Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

File Scanned: vuln_model1.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

```
def forward(self,
    x: Tensor) -> Tensor:
  debug = self.debug
  if debug:
    print("Debug mode on")
  else:
    pass
  layer1 = self.layer1
  return (layer1).forward(x, )

```

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Static Vulnerabilities

Line	Code	Severity	Attack
8	layer1 = self.layer1	Medium	Lack of Model Obfuscation / Plaintext Metadata
9	return (layer1).forward(x,)	Medium	Lack of Model Obfuscation / Plaintext Metadata
1	No encryption or signature detected	Medium	Missing or Weak File Protection
3	debug = self.debug	Low	Exposed Debugging Information
4	if debug:	Low	Exposed Debugging Information
5	print("Debug mode on")	Low	Exposed Debugging Information
1	def forward(self,	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%.