Unit 6: Using Linters to Support Python Testing

Required Reading

Firdaus, A., Ghani, I. & Jeong, S. (2014) Secure Feature Driven Development (SFDD) Model for Secure Software Development, Procedia Social and Behavioral Sciences 129:546-553.

Summary

The document introduces the Secure Feature Driven Development (SFDD) model, an enhanced version of the traditional Feature Driven Development (FDD) methodology, tailored for secure software development. Traditional agile approaches, including FDD, often neglect security, treating it as a non-functional requirement applied late in the process, which leads to vulnerabilities and delays. To address these limitations, SFDD incorporates key security principles such as least privilege, defense in depth, and complete mediation. The enhancements include the restructuring of FDD phases to improve efficiency by merging "Build and Design Features" into a single phase, integrating security measures within each phase (In-Phase Security), and introducing new phases, namely "Build Security by Feature" and "Test Security by Feature," to reinforce security after each phase. Additionally, SFDD introduces the role of a Security Master, responsible for overseeing and guiding security practices throughout the development lifecycle. These changes aim to embed security into every stage of development while maintaining the agility of the FDD methodology.

Reflection

The Secure Feature Driven Development model represents a significant step toward addressing the often-overlooked issue of security in agile methodologies. By integrating security considerations throughout the development lifecycle rather than relegating them to later stages, SFDD ensures that potential vulnerabilities are addressed proactively. This approach not only enhances the robustness of the final product but also aligns with the increasing emphasis on secure software in today's digital landscape. However, the additional layers of security and restructuring of processes could present challenges, particularly for teams new to these practices or those with limited resources. Achieving a balance between maintaining agility and implementing comprehensive security measures will be critical to the widespread adoption and success of SFDD in practical settings.

NASA (2007) Final Report of the International Space Station Independent Safety Task Force

Summary

The NASA document provides a comprehensive assessment of the International Space Station (ISS) by the Independent Safety Task Force. The report identifies threats and vulnerabilities to the ISS, including micrometeoroid impacts, on-board fires, toxic spills, and hardware or software failures. It evaluates the ISS Program's safety measures, risk mitigation strategies, and crosscutting management functions. The report highlights NASA's efforts to enhance ISS operations through robust system designs, detailed verification

processes, and international collaboration. Recommendations emphasize reducing micrometeoroid risks, ensuring a skilled workforce, and developing logistical solutions post-Shuttle retirement to sustain the station's viability. The ISS is presented as a model of complex international cooperation, balancing technological challenges and safety priorities.

Reflection

The ISS report underscores the complexities of maintaining a large-scale, multinational space operation while ensuring the safety of its crew and equipment. It reflects NASA's meticulous approach to risk management and proactive strategies to address potential vulnerabilities. The collaborative nature of the ISS, involving diverse international partners, exemplifies the potential and challenges of global cooperation in space exploration. However, the reliance on aging infrastructure, such as the Shuttle, and uncertainties surrounding new logistical solutions highlight the importance of forward-thinking policies and investment. The Task Force's findings stress the need for ongoing vigilance, adaptability, and support to sustain the ISS as a critical platform for scientific and technological advancements.

Government of the Netherlands (n.d.) Fighting Cybercrime in the Netherlands

Summary

The document "Fighting Cybercrime in the Netherlands" outlines the efforts of the National Cyber Security Centre (NCSC) in enhancing digital security within the country. The NCSC, operating under the National Coordinator for Counterterrorism and Security (NCTV), is responsible for monitoring online threats, advising organizations on cybersecurity measures, and updating security systems to prevent cyber incidents. The document highlights public awareness initiatives like the "Alert Online" campaign, which educates individuals and organizations on safe internet practices. Additionally, legislative measures are being introduced to empower law enforcement with the ability to investigate cybercriminals more effectively by intercepting data, remotely hacking suspects' devices, and blocking harmful online content. Furthermore, the document encourages responsible disclosure of security flaws in government systems, offering a structured way for individuals to report vulnerabilities.

Reflection

Reflecting on the content, it is clear that the Netherlands is taking a proactive and multifaceted approach to combat cybercrime by combining technological vigilance, public education, and legislative action. The emphasis on responsible disclosure fosters collaboration between the public and government agencies, which is crucial in maintaining a robust cybersecurity posture. However, the expansion of law enforcement powers raises questions about privacy and potential overreach, necessitating a careful balance between security and civil liberties. Overall, the document underscores the importance of a comprehensive strategy to address the evolving landscape of cyber threats.

The Computer Security Team (2020) Computer Security: Digital Stolen Goods of CERN?

Summary

The document discusses their proactive measures in combating digital security threats. Recognizing the pervasive risks in the digital world, such as phishing, stolen passwords, and compromised data, CERN’s Computer Security team engaged an external company specializing in monitoring underground markets like the Deep and Dark Web. The company identified potential vulnerabilities and weak points related to CERN’s infrastructure, including exposed passwords and potential attack vectors. Their findings, while not critical, highlighted minor issues that the CERN team promptly addressed. This process exemplifies CERN’s

commitment to maintaining robust security protocols and safeguarding its operations against cybercriminals.

Reflection

The report highlights the critical importance of vigilance in digital security, especially for organizations managing sensitive and high-value operations like CERN. By employing specialized external monitoring services, CERN demonstrates a forward-thinking approach to identifying and mitigating threats before they escalate. This practice not only enhances the organization's defense mechanisms but also serves as a model for other institutions to proactively address cybersecurity concerns. The swift response to identified issues underscores the importance of having a dedicated and efficient security team in place. However, it also raises awareness of the ever-evolving nature of cyber threats, reminding stakeholders of the constant need for adaptation and improvement.

Information Commisioner's Office (ICO) (n.d) Guide to the General Data Protection Regulation (GDPR)

Page not found

Additional Reading

Pillai, A.B. (2017) Software Architecture with Python. Birmingham, UK. Packt Publishing Ltd.

- Chapter 3.
- Chapter 4.
- Chapter 10.

Python.org (2020) PEP 0 -- Index of Python Enhancement Proposals (PEPs): Linters.

Mannino, J. (n.d.) Security in a Microservice World, OWASP.