Kubernetes static code analysis

Unique rules to find Security Hotspots in your KUBERNETES code

1. Mounting sensitive file system paths is security-sensitive
   Security Hotspot
2. Using host operating system namespaces is security-sensitive
   Security Hotspot
3. Allowing process privilege escalations is security-sensitive
   Security Hotspot
4. Exposing Docker sockets is security-sensitive
   Security Hotspot
5. Running containers in privileged mode is security-sensitive
   Security Hotspot
6. Setting capabilities is security-sensitive
   Security Hotspot
7. Kubernetes parsing failure
   Code Smell