TOP 10 Java Security mistakes AppSec Malpractice

Documented clearly

Depending on Initialization

- All variables should be made private
- Access only via the secure get and set method
- Each object should have the initialized private Boolean variable added to it
- If you are implementing static initializers, make sure all static variables are private and use classInitialized

Allow the Echoing Of Sensitive Data to the UI

Relying on Package Scope

Overdoing of Serialization and Deserialization

Hard Coding

- insertion of sensitive passwords, user IDs, PINs and other personal data inside the code

Not Paying Attention to Class Cloneability

Minimize the Usage of Use Inner Classes

Not Finalizing Classes

- document the unfinalized ones if really needed

Not Restricting Access to Classes and Variables

Dr. Kleinhirn.eu