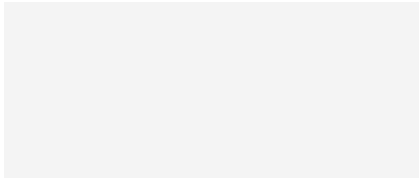
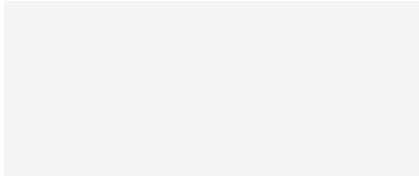


Automating Secure Coding Compliance with Box AI and WCA

Step 1: Extracting Secure Coding Guidelines with Box AI

- **Objective:** Use Box AI to automatically extract essential security rules from the "Secure Coding Guidelines v1.docx" document.
- **Process:** Train a Box AI model on a dataset of secure coding guidelines or use pre-built models to analyze the document's text, identify relevant sections, and extract key rules and descriptions.
- **Output:** A structured representation of the extracted rules in a dictionary format, containing rule categories (e.g., "Secret Management", "Cryptography") and corresponding regex patterns or descriptions of violations.

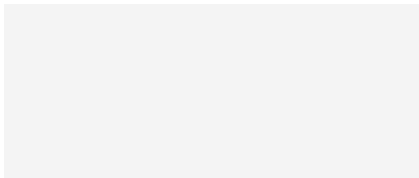
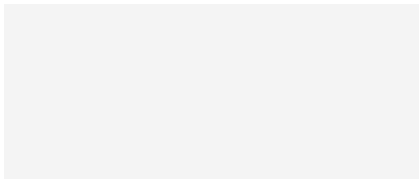


Step 2: Crafting the Problem Statement and Provide Context

- **Problem Statement:** Create a clear and concise problem statement outlining the task: to create a Python script that automatically detects potential security violations in code based on the extracted rules.
- **Contextual Information:** Include the extracted key rules from Box AI in the problem statement, providing the script with specific criteria to look for.
- **Pseudo Code:** Provide a pseudo code snippet with intentional vulnerabilities for testing purposes.

Step 3: Developing the Python Script

- **Regex Patterns:** Craft regular expressions (regex) to match code patterns indicative of each security violation using the extracted rules from Box AI.
- **Violation Detection Logic:** Implement functions to scan the provided pseudo code for matches against these regex patterns.
- **Reporting Violations:** Generate informative messages detailing the rule violated, a description of the issue, and examples from the code when violations are detected.



Step 4: Execution and Analysis

- **Running the Script:** Execute the Python script to analyze the pseudo code for potential security vulnerabilities.
- **Output Interpretation:** Interpret the script's output to gain insights into identified violations and understand security weaknesses in the code.

Key Benefits of This Approach

- **Automation:** Box AI automates the initial step of rule extraction, saving time and effort compared to manual review.