Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

File Scanned: vuln_model2.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

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Model File Content

```
1: <Could not parse model code: Can't get attribute 'VulnModel' on <module '__main__' from 'C:\\Users\
```

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	<Could not parse model code: Can't get at	Low	Exposed Debugging Information
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%.