Accuracy Metrics

Accuracy of the fine-tuned model was measured based on 6 metrics.

Dataset: The dataset was created by mapping the CVE_ID to corresponding CWE_ID, Pillar and BaseSeverity. (Pillar - A weakness that is the most abstract type of weakness and represents a theme for all class/base/variant weaknesses related to it.).

CVE_ID	CWE_ID	Base Severity	Pillar
CVE-2004-1125	CWE-20	High	707
CVE-2018-9144	CWE-125	Medium	664
CVE-2004-0276	CWE-20	Medium	707
CVE-2009-4249	CWE-79	Low	707

1. Direct CVE Mapping

Here Predicted CVE_ID from the Generated model output is match agianst the Expected CVE_ID for the model input.

2. CVE to CWE Mapping

Here CVE_ID is captured from the actual output and mapped to the corresponding CWE_ID. Then match it against the CWE_ID of the generated model output.

3. Direct CWE Mapping

Here Predicted CWE_ID from the Generated model output is match agianst the Expected CWE_ID for the model input.

4. CVE to Pillar Mapping

The CVE_ID from the generated output is mapped to the corresponding Pillar and CWE_ID from the generated output is mapped to corresponding pillar and look for matches.

5. CWE to Pillar Mapping

The CWE_ID from the generated output is mapped to the corresponding pillar and CWE_ID from actual output is mapped to the corresponding pillar and look for matches.

6. Actual CVE to Generated CVE Pillar Mapping

The CVE_ID from the actual output is mapped to the corresponding Pillar and CVE_ID from generated output is mapped to the corresponding pillar and look for matches.

7. CVE to Baseseverity mapping

The CVE_ID from the actual output is mapped to the corresponding Base_Severity and the CVE_ID from the generated output is mapped to the corresponding Base_Severity and look for matches.