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: PytorchStreamReader failed locating file constants.pkl: file not found
```

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	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

Dynamic Input Validation

No input validation detected in model forward method.

```
Model does not check for input shape or type.
```

Swajyot Technologies Pvt Ltd

Vulnerability Scan Report

Adversarial Vulnerabilities

Adversarial Robustness

Model is highly susceptible to adversarial attacks.

```
FGSM attack reduced accuracy to 10%.
```