# 恶意文件检测与鲁棒性好的机器学习模型建立

**摘要：**随着信息安全技术的迅速发展，对于恶意文件检测越来越重要（如PDF检测）。由于文件结构的多样性，使得其很容易受到攻击者利用文件来发起攻击。在本文中，我们主要是为了构建一个鲁棒性好的机器学习分类器。我们收集了大约20万个样本，使用机器学习来训练并对模型进行优化。实验结果表明最后我们的模型准确率高哒99.82%，于此同时误报率仅低于0.01%。并且，通过对抗性机器学习之后，表示该模型具有很好的鲁棒性和抗攻击能力。最后，我们也证明了