Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

File Scanned: basic.pt

This report provides a detailed analysis of the uploaded machine learning model file, highlighting any detected vulnerabilities and summarizing the results in a clear, professional format.

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Table of Contents

Model File Content

```
1: def forward(self,
2:     x: Tensor) -> Tensor:
3:     custom = self.custom
4:     return (custom).forward(x, )
5:
```

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Static Vulnerabilities

Line	Code	Severity	Attack
1	No encryption or signature detected	Medium	Missing or Weak File Protection
1	def forward(self,	High	Custom Layers or Unsafe Code Artifacts
3	custom = self.custom	High	Custom Layers or Unsafe Code Artifacts
4	return (custom).forward(x,)	High	Custom Layers or Unsafe Code Artifacts
1	No documentation or comments found	Low	Missing Model Documentation
1	File permissions: 666	High	Overly Permissive Permissions

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Dynamic Vulnerabilities

Vulnerability	Severity	Description	Details
-	-	No input validation d	Model does not check for input shape or type.

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Adversarial Vulnerabilities

Vulnerability	Severity	Description	Details
-	-	Model is highly susc	FGSM attack reduced accuracy to 10%.