data it encrypts
- DON'T hard code cryptographic keys in the code
- DON'T create your own cryptographic algorithms or use broken algorithms
- DO use known good algorithms provided by your framework (AES-256, Argon2, PBKDF2)
- DO have a security expert review any code using cryptography
- DO encrypt data at rest and in transit
- DO use secure key vaults to store cyrptographic keys (Vault, AWS KMS, and Azure Key Vault)

Don't Trust the User

Automation is Your Friend

1. Establish your level of trust
2. Security by design
3. Securing the pipeline
4. Automate responses

Keep It Secure and Simple (KISS)

Threat Model Your Software

Dr. Kiarash.au

Source: securityboulevard.com/2019/08/5-secure-coding-practices-you-actually-need-principles-for-secure-code-every-time/