SURVEY STUDY – CODEBOOK

"What Can Self-Admitted Technical Debt Tell Us About Security? A Mixed-Methods Study" Díaz Ferreyra, Nicolás E., Shahin, Mojtaba, Zahedi, Mansorreh, and Scandariato, Ricardo. In 21th International Conference on Mining Software Repositories (MSR '24) 2024.

THEME	CODE	DESCRIPTION	EXAMPLES
SSATD MOTIVATIONS	**Improve project quality**	Comments that refer to the importance of security pointers for the quality of OSS projects.	*P60: "Security pointers can help to improve the quality of code reviews by providing reviewers with information about potential security risks in the code being reviewed."*
	Comply with regulations and standards	Comments addressing the relevance of security pointers for compliance with standards and regulations.	*P212: "The company I work for does not truly care about the benefits of good security pointers, instead the company is forced to do them due to compliance and regulation..."*
	Facilitate collaboration	Comments that describe how documenting security pointers supports others in the identification and fixing of insecure code sections.	*P92: "I use annotations and comments related to security in software as a note to collaborators and myself to be aware of these issues, especially if problems are easily introduced or something is confusing without more intimate knowledge of why something was done. That is, I add this information as form of documentation and to be proactive."*
	Self-reminders	Comments that describe how security pointers can help track the progress of development activities and support secure coding practices.	*P98: "Just to remember what could be wrong in the future. I mean, there is a high probability that if I do not write something I will forget it in some months, when I may retake/reanalyse the project."*
	Promote a security culture	Comments describing how pointers can help promote a security-aware culture across development teams.	*P59: "Educating my fellow contributors in producing better code, preventing mistakes if they modify my contributions and improving the community I am in by nudging them towards best practices."*
SSATD RISKS	**Exposing vulnerabilities**	Comments suggesting that security pointers may facilitate vulnerability exploits in code	*P60: "Security pointers can make OSS more attractive to attackers, as they can provide a roadmap for exploiting vulnerabilities."*
	Security misconceptions	Comments mentioning that pointers may not be accurate and mislead developers.	*P190: "...if these tips are not clear or if they give the wrong advice, people might make mistakes and accidentally make the software less secure. So, it's really important that the tips are correct and easy to follow for them to be helpful."*
	Exposure of sensitive information	Comments concerned with the possibility that pointers could reveal sensitive information (e.g., passwords, secrets, and credentials) to untrusted audiences that unauthorized parties may exploit.	*P127: "Security pointers may contain sensitive information such as passwords, API keys, or other credentials that can be exposed to unauthorized parties if not handled properly"*